GE VERNOVA

MiCOM P40 Agile

P54A, P54B, P54C, P54E

Technical Manual
Single Breaker Multi-End Current Differential IED (Non Distance)

Hardware Version: M, P
Firmware Version: 91 and 92
Publication Reference: P54xMED-TM-EN-4



Copyright statement

Copyright © 2026 GE Vernova. All rights reserved.

GridBeats, Universal Relay, Multilin, MiCOM, S1 Agile, P40 Agile, DS Agile, EnerVista, CyberSentry, HardFiber, FlexLogic, FlexElement, FlexCurve, FlexAnalog, FlexInteger and FlexState are trademarks or registered trademarks of GE Vernova.

The contents of this manual are the property of GE Vernova. This documentation is provided on license and may not be reproduced in whole or in part without the permission of GE Vernova. The content of this manual is for informational use only and information contained in this document is indicative only. No representation or warranty is given or should be relied on that it is complete or correct or will apply to any particular project. This will depend on the technical and commercial circumstances. It is provided without liability and is subject to change without notice.

Disclaimer

It is the responsibility of the user to verify and validate the suitability of all GE Vernova Grid Automation products. This equipment must be used within its design limits. The proper application including the configuration and setting of this product to suit the power system assets is the responsibility of the user, who is also required to ensure that all local or regional safety guidelines are adhered to. Incorrect application of this product could risk damage to property/the environment, personal injuries or fatalities and shall be the sole responsibility of the person/entity applying and qualifying the product for use.

The content of this document has been developed to provide guidance to properly install, configure and maintain this product for its intended applications. This guidance is not intended to cover every possible contingency that may arise during commissioning, operation, service, or maintenance activities. Should you encounter any circumstances not clearly addressed in this document, contact your local GE Vernova service site.

It is the sole responsibility of the user to secure their network and associated devices against cybersecurity intrusions or attacks. GE Vernova and its affiliates are not liable for any damages or losses arising from or related to such security intrusion or attacks.

The information contained in this document is subject to change without notice.

Warranty

GE Vernova warrants most of its manufactured products for 10 years from the date of shipping.

For warranty details including any limitations and disclaimers, see the Terms and Conditions at:

https://www.gevernova.com/grid-solutions/multilin/warranty.htm

Major changes

For information on the updates included in this release of the manual, please refer to the latest release notes.

Contents

Chapter 1 Introduction 1

1.1 Chapter Overview 2
1.2 Foreword 3
1.2.1 Target Audience 3
1.2.2 Typographical Conventions 3
1.2.3 Nomenclature 4
1.2.4 Compliance 4
1.3 Product Scope 5
1.3.1 Ordering Options 6
1.4 Features and Functions 7
1.4.1 Current Differential Protection Functions 7
1.4.2 Protection Functions 7
1.4.3 Control Functions 7
1.4.4 Measurement Functions 8
1.4.5 Communication Functions 8
1.5 Logic Diagrams 9
1.6 Functional Overview 11

Chapter 2 Safety Information 12

2.1 Chapter Overview 13
2.2 Health and Safety 14
2.3 Symbols 15
2.4 Installation, Commissioning and Servicing 16
2.4.1 Lifting Hazards 16
2.4.2 Electrical Hazards 16
2.4.3 UL/CSA/CUL Requirements 17
2.4.4 Fusing Requirements 17
2.4.5 Equipment Connections 18
2.4.6 Protection Class 1 Equipment Requirements 18
2.4.7 Pre-energisation Checklist 19
2.4.8 Peripheral Circuitry 19
2.4.9 Upgrading/Servicing 21
2.5 Decommissioning and Disposal 22
2.6 Regulatory Compliance 23
2.6.1 EMC Compliance: 2014/30/EU 23
2.6.2 LVD Compliance: 2014/35/EU 23
2.6.3 R&TTE Compliance: 2014/53/EU 23
2.6.4 UL/CUL Compliance 23

Chapter 3 Hardware Design 24

3.1 Chapter Overview 25
3.2 Hardware Architecture 26
3.2.1 Coprocessor Hardware Architecture 26
3.3 Mechanical Implementation 28
3.3.1 Housing Variants 28
3.3.2 List of Boards 29
3.4 Front Panel 30
3.4.1 Front Panel 30
3.4.1.1 Front Panel Compartments 30
3.4.1.2 Keypad 31
3.4.1.3 USB Port 31

3.4.1.4 Fixed Function LEDs 32
3.4.1.5 Function Keys 32
3.4.1.6 Programable LEDs 32
3.5 Rear Panel 33
3.5.1 Terminal Block Ingress Protection 34
3.6 Boards and Modules 35
3.6.1 PCBs 35
3.6.2 Subassemblies 35
3.6.3 Main Processor Board 36
3.6.4 Power Supply Board 37
3.6.4.1 Watchdog 39
3.6.4.2 Rear Serial Port 40
3.6.5 Input Module - 1 Transformer Board 41
3.6.5.1 Input Module Circuit Description 42
3.6.5.2 Input Board 43
3.6.6 Standard Output Relay Board 45
3.6.7 IRIG-B Board 46
3.6.8 Fibre Optic Board 47
3.6.9 Rear Communication Board 48
3.6.10 Redundant Ethernet Board (Hardware Option R/S/T) 49
3.6.11 Single Ethernet Board (Hardware Option U) 50
3.6.12 Redundant Ethernet Board (Hardware Option W/Y) 52
3.6.13 Retrofit of Ethernet Cards Hardware Option R/S/T with Hardware Option U/W/Y 53
3.6.14 Coprocessor Board 55
3.6.14.1 Current Differential Inputs 56
3.6.14.2 Coprocessor board with 1PPS input 56

Chapter 4 Software Design 57

4.1 Chapter Overview 58
4.2 Software Design Overview 59
4.3 System Level Software 60
4.3.1 Real Time Operating System 60
4.3.2 System Services Software 60
4.3.3 Self-Diagnostic Software 60
4.3.4 Startup Self-Testing 60
4.3.4.1 System Boot 60
4.3.4.2 System Level Software Initialisation 61
4.3.4.3 Co-processor Initialisation 61
4.3.4.4 Platform Software Initialisation and Monitoring 61
4.3.5 Continuous Self-Testing 61
4.4 Platform Software 63
4.4.1 Record Logging 63
4.4.2 Settings Database 63
4.4.3 Interfaces 63
4.5 Protection and Control Functions 64
4.5.1 Acqusition of Power System Input Signals 64
4.5.2 Frequency Tracking of Input Signal Acquisition 64
4.5.3 Input Signal Filtering 64
4.5.4 Fourier Signal Filtering 65
4.5.4.1 Combined Fourier Filter Response 65
4.5.5 Fault Locator 66
4.5.6 Disturbance Recorder 66
4.5.7 Event Recorder Interface 66
4.5.8 Scheme Logic Interface 67
4.5.9 Programmable Scheme Logic 67
4.5.10 Direct Use of Sampled Values 67

4.5.11 Function Key Interface 67

Chapter 5 Configuration 69

5.1 Chapter Overview 70
5.2 Settings Application Software 71
5.3 Using the HMI Panel 72
5.3.1 Navigating the HMI Panel 73
5.3.2 Getting Started 73
5.3.3 Default Display 74
5.3.4 Default Display Navigation 75
5.3.5 Password Entry 76
5.3.6 Processing Alarms and Records 76
5.3.7 Menu Structure 77
5.3.8 Changing the Settings 78
5.3.9 Direct Access (The Hotkey menu) 79
5.3.9.1 Setting Group Selection Using Hotkeys 79
5.3.9.2 Control Inputs 79
5.3.9.3 Circuit Breaker Control 80
5.3.10 Function Keys 80
5.4 Line Parameters 82
5.4.1 Tripping Mode 82
5.4.1.1 CB Trip Conversion Logic Diagram 82
5.4.2 Residual Compensation 82
5.4.3 Mutual Compensation 83
5.5 Date and Time Configuration 85
5.5.1 Using an SNTP Signal 85
5.5.2 Using an IRIG-B Signal 85
5.5.3 Using an IEEE 1588 PTP Signal 85
5.5.4 Without a Timing Source Signal 86
5.5.5 Time Zone Compensation 86
5.5.6 Daylight Saving Time Compensation 87
5.6 Settings Group Selection 88

Chapter 6 Current Differential Protection 89

6.1 Chapter Overview 90
6.2 Current Differential Protection Principle 91
6.2.1 Numerical Current Differential Protection 91
6.3 Implementation of Numerical Current Differential Protection for Multi-Termnial Applications 92
6.3.1 Multi-terminal Numerical Current Differential Protection Design 94
6.3.2 Multi-terminal Current Differential Protection Scheme Topology 95
6.3.2.1 Electrical Network Topology 95
6.3.2.2 Communications Network Topology 98
6.3.3 Sampling of Current Signals 101
6.3.4 Compensating for Different CT Ratios 102
6.3.5 Communication of Current Signals 103
6.3.5.1 Communication of Current Signals - Transmission 103
6.3.5.2 IEEE C37.94 Redundant Ring Communications Presentation 105
6.3.5.3 Communication of Current Signals - Reception 106
6.3.6 Synchronisation of Current Signals 106
6.3.6.1 Relative Time Alignment of Current Signals 106
6.3.6.2 Data Frame Alignment of Current Signals Across Scheme 107
6.3.7 Simple Biased Current Differential Characteristic 108
6.3.7.1 Calculation of Differential and Biased Currents 109
6.3.7.2 Dual-Slope Biased Differential Characteristic 110

6.3.7.3 Current Differential Protection Logic 112
6.3.8 Capacitive Charging Current Compensation 112
6.3.9 CT Saturation 113
6.3.10 CT Ringdown 117
6.3.11 Switched Communication Path Supervision 118
6.3.12 Overall Biased Current Differential Characteristic 120
6.4 Current Differential Protection-Auxiliary Functions 121
6.4.1 Current Differential Intertripping 121
6.4.2 Stub Bus Differential Protection 122
6.4.3 CT Requirements 122
6.4.3.1 Recommended CT Classes 123
6.4.3.2 Current Differential Requirements 123
6.5 Differential IED compatibility with previous versions 124
6.6 Communications Interfacing 125
6.6.1 Fibre-Optic Teleprotection Communication Interface 125
6.6.2 Multiplexer-Compatible Teleprotection Communication Interface According to IEEE C37.94 125
6.7 Application Notes 127
6.7.1 Setting up a Scheme 127
6.7.2 Setting Up the Phase Differential Characteristic 129
6.7.3 Sensitivity Under Heavy Loads 130
6.7.4 Permissive Intertripping 131
6.7.5 CT Ratio Correction Setting Guidelines 131
6.7.6 Feeders with Small Tapped Loads 132
6.7.7 Setting a Two-Terminal Phase Current Differential Element 132
6.7.8 Setting a Three or More Terminal Phase Current Differential Element 133
6.7.9 Fault Location 135

Chapter 7 Non-Aided Schemes 137

7.1 Chapter Overview 138
7.2 Trip On Close Schemes 139
7.2.1 Switch On To Fault (SOTF) 140
7.2.1.1 Switch Onto Fault Mode 140
7.2.2 Trip On Reclose (TOR) 140
7.2.2.1 Trip On Reclose Mode 141

Chapter 8 Autoreclose 142

8.1 Chapter Overview 143
8.2 Introduction to Autoreclose 144
8.3 Autoreclose Implementation 145
8.3.1 Autoreclose Logic Inputs from External Sources 146
8.3.1.1 Circuit Breaker Healthy Input 146
8.3.1.2 Inhibit Autoreclose Input 146
8.3.1.3 Block Autoreclose Input 146
8.3.1.4 Reset Lockout Input 147
8.3.1.5 Pole Discrepancy Input 147
8.3.1.6 External Trip Indication 147
8.3.2 Autoreclose Logic Inputs 147
8.3.2.1 Trip Initiation Signals 147
8.3.2.2 Circuit Breaker Status Inputs 147
8.3.2.3 System Check Signals 147
8.3.3 Autoreclose Logic Outputs 147
8.3.4 Autoreclose Operating Sequence 148
8.3.4.1 AR Timing Sequence - Transient Fault 148
8.3.4.2 AR Timing Sequence - Evolving/Permanent Fault 148
8.3.4.3 AR Timing Sequence - Evolving/Permanent Fault Single-phase 149

8.4 Autoreclose System Map 150
8.4.1 Autoreclose System Map Diagrams 151
8.4.2 Autoreclose Internal Signals 155
8.4.3 Autoreclose DDB Signals 158
8.5 Logic Modules 164
8.5.1 Circuit Breaker Status Monitor 164
8.5.1.1 CB State Monitor Logic diagram 165
8.5.2 Circuit Breaker Open Logic 166
8.5.2.1 Circuit Breaker Open Logic Diagram 166
8.5.3 Circuit Breaker in Service Logic 166
8.5.3.1 Circuit Breaker in Service Logic Diagram 167
8.5.3.2 Autoreclose OK Logic Diagram 167
8.5.4 Autoreclose Enable 167
8.5.4.1 Autoreclose Enable Logic Diagram 168
8.5.5 Autoreclose Modes 168
8.5.5.1 Single-Phase and Three-Phase Autoreclose 168
8.5.5.2 Autoreclose Modes Enable Logic Diagram 169
8.5.6 AR Force Three-Phase Trip Logic 169
8.5.6.1 AR Force Three-Phase Trip Logic Diagram 170
8.5.7 Autoreclose Initiation Logic 170
8.5.7.1 Autoreclose Initiation Logic Diagram 171
8.5.7.2 Autoreclose Trip Test Logic Diagram 171
8.5.7.3 AR External Trip Initiation Logic Diagram 172
8.5.7.4 Protection Reoperation and Evolving Fault Logic Diagram 173
8.5.7.5 Fault Memory Logic Diagram 173
8.5.8 Autoreclose In Progress 173
8.5.8.1 Autoreclose In Progress Logic Diagram 174
8.5.9 Sequence Counter 174
8.5.9.1 Autoreclose Sequence Counter Logic Diagram 175
8.5.10 Autoreclose Cycle Selection 175
8.5.10.1 Single-Phase Autoreclose Cycle Selection Logic Diagram 175
8.5.10.2 3-phase Autoreclose Cycle Selection 176
8.5.11 Dead Time Control 176
8.5.11.1 Dead Time Start Enable Logic Diagram 177
8.5.11.2 1-phase Dead Time Logic Diagram 178
8.5.11.3 3-phase Dead Time Logic Diagram 179
8.5.12 Circuit Breaker Autoclose 179
8.5.12.1 Circuit Breaker Autoclose Logic Diagram 180
8.5.13 Reclaim Time 180
8.5.13.1 Prepare Reclaim Initiation Logic Diagram 181
8.5.13.2 Reclaim Time Logic Diagram 181
8.5.13.3 Successful Autoreclose Signals Logic Diagram 182
8.5.13.4 Autoreclose Reset Successful Indication Logic Diagram 182
8.5.14 CB Healthy and System Check Timers 182
8.5.14.1 CB Healthy and System Check Timers Logic Diagram 183
8.5.15 Autoreclose Shot Counters 183
8.5.15.1 Autoreclose Shot Counters Logic Diagram 184
8.5.16 Circuit Breaker Control 185
8.5.16.1 CB Control Logic Diagram 185
8.5.17 Circuit Breaker Trip Time Monitoring 185
8.5.17.1 CB Trip Time Monitoring Logic Diagram 186
8.5.18 Autoreclose Lockout 186
8.5.18.1 CB Lockout Logic Diagram 187
8.5.19 Reset Circuit Breaker Lockout 187
8.5.19.1 Reset CB Lockout Logic Diagram 188
8.5.20 Pole Discrepancy 188
8.5.20.1 Pole Discrepancy Logic Diagram 189
8.5.21 Circuit Breaker Trip Conversion 189

8.5.21.1 CB Trip Conversion Logic Diagram 189
8.5.22 Monitor Checks for CB Closure 189
8.5.22.1 Check Synchronisation Monitor for CB Closure 190
8.5.22.2 Voltage Monitor for CB Closure 191
8.5.23 Synchronisation Checks for CB Closure 191
8.5.23.1 Three-phase Autoreclose System Check Logic Diagram 193
8.5.23.2 CB Manual Close System Check Logic Diagram 194
8.6 Setting Guidelines 195
8.6.1 De-ionising Time Guidance 195
8.6.2 Dead Timer Setting Guidelines 195
8.6.2.1 Example Dead Time Calculation 195
8.6.3 Reclaim Time Setting Guidelines 196

Chapter 9 CB Fail Protection 197

9.1 Chapter Overview 198
9.2 Circuit Breaker Fail Protection 199
9.3 Circuit Breaker Fail Implementation 200
9.3.1 Circuit Breaker Fail Timers 200
9.3.2 Zero Crossing Detection 200
9.4 Circuit Breaker Fail Logic 202
9.4.1 Circuit Breaker Fail Logic - Part 1 202
9.4.2 Circuit Breaker Fail Logic - Part 2 203
9.4.3 Circuit Breaker Fail Logic - Part 3 204
9.4.4 Circuit Breaker Fail Logic - Part 4 205
9.5 Application Notes 206
9.5.1 Reset Mechanisms for CB Fail Timers 206
9.5.2 Setting Guidelines (CB fail Timer) 206
9.5.3 Setting Guidelines (Undercurrent) 207

Chapter 10 Current Protection Functions 208

10.1 Chapter Overview 209
10.2 Overcurrent Protection Principles 210
10.2.1 IDMT Characteristics 210
10.2.1.1 IEC 60255 IDMT Curves 211
10.2.1.2 European Standards 213
10.2.1.3 North American Standards 214
10.2.1.4 IEC and IEEE Inverse Curves 216
10.2.1.5 Differences Between the North american and European Standards 217
10.2.1.6 Programmable Curves 217
10.2.2 Principles of Implementation 217
10.2.2.1 Timer Hold Facility 218
10.3 Phase Fault Overcurrent Protection 220
10.3.1 POC Implementation 220
10.3.2 Directional Element 220
10.3.3 POC Logic 222
10.4 Negative Sequence Overcurrent Protection 223
10.4.1 Negative Sequence Overcurrent Protection Implementation 223
10.4.2 Directional Element 223
10.4.3 NPSOC Logic 224
10.4.4 Application Notes 224
10.4.4.1 Setting Guidelines (Current Threshold) 224
10.4.4.2 Setting Guidelines (Time Delay) 224
10.4.4.3 Setting Guidelines (Directional element) 225
10.5 Earth Fault Protection 226
10.5.1 Earth Fault Protection Implementation 226

10.5.2 IDG Curve 226
10.5.3 Directional Element 227
10.5.3.1 Residual Voltage Polarisation 227
10.5.3.2 Negative Sequence Polarisation 228
10.5.4 Earth Fault Protection Logic 229
10.5.5 Application Notes 229
10.5.5.1 Residual Voltage Polarisation Setting Guidelines 229
10.5.5.2 Setting Guidelines (Directional Element) 229
10.6 Sensitive Earth Fault Protection 231
10.6.1 SEF Protection Implementation 231
10.6.2 EPATR B Curve 231
10.6.3 Sensitive Earth Fault Protection Logic 232
10.6.4 Application Notes 233
10.6.4.1 Insulated Systems 233
10.6.4.2 Setting Guidelines (Insulated Systems) 234
10.7 High Impedance REF 236
10.7.1 High Impedance REF Principle 236
10.8 Thermal Overload Protection 238
10.8.1 Single Time Constant Characteristic 238
10.8.2 Dual Time Constant Characteristic 238
10.8.3 Thermal Overload Protection Implementation 239
10.8.4 Thermal Overload Protection Logic 239
10.8.5 Application Notes 239
10.8.5.1 Setting Guidelines for Dual Time Constant Characteristic 239
10.8.5.2 Setting Guidelines for Single Time Constant Characteristic 241
10.9 Broken Conductor Protection 242
10.9.1 Broken Conductor Protection Implementation 242
10.9.2 Broken Conductor Protection Logic 242
10.9.3 Application Notes 242
10.9.3.1 Setting Guidelines 242

Chapter 11 Voltage Protection Functions 244

11.1 Chapter Overview 245
11.2 Undervoltage Setting Guidelines 246
11.3 Undervoltage Protection 247
11.3.1 Undervoltage Protection Implementation 247
11.3.2 Undervoltage Protection Logic 248
11.3.3 Application Notes 249
11.3.3.1 Undervoltage Setting Guidelines 249
11.4 Overvoltage Protection 250
11.4.1 Overvoltage Protection Implementation 250
11.4.2 Overvoltage Protection Logic 251
11.4.3 Application Notes 252
11.4.3.1 Overvoltage Setting Guidelines 252
11.5 Compensated Overvoltage 253
11.6 Residual Overvoltage Protection 254
11.6.1 Residual Overvoltage Protection Implementation 254
11.6.2 Residual Overvoltage Logic 255
11.6.3 Application Notes 255
11.6.3.1 Calculation for Solidly Earthed Systems 255
11.6.3.2 Calculation for Impedance Earthed Systems 256
11.6.3.3 Setting Guidelines 257

Chapter 12 Frequency Protection Functions 258

12.1 Chapter Overview 259

12.2 Frequency Protection 260
12.2.1 Underfrequency Protection 260
12.2.1.1 Underfrequency Protection Implementation 260
12.2.1.2 Underfrequency Protection logic 261
12.2.1.3 Application Notes 261
12.2.2 Overfrequency Protection 261
12.2.2.1 Overfrequency Protection Implementation 261
12.2.2.2 Overfrequency Protection logic 262
12.2.2.3 Application Notes 262
12.3 Independent R.O.C.O.F Protection 263
12.3.1 Independent R.O.C.O.F Protection Implementation 263
12.3.2 Independent R.O.C.O.F Protection Logic 264

Chapter 13 Monitoring and Control 265

13.1 Chapter Overview 266
13.2 Event Records 267
13.2.1 Event Types 267
13.2.1.1 Opto-input Events 268
13.2.1.2 Contact Events 268
13.2.1.3 Alarm Events 268
13.2.1.4 Fault Record Events 269
13.2.1.5 Maintenance Events 269
13.2.1.6 Protection Events 269
13.2.1.7 Security Events 270
13.2.1.8 Platform Events 270
13.3 Disturbance Recorder 271
13.4 Measurements 272
13.4.1 Measured Quantities 272
13.4.2 Measurement Setup 272
13.4.3 Fault Locator 272
13.4.4 Opto-input Time Stamping 272
13.5 CB Condition Monitoring 273
13.5.1 Broken Current Accumulator 274
13.5.2 CB Trip Counter 274
13.5.3 CB Operating Time Accumulator 275
13.5.4 Excessive Fault Frequency Counter 275
13.5.5 Reset Lockout Alarm 276
13.5.6 CB Condition Monitoring Logic 277
13.5.7 Reset Circuit Breaker Lockout 277
13.5.7.1 Reset CB Lockout Logic Diagram 278
13.5.8 Application Notes 278
13.5.8.1 Setting the Thresholds for the Total Broken Current 278
13.5.8.2 Setting the thresholds for the Number of Operations 279
13.5.8.3 Setting the thresholds for the Operating Time 279
13.5.8.4 Setting the Thresholds for Excesssive Fault Frequency 279
13.6 CB State Monitoring 280
13.6.1 CB State Monitor Logic diagram 281
13.7 Circuit Breaker Control 282
13.7.1 CB Control using the IED Menu 282
13.7.2 CB Control using the Hotkeys 283
13.7.3 CB Control using the Function Keys 283
13.7.4 CB Control using the Opto-inputs 284
13.7.5 Remote CB Control 284
13.7.6 CB Healthy Check 285
13.7.7 Synchronisation Check 285
13.7.8 CB Control AR Implications 285

13.7.9 CB Control Logic Diagram 286
13.8 Pole Dead Function 287
13.8.1 Pole Dead Logic 287
13.9 CB Condition Monitoring 289
13.10 System Checks 290
13.10.1 System Checks Implementation 290
13.10.1.1 VT Connections 290
13.10.1.2 Voltage Monitoring 291
13.10.1.3 Check Synchronisation 291
13.10.1.4 Check Syncronisation Vector Diagram 291
13.10.2 Voltage Monitor for CB Closure 293
13.10.3 Check Synchronisation Monitor for CB Closure 294
13.10.4 System Check PSL 295
13.10.5 Application Notes 295
13.10.5.1 Predictive Closure of Circuit Breaker 295
13.10.5.2 Voltage and Phase Angle Correction 295

Chapter 14 Supervision 297

14.1 Chapter Overview 298
14.2 Voltage Transformer Supervision 299
14.2.1 Loss of One or Two Phase Voltages 299
14.2.2 Loss of all Three Phase Voltages 299
14.2.3 Absence of all Three Phase Voltages on Line Energisation 299
14.2.4 VTS Implementation 300
14.2.5 VTS Logic 301
14.3 Current Transformer Supervision 303
14.3.1 Differential CTS 303
14.3.2 Differential CTS Logic 304
14.3.3 Standard CTS Implementation 304
14.3.4 Standard CTS Logic 305
14.3.5 CTS Blocking 305
14.3.6 Application Notes 306
14.3.6.1 Setting Guidelines 306
14.3.6.2 Differential CTS Setting Guidelines 306
14.4 Trip Circuit Supervision 307
14.4.1 Trip Circuit Supervision Scheme 1 307
14.4.1.1 Resistor Values 307
14.4.1.2 PSL for TCS Scheme 1 308
14.4.2 Trip Circuit Supervision Scheme 2 308
14.4.2.1 Resistor Values 309
14.4.2.2 PSL for TCS Scheme 2 309
14.4.3 Trip Circuit Supervision Scheme 3 309
14.4.3.1 Resistor Values 310
14.4.3.2 PSL for TCS Scheme 3 310

Chapter 15 Digital I/O and PSL Configuration 311

15.1 Chapter Overview 312
15.2 Configuring Digital Inputs and Outputs 313
15.3 Scheme Logic 314
15.3.1 PSL Editor 315
15.3.2 PSL Schemes 315
15.3.3 PSL Scheme Version Control 315
15.4 Configuring the Opto-Inputs 316
15.5 Assigning the Output Relays 317
15.6 Fixed Function LEDs 318

15.6.1 Trip LED Logic 318
15.7 Configuring Programmable LEDs 319
15.8 Function Keys 321
15.9 Control Inputs 322

Chapter 16 Fibre Teleprotection 323

16.1 Chapter Overview 324
16.2 Fibre Teleprotection Implementation 325
16.2.1 Error Handling for Protection Communications 325
16.3 Communications Supervision 326
16.4 IM64 Logic 327
16.5 Application Notes 329
16.5.1 Scheme Reconfiguration 329
16.5.2 Alarm Management 329
16.5.3 Alarm Logic 330
16.5.4 Two-ended Scheme Extended Supervision 330
16.5.5 Multi-terminal Scheme Extended Supervision 331

Chapter 17 Electrical Teleprotection 332

17.1 Chapter Overview 333
17.2 Introduction 334
17.3 Teleprotection Scheme Principles 335
17.3.1 Direct Tripping 335
17.3.2 Permissive Tripping 335
17.4 Implementation 336
17.5 Configuration 337
17.6 Connecting to Electrical InterMiCOM 339
17.6.1 Short Distance 339
17.6.2 Long Distance 339
17.7 Application Notes 340

Chapter 18 Communications 342

18.1 Chapter Overview 343
18.2 Communication Interfaces 344
18.3 Serial Communication 345
18.3.1 USB Front Port 345
18.3.2 EIA(RS)485 Bus 345
18.3.2.1 EIA(RS)485 Biasing Requirements 346
18.3.3 K-Bus 346
18.4 Ethernet Communication 348
18.5 Board Variants 349
18.6 Configuring IP Addresses 350
18.6.1 Configuring the IED IP Address 350
18.6.2 Configuring the REB IP Address (R/S/T) only 350
18.6.2.1 Configuring the Last Octet (SHP, DHP, RSTP) 351
18.7 Redundant Ethernet Configurator 354
18.7.1 Connecting the IED to a PC 354
18.7.2 Installing the Configurator 354
18.7.3 Starting the Configurator 355
18.7.4 Device Identification 355
18.7.5 Selecting the Device Mode 355
18.7.6 Filter by Board Type 355
18.7.7 Password Configuration 355
18.7.8 IP Address Configuration 355

18.7.9	SNTP IP Address Configuration	356
18.7.10	Check MAC Table for Connected Equipment	356
18.7.11	PRP Configuration	356
18.7.12	HSR Configuration	356
18.7.13	RSTP Configuration	357
18.7.14	Bridge parameters	357
18.7.15	Port Parameters	357
18.7.16	Port States	358
18.7.17	Failover Configuration	358
18.7.18	Filtering Database	358
18.7.19	End of Session	359
18.8	**Redundancy Protocols**	**360**
18.8.1	Parallel Redundancy Protocol (PRP)	360
18.8.1.1	PRP Networks	360
18.8.1.2	Network Elements	360
18.8.2	High-Availability Seamless Redundancy (HSR)	361
18.8.2.1	HSR Multicast Topology	361
18.8.2.2	HSR Unicast Topology	362
18.8.2.3	HSR Application in the Substation	363
18.8.3	Rapid Spanning Tree Protocol (RSTP)	363
18.8.4	Failover	364
18.9	**General Functions for Redundant Ethernet Boards**	**365**
18.9.1	Forwarding	365
18.10	**Simple Network Management Protocol (SNMP)**	**366**
18.10.1	SNMP Management Information Bases	366
18.10.2	Main Processor MIBS Structure	366
18.10.3	Redundant Ethernet Board MIB Structure	367
18.10.4	Accessing the MIB	371
18.10.5	Main Processor SNMP Configuration	371
18.11	**Data Protocols**	**373**
18.11.1	Courier	373
18.11.1.1	Physical Connection and Link Layer	373
18.11.1.2	Courier Database	374
18.11.1.3	Settings Categories	374
18.11.1.4	Setting Changes	374
18.11.1.5	Event Extraction	374
18.11.1.6	Disturbance Record Extraction	376
18.11.1.7	Programmable Scheme Logic Settings	376
18.11.1.8	Time Synchronisation	377
18.11.1.9	Courier Configuration	377
18.11.2	IEC 60870-5-103	378
18.11.2.1	Physical Connection and Link Layer	379
18.11.2.2	Initialisation	379
18.11.2.3	Time Synchronisation	379
18.11.2.4	Configurable IEC 60870-5-103 Signal List	379
18.11.2.5	Spontaneous Events	380
18.11.2.6	General Interrogation (GI)	380
18.11.2.7	Cyclic Measurements	380
18.11.2.8	Commands	380
18.11.2.9	Test Mode	380
18.11.2.10	Disturbance Records	380
18.11.2.11	Command/Monitor Blocking	381
18.11.2.12	IEC 60870-5-103 Configuration	381
18.11.3	DNP 3.0	382
18.11.3.1	Physical Connection and Link Layer	382
18.11.3.2	Object 1 Binary Inputs	382
18.11.3.3	Object 10 Binary Outputs	383
18.11.3.4	Object 20 Binary Counters	384

18.11.3.5 Object 30 Analogue Input 384
18.11.3.6 Object 40 Analogue Output 384
18.11.3.7 Object 50 Time Synchronisation 384
18.11.3.8 DNP3 Device Profile 385
18.11.3.9 DNP3 Configuration 393
18.11.4 IEC 61850 394
18.11.4.1 Benefits of IEC 61850 394
18.11.4.2 IEC 61850 Interoperability 394
18.11.4.3 The IEC 61850 Data Model 395
18.11.4.4 IEC 61850 in MiCOM IEDs 395
18.11.4.5 IEC 61850 Data Model Implementation 396
18.11.4.6 IEC 61850 Communication Services Implementation 396
18.11.4.7 IEC 61850 Peer-to-peer (GOOSE) communications 396
18.11.4.8 GOOSE Message Validation 396
18.11.4.9 Mapping GOOSE Messages to Virtual Inputs 396
18.11.4.10 Ethernet Functionality 397
18.11.4.11 IEC 61850 Configuration 397
18.11.4.12 Selection of the IEC 61850 Edition 398
18.11.4.13 IEC 61850 Edition 2 399
18.11.5 Read Only Mode 402
18.11.5.1 IEC 60870-5-103 Protocol Blocking 403
18.11.5.2 Courier Protocol Blocking 403
18.11.5.3 IEC 61850 Protocol Blocking 404
18.11.5.4 Read-Only Settings 404
18.11.5.5 Read-Only DDB Signals 404
18.12 Time Synchronisation 405
18.12.1 IRIG-B 405
18.12.1.1 IRIG-B Implementation 406
18.12.2 SNTP 406
18.12.2.1 Loss of SNTP Server Signal Alarm 406
18.12.3 IEEE 1588 Precision time Protocol 406
18.12.3.1 Accuracy and Delay Calculation 407
18.12.3.2 PTP Domains 407
18.12.4 Time Synchronisation using the Communication Protocols 407
18.12.5 Real Time Clock Synchronisation via Opto-inputs 408

Chapter 19 Cybersecurity 409

19.1 Disclaimer 410
19.2 Overview 411
19.3 The Need for Cybersecurity 412
19.4 Standards 413
19.4.1 NERC Compliance 413
19.4.1.1 CIP 002 414
19.4.1.2 CIP 003 414
19.4.1.3 CIP 004 414
19.4.1.4 CIP 005 414
19.4.1.5 CIP 006 414
19.4.1.6 CIP 007 415
19.4.1.7 CIP 008 415
19.4.1.8 CIP 009 415
19.4.2 IEEE 1686-2013 415
19.5 Cyber-Security Implementation 417
19.5.1 Initial Setup 417
19.6 Roles and Permissions 418
19.6.1 Roles 418
19.6.2 Permissions 419
19.7 Authentication 421

19.7.1 Authentication Methods 421
19.7.2 Bypass 421
19.7.3 Login 422
19.7.3.1 Front Panel Login 423
19.7.3.2 MiCOM S1 Login 423
19.7.3.3 Warning Banner 423
19.7.3.4 Login Failed 423
19.7.4 User Sessions 423
19.7.5 User Locking Policy 424
19.7.6 Logout 425
19.7.6.1 Front Panel Logout 425
19.7.6.2 MiCOM S1 Logout 425
19.7.7 Device Users 426
19.7.8 Password Policy 426
19.7.9 Change Password 426
19.7.10 RADIUS 426
19.7.10.1 RADIUS Users 427
19.7.10.2 RADIUS Client 427
19.7.10.3 RADIUS Server Settings 428
19.7.10.4 RADIUS Accounting 428
19.7.10.5 RADIUS Client-Server Validation 428
19.7.11 Recovery 429
19.7.11.1 Restore to Local Factory Default 429
19.7.11.2 Password Reset Procedure 429
19.7.11.3 Access Level DDBs 430
19.7.12 Disabling Physical Ports 431
19.7.13 Disabling Logical Ports 431
19.8 Security Event Management 433
19.8.1 Security Events: Courier 433
19.8.2 Syslog 435
19.8.3 Syslog Client 436
19.8.4 Syslog Functionality 436

Chapter 20 Installation 438

20.1 Chapter Overview 439
20.2 Handling the Goods 440
20.2.1 Receipt of the Goods 440
20.2.2 Unpacking the Goods 440
20.2.3 Storing the Goods 440
20.2.4 Dismantling the Goods 440
20.3 Mounting the Device 441
20.3.1 Flush Panel Mounting 441
20.3.2 Rack Mounting 441
20.4 Cables and Connectors 443
20.4.1 Terminal Blocks 443
20.4.2 Power Supply Connections 444
20.4.3 Earth Connnection 444
20.4.4 Current Transformers 444
20.4.5 Voltage Transformer Connections 445
20.4.6 Watchdog Connections 445
20.4.7 EIA(RS)485 and K-Bus Connections 445
20.4.8 IRIG-B Connection 445
20.4.9 Opto-input Connections 445
20.4.10 Output Relay Connections 446
20.4.11 Ethernet Metallic Connections 446
20.4.12 Ethernet Fibre Connections 446

20.4.13 USB Connection 446
20.4.14 GPS Fibre Connection 446
20.4.15 Fibre Communication Connections 447
20.5 Case Dimensions 448
20.5.1 Case Dimensions 40TE 448
20.5.2 Case Dimensions 60TE 449
20.5.3 Case Dimensions 80TE 450

Chapter 21 Commissioning Instructions 451

21.1 Chapter Overview 452
21.2 General Guidelines 453
21.3 Commissioning Test Menu 454
21.3.1 Opto I/P Status Cell (Opto-input Status) 454
21.3.2 Relay O/P Status Cell (Relay Output Status) 454
21.3.3 Test Port Status Cell 454
21.3.4 Monitor Bit 1 to 8 Cells 454
21.3.5 Test Mode Cell 455
21.3.6 Test Pattern Cell 455
21.3.7 Contact Test Cell 455
21.3.8 Test LEDs Cell 455
21.3.9 Test Autoreclose Cell 455
21.3.10 Loopback Mode 456
21.3.11 IM64 Test Pattern 456
21.3.12 IM64 Test Mode 456
21.3.13 Red and Green LED Status Cells 456
21.4 Commissioning Equipment 457
21.4.1 Recommended Commissioning Equipment 457
21.4.2 Essential Commissioning Equipment 457
21.4.3 Advisory Test Equipment 458
21.5 Product Checks 459
21.5.1 Product Checks with the IED De-energised 459
21.5.1.1 Visual Inspection 459
21.5.1.2 Current Transformer Shorting Contacts 460
21.5.1.3 Insulation 460
21.5.1.4 External Wiring 460
21.5.1.5 Watchdog Contacts 460
21.5.1.6 Power Supply 461
21.5.2 Pxxx_CI_ProductChecksEnergised 461
21.5.2.1 Watchdog Contacts 461
21.5.2.2 Test LCD 461
21.5.2.3 Date and Time 462
21.5.2.4 Test LEDs 462
21.5.2.5 Test Alarm and Out-of-Service LEDs 463
21.5.2.6 Test Trip LED 463
21.5.2.7 Test User-programmable LEDs 463
21.5.2.8 Test Opto-inputs 463
21.5.2.9 Test Output Relays 463
21.5.2.10 Test Serial Communication Port RP1 463
21.5.2.11 Test Serial Communication Port RP2 465
21.5.2.12 Test Ethernet Communication 466
21.5.3 Secondary Injection Tests 466
21.5.3.1 Test Current Inputs 466
21.5.3.2 Test Voltage Inputs 466
21.6 Electrical Intermicom Communication Loopback 468
21.6.1 Setting up the Loopback 468
21.6.2 Loopback Test 468

21.6.2.1 InterMicom Command Bits 469
21.6.2.2 InterMicom Channel Diagnostics 469
21.6.2.3 Simulating a Channel Failure 469
21.7 Intermicom 64 Communication 470
21.7.1 Checking the Interface 470
21.7.2 Setting up the Loopback 470
21.7.3 Loopback Test 471
21.8 Setting Checks 472
21.8.1 Apply Application-specific Settings 472
21.8.1.1 Transferring Settings from a Settings File 472
21.8.1.2 Entering settings using the HMI 472
21.9 IEC 61850 Edition 2 Testing 474
21.9.1 Using IEC 61850 Edition 2 Test Modes 474
21.9.1.1 IED Test Mode Behaviour 474
21.9.1.2 Sampled Value Test Mode Behaviour 474
21.9.2 Simulated Input Behaviour 475
21.9.3 Testing Examples 476
21.9.3.1 Test Procedure for Real Values 476
21.9.3.2 Test Procedure for Simulated Values - No Plant 477
21.9.3.3 Test Procedure for Simulated Values - With Plant 477
21.9.3.4 Contact Test 478
21.10 Current Differential Protection 479
21.10.1 Current Differential Bias Characteristic 479
21.10.2 Current Differential Bias Testing 479
21.10.2.1 Lower Slope 480
21.10.2.2 Upper Slope 481
21.10.3 Current Differential Operation and Contact Assignment 481
21.11 Protection Timing Checks 483
21.11.1 Dependency Conditions 483
21.11.2 Overcurrent Check 483
21.11.3 Connecting the Test Circuit 483
21.11.4 Performing the Test 484
21.11.5 Check the Operating Time 484
21.12 System Check and Check Synchronism 485
21.12.1 Check Synchronism Pass 485
21.12.2 Check Synchronism Fail 485
21.13 Check Trip and Autoreclose Cycle 486
21.14 End-to-End Communication Tests 487
21.14.1 Remove Local Loopbacks 487
21.14.1.1 Restoring Direct Fibre Connections 487
21.14.1.2 Restoring C37.94 Fibre Connections 488
21.14.2 Remove Remote Loopbacks 488
21.14.3 Verify Communication between IEDs 488
21.15 Onload Checks 489
21.15.1 Confirm Voltage Connections 489
21.15.2 Confirm Current Connections 489
21.15.3 Measure Capacitive Charging Current 490
21.15.4 Check Differential Current 490
21.15.5 Check Current Transformer Polarity 490
21.15.6 On-load Directional Test 490
21.16 Final Checks 491

Chapter 22 Maintenance and Troubleshooting 492

22.1 Chapter Overview 493
22.2 Maintenance 494
22.2.1 Maintenance Checks 494

22.2.1.1 Alarms 494
22.2.1.2 Opto-isolators 494
22.2.1.3 Output Relays 494
22.2.1.4 Measurement Accuracy 494
22.2.2 Replacing the Device 495
22.2.3 Repairing the Device 496
22.2.4 Removing the front panel 496
22.2.5 Replacing PCBs 497
22.2.5.1 Replacing the main processor board 497
22.2.5.2 Replacement of communications boards 498
22.2.5.3 Replacement of the input module 499
22.2.5.4 Replacement of the power supply board 499
22.2.5.5 Replacement of the I/O boards 500
22.2.6 Recalibration 500
22.2.7 Supercapacitor Discharged 500
22.2.8 Cleaning 501
22.3 Troubleshooting 502
22.3.1 Self-Diagnostic Software 502
22.3.2 Power-up Errors 502
22.3.3 Error Message or Code on Power-up 502
22.3.4 Out of Service LED on at power-up 503
22.3.5 Error Code during Operation 504
22.3.6 Mal-operation during testing 504
22.3.6.1 Failure of Output Contacts 504
22.3.6.2 Failure of Opto-inputs 504
22.3.6.3 Incorrect Analogue Signals 505
22.3.7 Coprocessor board failures 505
22.3.7.1 Signalling failure alarm (on its own) 505
22.3.7.2 C diff failure alarm (on its own) 505
22.3.7.3 Signalling failure and C diff failure alarms together 505
22.3.7.4 Incompatible IED 505
22.3.7.5 Comms changed 505
22.3.7.6 IEEE C37.94 fail 505
22.3.8 PSL Editor Troubleshooting 506
22.3.8.1 Diagram Reconstruction 506
22.3.8.2 PSL Version Check 506
22.3.9 Repair and Modification Procedure 506

Chapter 23 Technical Specifications 508

23.1 Chapter Overview 509
23.2 Interfaces 510
23.2.1 Front USB Port 510
23.2.2 Rear Serial Port 1 510
23.2.3 Fibre Rear Serial Port 1 510
23.2.4 Rear Serial Port 2 510
23.2.5 Optional Rear Serial Port (SK5) 511
23.2.6 IRIG-B (Demodulated) 511
23.2.7 IRIG-B (Modulated) 511
23.2.8 Rear Ethernet Port Copper 511
23.2.9 Rear Ethernet Port Fibre (Hardware Option (R/S/T) 512
23.2.9.1 100 Base FX Receiver Characteristics 512
23.2.9.2 100 Base FX Transmitter Characteristics 512
23.2.10 Rear Ethernet Port Fibre (Hardware Option U/W/Y) 512
23.2.10.1 100 Base FX Receiver Characteristics 513
23.2.10.2 100 Base FX Transmitter Characteristics 513
23.2.11 Fibre Teleprotection Interface 513
23.3 Protection Functions 515

23.3.1	Phase Current Differential Protection	515
23.3.2	Fibre Teleprotection Transfer Times	515
23.3.3	Autoreclose and Check Synychronism	516
23.3.4	Phase Overcurrent Protection	516
23.3.4.1	Phase Overcurrent Directional Parameters	516
23.3.5	Earth Fault Protection	516
23.3.5.1	Earth Fault Directional Parameters	517
23.3.6	Sensitive Earth Fault Protection	517
23.3.6.1	Sensitive Earth Fault Protection Directional Element	517
23.3.7	Restricted Earth Fault Protection	518
23.3.8	Negative Sequence Overcurrent Protection	518
23.3.8.1	Negative Sequence Overcurrent Protection Directional Parameters	518
23.3.9	Circuit Breaker Fail and Undercurrent Protection	518
23.3.10	Broken Conductor Protection	519
23.3.11	Thermal Overload Protection	519
23.4	**Monitoring, Control and Supervision**	**520**
23.4.1	Voltage Transformer Supervision	520
23.4.2	Standard Current Transformer Supervision	520
23.4.3	Differential Current Transformer Supervision	520
23.4.4	CB State and Condition Monitoring	520
23.4.5	PSL Timers	521
23.5	**Measurements and Recording**	**522**
23.5.1	General	522
23.5.2	Disturbance Records	522
23.5.3	Event, Fault and Maintenance Records	522
23.5.4	Fault Locator	522
23.6	**Ratings**	**523**
23.6.1	AC Measuring Inputs	523
23.6.2	Current Transformer Inputs	523
23.6.3	Voltage Transformer Inputs	523
23.6.4	Auxiliary Supply Voltage	523
23.6.5	Nominal Burden	524
23.6.6	Power Supply Interruption	524
23.6.7	Supercapacitor	525
23.7	**Input/Output Connections**	**526**
23.7.1	Isolated Digital Inputs	526
23.7.1.1	Nominal Pickup and Reset Thresholds	526
23.7.2	Standard Output Contacts	526
23.7.3	High Break Output Contacts	527
23.7.4	Watchdog Contacts	527
23.8	**Mechanical Specifications**	**528**
23.8.1	Physical Parameters	528
23.8.2	Enclosure Protection	528
23.8.3	Mechanical Robustness	528
23.8.4	Transit Packaging Performance	528
23.9	**Type Tests**	**529**
23.9.1	Insulation	529
23.9.2	Creepage Distances and Clearances	529
23.9.3	High Voltage (Dielectric) Withstand	529
23.9.4	Impulse Voltage Withstand Test	529
23.10	**Environmental Conditions**	**530**
23.10.1	Ambient Temperature Range	530
23.10.2	Temperature Endurance Test	530
23.10.3	Ambient Humidity Range	530
23.10.4	Corrosive Environments	530
23.11	**Electromagnetic Compatibility**	**531**

23.11.1 1 MHz Burst High Frequency Disturbance Test 531
23.11.2 Damped Oscillatory Test 531
23.11.3 Immunity to Electrostatic Discharge 531
23.11.4 Electrical Fast Transient or Burst Requirements 531
23.11.5 Surge Withstand Capability 531
23.11.6 Surge Immunity Test 531
23.11.7 Immunity to Radiated Electromagnetic Energy 532
23.11.8 Radiated Immunity from Digital Communications 532
23.11.9 Radiated Immunity from Digital Radio Telephones 532
23.11.10 Immunity to Conducted Disturbances Induced by Radio Frequency Fields 532
23.11.11 Magnetic Field Immunity 533
23.11.12 Conducted Emissions 533
23.11.13 Radiated Emissions 533
23.11.14 Power Frequency 533
23.12 Regulatory Compliance 534
23.12.1 EMC Compliance: 2014/30/EU 534
23.12.2 LVD Compliance: 2014/35/EU 534
23.12.3 R&TTE Compliance: 2014/53/EU 534
23.12.4 UL/CUL Compliance 534

Appendix A Ordering Options 535

Appendix B Settings and Signals 540

Appendix C Wiring Diagrams 542

Appendix D Hardware/Communications Compatibility Matrix Tables 561

CHAPTER 1

INTRODUCTION

1.1 CHAPTER OVERVIEW

This chapter provides some general information about the technical manual and an introduction to the device(s) described in this technical manual.

This chapter contains the following sections:

Chapter Overview 2
Foreword 3
Product Scope 5
Features and Functions 7
Logic Diagrams 9
Functional Overview 11

1.2 FOREWORD

This technical manual provides a functional and technical description of GE Vernova's P54A, P54B, P54C, P54E transmission protection IED, as well as a comprehensive set of instructions for using the device. The level at which this manual is written assumes that you are already familiar with protection engineering and have experience in this discipline. The description of principles and theory is limited to that which is necessary to understand the product. For further details on general protection engineering theory, we refer you to GE Vernova's publication, Protection and Automation Application Guide, which is available online or from our Contact Centre.

We have attempted to make this manual as accurate, comprehensive and user-friendly as possible. However we cannot guarantee that it is free from errors. Nor can we state that it cannot be improved. We would therefore be very pleased to hear from you if you discover any errors, or have any suggestions for improvement. Our policy is to provide the information necessary to help you safely specify, engineer, install, commission, maintain, and eventually dispose of this product. We consider that this manual provides the necessary information, but if you consider that more details are needed, please contact us.

All feedback should be sent to our contact centre via:

GA.support@gevernova.com

1.2.1 TARGET AUDIENCE

This manual is aimed towards all professionals charged with installing, commissioning, maintaining, troubleshooting, or operating any of the products within the specified product range. This includes installation and commissioning personnel as well as engineers who will be responsible for operating the product.

The level at which this manual is written assumes that installation and commissioning engineers have knowledge of handling electronic equipment. Also, system and protection engineers have a thorough knowledge of protection systems and associated equipment.

1.2.2 TYPOGRAPHICAL CONVENTIONS

The following typographical conventions are used throughout this manual.

- The names for special keys appear in capital letters.
  For example: ENTER
- When describing software applications, menu items, buttons, labels etc as they appear on the screen are written in bold type.
  For example: Select **Save** from the file menu.
- Filenames and paths use the courier font
  For example: `Example\File.text`
- Special terminology is written with leading capitals
  For example: Sensitive Earth Fault
- If reference is made to the IED's internal settings and signals database, the menu group heading (column) text is written in upper case italics
  For example: The *SYSTEM DATA* column
- If reference is made to the IED's internal settings and signals database, the setting cells and DDB signals are written in bold italics
  For example: The ***Language*** cell in the *SYSTEM DATA* column
- If reference is made to the IED's internal settings and signals database, the value of a cell's content is written in the Courier font
  For example: The ***Language*** cell in the *SYSTEM DATA* column contains the value *`English`*

1.2.3 NOMENCLATURE

Due to the technical nature of this manual, many special terms, abbreviations and acronyms are used throughout the manual. Some of these terms are well-known industry-specific terms while others may be special product-specific terms used by GE Vernova. The first instance of any acronym or term used in a particular chapter is explained. In addition, a separate glossary is available on the GE Vernova website, or from the GE Vernova contact centre.

We would like to highlight the following changes of nomenclature however:

- The word 'relay' is no longer used to describe the device itself. Instead, the device is referred to as the 'IED' (Intelligent Electronic Device), the 'device', or the 'product'. The word 'relay' is used purely to describe the electromechanical components within the device, i.e. the output relays.
- British English is used throughout this manual.
- The British term 'Earth' is used in favour of the American term 'Ground'.

1.2.4 COMPLIANCE

The device has undergone a range of extensive testing and certification processes to ensure and prove compatibility with all target markets. A detailed description of these criteria can be found in the Technical Specifications chapter.

1.3 PRODUCT SCOPE

The P54A, P54B, P54C, and P54E form a range of similar devices that can be used together in combination to realise numerical, phase-segregated, low-impedance, biased current differential protection schemes for multi-terminal, multi-composition transmission and distribution lines feeders and cables for circuit configurations having up to a maximum of 6 line-ends.

Different models are available to protect schemes that range from simple compact two-terminal applications through to more demanding wide-area mixed conductor technology configurations in which capacitive reactance introduces significant charging currents that challenge convention. The more demanding applications are catered for by products which include inputs to measure system voltages as well as currents.

All models (including the basic P54A) realise phase-segregated current differential protection through the combination of three-phase current inputs, fibre optic communications and a self-synchronising technique for time-alignment of the processing in all devices (known as 'ping-pong') to implement Kirchoff's Law.

Some devices in the range (P54B, P54C, and P54E) add an extra CT input to provide sensitive earth fault protection, as well as a set of VT inputs to support inclusion of autoreclose and check-synchronism functionality.

P54C and P54E take advantage of increasing case sizes (P54C - 60TE, P54E - 80TE) to offer expansion for extra digital inputs and outputs including high-speed high-break outputs.

The functionality implemented across the range of devices is summarised in the following table:

Variant		Version 92							Version 91						
Feature	Enabler	P54A	P54B	P54C		P54E			P54A	P54B	P54C		P54E		
Current Differential	4 CTs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Overcurrent		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sensitive Earth Fault	5th CT		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Voltage Protection	4 VTs		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Directional Overcurrent			✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Frequency Protection			✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Capacitive Charging Compensation		No	No	No	No	No	No	No							
3-Pole Autoreclose C/W Check Sync	8 Opto Inputs + 8 Standard Outputs		✓							✓					
1- or 3- Pole Autoreclose C/W Check Sync	16 Opto Inputs + 8 Standard Outputs (expandable)			✓	✓						✓	✓			
1- or 3- Pole Autoreclose C/W Check Sync	24 Opto Inputs + 16 Standard Outputs (expandable)					✓	✓	✓					✓	✓	✓
+16 Standard Outputs	I/O Expansion						✓	✓						✓	✓
+8 Standard Outputs				✓					✓						
+4 Fast High-Break Out					✓					✓					
+8 Fast High-Break Out						✓					✓				
+32 Standard Outputs															
+8 Opto Inputs								✓							✓
Function Keys	60TE Case			✓	✓						✓	✓			
	80TE Case					✓	✓	✓					✓	✓	✓

Key features for each product are described below:

- P54A compact (40TE width case), economical line differential protection without VT inputs, offering non-directional backup protection.
- P54B compact (40TE width case), economical line differential protection with directionalised back-up protection and inbuilt reclosing and check synchronism.
- P54C transmission-class 1- or 3-pole tripping line differential protection with back-up protection and inbuilt reclosing and check synchronism (60TE width case).
- P54E transmission-class 1- or 3-pole tripping line differential protection with back-up protection and inbuilt reclosing and check synchronism with a large number of binary I/O for traditional hardwired schemes (80TE width case).
- SW91 particularly suitable for cabled networks with significant capacitive charging currents.

P54A, P54B, P54C, and P54E share many common characteristics with other MiCOM Agile P54 current differential products but they are not compatible devices. Whereas P541, P542, P543, P544, P545, and P546 use a Fourier-filtering approach that is ideally suited to the protection of two- and three- terminals lines, P54A, P54B, P54C, and P54E manage the sampled-values of current signals with a co-ordinated scheme-wide approach to provide a robust solution to the problems associated with protecting circuits where the number of terminals can extend up to a maximum of six.

1.3.1 ORDERING OPTIONS

All current models and variants for this product are defined in an interactive spreadsheet called the CORTEC. This is available on the company website.

Alternatively, you can obtain it via the Contact Centre at: GA.support@gevernova.com

A copy of the CORTEC is also supplied as a static table in the Appendices of this document. However, it should only be used for guidance as it provides a snapshot of the interactive data taken at the time of publication.

1.4 FEATURES AND FUNCTIONS

1.4.1 CURRENT DIFFERENTIAL PROTECTION FUNCTIONS

Feature	IEC 61850	ANSI
Phase segregated current differential protection	DifPDIF1	87L
Between 2 and 6 terminal lines/cables		
Self-synchronisation feature		
InterMiCOM^{64} teleprotection for direct device-to-device communication (optional)		

1.4.2 PROTECTION FUNCTIONS

Feature	IEC 61850	ANSI
Tripping mode (1 & 3 pole)	PTRC	
ABC and ACB phase rotation		
Phase overcurrent, with optional directionality (4 stages)	OcpPTOC/RDIR	50/51/67
Earth/Ground overcurrent stages, with optional directionality (4 stages)	EfdPTOC/RDIR	50N/51N/ 67N
Sensitive Earth Fault (SEF) (4 stages)	SenPTOC/RDIR	50N/51N/67N
High impedance restricted earth fault (REF)	SenRefPDIF	64
Negative sequence overcurrent stages, with optional directionality (4 stages)	NgcPTOC/RDIR	67/46
Broken conductor, used to detect open circuit faults		46
Thermal overload protection	ThmPTTR	49
Phase directional power (4 stages)	PdpPDOP/PDUP	32
Undervoltage protection (2 stages)	VtpPhsPTUV	27
Overvoltage protection (2 stages)	VtpPhsPTOV	59
Remote overvoltage protection (2 stages)	VtpCmpPTOV	59R
Residual voltage protection (2 stages)	VtpResPTOV	59N
Underfrequency protection (4 stages)	FrqPTUF	81
Overfrequency protection (2 stages)	FrqPTOF	81
Rate of change of frequency protection (4 stages)	DfpPFRC	81
High speed breaker fail suitable for re-tripping and back-tripping (2 stages)	RBRF	50BF
Current Transformer supervision		46
Voltage Transformer supervision		47/27
Auto-reclose (4 shots)	RREC	79
Check synchronisation (2 stages)	RSYN	25

1.4.3 CONTROL FUNCTIONS

Feature	IEC 61850	ANSI
Watchdog contacts		
Read-only mode		
Function keys	FnkGGIO	
Programmable LEDs	LedGGIO	

Feature	IEC 61850	ANSI
Programmable hot keys		
Programmable allocation of digital inputs and outputs		
Fully customisable menu texts		
Circuit breaker control, status & condition monitoring	XCBR	52
CT supervision		
VT supervision		
Trip circuit and coil supervision		
Control inputs	PloGGIO1	
Power-up diagnostics and continuous self-monitoring		
Dual rated 1A and 5A CT inputs		
Alternative setting groups (4)		
Graphical programmable scheme logic (PSL)		
Fault locator	RFLO	

1.4.4 MEASUREMENT FUNCTIONS

Measurement Function	IEC 61850	ANSI
Measurement of all instantaneous & integrated values (Exact range of measurements depend on the device model)		MET
Disturbance recorder for waveform capture - specified in samples per cycle	RDRE	DFR
Fault Records		
Maintenance Records		
Event Records/Event logging		Event records
Time Stamping of Opto-inputs	Yes	Yes

1.4.5 COMMUNICATION FUNCTIONS

Feature	ANSI
NERC compliant cyber-security	
Front RS232 serial communication port for configuration	16S
Rear serial RS485 communication port for SCADA control	16S
2 Additional rear serial communication ports for SCADA control and teleprotection (fibre and copper) (optional)	16S
Ethernet communication (optional)	16E
Redundant Ethernet communication (optional)	16E
Courier Protocol	16S
IEC 61850 Edition 1 or Edition 2 (optional)	16E
IEC 60870-5-103 (optional)	16S
DNP3.0 over serial link (optional)	16S
DNP3.0 over Ethernet (optional)	16E
SNMP	16E
IRIG-B time synchronisation (optional)	CLK
IEEE 1588 PTP (Edition 2 devices only)	

1.5 LOGIC DIAGRAMS

This technical manual contains many logic diagrams, which should help to explain the functionality of the device. Although this manual has been designed to be as specific as possible to the chosen product, it may contain diagrams, which have elements applicable to other products. If this is the case, a qualifying note will accompany the relevant part.

The logic diagrams follow a convention for the elements used, using defined colours and shapes. A key to this convention is provided below. We recommend viewing the logic diagrams in colour rather than in black and white. The electronic version of the technical manual is in colour, but the printed version may not be. If you need coloured diagrams, they can be provided on request by calling the contact centre and quoting the diagram number.

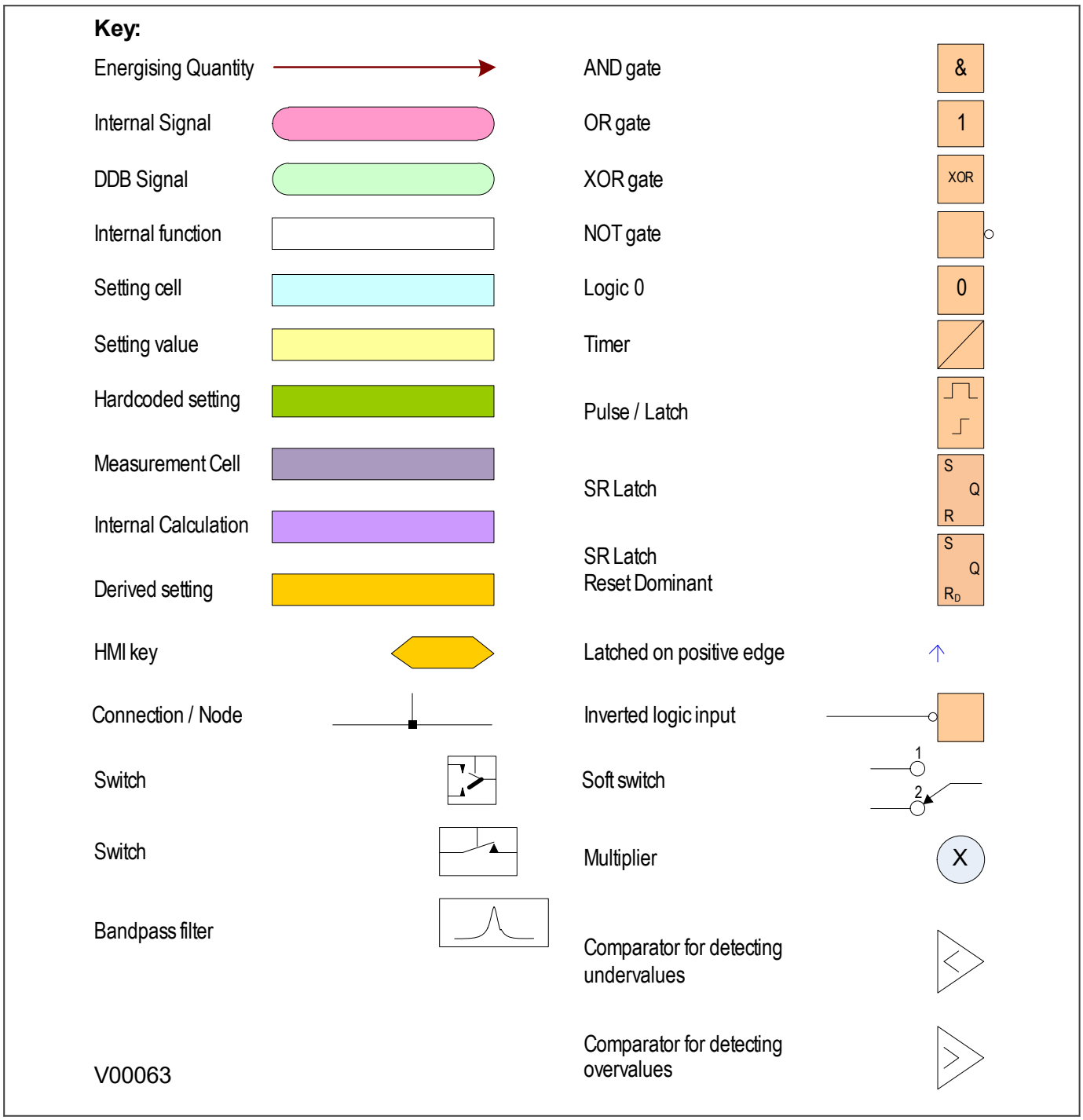


Figure 1: Key to logic diagrams

1.6 FUNCTIONAL OVERVIEW

This diagram is applicable to several multi-end current differential protection products; P54A, P54B, P54C and P54E. Use the diagram key to determine the features relevant to the product described in this technical manual.

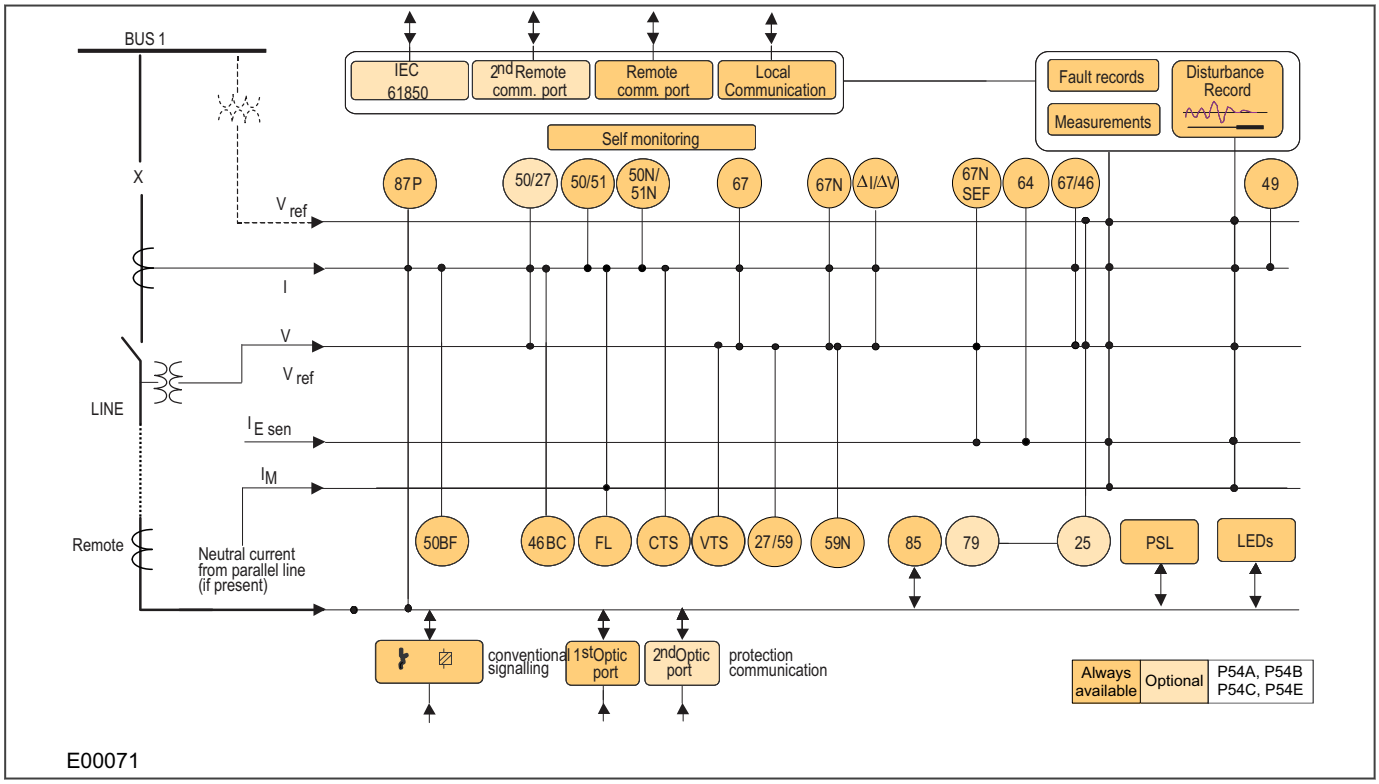


Figure 2: Functional overview

CHAPTER 2

SAFETY INFORMATION

2.1 CHAPTER OVERVIEW

This chapter provides information about the safe handling of the equipment. The equipment must be properly installed and handled in order to maintain it in a safe condition and to keep personnel safe at all times. You must be familiar with information contained in this chapter before unpacking, installing, commissioning, or servicing the equipment.

This chapter contains the following sections:

Chapter Overview 13

Health and Safety 14

Symbols 15

Installation, Commissioning and Servicing 16

Decommissioning and Disposal 22

Regulatory Compliance 23

2.2 HEALTH AND SAFETY

Personnel associated with the equipment must be familiar with the contents of this Safety Information.

When electrical equipment is in operation, dangerous voltages are present in certain parts of the equipment. Improper use of the equipment and failure to observe warning notices will endanger personnel.

Only qualified personnel may work on or operate the equipment. Qualified personnel are individuals who are:

- Familiar with the installation, commissioning, and operation of the equipment and the system to which it is being connected.
- Familiar with accepted safety engineering practises and are authorised to energise and de-energise equipment in the correct manner.
- Trained in the care and use of safety apparatus in accordance with safety engineering practises
- Tained in emergency procedures (first aid).

The documentation provides instructions for installing, commissioning and operating the equipment. It cannot, however cover all conceivable circumstances. In the event of questions or problems, do not take any action without proper authorisation. Please contact your local sales office and request the necessary information.

2.3 SYMBOLS

Throughout this manual you will come across the following symbols. You will also see these symbols on parts of the equipment.



Caution:
Refer to equipment documentation. Failure to do so could result in damage to the equipment



Warning:
Risk of electric shock



Warning:
Risk of damage to eyesight



Earth terminal. *Note: This symbol may also be used for a protective conductor (earth) terminal if that terminal is part of a terminal block or sub-assembly.*



Protective conductor (earth) terminal



Instructions on disposal requirements

Note:
The term 'Earth' used in this manual is the direct equivalent of the North American term 'Ground'.

2.4 INSTALLATION, COMMISSIONING AND SERVICING

2.4.1 LIFTING HAZARDS

Many injuries are caused by:

- Lifting heavy objects
- Lifting things incorrectly
- Pushing or pulling heavy objects
- Using the same muscles repetitively

Plan carefully, identify any possible hazards and determine how best to move the product. Look at other ways of moving the load to avoid manual handling. Use the correct lifting techniques and Personal Protective Equipment (PPE) to reduce the risk of injury.

2.4.2 ELECTRICAL HAZARDS



Caution:
All personnel involved in installing, commissioning, or servicing this equipment must be familiar with the correct working procedures.



Caution:
Consult the equipment documentation before installing, commissioning, or servicing the equipment.



Caution:
Always use the equipment as specified. Failure to do so will jeopardise the protection provided by the equipment.



Warning:
Removal of equipment panels or covers may expose hazardous live parts. Do not touch until the electrical power is removed. Take care when there is unlocked access to the rear of the equipment.



Warning:
Isolate the equipment before working on the terminal strips.



Warning:
Use a suitable protective barrier for areas with restricted space, where there is a risk of electric shock due to exposed terminals.



Caution:
Disconnect power before disassembling. Disassembly of the equipment may expose sensitive electronic circuitry. Take suitable precautions against electrostatic voltage discharge (ESD) to avoid damage to the equipment.



Warning:
NEVER look into optical fibres or optical output connections. Always use optical power meters to determine operation or signal level.



Warning:
Testing may leave capacitors charged to dangerous voltage levels. Discharge capacitors by reducing test voltages to zero before disconnecting test leads.



Caution:
Operate the equipment within the specified electrical and environmental limits.



Caution:
Before cleaning the equipment, ensure that no connections are energised. Use a lint free cloth dampened with clean water.

Note:
Contact fingers of test plugs are normally protected by petroleum jelly, which should not be removed.

2.4.3 UL/CSA/CUL REQUIREMENTS

The information in this section is applicable only to equipment carrying UL/CSA/CUL markings.



Caution:
Equipment intended for rack or panel mounting is for use on a flat surface of a Type 1 enclosure, as defined by Underwriters Laboratories (UL).



Caution:
To maintain compliance with UL and CSA/CUL, install the equipment using UL/CSA-recognised parts for: cables, protective fuses, fuse holders and circuit breakers, insulation crimp terminals, and replacement internal batteries.

2.4.4 FUSING REQUIREMENTS



Caution:
Where UL/CSA listing of the equipment is required for external fuse protection, a UL or CSA Listed fuse must be used for the auxiliary supply. The listed protective fuse type is: Class J time delay fuse, with a maximum current rating of 15 A and a minimum DC rating of 250 V dc (for example type AJT15).



Caution:
Where UL/CSA listing of the equipment is not required, a high rupture capacity (HRC) fuse type with a maximum current rating of 16 Amps and a minimum dc rating of 250 V dc may be used for the auxiliary supply (for example Red Spot type NIT or TIA).
For P50 models, use a 1A maximum T-type fuse.
For P60 models, use a 4A maximum T-type fuse.



Caution:
Digital input circuits should be protected by a high rupture capacity NIT or TIA fuse with maximum rating of 16 A. for safety reasons, current transformer circuits must never be fused. Other circuits should be appropriately fused to protect the wire used.



Caution:
CTs must NOT be fused since open circuiting them may produce lethal hazardous voltages

2.4.5 EQUIPMENT CONNECTIONS



Warning:
Terminals exposed during installation, commissioning and maintenance may present a hazardous voltage unless the equipment is electrically isolated.



Caution:
Tighten M4 clamping screws of heavy duty terminal block connectors to a nominal torque of 1.3 Nm.
Tighten captive screws of terminal blocks to 0.5 Nm minimum and 0.6 Nm maximum.



Caution:
Always use insulated crimp terminations for voltage and current connections.



Caution:
Always use the correct crimp terminal and tool according to the wire size.



Caution:
Watchdog (self-monitoring) contacts are provided to indicate the health of the device on some products. We strongly recommend that you hard wire these contacts into the substation's automation system, for alarm purposes.

2.4.6 PROTECTION CLASS 1 EQUIPMENT REQUIREMENTS



Caution:
Earth the equipment with the supplied PCT (Protective Conductor Terminal).



Caution:
Do not remove the PCT.



Caution:
The PCT is sometimes used to terminate cable screens. Always check the PCT's integrity after adding or removing such earth connections.



Caution:
Use a locknut or similar mechanism to ensure the integrity of stud-connected PCTs.



Caution:
The recommended minimum PCT wire size is 2.5 mm² for countries whose mains supply is 230 V (e.g. Europe) and 3.3 mm² for countries whose mains supply is 110 V (e.g. North America). This may be superseded by local or country wiring regulations. For P60 products, the recommended minimum PCT wire size is 6 mm². See product documentation for details.



Caution:
The PCT connection must have low-inductance and be as short as possible.



Caution:
All connections to the equipment must have a defined potential. Connections that are pre-wired, but not used, should be earthed, or connected to a common grouped potential.

2.4.7 PRE-ENERGISATION CHECKLIST



Caution:
Check voltage rating/polarity (rating label/equipment documentation).



Caution:
Check CT circuit rating (rating label) and integrity of connections.



Caution:
Check protective fuse or miniature circuit breaker (MCB) rating.



Caution:
Check integrity of the PCT connection.



Caution:
Check voltage and current rating of external wiring, ensuring it is appropriate for the application.

2.4.8 PERIPHERAL CIRCUITRY



Warning:
Do not open the secondary circuit of a live CT since the high voltage produced may be lethal to personnel and could damage insulation. Short the secondary of the line CT before opening any connections to it.

Note:
For most GE Vernova equipment with ring-terminal connections, the threaded terminal block for current transformer termination is automatically shorted if the module is removed. Therefore external shorting of the CTs may not be required. Check the equipment documentation and wiring diagrams first to see if this applies.



Caution:
Where external components such as resistors or voltage dependent resistors (VDRs) are used, these may present a risk of electric shock or burns if touched.



Warning:
Take extreme care when using external test blocks and test plugs such as the MMLG, MMLB and P990, as hazardous voltages may be exposed. Ensure that CT shorting links are in place before removing test plugs, to avoid potentially lethal voltages.



Warning:
Data communication cables with accessible screens and/or screen conductors, (including optical fibre cables with metallic elements), may create an electric shock hazard in a sub-station environment if both ends of the cable screen are not connected to the same equipotential bonded earthing system.

To reduce the risk of electric shock due to transferred potential hazards:

i. The installation shall include all necessary protection measures to ensure that no fault currents can flow in the connected cable screen conductor.

ii. The connected cable shall have its screen conductor connected to the protective conductor terminal (PCT) of the connected equipment at both ends. This connection may be inherent in the connectors provided on the equipment but, if there is any doubt, this must be confirmed by a continuity test.

iii. The protective conductor terminal (PCT) of each piece of connected equipment shall be connected directly to the same equipotential bonded earthing system.

iv. If, for any reason, both ends of the cable screen are not connected to the same equipotential bonded earth system, precautions must be taken to ensure that such screen connections are made safe before work is done to, or in proximity to, any such cables.

v. No equipment shall be connected to any download or maintenance circuits or connectors of this product except temporarily and for maintenance purposes only.

vi. Equipment temporarily connected to this product for maintenance purposes shall be protectively earthed (if the temporary equipment is required to be protectively earthed), directly to the same equipotential bonded earthing system as the product.



Warning:
Small Form-factor Pluggable (SFP) modules which provide copper Ethernet connections typically do not provide any additional safety isolation. Copper Ethernet SFP modules must only be used in connector positions intended for this type of connection.

2.4.9 UPGRADING/SERVICING



Warning:
Do not insert or withdraw modules, PCBs or expansion boards from the equipment while energised, as this may result in damage to the equipment. Hazardous live voltages would also be exposed, endangering personnel.



Caution:
Internal modules and assemblies can be heavy and may have sharp edges. Take care when inserting or removing modules into or out of the IED.

2.5 DECOMMISSIONING AND DISPOSAL



Caution:
Before decommissioning, completely isolate the equipment power supplies (both poles of any dc supply). The auxiliary supply input may have capacitors in parallel, which may still be charged. To avoid electric shock, discharge the capacitors using the external terminals before decommissioning.



Caution:
Avoid incineration or disposal to water courses. Dispose of the equipment in a safe, responsible and environmentally friendly manner, and if applicable, in accordance with country-specific regulations.

2.6 REGULATORY COMPLIANCE

Compliance with the European Commission Directive on EMC and LVD is demonstrated using a technical file.

CE

2.6.1 EMC COMPLIANCE: 2014/30/EU

The product specific Declaration of Conformity (DoC) lists the relevant harmonised standard(s) or conformity assessment used to demonstrate compliance with the EMC directive.

2.6.2 LVD COMPLIANCE: 2014/35/EU

The product specific Declaration of Conformity (DoC) lists the relevant harmonised standard(s) or conformity assessment used to demonstrate compliance with the LVD directive.

Safety related information, such as the installation I overvoltage category, pollution degree and operating temperature ranges are specified in the Technical Data section of the relevant product documentation and/or on the product labelling.

Unless otherwise stated in the Technical Data section of the relevant product documentation, the equipment is intended for indoor use only. Where the equipment is required for use in an outdoor location, it must be mounted in a specific cabinet or housing to provide the equipment with the appropriate level of protection from the expected outdoor environment.

2.6.3 R&TTE COMPLIANCE: 2014/53/EU

Radio and Telecommunications Terminal Equipment (R&TTE) directive 2014/53/EU.

Conformity is demonstrated by compliance to both the EMC directive and the Low Voltage directive, to zero volts.

2.6.4 UL/CUL COMPLIANCE

If marked with this logo, the product is compliant with the requirements of the Canadian and USA Underwriters Laboratories.

The relevant UL file number and ID is shown on the equipment.

c UL us

CHAPTER 3

HARDWARE DESIGN

3.1 CHAPTER OVERVIEW

This chapter provides information about the product's hardware design.

This chapter contains the following sections:

Chapter Overview 25
Hardware Architecture 26
Mechanical Implementation 28
Front Panel 30
Rear Panel 33
Boards and Modules 35

3.2 HARDWARE ARCHITECTURE

The main components comprising devices based on the Px4x platform are as follows:

- The housing, consisting of a front panel and connections at the rear
- The Main processor module consisting of the main CPU (Central Processing Unit), memory and an interface to the front panel HMI (Human Machine Interface)
- A selection of plug-in boards and modules with presentation at the rear for the power supply, communication functions, digital I/O, analogue inputs, and time synchronisation connectivity

All boards and modules are connected by a parallel data and address bus, which allows the processor module to send and receive information to and from the other modules as required. There is also a separate serial data bus for conveying sampled data from the input module to the CPU. These parallel and serial databuses are shown as a single interconnection module in the following figure, which shows typical modules and the flow of data between them.

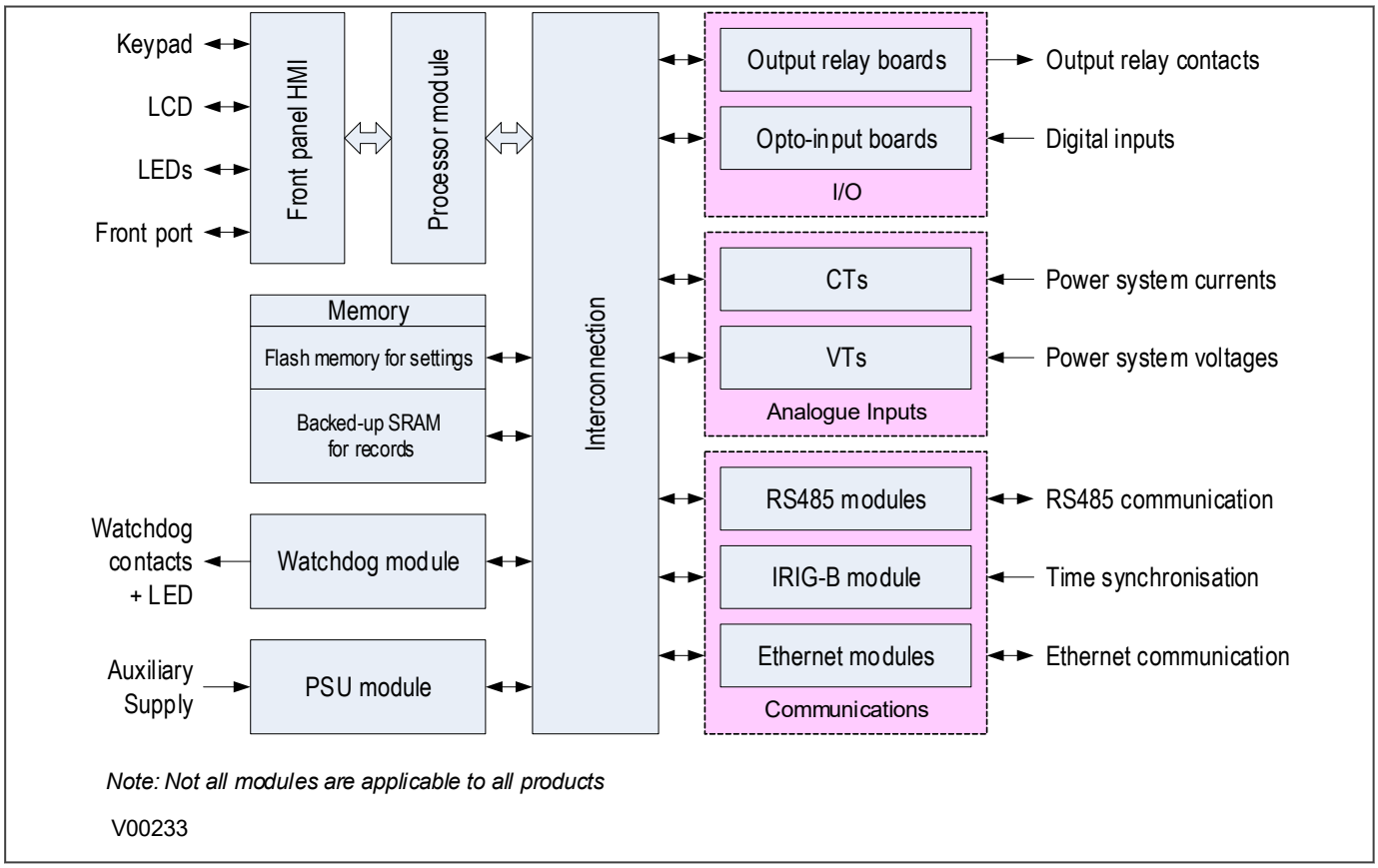


Figure 3: Hardware architecture

3.2.1 COPROCESSOR HARDWARE ARCHITECTURE

Some products are equipped with a coprocessor board for extra computing power. There are several variants of coprocessor board, depending on the required communication requirements. Some models do not need any external communication inputs, some models need inputs for current differential functionality and some models need an input for GPS time synchronisation.

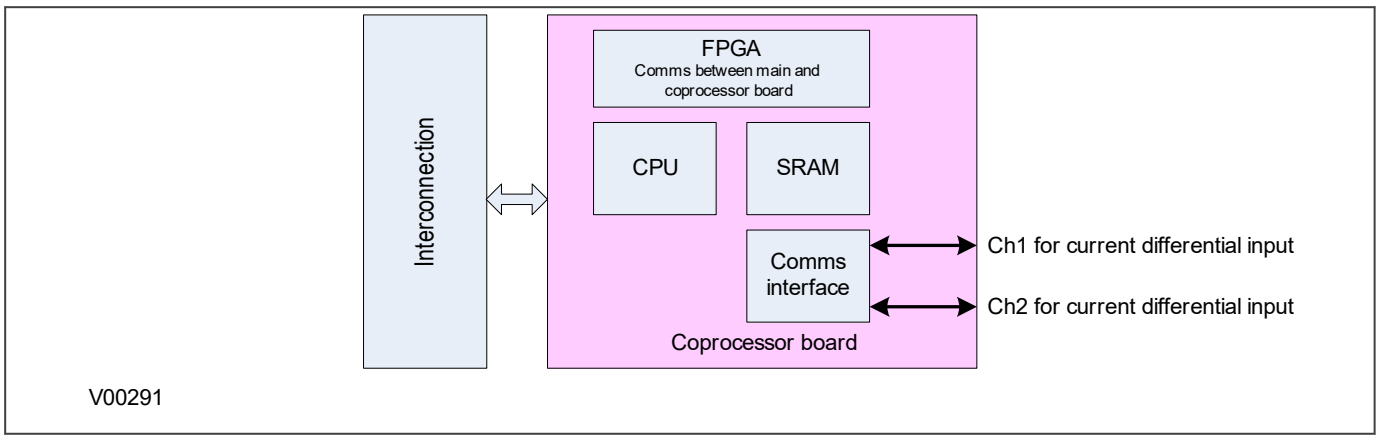


Figure 4: Coprocessor hardware architecture

3.3 MECHANICAL IMPLEMENTATION

All products based on the Px4x platform have common hardware architecture. The hardware is modular and consists of the following main parts:

- Case and terminal blocks
- Boards and modules
- Front panel

The case comprises the housing metalwork and terminal blocks at the rear. The boards fasten into the terminal blocks and are connected together by a ribbon cable. This ribbon cable connects to the processor in the front panel.

The following diagram shows an exploded view of a typical product. The diagram shown does not necessarily represent exactly the product model described in this manual.

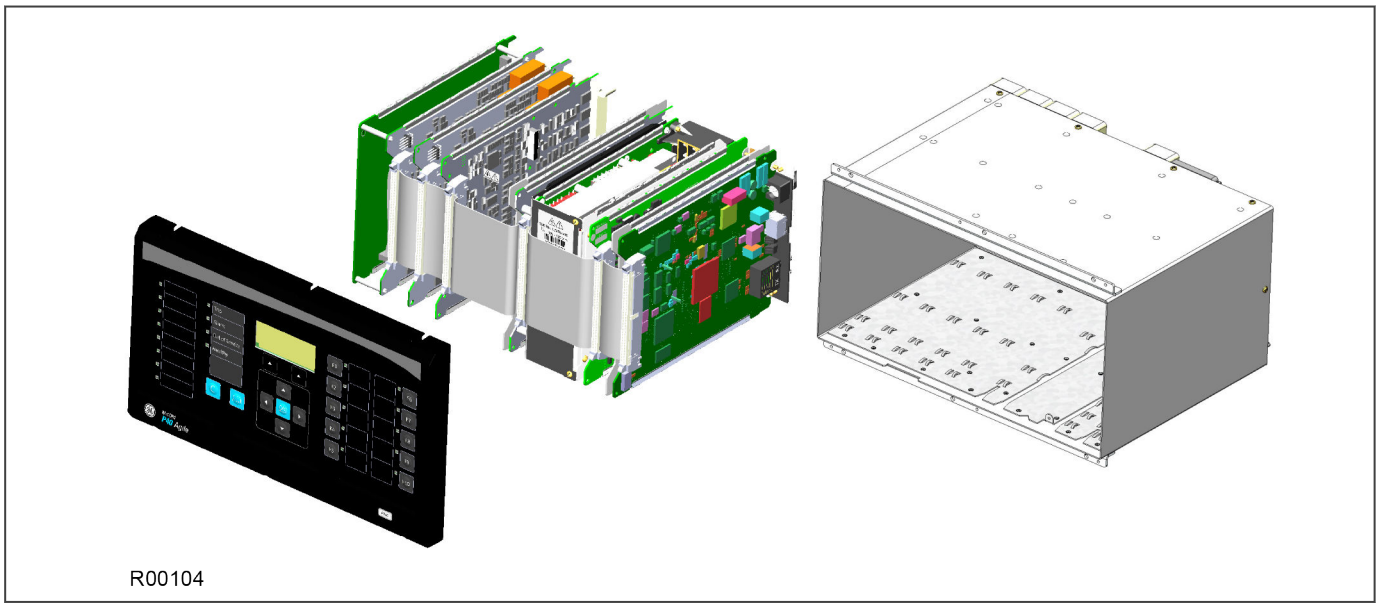


Figure 5: Exploded view of IED

3.3.1 HOUSING VARIANTS

The Px4x range of products are implemented in a range of case sizes. Case dimensions for industrial products usually follow modular measurement units based on rack sizes. These are: U for height and TE for width, where:

- 1U = 1.75 inches = 44.45 mm
- 1TE = 0.2 inches = 5.08 mm

The products are available in panel-mount or standalone versions. All products are nominally 4U high. This equates to 177.8 mm or 7 inches.

The cases are pre-finished steel with a conductive covering of aluminium and zinc. This provides good grounding at all joints, providing a low resistance path to earth that is essential for performance in the presence of external noise.

The case width depends on the product type and its hardware options. There are three different case widths for the described range of products: 40TE, 60TE and 80TE. The case dimensions and compatibility criteria are as follows:

Case width (TE)	Case width (mm)	Case width (inches)
40TE	203.2	8
60TE	304.8	12
80TE	406.4	16

Note:
Not all case sizes are available for all models.

3.3.2 LIST OF BOARDS

The product's hardware consists of several modules drawn from a standard range. The exact specification and number of hardware modules depends on the model number and variant. Depending on the exact model, the product in question will use a selection of the following boards.

Board	Use
Main Processor board - 40TE or smaller	Main Processor board - without support for function keys
Main Processor board - 60TE or larger	Main Processor board - with support for function keys
Power supply board - 24/54V DC	Power supply input. Accepts DC voltage between 24V and 54V
Power supply board - 48/125V DC	Power supply input. Accepts DC voltage between 48V and 125V
Power supply board - 110/250V DC	Power supply input. Accepts DC voltage between 110V and 125V
Transformer board	Contains the voltage and current transformers
Input board	Contains the A/D conversion circuitry
Input board with opto-inputs	Contains the A/D conversion circuitry + 8 digital opto-inputs
Output relay output board	Standard output relay board
High-break output relay board	Output relay board with high breaking capacity relays
IRIG-B board - modulated input	Interface board for modulated IRIG-B timing signal
IRIG-B board - demodulated input	Interface board for demodulated IRIG-B timing signal
Fibre board	Interface board for fibre-based RS485 connection
Fibre board + IRIG-B	Interface board for fibre-based RS485 connection + demodulated IRIG-B
2nd rear communications board	Interface board for RS232/RS485 connections
2nd rear communications board with IRIG-B input	Interface board for RS232/RS485 + IRIG-B connections
Redundant Ethernet RSTP + PRP + HSR + Failover universal IRIG-B	2 ST duplex redundant Ethernet ports running RSTP + PRP + HSR + Failover (two fibre pairs), with onboard universal IRIG-B (Hardware option R)
Redundant Ethernet RSTP + PRP + HSR + Failover universal IRIG-B	2 RJ45 duplex redundant Ethernet ports running RSTP + PRP + HSR + Failover (two copper pairs), with on-board universal IRIG-B (Hardware option S)
Single Ethernet RSTP + PRP + HSR + Failover universal IRIG-B	Single Ethernet port running RSTP + PRP + HSR + Failover (one copper, RJ45 one ST multi-mode fibre optic), with on-board universal IRIG-B (Hardware option T)
Single Ethernet, universal IRIG-B, IEEE1588	Single LC duplex Ethernet port (one LC multi-mode fibre optic) with universal IRIG-B (Hardware option U)
Redundant Ethernet RSTP + PRP + HSR + Failover universal IRIG-B	2 RJ45 duplex redundant Ethernet ports running RSTP + PRP + HSR + Failover (two copper pairs), with on-board universal IRIG-B (Hardware option W)
Redundant Ethernet RSTP + PRP + HSR + Failover universal IRIG-B	2 LC duplex redundant Ethernet ports running RSTP + PRP + HSR + Failover (two fibre pairs), with on-board universal IRIG-B (Hardware option Y)
Coprocessor board with dual fibre inputs	Coprocessor board with fibre connections for current differential inputs

3.4 FRONT PANEL

3.4.1 FRONT PANEL

Depending on the exact model and chosen options, the product will be housed in either a 40TE, 60TE or 80TE case. By way of example, the following diagram shows the front panel of a typical 60TE unit. The front panels of the products based on 40TE and 80TE cases have a lot of commonality and differ only in that the 40TE front panel does not include 10 function keys with their associated user-programmable LEDs.



R00298

Figure 6: Front panel (60TE)

The front panel consists of:

- Top and bottom compartments with hinged cover
- LCD display
- Keypad
- USB Type B port inside the bottom compartment
- Fixed function LEDs
- Function keys and LEDs (60TE and 80TE models)
- Programmable LEDs

3.4.1.1 FRONT PANEL COMPARTMENTS

The top compartment contains labels for the:

- Order code, Serial number and Test ID.

Note:
The Test ID on the label in the top compartment of the front panel is the serial number of the relay and consists of 6 numeric and 1 alphanumeric characters, for example 123456Z. The serial number is also shown in the System Data menu of the HMI. This serial number can be used to obtain the recovery password from the Contact Centre.
The serial number on the label in the top compartment of the front panel is the SAP manufacturing serial number and consists of 8 numeric characters, for example 37123456.

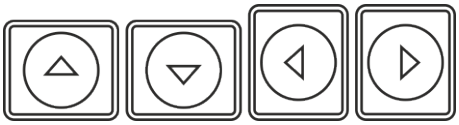
- Current and voltage ratings

The bottom compartment contains:

- USB type B port

3.4.1.2 KEYPAD

The keypad consists of the following keys:

4 arrow keys to navigate the menus (organised around the Enter key)	
An enter key for executing the chosen option	
A clear key for clearing the last command	
A read key for viewing larger blocks of text (arrow keys now used for scrolling)	
2 hot keys for scrolling through the default display and for control of setting groups. These are situated directly below the LCD display.	

3.4.1.2.1 LIQUID CRYSTAL DISPLAY

The LCD is a high resolution monochrome display with 16 characters by 3 lines and controllable back light.

3.4.1.3 USB PORT

The USB port is situated inside the bottom compartment, and is used to communicate with a locally connected PC. It has two main purposes:

- To transfer settings information to/from the PC from/to the device.
- For downloading firmware updates and menu text editing.

The port is intended for temporary connection during testing, installation and commissioning. It is not intended to be used for permanent SCADA communications. This port supports the Courier communication protocol only. Courier is a proprietary communication protocol to allow communication with a range of protection equipment, and between the device and the Windows-based support software package.

You can connect the unit to a PC with a USB cable up to 5 m in length.

The inactivity timer for the front port is set to 15 minutes. This controls how long the unit maintains its level of password access on the front port. If no messages are received on the front port for 15 minutes, any password access level that has been enabled is cancelled.

Note:
The front USB port does not support automatic extraction of event and disturbance records, although this data can be accessed manually.



Caution:
When not in use, always close the cover of the USB port to prevent contamination.

3.4.1.4 FIXED FUNCTION LEDS

Four fixed-function LEDs on the left-hand side of the front panel indicate the following conditions.

- Trip (Red) switches ON when the IED issues a trip signal. It is reset when the associated fault record is cleared from the front display. Also the trip LED can be configured as self-resetting.
- Alarm (Yellow) flashes when the IED registers an alarm. This may be triggered by a fault, event or maintenance record. The LED flashes until the alarms have been accepted (read), then changes to constantly ON. When the alarms are cleared, the LED switches OFF.
- Out of service (Yellow) is ON when the IED's functions are unavailable.
- Healthy (Green) is ON when the IED is in correct working order, and should be ON at all times. It goes OFF if the unit's self-tests show there is an error in the hardware or software. The state of the healthy LED is reflected by the watchdog contacts at the back of the unit.

3.4.1.5 FUNCTION KEYS

The programmable function keys are available for custom use for some models.

Factory default settings associate specific functions to these keys, but by using programmable scheme logic, you can change the default functions of these keys to fit specific needs. Adjacent to these function keys are programmable LEDs, which are usually set to be associated with their respective function keys.

3.4.1.6 PROGRAMABLE LEDS

The device has a number of programmable LEDs, which can be associated with PSL-generated signals. The programmable LEDs for most models are tri-colour and can be set to RED, YELLOW or GREEN. However the programmable LEDs for some models are single-colour (red) only. The single-colour LEDs can be recognised by virtue of the fact they are large and slightly oval, whereas the tri-colour LEDs are small and round.

3.5 REAR PANEL

The MiCOM Px40 series uses a modular construction. Most of the internal structure consists of boards and modules that fit into slots. Some of the boards plug into terminal blocks, which are bolted onto the rear of the unit. However, some boards such as the communications boards have their own connectors. The rear panel consists of these terminal blocks plus the rears of the communications boards.

The back panel cut-outs and slot allocations vary. This depends on the product, the type of boards and the terminal blocks needed to populate the case. The following diagram shows a typical rear view of a case populated with various boards.

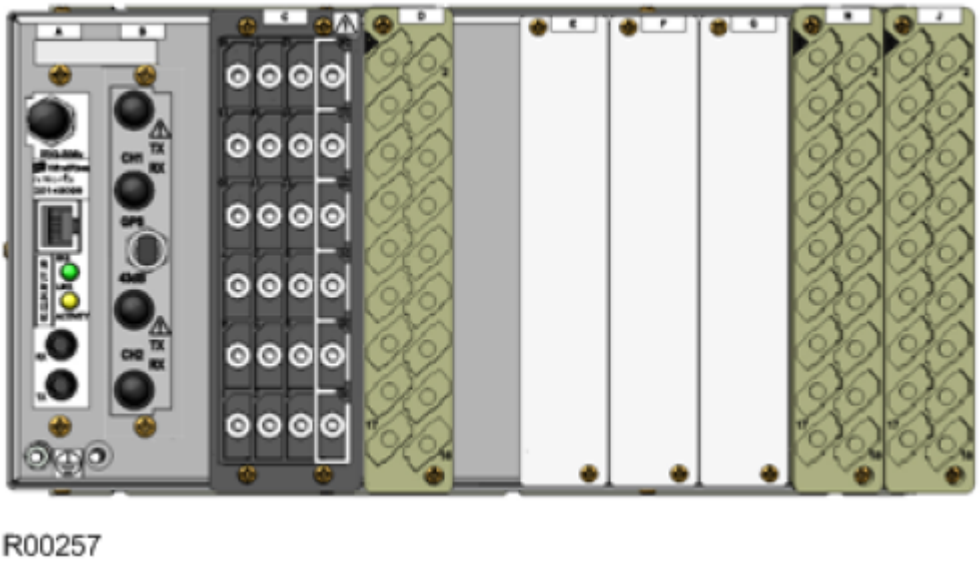


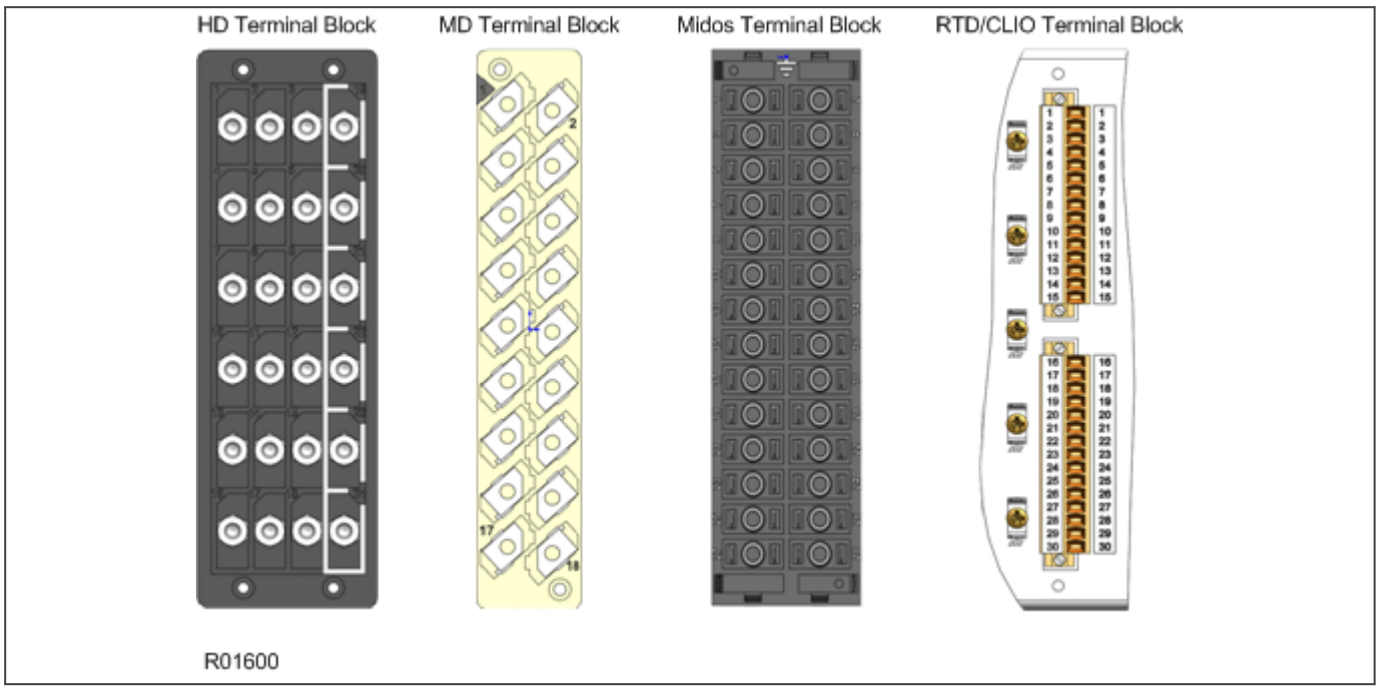
Figure 7: Rear view of populated case

Note:
This diagram is just an example and may not show the exact product described in this manual. It also does not show the full range of available boards, just a typical arrangement.

Not all slots are the same size. The slot width depends on the type of board or terminal block. For example, HD (heavy duty) terminal blocks, as required for the analogue inputs, require a wider slot size than MD (medium duty) terminal blocks. The board positions are not generally interchangeable. Each slot is designed to house a particular type of board. Again this is model-dependent.

The device may use some of the terminal block types shown in the following diagram. The terminal blocks are fastened to the rear panel with screws.

- Heavy duty (HD) terminal blocks for CT and VT circuits
- Medium duty (MD) terminal blocks for the power supply, opto-inputs, relay outputs and rear communications port
- MiDOS terminal blocks for CT and VT circuits
- RTD/CLIO terminal block for connection to analogue transducers (refer to CORTEC options)



Note:
Not all products use all types of terminal blocks. The product described in this manual may use one or more of the above types.

3.5.1 TERMINAL BLOCK INGRESS PROTECTION

IP2x shields and side cover panels are designed to provide IP20 ingress protection for MiCOM terminal blocks. The shields and covers may be attached during installation or retrofitted to upgrade existing installations - see figure below. For more information, contact your local sales office or our worldwide Contact Centre.

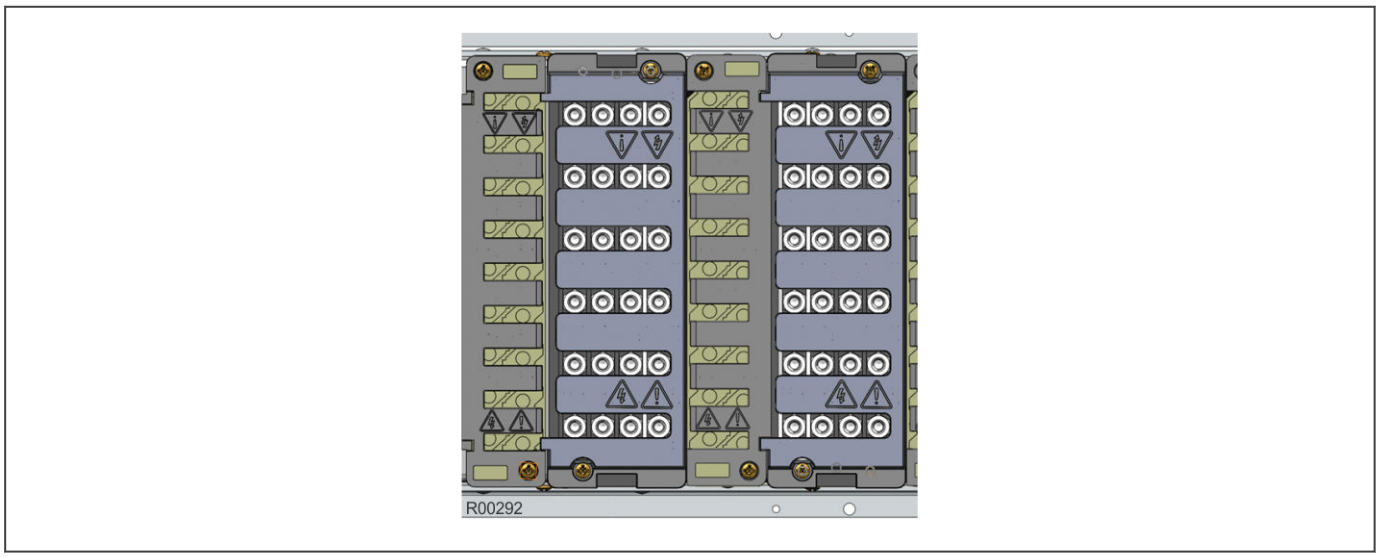


Figure 8: Example - fitted IP2x shields (cabling omitted for clarity)

3.6 BOARDS AND MODULES

Each product comprises a selection of PCBs (Printed Circuit Boards) and subassemblies, depending on the chosen configuration.

3.6.1 PCBS

A PCB typically consists of the components, a front connector for connecting into the main system parallel bus via a ribbon cable, and an interface to the rear. This rear interface may be:

- Directly presented to the outside world (as is the case for communication boards such as Ethernet Boards)
- Presented to a connector, which in turn connects into a terminal block bolted onto the rear of the case (as is the case for most of the other board types)

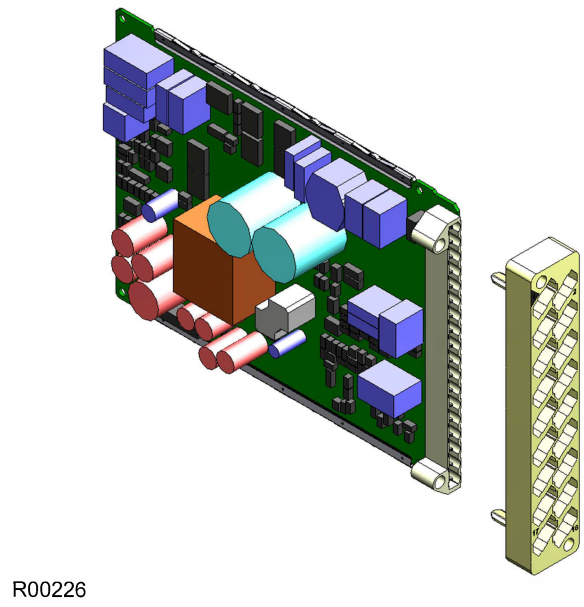


Figure 9: Rear connection to terminal block

3.6.2 SUBASSEMBLIES

A sub-assembly consists of two or more boards bolted together with spacers and connected with electrical connectors. It may also have other special requirements such as being encased in a metal housing for shielding against electromagnetic radiation.

Boards are designated by a part number beginning with ZN, whereas pre-assembled sub-assemblies are designated with a part number beginning with GN. Sub-assemblies, which are put together at the production stage, do not have a separate part number.

The products in the Px40 series typically contain two sub-assemblies:

- The power supply assembly comprising:
  - A power supply board
  - An output relay board
- The input module comprising:
  - One or more transformer boards, which contains the voltage and current transformers (partially or fully populated)
  - One or more input boards
  - Metal protective covers for EM (electromagnetic) shielding

The input module is pre-assembled and is therefore assigned a GN number, whereas the power supply module is assembled at production stage and does not therefore have an individual part number.

3.6.3 MAIN PROCESSOR BOARD

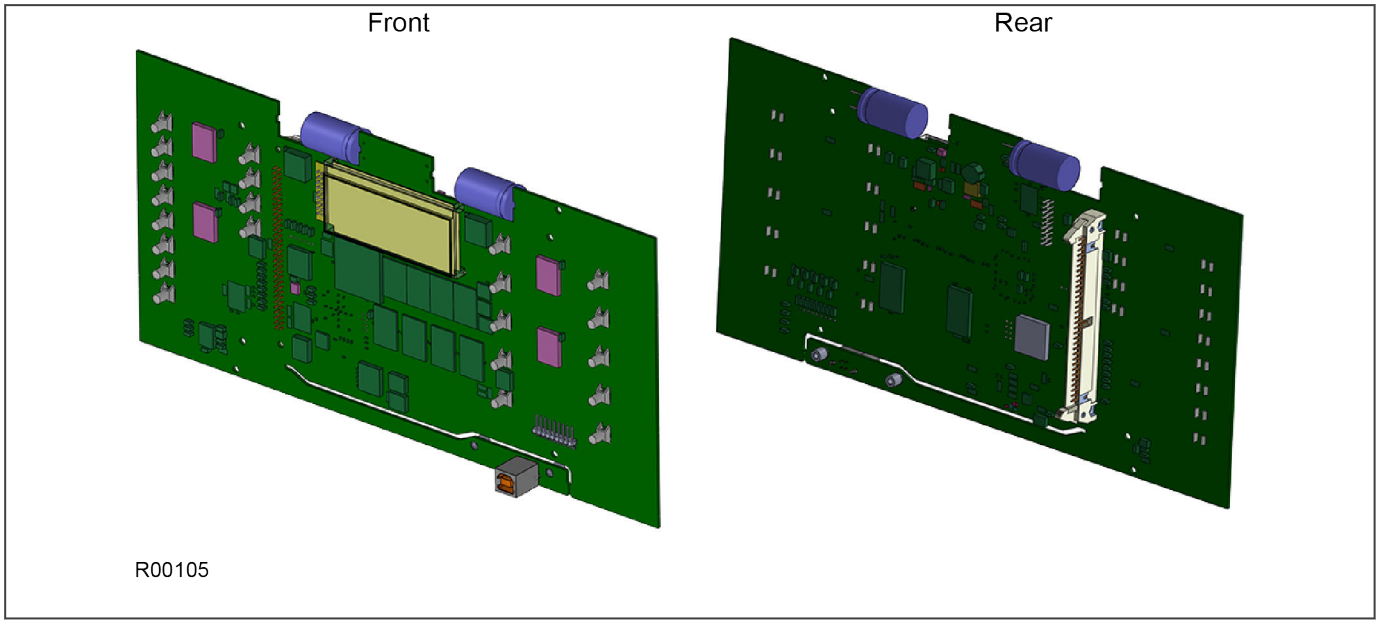


Figure 10: Main processor board

The main processor board performs all calculations and controls the operation of all other modules in the IED, including the data communication and user interfaces. This is the only board that does not fit into one of the slots. It resides in the front panel and connects to the rest of the system using an internal ribbon cable.

The LCD and LEDs are mounted on the processor board along with the front panel communication ports.

The memory on the main processor board is split into two categories: volatile and non-volatile. The volatile memory is fast access SRAM, used by the processor to run the software and store data during calculations. The non-volatile memory is sub-divided into two groups:

- Flash memory to store software code, text and configuration data including the present setting values.
- Supercapacitor-backed SRAM to store disturbance, event, fault and maintenance record data.

There are two board types available depending on the size of the case:

- For models in 40TE cases
- For models in 60TE cases and larger

3.6.4 POWER SUPPLY BOARD

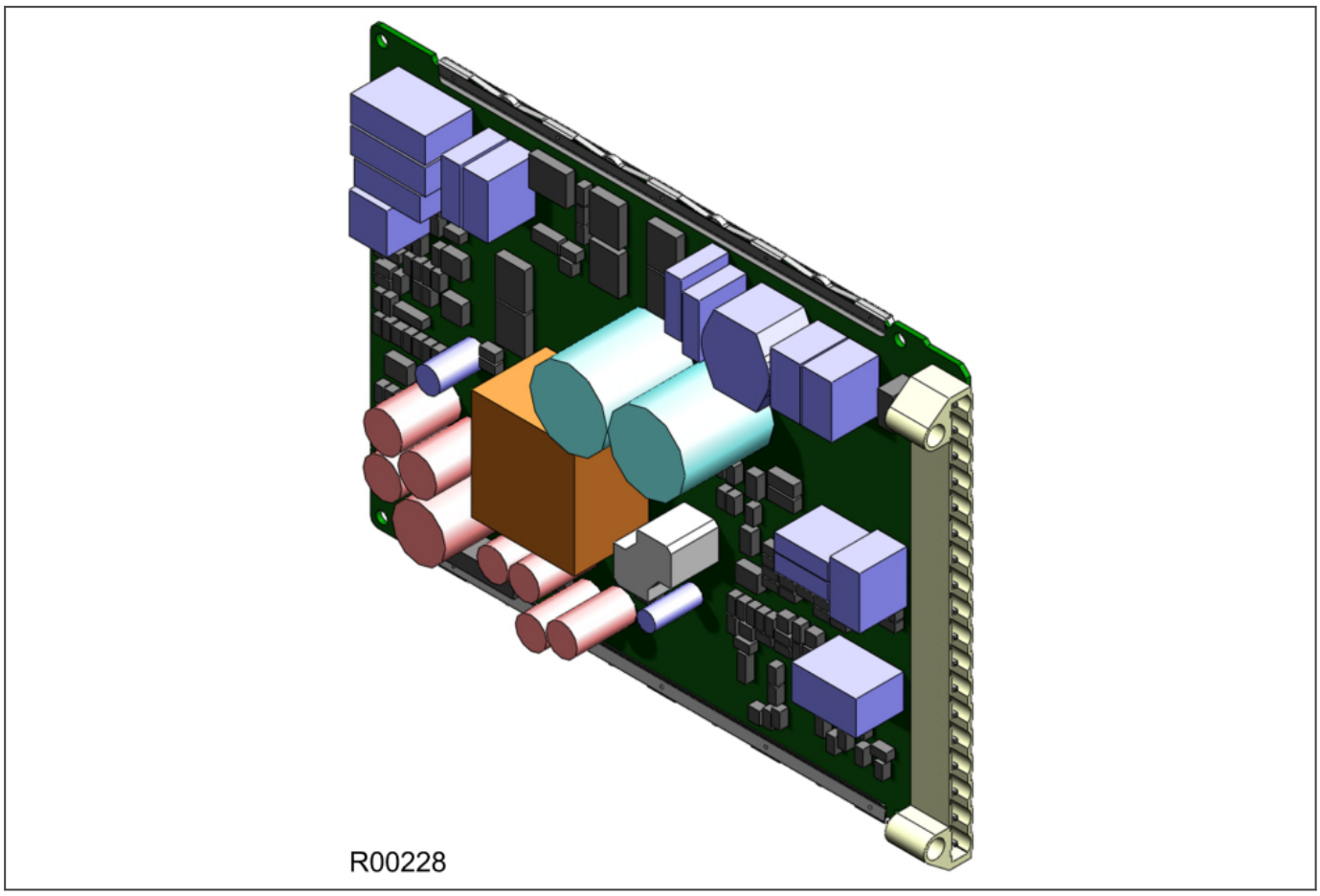


Figure 11: Power supply board

The power supply board provides power to the unit. One of three different configurations of the power supply board can be fitted to the unit. This is specified at the time of order and depends on the magnitude of the supply voltage that will be connected to it.

There are three board types, which support the following voltage ranges:

- 24/54 V DC
- 48/125 V DC or 40-100V AC
- 110/250 V DC or 100-240V AC

The power supply board connector plugs into a medium duty terminal block. This terminal block is always positioned on the right hand side of the unit looking from the rear.

The power supply board is usually assembled together with a relay output board to form a complete subassembly, as shown in the following diagram.

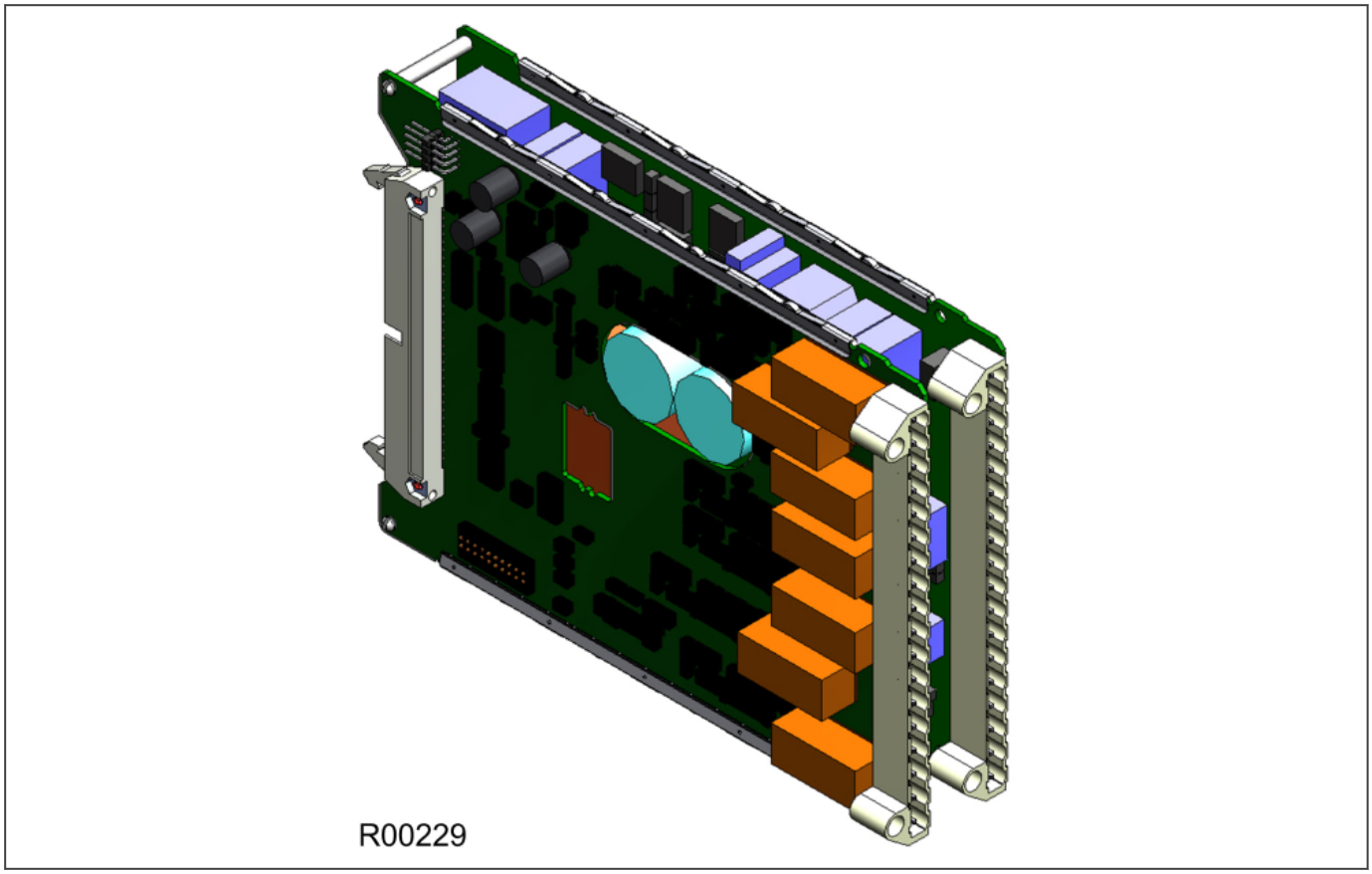


Figure 12: Power supply assembly

The power supply outputs are used to provide isolated power supply rails to the various modules within the unit. Three voltage levels are used by the unit's modules:

- 5.1 V for all of the digital circuits
- +/- 16 V for the analogue electronics such as on the input board
- 22 V for driving the output relay coils.

All power supply voltages, including the 0 V earth line, are distributed around the unit by the 64-way ribbon cable.

The power supply board incorporates inrush current limiting. This limits the peak inrush current to approximately 10 A.

Power is applied to pins 1 and 2 of the terminal block, where pin 1 is negative and pin 2 is positive. The pin numbers are clearly marked on the terminal block as shown in the following diagram.

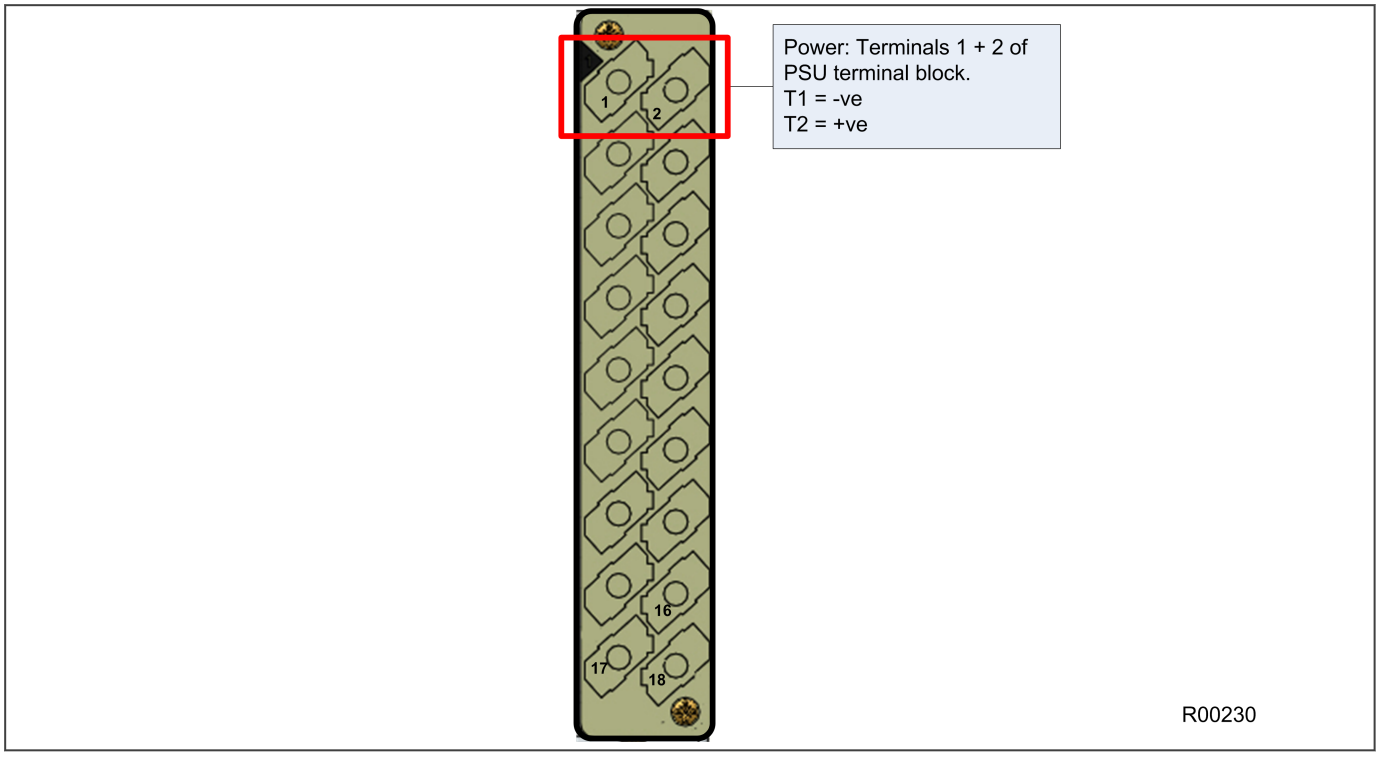


Figure 13: Power supply terminals

3.6.4.1 WATCHDOG

The Watchdog contacts are also hosted on the power supply board. The Watchdog facility provides two output relay contacts, one normally open and one normally closed. These are used to indicate the health of the device and are driven by the main processor board, which continually monitors the hardware and software when the device is in service.

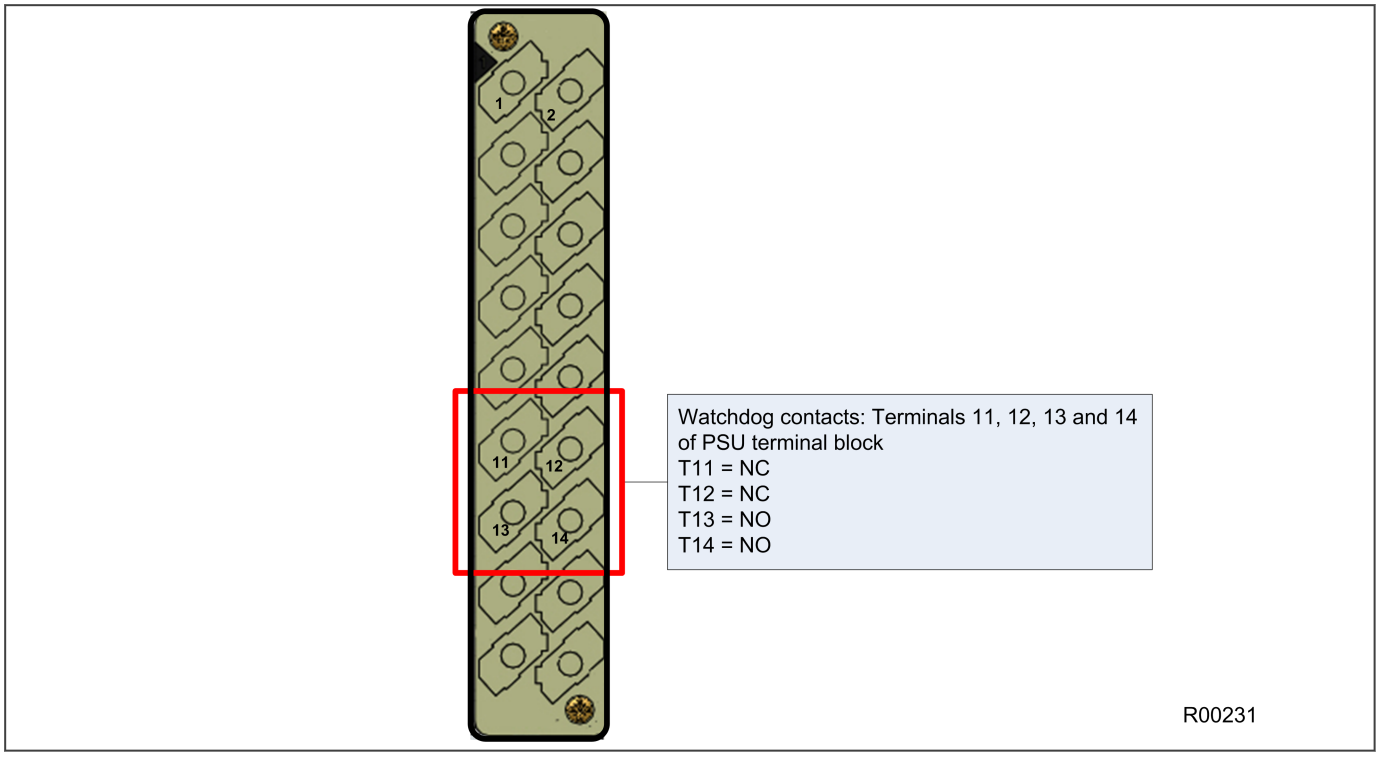


Figure 14: Watchdog contact terminals

3.6.4.2 REAR SERIAL PORT

The rear serial port (RP1) is housed on the power supply board. This is a three-terminal EIA(RS)485 serial communications port and is intended for use with a permanently wired connection to a remote control centre for SCADA communication. The interface supports half-duplex communication and provides optical isolation for the serial data being transmitted and received.

The physical connectivity is achieved using three screw terminals; two for the signal connection, and the third for the earth shield of the cable. These are located on pins 16, 17 and 18 of the power supply terminal block, which is on the far right looking from the rear. The interface can be selected between RS485 and K-bus. When the K-Bus option is selected, the two signal connections are not polarity conscious.

The polarity independent K-bus can only be used for the Courier data protocol. The polarity conscious MODBUS, IEC 60870-5-103 and DNP3.0 protocols need RS485.

The following diagram shows the rear serial port. The pin assignments are as follows:

- Pin 16: Earth shield
- Pin 17: Negative signal
- Pin 18: Positive signal

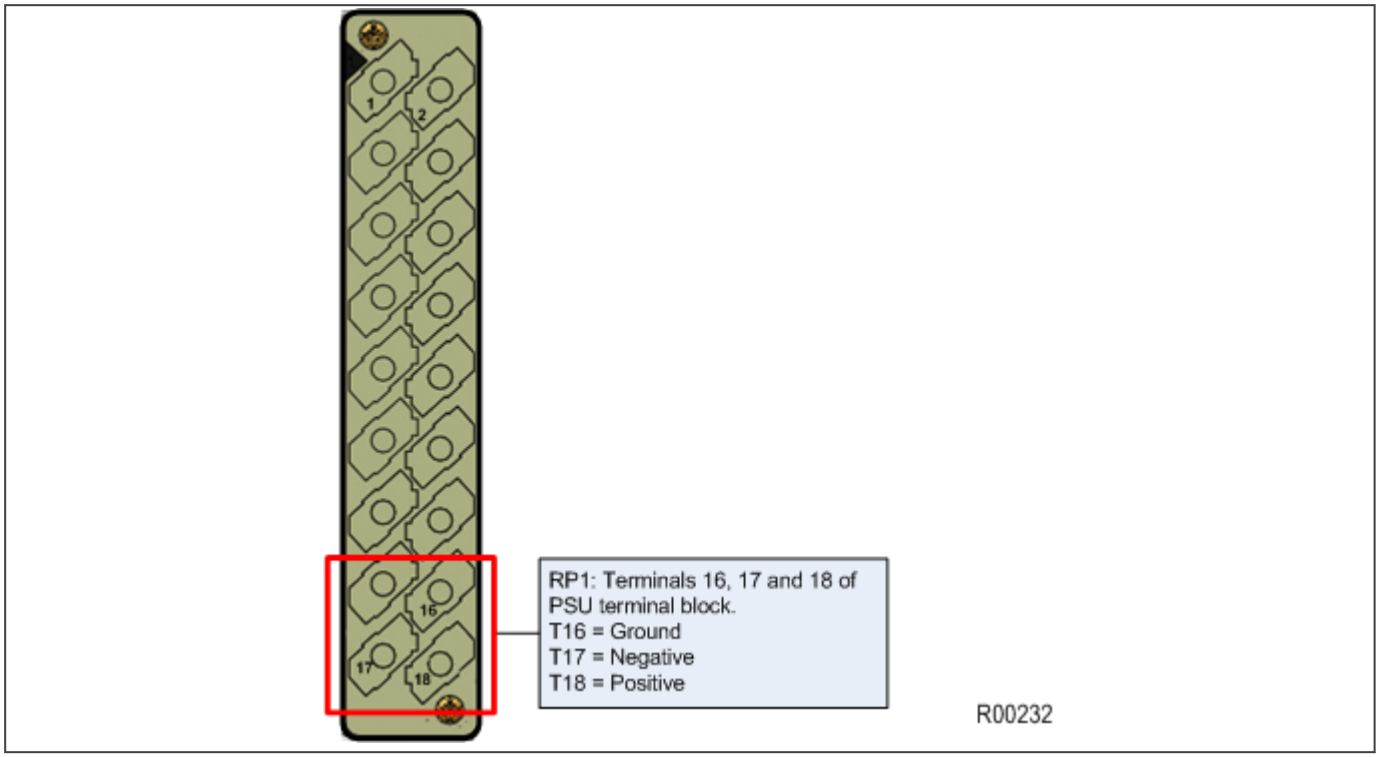


Figure 15: Rear serial port terminals

An additional serial port with D-type presentation is available as an optional board, if required.

3.6.5 INPUT MODULE - 1 TRANSFORMER BOARD

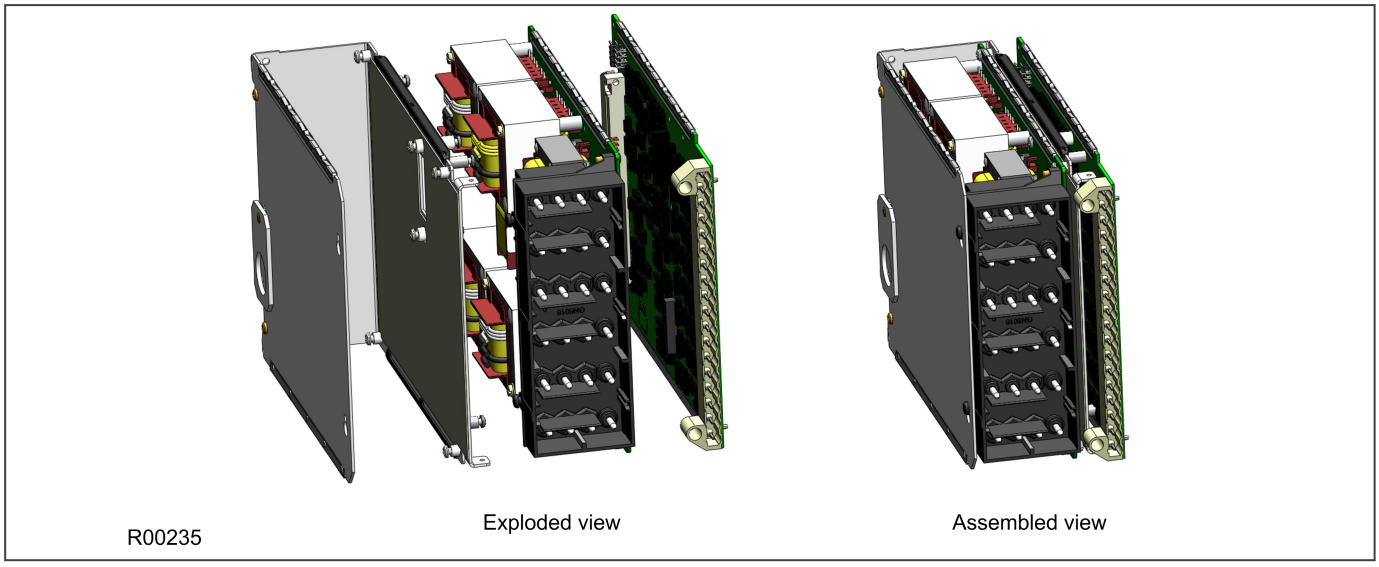


Figure 16: Input module - 1 transformer board

The input module consists of the main input board coupled together with an instrument transformer board. The instrument transformer board contains the voltage and current transformers, which isolate and scale the analogue input signals delivered by the system transformers. The input board contains the A/D conversion and digital processing circuitry, as well as eight digital isolated inputs (opto-inputs).

The boards are connected together physically and electrically. The module is encased in a metal housing for shielding against electromagnetic interference.

3.6.5.1 INPUT MODULE CIRCUIT DESCRIPTION

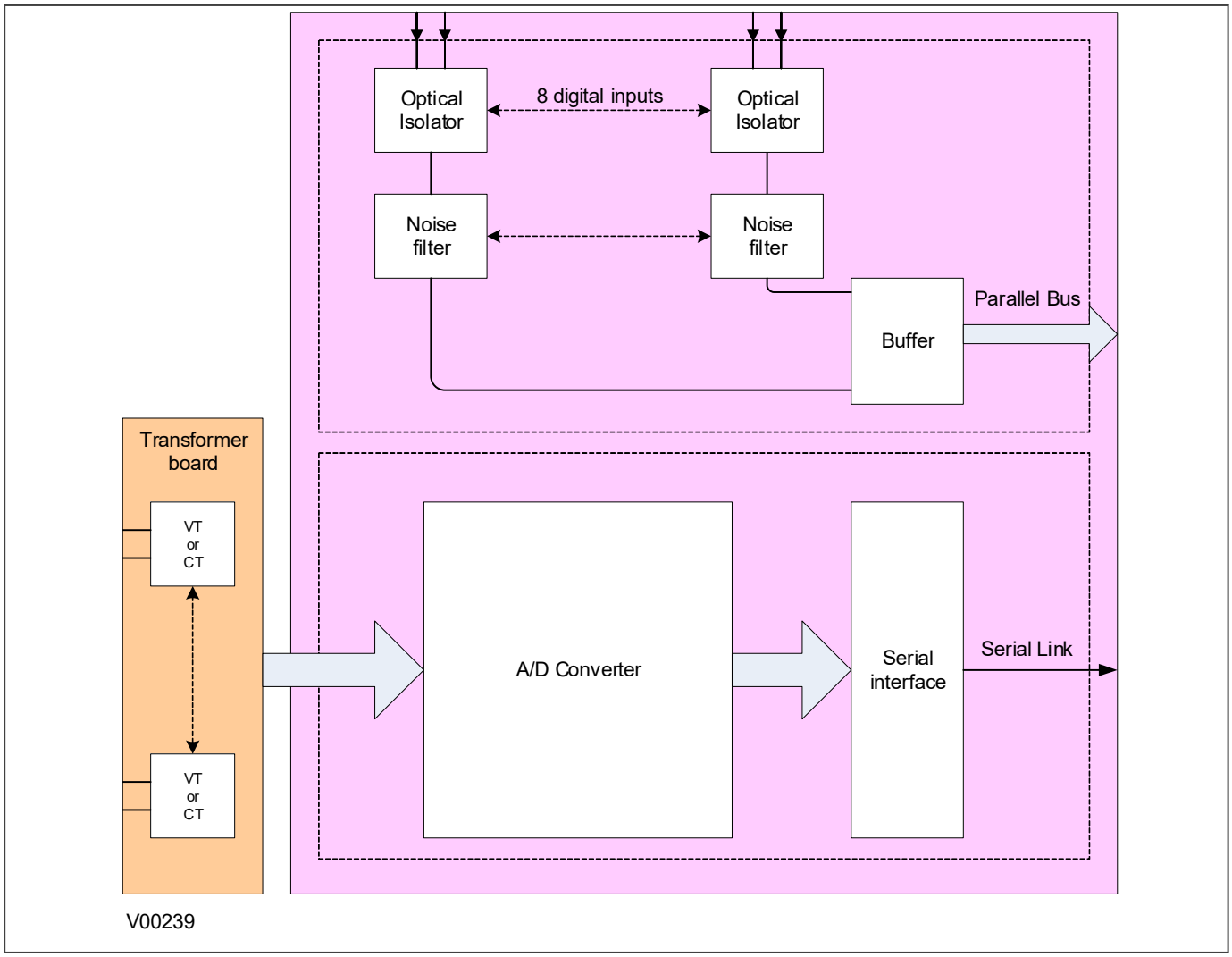


Figure 17: Input module schematic

A/D conversion

The differential analogue inputs from the CT and VT transformers are presented to the main input board as shown. Each differential input is first converted to a single input quantity referenced to the input board's earth potential. The analogue inputs are sampled and converted to digital, then filtered to remove unwanted properties. The samples are then passed through a serial interface module which outputs data on the serial sample data bus.

The calibration coefficients are stored in non-volatile memory. These are used by the processor board to correct for any amplitude or phase errors introduced by the transformers and analogue circuitry.

Opto-isolated inputs

The other function of the input board is to read in the state of the digital inputs. As with the analogue inputs, the digital inputs must be electrically isolated from the power system. This is achieved by means of the 8 on-board optical isolators for connection of up to 8 digital signals. The digital signals are passed through an optional noise filter before being buffered and presented to the unit's processing boards in the form of a parallel data bus.

This selectable filtering allows the use of a pre-set filter of ½ cycle which renders the input immune to induced power-system noise on the wiring. Although this method is secure it can be slow, particularly for inter-tripping. This

can be improved by switching off the ½ cycle filter, in which case one of the following methods to reduce ac noise should be considered.

- Use double pole switching on the input
- Use screened twisted cable on the input circuit

The opto-isolated logic inputs can be configured for the nominal battery voltage of the circuit for which they are a part, allowing different voltages for different circuits such as signalling and tripping.

Note:
The opto-input circuitry can be provided without the A/D circuitry as a separate board, which can provide supplementary opto-inputs.

3.6.5.2 INPUT BOARD

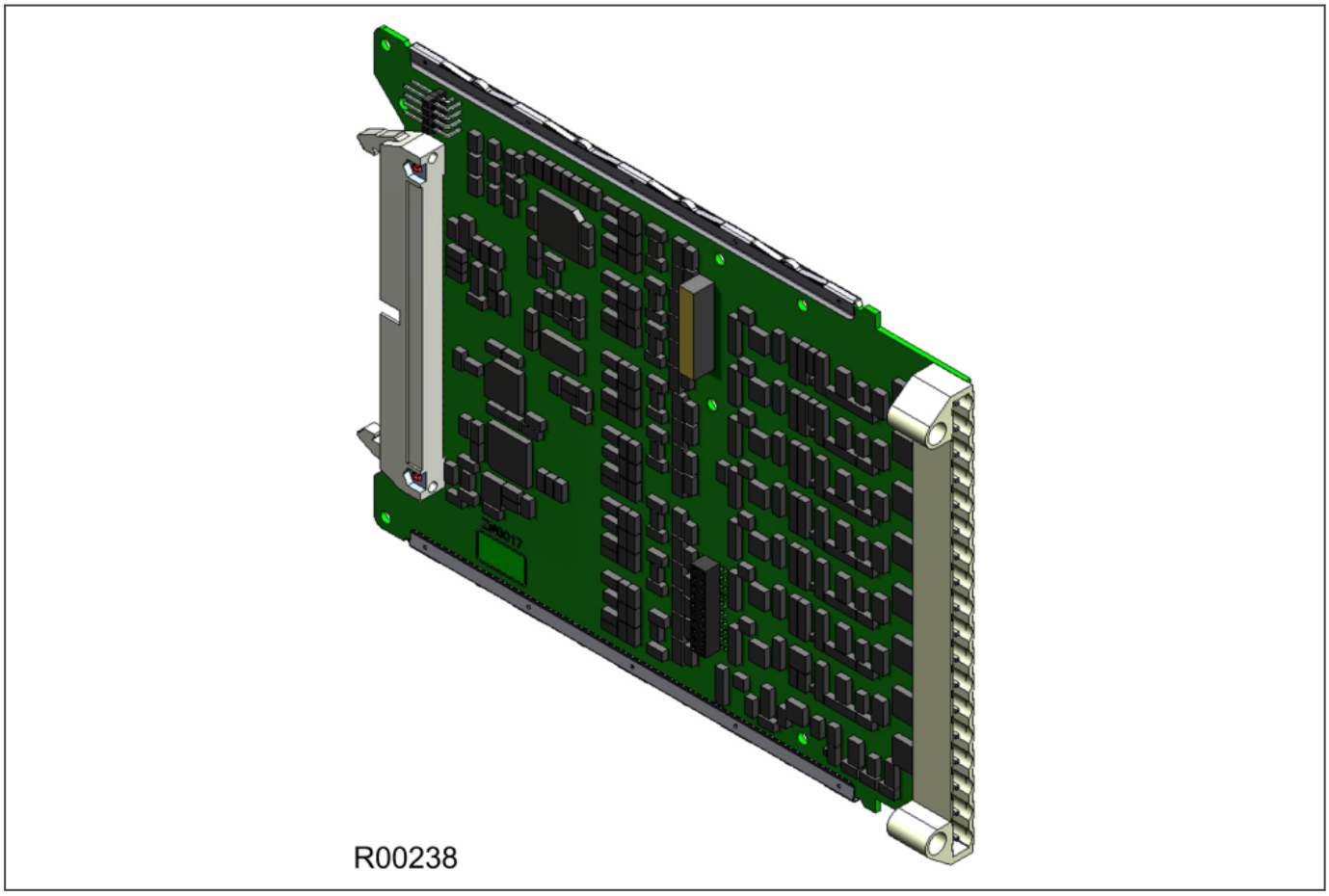


Figure 18: Input board

The input board is used to convert the analogue signals delivered by the current and voltage transformers into digital quantities used by the IED. This input board also has on-board opto-input circuitry, providing eight optically-isolated digital inputs and associated noise filtering and buffering. These opto-inputs are presented to the user by means of an MD terminal block, which sits adjacent to the analogue inputs HD terminal block.

The input board is connected physically and electrically to the transformer board to form a complete input module.

The terminal numbers of the opto-inputs are as follows:

Terminal Number	Opto-input
Terminal 1	Opto 1 -ve
Terminal 2	Opto 1 +ve
Terminal 3	Opto 2 -ve
Terminal 4	Opto 2 +ve
Terminal 5	Opto 3 -ve
Terminal 6	Opto 3 +ve
Terminal 7	Opto 4 -ve
Terminal 8	Opto 4 +ve
Terminal 9	Opto 5 -ve
Terminal 10	Opto 5 +ve
Terminal 11	Opto 6 -ve
Terminal 12	Opto 6 +ve
Terminal 13	Opto 7 –ve
Terminal 14	Opto 7 +ve
Terminal 15	Opto 8 –ve
Terminal 16	Opto 8 +ve
Terminal 17	Common
Terminal 18	Common

3.6.6 STANDARD OUTPUT RELAY BOARD

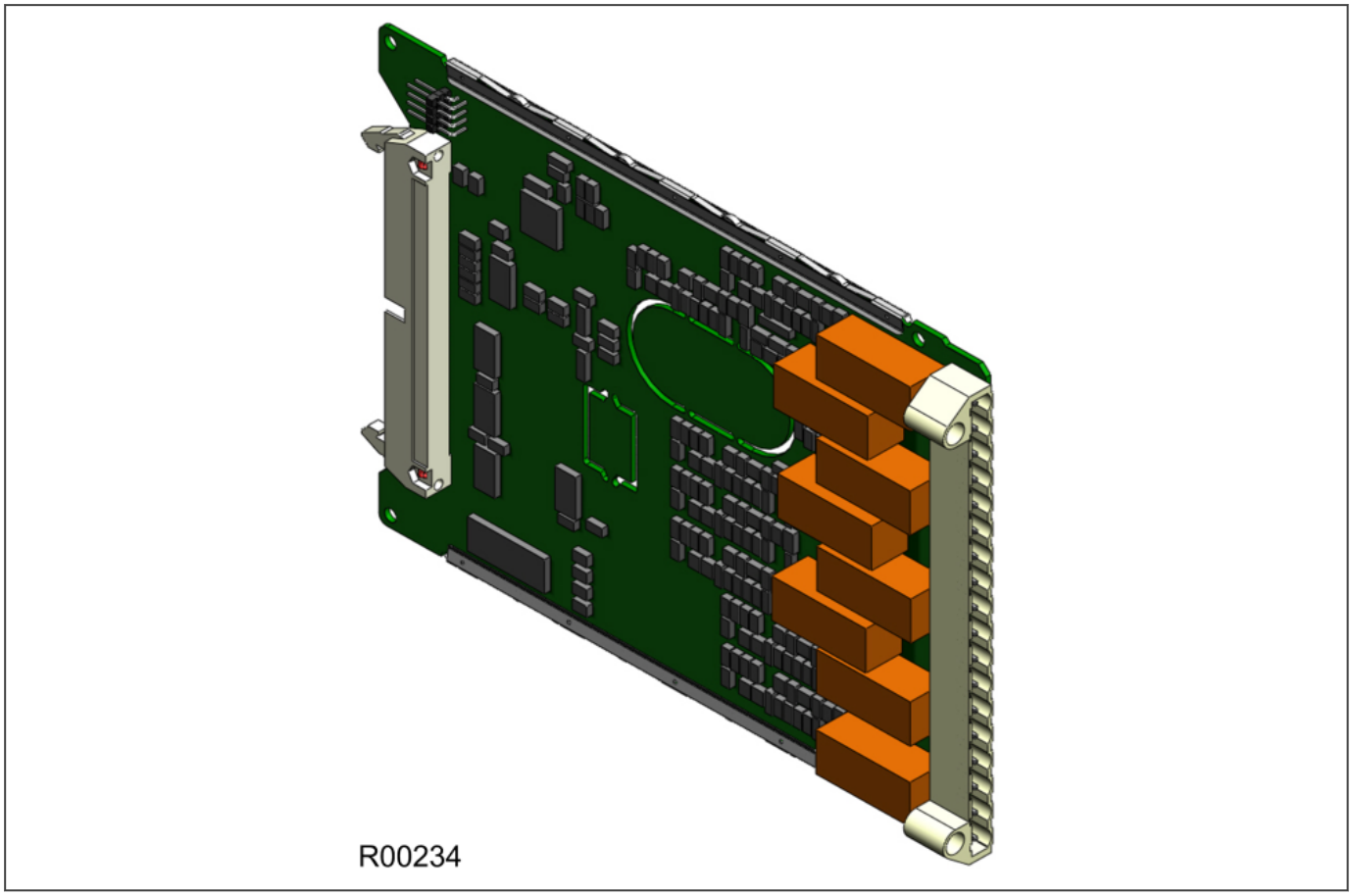


Figure 19: Standard relay output board - 8 contacts

This output relay board has 8 relays with 6 Normally Open contacts and 2 Changeover contacts.

The output relay board is provided together with the power supply board as a complete assembly, or independently for the purposes of relay output expansion.

There are two cut-out locations in the board. These can be removed to allow power supply components to protrude when coupling the output relay board to the power supply board. If the output relay board is to be used independently, these cut-out locations remain intact.

The terminal numbers are as follows:

Terminal Number	Output Relay
Terminal 1	Relay 1 NO
Terminal 2	Relay 1 NO
Terminal 3	Relay 2 NO
Terminal 4	Relay 2 NO
Terminal 5	Relay 3 NO
Terminal 6	Relay 3 NO
Terminal 7	Relay 4 NO
Terminal 8	Relay 4 NO

Terminal Number	Output Relay
Terminal 9	Relay 5 NO
Terminal 10	Relay 5 NO
Terminal 11	Relay 6 NO
Terminal 12	Relay 6 NO
Terminal 13	Relay 7 changeover
Terminal 14	Relay 7 changeover
Terminal 15	Relay 7 common
Terminal 16	Relay 8 changeover
Terminal 17	Relay 8 changeover
Terminal 18	Relay 8 common

3.6.7 IRIG-B BOARD

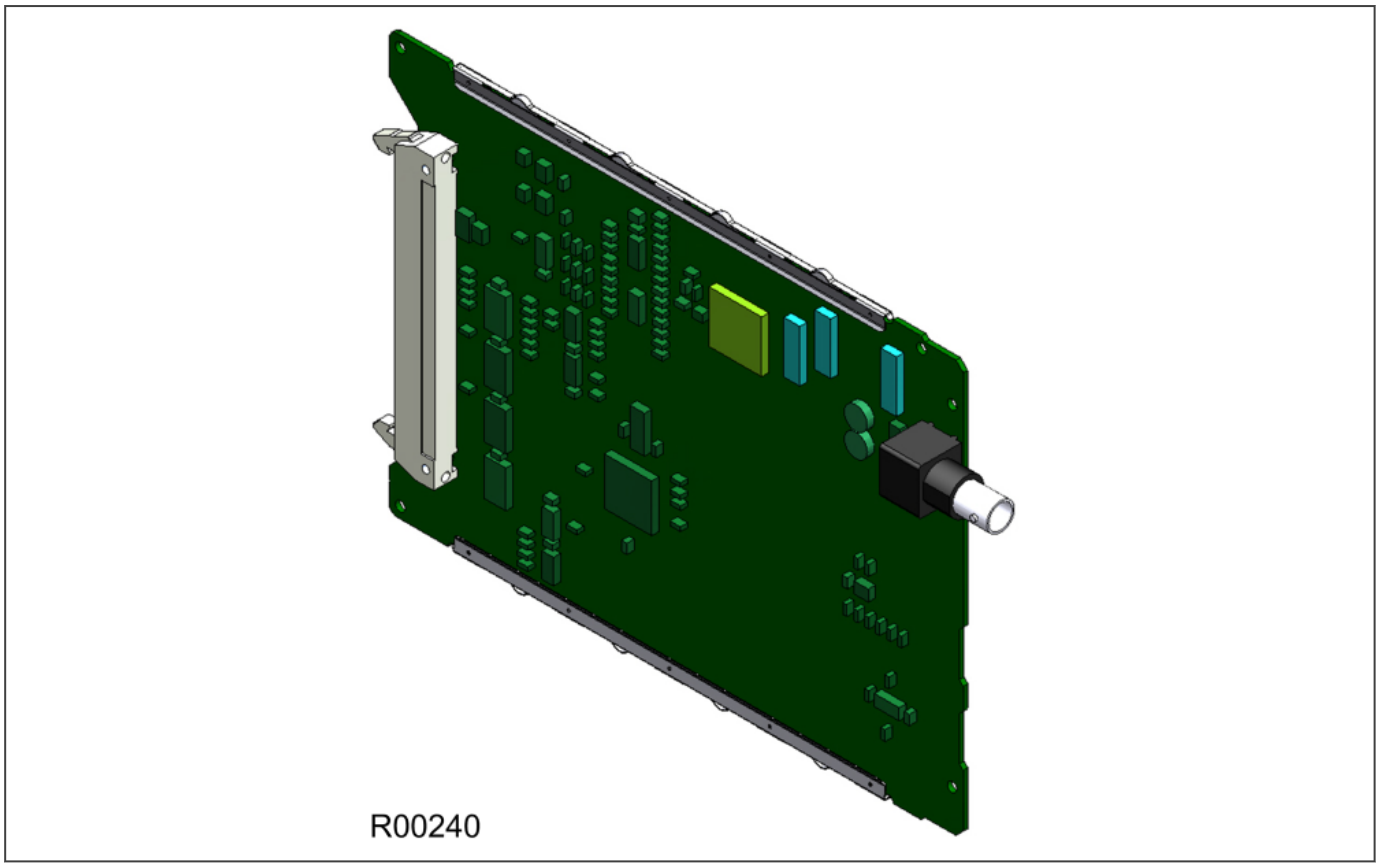


Figure 20: IRIG-B board

The IRIG-B board can be fitted to provide an accurate timing reference for the device. The IRIG-B signal is connected to the board via an BNC connector. The timing information is used to synchronise the IED's internal real-time clock to an accuracy of 1 ms. The internal clock is then used for time tagging events, fault, maintenance and disturbance records.

IRIG-B interface is available in modulated or demodulated formats.

The IRIG-B facility is provided in combination with other functionality on a number of additional boards, such as:

- Fibre board with IRIG-B
- Second rear communications board with IRIG-B
- Ethernet board with IRIG-B
- Redundant Ethernet board with IRIG-B

There are three types of each of these boards; one type which accepts a modulated IRIG-B input, one type which accepts a demodulated IRIG-B input and one type which accepts a universal IRIG-B input. The order code will indicate which variant it supports.

3.6.8 FIBRE OPTIC BOARD

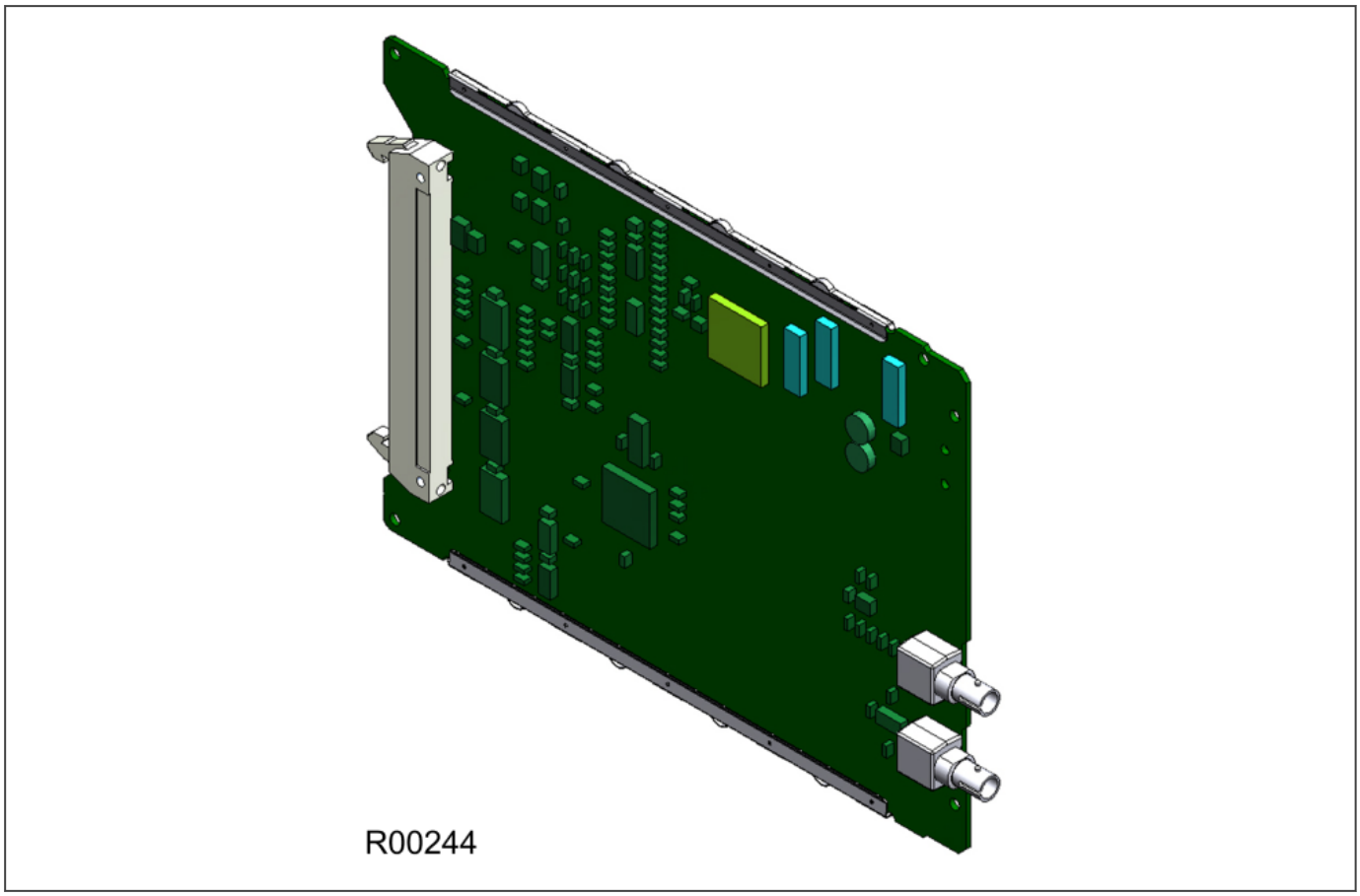


Figure 21: Fibre optic board

This board provides an interface for communicating with a master station. This communication link can use all compatible protocols (Courier, IEC 60870-5-103, MODBUS and DNP 3.0). It is a fibre-optic alternative to the metallic RS485 port presented on the power supply terminal block. The metallic and fibre optic ports are mutually exclusive.

The fibre optic port uses BFOC 2.5 ST connectors.

The board comes in two varieties; one with an IRIG-B input and one without:

3.6.9 REAR COMMUNICATION BOARD

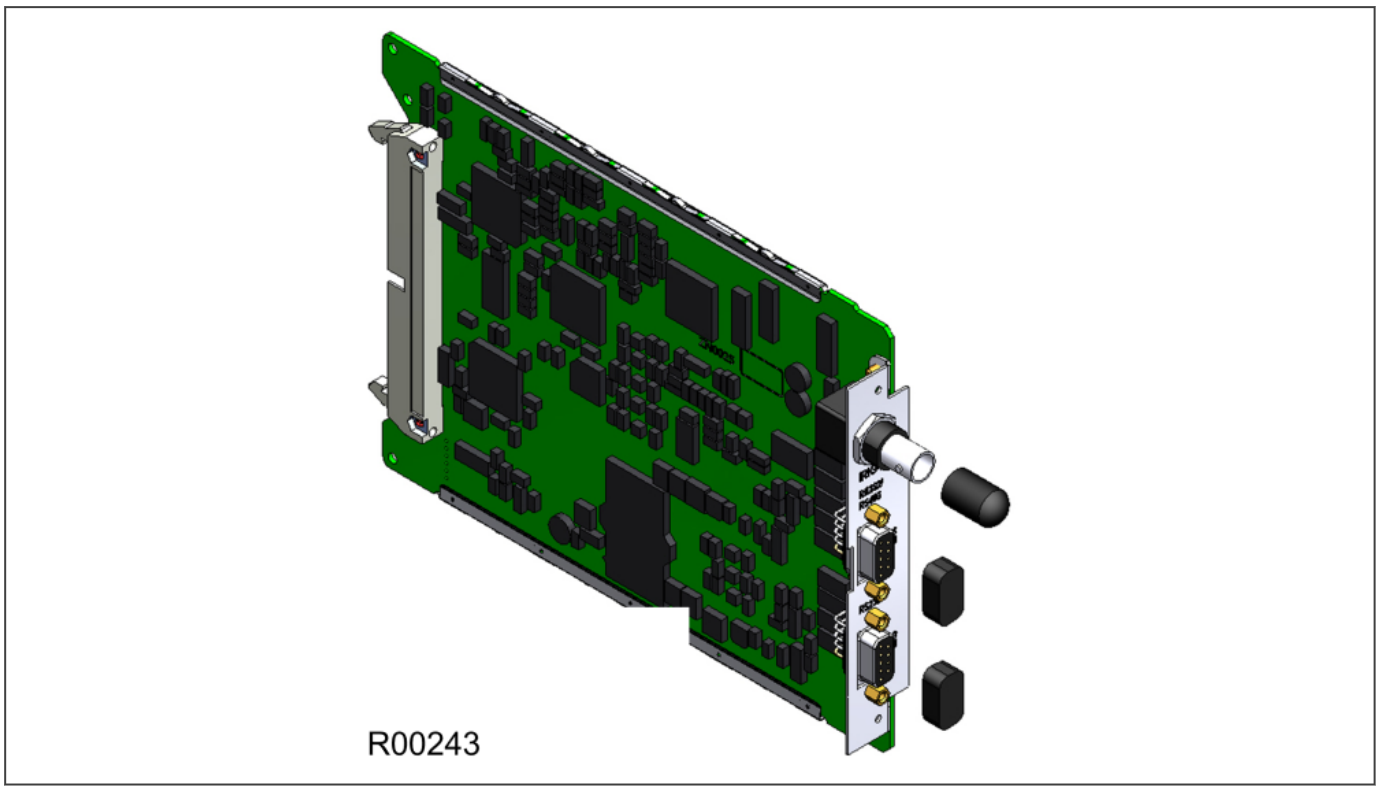


Figure 22: Rear communication board

The optional communications board containing the secondary communication ports provide two serial interfaces presented on 9 pin D-type connectors. These interfaces are known as SK4 and SK5. Both connectors are female connectors, but are configured as DTE ports. This means pin 2 is used to transmit information and pin 3 to receive.

SK4 can be used with RS232, RS485 and K-bus. SK5 can only be used with RS232 and is used for electrical teleprotection. The optional rear communications board and IRIG-B board are mutually exclusive since they use the same hardware slot. However, the board comes in two varieties; one with an IRIG-B input and one without.

3.6.10 REDUNDANT ETHERNET BOARD (HARDWARE OPTION R/S/T)

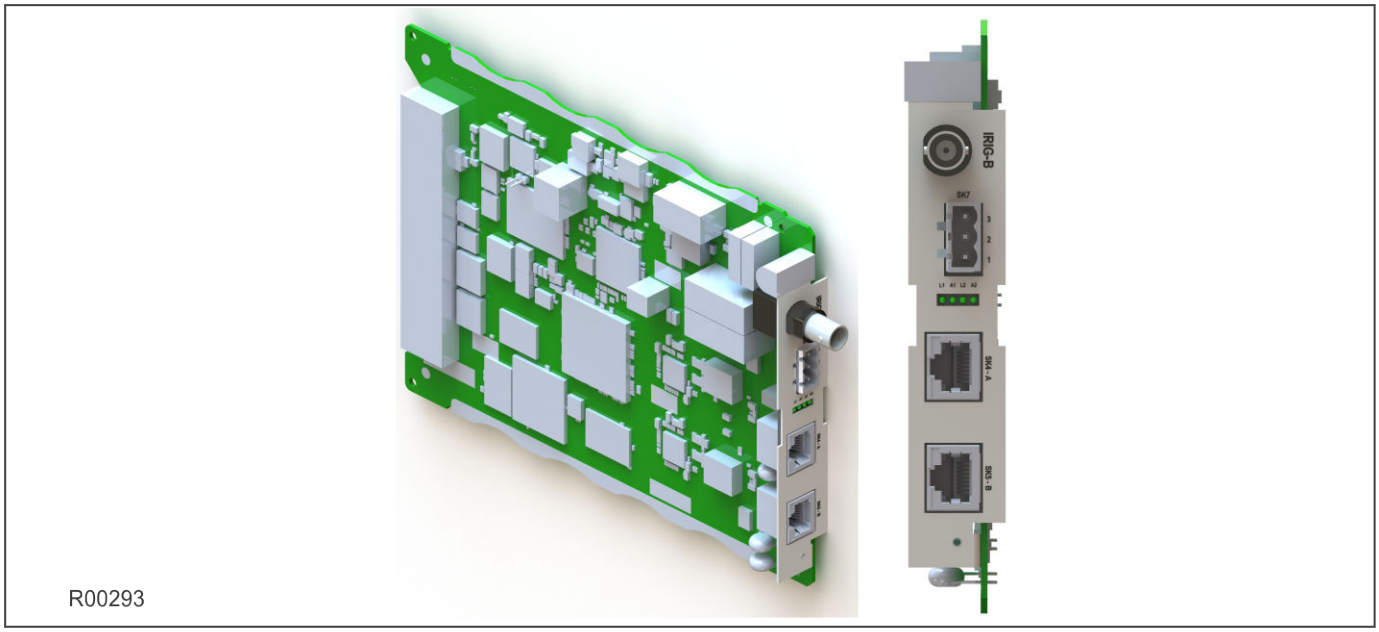


Figure 23: Redundant Ethernet board

This board provides dual redundant Ethernet together with an IRIG-B interface for timing.

Different board variants are available, depending on the redundancy protocol and the type of IRIG-B signal (unmodulated and modulated). The available redundancy protocols are:

- RSTP (Rapid Spanning Tree Protocol)
- PRP (Parallel Redundancy Protocol)
- HSR (High-availability Seamless Redundancy)
- Failover

There are several variants for this board as follows:

- 100 Mbps redundant Ethernet running RSTP + PRP + HSR + Failover (two fibre pairs), with on-board universal IRIG-B
- 100 Mbps redundant Ethernet running RSTP + PRP + HSR + Failover (two copper pairs), with on-board universal IRIG-B
- 100 Mbps redundant Ethernet running RSTP + PRP + HSR + Failover (one copper, one multi-mode fibre), with on-board universal IRIG-B

The Ethernet and other connection details are described below:

IRIG-B Connector

- Centre connection: Signal
- Outer connection: Earth

Link Fail Connector (Ethernet Board Watchdog Relay)

Pin	Closed	Open
1-2	Link fail Channel 1 (A)	Link ok Channel 1 (A)
2-3	Link fail Channel 2 (B)	Link ok Channel 2 (B)

LEDs

LED	Function	On	Off	Flashing
Green	Link	Link ok	Link broken	
Yellow	Activity	Running		PRP, RSTP traffic

Optical Fibre Connectors (ST)

Connector	RSTP	PRP	HSR
A	RX1	RXA	RXA
B	TX1	TXA	TXA
C	RX2	RXB	RXB
D	TX2	TXB	TXB

RJ45 Connector

Pin	Signal Name	Signal Definition
1	TXP	Transmit (positive)
2	TXN	Transmit (negative)
3	RXP	Receive (positive)
4	-	Not used
5	-	Not used
6	RXN	Receive (negative)
7	-	Not used
8	-	Not used

3.6.11 SINGLE ETHERNET BOARD (HARDWARE OPTION U)

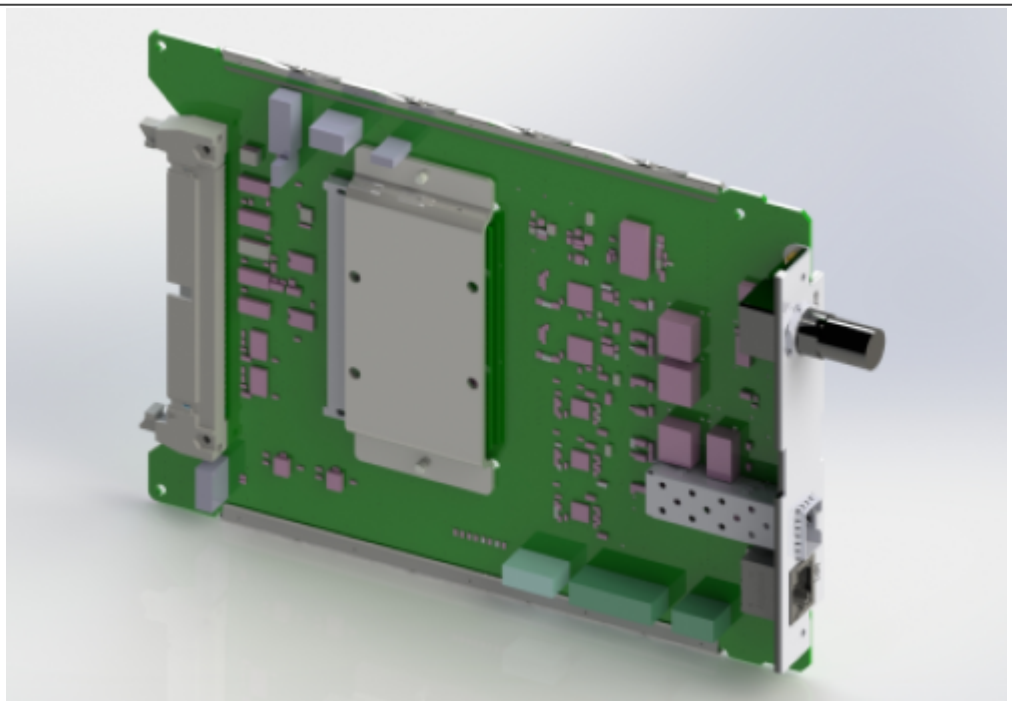




Figure 24: Ethernet board

This board provides one optical 100Mbps LC duplex Ethernet port (NP2A) for station bus communications, with a universal IRIG-B interface for time synchronisation. The NP1 Ethernet port is not active.

The Ethernet and other connection details are described below:

UNIVERSAL IRIG-B Connector

- Centre connection: Signal
- Outer connection: Earth

LC Optical Fibre Connector (NP2A only)

Connector	SFP
A	TX
B	RX

3.6.12 REDUNDANT ETHERNET BOARD (HARDWARE OPTION W/Y)

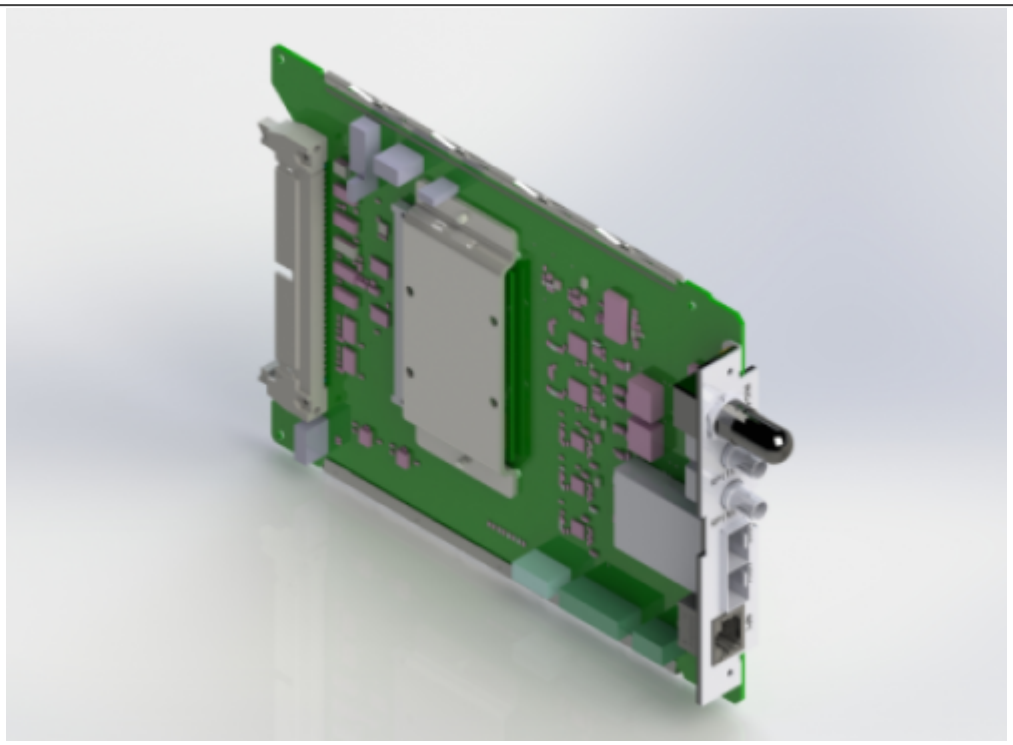




Figure 25: Redundant Ethernet board

This board provides dual redundant Ethernet (NP2A and NP2B) for station bus communications, with a universal IRIG-B interface for time synchronisation. The NP1 Ethernet port is not active.

The available redundancy protocols are:

- RSTP (Rapid Spanning Tree Protocol)
- PRP (Parallel Redundancy Protocol)
- HSR (High-availability Seamless Redundancy)
- Failover

There are several variants for this board as follows:

Two RJ45 duplex redundant 10/100Mbps Ethernet ports running RSTP + PRP + HSR + Failover, with on-board universal IRIG-B.

Two LC duplex redundant 100Mbps Ethernet ports running RSTP + PRP + HSR + Failover, with on-board universal IRIG-B.

The Ethernet and other connection details are described below:

UNIVERSAL IRIG-B Connector

- Centre connection: Signal
- Outer connection: Earth

LC Optical Fibre Connector (only for NP2A or NP2B when ordering fibre ports on station bus ports)

Connector	SFP
A	TX
B	RX

RJ45 Connector (NP1 or NP2A/NP2B when ordering two copper ports on station bus ports only)

Pin	Signal Name	Signal Definition
1	TXP	Transmit (positive)
2	TXN	Transmit (negative)
3	RXP	Receive (positive)
4	-	Not used
5	-	Not used
6	RXN	Receive (negative)
7	-	Not used
8	-	Not used

3.6.13 RETROFIT OF ETHERNET CARDS HARDWARE OPTION R/S/T WITH HARDWARE OPTION U/W/Y

Some Px4x relays with 9x software will continue to support Ethernet boards with CORTEC Hardware options R/S/T, and also a newer version of the Ethernet board with Hardware option U/W/Y. The following information will help customers who want to retrofit existing installations using the new U/W/Y boards.

General considerations:

- The model number of the IED will change to accommodate the new Ethernet board options U/W/Y if replacing any of the R/S/T Ethernet board options.
- Software 9x requires a new minor software upgrade to support the new Ethernet board options U/W/Y. The same minor software release will support both U/W/Y and R/S/T. Customers ordering 9x software without an Ethernet board option, won't need the upgrade.
- S1 Agile can convert settings and PSL files from hardware with the old R/S/T board to the new U/W/Y Ethernet board options for 9x software.

Hardware review:

- Ethernet card R is a redundant Ethernet station bus card with 2 fibre optic ports with ST connectors. This card can be replaced with the new redundant Ethernet card Y which has 2 LC connectors.
    - **Impact:** The connectors are now LC, so the entire fibre needs to be replaced with a compatible one for the new connector, or an adaptor and a new small patchcord with the new connector.
- Ethernet card S is a redundant Ethernet station bus card with 2 RJ45 copper ports. This card can be replaced with the new redundant Ethernet card W which has 2 RJ45 copper ports.
    - **Impact:** No impact on port connections.
- Ethernet card T is a redundant Ethernet station bus card with a multi-mode fibre optic (ST) port and a copper RJ45 port. There is no like for like card in the new variant. If redundancy is not being used, the U Ethernet card provides a single multi-mode fibre optic (LC) port. If a single RJ45 copper Ethernet port is required Ethernet card W can be used in Failover mode. If redundancy is needed, either a variant W or a variant Y can be used depending on whether two copper or two fibre ports can be accommodated.
    - **Impact:** The impact depends on the application and the availability of fibre connectors. The new cards provide a solution for different applications except when a copper and fibre pairing in redundant mode are required.

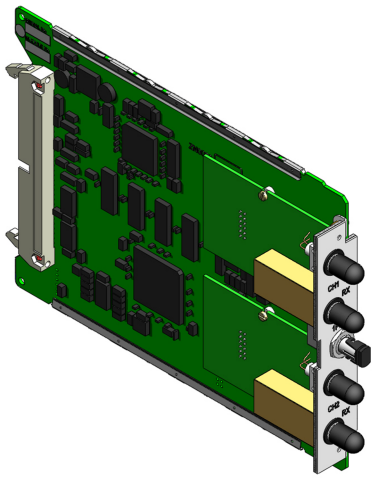
Link Status monitoring:

- Ethernet cards R/S/T have a link status contact (watchdog) and LED. Ethernet cards U/W/Y have no physical contact for the link status because this functionality is fully embedded into the main processor.
    - **Impact:** There are two independent link status contacts (watchdog) in the R/S/T cards, one for each channel.
    - In the 9x software supporting the new U/W/Y Ethernet boards and older R/S/T boards, there is a new IEC 61850 logical node (LCCH) to monitor the 2 redundant channels' link status, with two data attributes (DA), one for each channel, which can be used by the SCADA for monitoring.
    - In the 91_I software supporting the new U/W/Y Ethernet boards there is a new IEC 61850 logical node (LCCH) to monitor the 2 redundant channels' link status, with two data attributes (DA), one for each channel, which can be used by the SCADA for monitoring.
    - There also are 2 new link status DDBs in the PSL. NP2A port status and NP2B port status. NP2A is the LAN A channel, NP2B is the LAN B channel. The DDBs can be connected in the PSL as required, for example they can be linked to LEDs for visual indication or output contacts for connection to RTU (similar to how the fixed contacts worked in the R/S/T cards).
    - A NIC Link Fail DDB is also available for U/W/Y Ethernet boards. This DDB monitors the overall status of the Ethernet communications and is triggered if both channels are disconnected.

S1 Agile tools and configuration files:

- **S1 Agile:** A new version of S1 Agile, 3.2.0, is available to support the new hardware options U/W/Y. Configuration of the U/W/Y Ethernet ports can be done using the IED Configurator tool of S1 Agile compared to the configuration of the R/S/T Ethernet ports via the Redundant Ethernet Configurator tool of S1 Agile.
- **MCL Files:** The MCL template has changed to version 5.1 for the U/W/Y Ethernet ports. Should a user want to reuse an existing MCL file, version 5.0 (R/S/T options), they need to reload the new ICD template using the IED Configurator tool.
- **PSL Files:** A new default PSL file is available for the new software release which include the 2 new DDBs described above. For users with previous R/S/T PSL files, they can be converted to include the 2 new DDBs, using the PSL conversion tool in S1 Agile for software version 9x only. New PSL files for the U/W/Y Ethernet hardware options are provided via the Data Model Manager.
- **ICD Files:** A new ICD file to support the new software release is provided via the Data Model Manager.

3.6.14 COPROCESSOR BOARD



R00248

Figure 26: Fully populated Coprocessor board

Note:
The above figure shows a coprocessor complete with GPS input and 2 fibre-optic serial data interfaces, and is not necessarily representative of the product and model described in this manual. These interfaces will not be present on boards that do not require them.

Where applicable, a second processor board is used to process the special algorithms associated with the device. This second processor board provides fast access (zero wait state) SRAM for use with both program and data memory storage. This memory can be accessed by the main processor board via the parallel bus. This is how the software is transferred from the flash memory on the main processor board to the coprocessor board on power up. Further communication between the two processor boards is achieved via interrupts and the shared SRAM. The serial bus carrying the sample data is also connected to the co-processor board, using the processor's built-in serial port, as on the main processor board.

There are several different variants of this board, which can be chosen depending on the exact device and model. The variants are:

- Coprocessor board with current differential inputs and GPS input
- Coprocessor board with current differential inputs only
- Coprocessor board with GPS input only

3.6.14.1 CURRENT DIFFERENTIAL INPUTS

Where applicable, the coprocessor board can be equipped with up to two daughter boards, each containing a fibre-optic interface for a serial data link. BFOC 2.5 ST connectors are used for this purpose. One or two channels are provided, each channel comprising a fibre pair for transmitting and receiving (Rx Tx). These channels are labelled Ch1 and Ch2. These serial data links are used to transfer information between two or three IEDs for current differential applications.

3.6.14.2 COPROCESSOR BOARD WITH 1PPS INPUT

In some applications, where the communication links between two remote devices are provided by a third party telecommunications partner, the transmit and receive paths associated with one channel may differ considerably in length, resulting in very different transmission and receive times.

If, for example, Device A is transmitting to Device B information about the value of its measured current, the information Device A is receiving from Device B about the current measured at the same time, may reach device B at a different time. This has to be compensated for. A 1pps GPS timing signal applied to both devices will help the IEDs achieve this, because it is possible to measure the exact time taken for both transmission and receive paths.

Note:
The 1 pps signal is always supplied by a GPS receiver (such as a RT430).

Note:
This signal is used to control the sampling process, and timing calculations and is not used for time stamping or real time synchronisation.

CHAPTER 4

SOFTWARE DESIGN

4.1 CHAPTER OVERVIEW

This chapter describes the software design of the IED.

This chapter contains the following sections:

Chapter Overview 58
Software Design Overview 59
System Level Software 60
Platform Software 63
Protection and Control Functions 64

4.2 SOFTWARE DESIGN OVERVIEW

The device software can be conceptually categorised into several elements as follows:

- The system level software
- The platform software
- The protection and control software

These elements are not distinguishable to the user, and the distinction is made purely for the purposes of explanation. The following figure shows the software architecture.

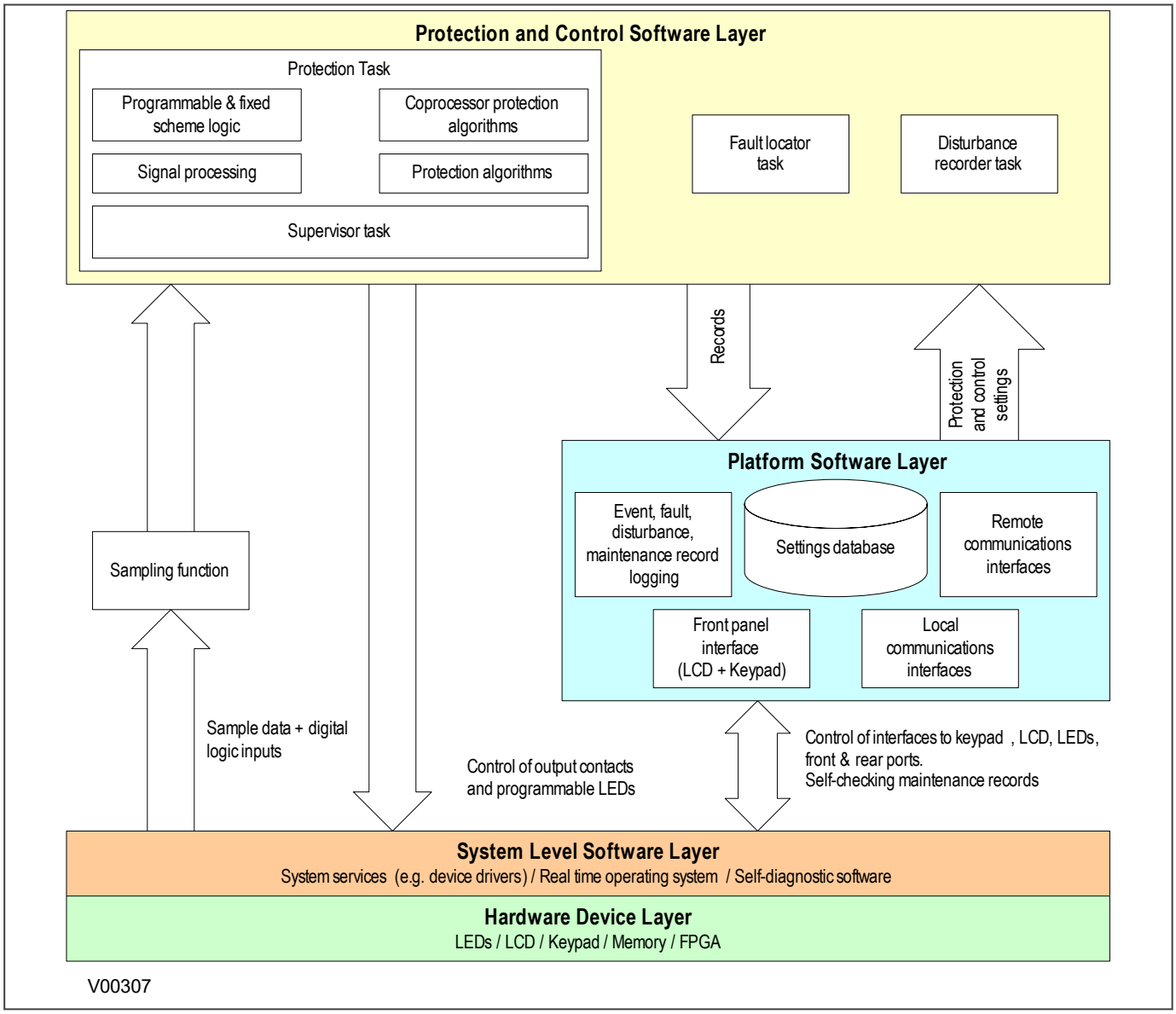


Figure 27: Software architecture

The software, which executes on the main processor, can be divided into a number of functions as illustrated above. Each function is further broken down into a number of separate tasks. These tasks are then run according to a scheduler. They are run at either a fixed rate or they are event driven. The tasks communicate with each other as and when required.

4.3 SYSTEM LEVEL SOFTWARE

4.3.1 REAL TIME OPERATING SYSTEM

The real-time operating system is used to schedule the processing of the various tasks. This ensures that they are processed in the time available and in the desired order of priority. The operating system also plays a part in controlling the communication between the software tasks, through the use of operating system messages.

4.3.2 SYSTEM SERVICES SOFTWARE

The system services software provides the layer between the hardware and the higher-level functionality of the platform software and the protection and control software. For example, the system services software provides drivers for items such as the LCD display, the keypad and the remote communication ports. It also controls things like the booting of the processor and the downloading of the processor code into DRAM at startup.

4.3.3 SELF-DIAGNOSTIC SOFTWARE

The device includes several self-monitoring functions to check the operation of its hardware and software while in service. If there is a problem with the hardware or software, it should be able to detect and report the problem, and attempt to resolve the problem by performing a reboot. In this case, the device would be out of service for a short time, during which the ‘Healthy’ LED on the front of the device is switched OFF and the watchdog contact at the rear is ON. If the restart fails to resolve the problem, the unit takes itself permanently out of service; the ‘Healthy’ LED stays OFF and watchdog contact stays ON.

If a problem is detected by the self-monitoring functions, the device attempts to store a maintenance record to allow the nature of the problem to be communicated to the user.

The self-monitoring is implemented in two stages: firstly a thorough diagnostic check which is performed on boot-up, and secondly a continuous self-checking operation, which checks the operation of the critical functions whilst it is in service.

4.3.4 STARTUP SELF-TESTING

The self-testing takes a few seconds to complete, during which time the IEDs measurement, recording, control, and protection functions are unavailable. On a successful start-up and self-test, the ‘Healthy' state LED on the front of the device is switched on. If a problem is detected during the start-up testing, the device remains out of service until it is manually restored to working order.

The operations that are performed at start-up are:

1. System boot
2. System software initialisation
3. Platform software initialisation and monitoring

4.3.4.1 SYSTEM BOOT

The integrity of the Flash memory is verified using a checksum before the program code and stored data is loaded into RAM for execution by the processor. When the loading has been completed, the data held in RAM is compared to that held in the Flash memory to ensure that no errors have occurred in the data transfer and that the two are the same. The entry point of the software code in RAM is then called. This is the IEDs initialisation code.

4.3.4.2 SYSTEM LEVEL SOFTWARE INITIALISATION

The initialisation process initialises the processor registers and interrupts, starts the watchdog timers (used by the hardware to determine whether the software is still running), starts the real-time operating system and creates and starts the supervisor task. In the initialisation process the device checks the following:

- The status of the supercapacitor to maintain the real time clock
- The operation of the LCD controller
- The watchdog operation

At the conclusion of the initialisation software the supervisor task begins the process of starting the platform software.

4.3.4.3 CO-PROCESSOR INITIALISATION

This product features a co-processor board which hosts principal protection functions and supports associated time-critical teleprotection functionality.

The co-processor is responsible for receiving sampled values of analogue inputs and performing any specific signal filtering and processing required by the hosted protection algorithms. Communications are managed using the HDLC (high-level data link control) communication protocol and enable transfer of information needed between IEDs to implement unit protection schemes.

The co-processor interface initialises and maintains appropriate time synchronisation, as well as data and command transfer with the main processor for correct protection operation.

Co-processor board initialisation checks are also made as follows:

- A check is made for the presence of the co-processor board
- The DRAM on the co-processor board is checked

If any of these checks produces an error, the co-processor board is left out of service. The other protection functions provided by the main processor board are left in service.

4.3.4.4 PLATFORM SOFTWARE INITIALISATION AND MONITORING

When starting the platform software, the IED checks the following:

- The integrity of the data held in non-volatile memory (using a checksum)
- The operation of the real-time clock
- The optional IRIG-B function (if applicable)
- The presence and condition of the input board
- The analog data acquisition system (it does this by sampling the reference voltage)

At the successful conclusion of all of these tests the unit is entered into service and the application software is started up.

4.3.5 CONTINUOUS SELF-TESTING

When the IED is in service, it continually checks the operation of the critical parts of its hardware and software. The checking is carried out by the system services software and the results are reported to the platform software. The functions that are checked are as follows:

- The Flash memory containing all program code and language text is verified by a checksum.
- The code and constant data held in system memory is checked against the corresponding data in Flash memory to check for data corruption.
- The system memory containing all data other than the code and constant data is verified with a checksum.

- The integrity of the digital signal I/O data from the opto-inputs and the output relay coils is checked by the data acquisition function every time it is executed.
- The operation of the analog data acquisition system is continuously checked by the acquisition function every time it is executed. This is done by sampling the reference voltages.
- The operation of the optional Ethernet board is checked by the software on the main processor board. If the Ethernet board fails to respond an alarm is raised and the board is reset in an attempt to resolve the problem.
- The operation of the optional IRIG-B function is checked by the software that reads the time and date from the board.

In the event that one of the checks detects an error in any of the subsystems, the platform software is notified and it attempts to log a maintenance record.

If the problem is with the IRIG-B board, the device continues in operation. For problems detected in any other area, the device initiates a shutdown and re-boot, resulting in a period of up to 10 seconds when the functionality is unavailable.

A restart should clear most problems that may occur. If, however, the diagnostic self-check detects the same problem that caused the IED to restart, it is clear that the restart has not cleared the problem, and the device takes itself permanently out of service. This is indicated by the ‘’health-state’ LED on the front of the device, which switches OFF, and the watchdog contact which switches ON.

4.4 PLATFORM SOFTWARE

The platform software has three main functions:

- To control the logging of records generated by the protection software, including alarms, events, faults, and maintenance records
- To store and maintain a database of all of the settings in non-volatile memory
- To provide the internal interface between the settings database and the user interfaces, using the front panel interface and the front and rear communication ports

4.4.1 RECORD LOGGING

The logging function is used to store all alarms, events, faults and maintenance records. The records are stored in non-volatile memory to provide a log of what has happened. The IED maintains four types of log on a first in first out basis (FIFO). These are:

- Alarms
- Event records
- Fault records
- Maintenance records

The logs are maintained such that the oldest record is overwritten with the newest record. The logging function can be initiated from the protection software. The platform software is responsible for logging a maintenance record in the event of an IED failure. This includes errors that have been detected by the platform software itself or errors that are detected by either the system services or the protection software function. See the Monitoring and Control chapter for further details on record logging.

4.4.2 SETTINGS DATABASE

The settings database contains all the settings and data, which are stored in non-volatile memory. The platform software manages the settings database and ensures that only one user interface can modify the settings at any one time. This is a necessary restriction to avoid conflict between different parts of the software during a setting change.

Changes to protection settings and disturbance recorder settings, are first written to a temporary location SRAM memory. This is sometimes called 'Scratchpad' memory. These settings are not written into non-volatile memory immediately. This is because a batch of such changes should not be activated one by one, but as part of a complete scheme. Once the complete scheme has been stored in SRAM, the batch of settings can be committed to the non-volatile memory where they will become active.

4.4.3 INTERFACES

The settings and measurements database must be accessible from all of the interfaces to allow read and modify operations. The platform software presents the data in the appropriate format for each of the interfaces (LCD display, keypad and all the communications interfaces).

4.5 PROTECTION AND CONTROL FUNCTIONS

The protection and control software processes all of the protection elements and measurement functions. To achieve this it has to communicate with the system services software, the platform software as well as organise its own operations.

The protection task software has the highest priority of any of the software tasks in the main processor board. This ensures the fastest possible protection response.

The protection and control software provides a supervisory task, which controls the start-up of the task and deals with the exchange of messages between the task and the platform software.

4.5.1 ACQUSITION OF POWER SYSTEM INPUT SIGNALS

A sampling function controls the acquisition of sampled input data to the various protection and control and recording functions in this device.

Following successful initialisation from the system services software, the sampling function delivers a constant stream of input data to the Protection and Control software at a rate of 48 samples per cycle of the power system frequency. This means that on a 50Hz power system the nominal sampling rate is 2,400 Hz whereas, for a 60 Hz system, sampling will be at 2,880 Hz.

The sampled input data is consumed at different rates by the various protection, control, and recording functions according to specific application requirements and, typically, Fourier filters and/or disturbance recorders may be populated at sub-multiples of the device sampling rate (for example, 24 or 8 samples per cycle).

The following section, explains that the sampling rate is synchronised to the power system frequency by a frequency tracking algorithm. This ensures that for minor excursions in the system frequency, an exact number of samples are always acquired for every cycle, ensuring protection stability. In normal operation, the outputs from the protection elements are updated 16 times per cycle.

4.5.2 FREQUENCY TRACKING OF INPUT SIGNAL ACQUISITION

This device features a frequency tracking algorithm so that, even for small changes, its power system inputs are sampled exactly 48 times every power system cycle over the full rated frequency range. If the system frequency moves out of range, the sampling rate defaults according to the applied system frequency setting, at either 2,400 Hz for 50 Hz or 2,880 Hz for 60 Hz.

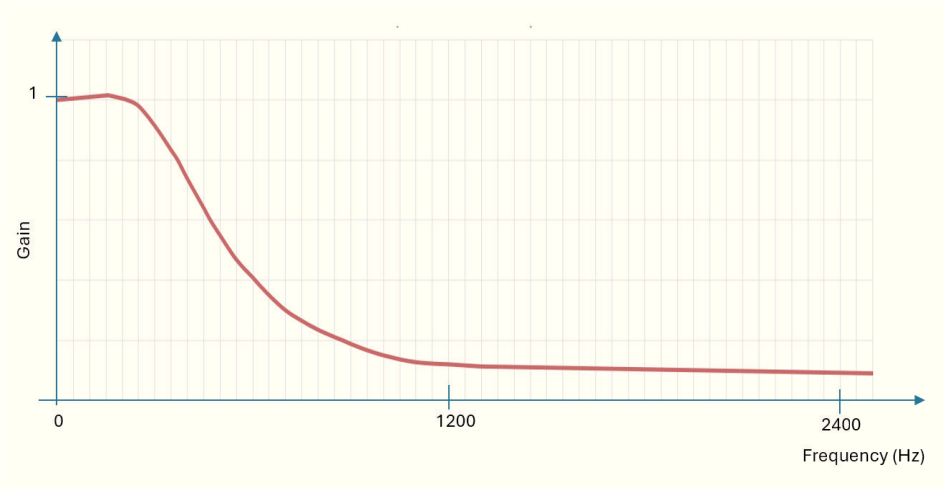
A recursive Fourier filter applied to the device’s analog inputs detects phase variations. From these changes, the precise system frequency can be determined. This is used to implement frequency tracking of the input signals acquisition, as well as to inform the protection and control and recording tasks about the measured system frequency. The frequency tracking controls the acquisition by adjusting the intervals between sampling instants to ensure that the number of samples acquired per cycle exactly matches the expected constant value. To execute, the frequency tracking requires that just one of the phase input voltage or phase input current signals is available. Availability thresholds are set as 10% Vn for voltage, and 5% In for current, and the frequency tracks off any available voltage or current input signal, prioritised in the order VA, VB, VC, IA, IB, IC.

4.5.3 INPUT SIGNAL FILTERING

Most of the protection algorithms in this product apply digital filtering to the sampled data input streams to extract useful information from power system analogue signals (phase current angles, for example). Fourier filters may be employed to provide useful information about specific frequency components, whereas other bespoke filters may facilitate the calculation of quantities such as fault impedances and distance-to-fault values.

Some of the functionality provided by this product, however, is better implemented using raw data that has not been subject to digital filtering. Un-processed raw data may be required by special (potentially very fast acting) protection functions or, more typically waveform recording and the calculation of true RMS values of current, voltage and

power for metering purposes. In these cases, the fidelity is defined by the anti-aliasing filters applied to the input signals for which the characteristics are defined by the following figure.



E80069

Figure 28: Anti-alias filter response

4.5.4 FOURIER SIGNAL FILTERING

Most protection and measurement functions in this device use single-cycle Fourier digital filtering to extract power frequency components.

The software to implement the Fourier filters acts on the sampled analogue input signals and is, along with the associated protection and control software, hosted on the main processor board.

The principal use of Fourier filters in this product is to provide measurements of fundamental components for current based protection, but Fourier filters may also be applied to extract fundamental signals for other protection functions such as voltage, as well as deriving harmonic components such as the second harmonic used to restrain current differential protection.

The magnitude and angle of fundamental frequency components of input signals are calculated using one complete cycle of the most recently acquired input data. In this case, the Fourier algorithm extracts the power frequency fundamental component from the input signal, presenting it in terms of magnitude and phase angle. This can be represented in either polar format or rectangular format, as required. Values for harmonic components can be similarly determined by appropriately varying the filters' input data streams and filter coefficients.

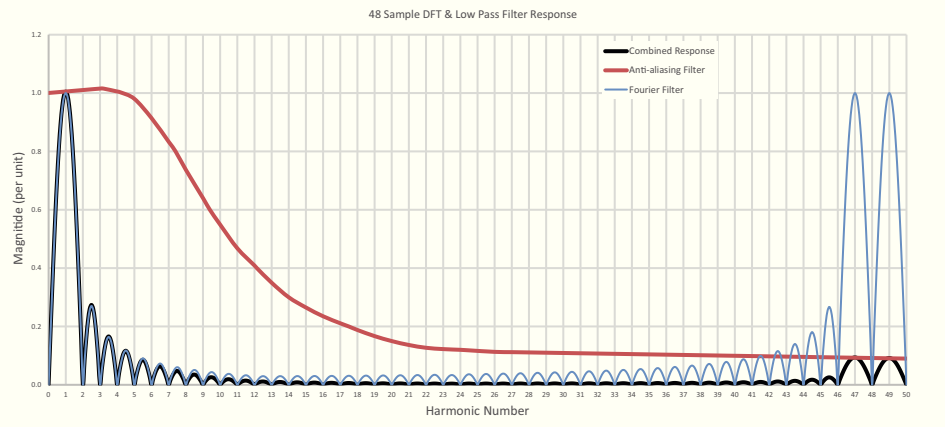
The Fourier filter acts as a function with zero gain at DC, unity gain at the fundamental, and with good harmonic rejection for all harmonic frequencies up to a value known as the Nyquist frequency (and equivalent to half the sampling frequency). Any frequency component of the input signal above this Nyquist frequency appears as an unwanted alias component causing problems. The introduction of low-pass filters to limit the input frequency spectrum to less than half that of the sampling frequency effectively prevents aliasing.

4.5.4.1 COMBINED FOURIER FILTER RESPONSE

In this product, the rate at which sampled data is made available to the protection and control software is 48 per cycle and so the required minimum cut-off frequency for the anti-aliasing filters is:

- 1200 Hz (for a 50 Hz system), or
- 1440 Hz for a 60 Hz system.

The following figure shows the frequency response of the combined anti-alias filter and 48-sample single-cycle Fourier filter implemented in this product.



E80021

Figure 29: Combined input filter response

4.5.5 FAULT LOCATOR

The fault locator uses 12 cycles of the analog input signals to calculate the fault location. The result is returned to the protection and control task, which includes it in the fault record. The pre-fault and post-fault voltages are also presented in the fault record. When the fault record is complete, including the fault location, the protection and control task sends a message to the supervisor task to log the fault record.

The Fault Locator is not available on all models.

4.5.6 DISTURBANCE RECORDER

The disturbance recorder operates as a separate task from the protection and control task and they both use the same input data. However, unlike in the protection functions where additional filters (such as Fourier) may be applied to refine the data processed, the only processing of the signals presented to the disturbance recorder (other than a calibration function) is that caused by the low-pass input filters employed to prevent aliasing. The filter effectively suppresses high-frequency components according to the anti-alias filter characteristic presented in the section on input signal filtering.

The disturbance recorder stores the waveforms of calibrated analogue channels and digital signals to a resolution of 48 samples/cycles. The recording time is user selectable. Typically, up to 100 waveforms, each up to 10.5 seconds duration can be stored. The disturbance recorder is supplied with data by the protection and control task once per cycle. The disturbance recorder collates the data that it receives into the required length disturbance record. The disturbance records can be extracted by settings application software such as S1 Agile, which can also store the data in COMTRADE format, therefore allowing the use of other packages to view the recorded data.

For more information see the Monitoring and Control chapter.

4.5.7 EVENT RECORDER INTERFACE

A change in any digital input signal or protection element output signal is used to indicate that an event has taken place. When this happens, the protection and control task sends a message to the supervisor task to indicate that an event is available to be processed and writes the event data to a fast buffer controlled by the supervisor task. A background task in the platform software then converts the data into a stored non-volatile record.

Maintenance records are a special category of event record which may be created during power-up or self-testing. Similar to other events, the supervisor task instructs the platform software to log a record when it receives a maintenance record message, but the maintenance records are stored in a separate register to simplify examination.

4.5.8 SCHEME LOGIC INTERFACE

Association of the protection and control algorithms implemented in this device with external plant relies on logical allocation of software inputs and outputs with physical inputs and outputs. The functionality which implements this is known as scheme logic. The scheme logic in this device consists of fixed components and programmable components. Fixed scheme logic components are hard-coded into the protection and control algorithm software modules. They have been designed to complement the protection and control objectives and cannot be changed by the user. User control over the operation of the devices' digital inputs and output is provided by a feature know as the programmable scheme logic (PSL). Executed in response to changes of state of inputs either from external plant, or from functional inputs from the user interfaces, or from internal logic state changes emanating from execution of the protection and control software, the scheme logic allows the user to combine factory-proven application scheme logic with versatile user-designed logic processing to control outputs and led indications.

4.5.9 PROGRAMMABLE SCHEME LOGIC

The purpose of the programmable scheme logic (PSL) is to allow you to configure your own protection schemes to suit your particular application. This is done with programmable logic gates and delay timers. To allow greater flexibility, different PSL is allowed for each of the four setting groups.

The input to the PSL is any combination of the status of the digital input signals from the opto-isolators on the input board, the outputs of the protection elements such as protection starts and trips, and the outputs of the fixed protection scheme logic (FSL). The fixed scheme logic provides the standard protection schemes. The PSL consists of software logic gates and timers. The logic gates can be programmed to perform a range of different logic functions and can accept any number of inputs. The timers are used either to create a programmable delay, and/or to condition the logic outputs, such as to create a pulse of fixed duration on the output regardless of the length of the pulse on the input. The outputs of the PSL are the LEDs on the front panel of the device and the output contacts at the rear.

The execution of the PSL logic is event driven. The logic is processed whenever any of its inputs change, for example as a result of a change in one of the digital input signals or a trip output from a protection element. Also, only the part of the PSL logic that is affected by the particular input change that has occurred is processed. This reduces the amount of processing time that is used by the PSL. The protection & control software updates the logic delay timers and checks for a change in the PSL input signals every time it runs.

The PSL can be configured to create very complex schemes. Because of this PSL design is achieved by means of a PC support package called the PSL Editor. This is available as part of the settings application software MiCOM S1 Agile.

4.5.10 DIRECT USE OF SAMPLED VALUES

Most of the IED's protection functionality uses the Fourier components calculated by the device's signal processing software. However RMS measurements and some special protection algorithms available in some products use the sampled values directly.

The disturbance recorder also uses the samples from the input module, in an unprocessed form. This is for waveform recording and the calculation of true RMS values of current, voltage and power for metering purposes.

In the case of special protection algorithms, using the sampled values directly provides exceptionally fast response because you do not have to wait for the signal processing task to calculate the fundamental. You can act on the sampled values immediately.

4.5.11 FUNCTION KEY INTERFACE

The function keys interface directly into the PSL as digital input signals. A change of state is only recognised when a key press is executed on average for longer than 200 ms. The time to register a change of state depends on whether the function key press is executed at the start or the end of a protection task cycle, with the additional hardware and software scan time included. A function key press can provide a latched (toggled mode) or output on key press only (normal mode) depending on how it is programmed. It can be configured to individual protection

scheme requirements. The latched state signal for each function key is written to non-volatile memory and read from non-volatile memory during device power up thus allowing the function key state to be reinstated after power-up, should power be inadvertently lost.

CHAPTER 5

CONFIGURATION

5.1 CHAPTER OVERVIEW

Each product has different configuration parameters according to the functions it has been designed to perform. There is, however, a common methodology used across the entire product series to set these parameters.

Some of the communications setup can only be carried out using the HMI, and cannot be carried out using settings applications software. This chapter includes concise instructions of how to configure the device, particularly with respect to the communications setup, as well as a description of the common methodology used to configure the device in general.

This chapter contains the following sections:

Chapter Overview 70
Settings Application Software 71
Using the HMI Panel 72
Line Parameters 82
Date and Time Configuration 85
Settings Group Selection 88

5.2 SETTINGS APPLICATION SOFTWARE

To configure this device you will need to use the Settings Application Software. The settings application software used in this range of IEDs is called MiCOM S1 Agile. It is a collection of software tools, which is used for setting up and managing the IEDs.

Although you can change many settings using the front panel HMI, some of the features cannot be configured without the Settings Application Software; for example the programmable scheme logic, or IEC61850 communications.

If you do not already have a copy of the Settings Application Software, you can obtain it from GE Vernova's contact centre.

To configure your product, you will need a data model that matches your product. When you launch the Settings Application Software, you will be presented with a panel that allows you to invoke the “Data Model Manager”. This will close the other aspects of the software in order to allow an efficient import of the chosen data model. If you don’t have, or can’t find, the data model relating to your product, please call the GE Vernova contact centre.

When you have loaded all the data models you need, you should restart the Settings Application Software and start to create a model of your system using the “System Explorer” panel.

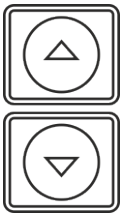
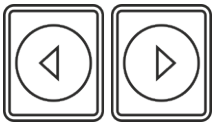
The software is designed to be intuitive, but help is available in an online help system and also the Settings Application Software user guide P40-M&CR-SAS-UG-EN-n, where 'Language' is a 2 letter code designating the language version of the user guide and 'n' is the latest version of the settings application software.

5.3 USING THE HMI PANEL

Using the HMI, you can:

- Display and modify settings
- View the digital I/O signal status
- Display measurements
- Display fault records
- Reset fault and alarm indications

The keypad provides full access to the device functionality using a range of menu options. The information is displayed on the LCD.

Keys	Description	Function
	Up and down cursor keys	To change the menu level or change between settings in a particular column, or changing values within a cell
	Left and right cursor keys	To change default display, change between column headings, or changing values within a cell
	ENTER key	For changing and executing settings
	Hotkeys	For executing commands and settings for which shortcuts have been defined
	Cancel key	To return to column header from any menu cell
	Read key	To read alarm messages
	Function keys (not all models)	For executing user programmable functions

Note:
As the LCD display has a resolution of 16 characters by 3 lines, some of the information is in a condensed mnemonic form.

5.3.1 NAVIGATING THE HMI PANEL

The cursor keys are used to navigate the menus. These keys have an auto-repeat function if held down continuously. This can be used to speed up both setting value changes and menu navigation. The longer the key is held pressed, the faster the rate of change or movement.

The navigation map below shows how to navigate the menu items.

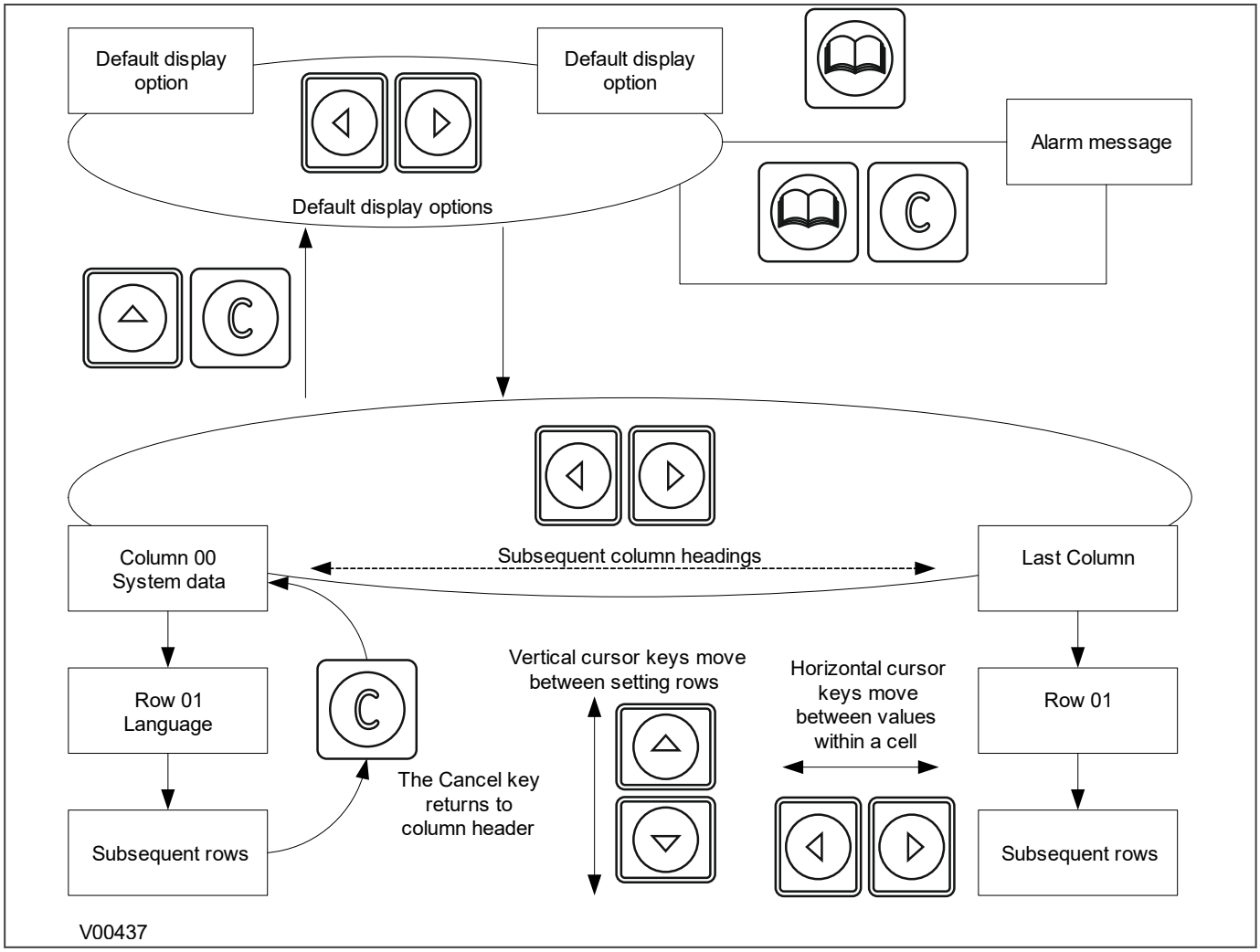


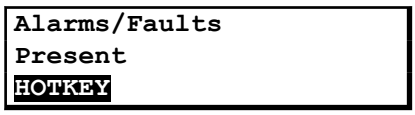
Figure 30: Navigating the HMI

5.3.2 GETTING STARTED

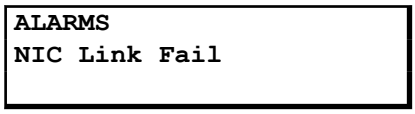
When you first start the IED, it will go through its power up procedure. After a few seconds it will settle down into one of the top level menus. There are two menus at this level:

- The Alarms menu for when there are alarms present
- The default display menu for when there are no alarms present.

If there are alarms present, the yellow Alarms LED will be flashing and the menu display will read as follows:



Even though the device itself should be in full working order when you first start it, an alarm could still be present, for example, if there is no network connection for a device fitted with a network card. If this is the case, you can read the alarm by pressing the 'Read' key.



If the device is fitted with an Ethernet card, you will first need to connect the device to an active Ethernet network to clear the alarm and get the default display.

If there are other alarms present, these must also be cleared before you can get into the default display menu options.

5.3.3 DEFAULT DISPLAY

The HMI contains a range of possible options that you can choose to be the default display. The options available are:

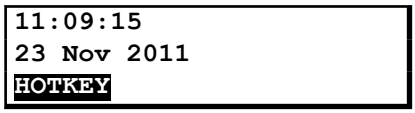
NERC Compliant banner

If the device is a cyber-security model, it will provide a NERC-compliant default display. If the device does not contain the cyber-security option, this display option is not available.



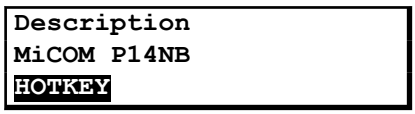
Date and time

For example:



Description (user-defined)

For example:



Plant reference (user-defined)

For example:

```
Plant Reference
MiCOM
HOTKEY
```

Access Level

For example:

```
Access Level
3
HOTKEY
```

In addition to the above, there are also displays for the system voltages, currents, power and frequency etc., depending on the device model.

5.3.4 DEFAULT DISPLAY NAVIGATION

The following diagram is an example of the default display navigation. In this example, we have used a cyber-secure model. This is an example only and may not apply in its entirety to all models. The actual display options available depend on the exact model.

Use the horizontal cursor keys to step through from one display to the next.

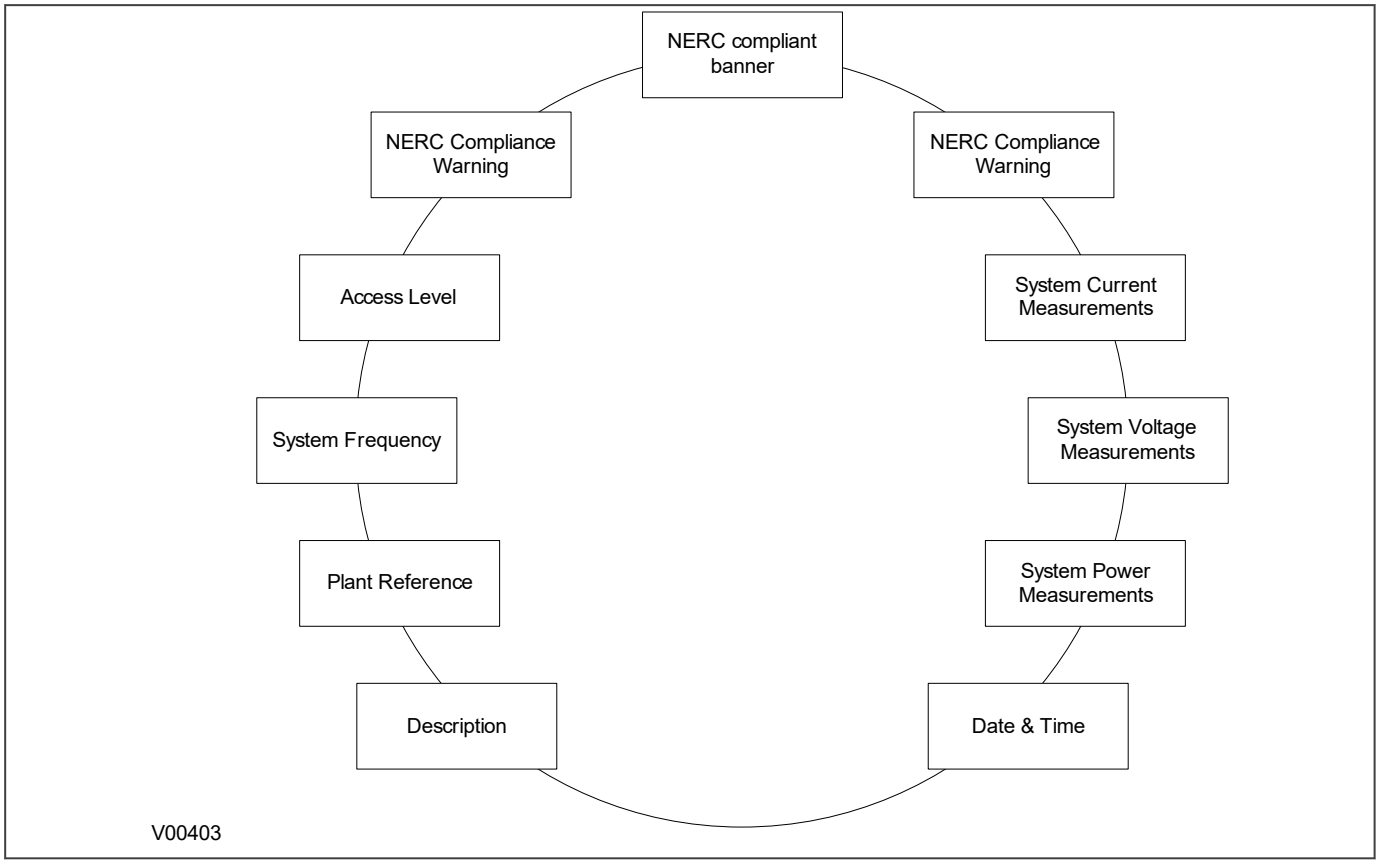


Figure 31: Default display navigation

If the device is cyber-secure but is not yet configured for NERC compliance (see Cyber-security chapter), a warning will appear when moving from the "NERC compliant" banner. The warning message is as follows:

```
DISPLAY NOT NERC
COMPLIANT. OK?
```

You will have to confirm with the **Enter** button before you can go any further.

Note:
Whenever the IED has an uncleared alarm the default display is replaced by the text Alarms/ Faults present. You cannot override this default display. However, you can enter the menu structure from the default display, even if the display shows the Alarms/Faults present message.

5.3.5 PASSWORD ENTRY

Configuring the default display (in addition to modification of other settings) requires level 3 access. You will be prompted for a password before you can make any changes, as follows. The default level 3 password is AAAA.

```
Enter Password
```

1. A flashing cursor shows which character field of the password can be changed. Press the up or down cursor keys to change each character (tip: pressing the up arrow once will return an upper case "A" as required by the default level 3 password).
2. Use the left and right cursor keys to move between the character fields of the password.
3. Press the **Enter** key to confirm the password. If you enter an incorrect password, an invalid password message is displayed then the display reverts to ***Enter password***. On entering a valid password a message appears indicating that the password is correct and which level of access has been unlocked. If this level is sufficient to edit the selected setting, the display returns to the setting page to allow the edit to continue. If the correct level of password has not been entered, the password prompt page appears again.
4. To escape from this prompt press the **Clear** key. Alternatively, enter the password using the ***Password*** setting in the *SYSTEM DATA* column. If the keypad is inactive for 15 minutes, the password protection of the front panel user interface reverts to the default access level.

To manually reset the password protection to the default level, select ***Password***, then press the CLEAR key instead of entering a password.

Note:
In the SECURITY CONFIG column, you can set the maximum number of attempts, the time window in which the failed attempts are counted and the time duration for which the user is blocked.

5.3.6 PROCESSING ALARMS AND RECORDS

If there are any alarm messages, they will appear on the default display and the yellow alarm LED flashes. The alarm messages can either be self-resetting or latched. If they are latched, they must be cleared manually.

1. To view the alarm messages, press the **Read** key. When all alarms have been viewed but not cleared, the alarm LED changes from flashing to constantly on, and the latest fault record appears (if there is one).
2. Scroll through the pages of the latest fault record, using the cursor keys. When all pages of the fault record have been viewed, the following prompt appears.

```
Press Clear To
Reset Alarms
```

3. To clear all alarm messages, press the **Clear** key. To return to the display showing alarms or faults present, and leave the alarms uncleared, press the **Read** key.
4. Depending on the password configuration settings, you may need to enter a password before the alarm messages can be cleared.
5. When all alarms are cleared, the yellow alarm LED switches off. If the red LED was on, this will also be switched off.

Note:
*To speed up the procedure, you can enter the alarm viewer using the **Read** key and subsequently pressing the **Clear** key. This goes straight to the fault record display. Press the **Clear** key again to move straight to the alarm reset prompt, then press the **Clear** key again to clear all alarms.*

5.3.7 MENU STRUCTURE

Settings, commands, records and measurements are stored in a local database inside the IED. When using the Human Machine Interface (HMI) it is convenient to visualise the menu navigation system as a table. Each item in the menu is known as a cell, which is accessed by reference to a column and row address. Each column and row is assigned a 2-digit hexadecimal numbers, resulting in a unique 4-digit cell address for every cell in the database. The main menu groups are allocated columns and the items within the groups are allocated rows, meaning a particular item within a particular group is a cell.

Each column contains all related items, for example all of the disturbance recorder settings and records are in the same column.

There are three types of cell:

- Settings: this is for parameters that can be set to different values
- Commands: this is for commands to be executed
- Data: this is for measurements and records to be viewed, which are not settable

Note:
Sometimes the term "Setting" is used generically to describe all of the three types.

The table below, provides an example of the menu structure:

SYSTEM DATA (Col 00)	VIEW RECORDS (Col 01)	MEASUREMENTS 1 (Col 02)	...
Language (Row 01)	"Select Event [0...n]" (Row 01)	IA Magnitude (Row 01)	...
Password (Row 02)	Menu Cell Ref (Row 02)	IA Phase Angle (Row 02)	...
Sys Fn Links (Row 03)	Time & Date (Row 03)	IB Magnitude (Row 03)	...
...	...	...	...

It is convenient to specify all the settings in a single column, detailing the complete Courier address for each setting. The above table may therefore be represented as follows:

Setting	Column	Row	Description
SYSTEM DATA	**00**	**00**	**First Column definition**
Language (Row 01)	00	01	First setting within first column
Password (Row 02)	00	02	Second setting within first column
Sys Fn Links (Row 03)	00	03	Third setting within first column
...	...	...	
VIEW RECORDS	**01**	**00**	**Second Column definition**
Select Event [0...n]	01	01	First setting within second column

Setting	Column	Row	Description
Menu Cell Ref	01	02	Second setting within second column
Time & Date	01	03	Third setting within second column
…	…	…	
MEASUREMENTS 1	**02**	**00**	**Third Column definition**
IA Magnitude	02	01	First setting within third column
IA Phase Angle	02	02	Second setting within third column
IB Magnitude	02	03	Third setting within third column
…	…	…	

The first three column headers are common throughout much of the product ranges. However the rows within each of these column headers may differ according to the product type. Many of the column headers are the same for all products within the series. However, there is no guarantee that the addresses will be the same for a particular column header. Therefore you should always refer to the product settings documentation and not make any assumptions.

5.3.8 CHANGING THE SETTINGS

1. Starting at the default display, press the **Down** cursor key to show the first column heading.
2. Use the horizontal cursor keys to select the required column heading.
3. Use the vertical cursor keys to view the setting data in the column.
4. To return to the column header, either press the Up cursor key for a second or so, or press the **Clear** key once. It is only possible to move across columns at the column heading level.
5. To return to the default display, press the Up cursor key or the **Clear** key from any of the column headings. If you use the auto-repeat function of the Up cursor key, you cannot go straight to the default display from one of the column cells because the auto-repeat stops at the column heading.
6. To change the value of a setting, go to the relevant cell in the menu, then press the **Enter** key to change the cell value. A flashing cursor on the LCD shows that the value can be changed. You may be prompted for a password first.
7. To change the setting value, press the **Up** and **Down** cursor keys. If the setting to be changed is a binary value or a text string, select the required bit or character to be changed using the horizontal cursor keys.
8. Press the **Enter** key to confirm the new setting value or the **Clear** key to discard it. The new setting is automatically discarded if it is not confirmed within 15 seconds.
9. For protection group settings and disturbance recorder settings, the changes must be confirmed before they are used. When all required changes have been entered, return to the column heading level and press the Down cursor key. Before returning to the default display, the following prompt appears.

```
Update settings?
ENTER or CLEAR
```

10. Press the **Enter** key to accept the new settings or press the **Clear** key to discard the new settings.

Note:
For the protection group and disturbance recorder settings, if the menu time-out occurs before the changes have been confirmed, the setting values are discarded. Control and support settings, howeverr, are updated immediately after they are entered, without the ***Update settings?*** *prompt.*

5.3.9 DIRECT ACCESS (THE HOTKEY MENU)

For settings and commands that need to be executed quickly or on a regular basis, the IED provides a pair of keys directly below the LCD display. These so called **Hotkeys** can be used to execute specified settings and commands directly.

The functions available for direct access using these keys are:

- Setting group selection
- Control inputs
- Circuit Breaker (CB) control functions

The availability of these functions is controlled by the ***Direct Access*** cell in the *CONFIGURATION* column. There are four options: *Disabled*, *Enabled*, *CB Ctrl only* and *Hotkey only*.

For the Setting Group selection and Control inputs, this cell must be set to either *Enabled* or *Hotkey only*. For CB Control functions, the cell must be set to *Enabled* or *CB Ctrl only*.

5.3.9.1 SETTING GROUP SELECTION USING HOTKEYS

In some models you can use the hotkey menu to select the settings group. By default, only Setting group 1 is enabled. Other setting groups will only be available if they are first enabled. To be able to select a different setting group, you must first enable them in the *CONFIGURATION* column.

To access the hotkey menu from the default display, you press the key directly below the HOTKEY text on the LCD. The following screen will appear.

```
←User32 STG GP→
HOTKEY MENU
            EXIT
```

Use the right cursor keys to enter the *SETTING GROUP* menu.

```
←Menu User01→
SETTING GROUP 1
Nxt Grp Select
```

Select the setting group with ***Nxt Grp*** and confirm by pressing ***Select***. If neither of the cursor keys is pressed within 20 seconds of entering a hotkey sub menu, the device reverts to the default display.

5.3.9.2 CONTROL INPUTS

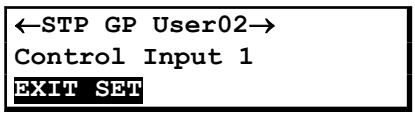
The control inputs are user-assignable functions. You can use the *CTRL I/P CONFIG* column to configure the control inputs for the hotkey menu. In order to do this, use the first setting ***Hotkey Enabled*** cell to enable or disable any of the 32 control inputs. You can then set each control input to latched or pulsed and set its command to *On/Off*, *Set/Reset*, *In/Out*, or *Enabled/Disabled*.

By default, the hotkey is enabled for all 32 control inputs and they are set to *Set/Reset* and are *Latched*.

To access the hotkey menu from the default display, you press the key directly below the HOTKEY text on the LCD. The following screen will appear.

```
←User32 STG GP→
HOTKEY MENU
            EXIT
```

Press the right cursor key twice to get to the first control input, or the left cursor key to get to the last control input.



Now you can execute the chosen function (Set/Reset in this case).

If neither of the cursor keys is pressed within 20 seconds of entering a hotkey sub menu, the device reverts to the default display.

5.3.9.3 CIRCUIT BREAKER CONTROL

You can open and close the controlled circuit breaker with the hotkey to the right, if enabled as described above. By default, hotkey access to the circuit breakers is disabled.

If hotkeyaccess to the circuit breakers has been enabled, the bottom right hand part of the display will read "Open or Close" depending on whether the circuit breaker is closed or open respectively:

For example:



To close the circuit breaker (in this case), press the key directly below CLOSE. You will be given an option to cancel or confirm.



More detailed information on this can be found in the Monitoring and Control chapter.

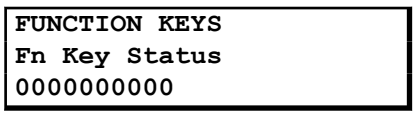
5.3.10 FUNCTION KEYS

Most products have a number of function keys for programming control functionality using the programmable scheme logic (PSL).

Each function key has an associated programmable tri-colour LED that can be programmed to give the desired indication on function key activation.

These function keys can be used to trigger any function that they are connected to as part of the PSL. The function key commands are in the *FUNCTION KEYS* column.

The first cell down in the *FUNCTION KEYS* column is the ***Fn Key Status*** cell. This contains a binary string, which represents the function key commands. Their status can be read from this binary string.



The next cell down (***Fn Key 1***) allows you to activate or disable the first function key (1). The ***Lock*** setting allows a function key to be locked. This allows function keys that are set to *Toggled* mode and their DDB signal active 'high', to be locked in their active state, preventing any further key presses from deactivating the associated function. Locking a function key that is set to the Normal mode causes the associated DDB signals to be permanently off. This safety feature prevents any inadvertent function key presses from activating or deactivating critical functions.

```
FUNCTION KEYS
Fn Key 1
Unlocked
```

The next cell down (***Fn Key 1 Mode***) allows you to set the function key to *Normal* or *Toggled*. In the Toggle mode the function key DDB signal output stays in the set state until a reset command is given, by activating the function key on the next key press. In the Normal mode, the function key DDB signal stays energised for as long as the function key is pressed then resets automatically. If required, a minimum pulse width can be programmed by adding a minimum pulse timer to the function key DDB output signal.

```
FUNCTION KEYS
Fn Key 1 Mode
Toggled
```

The next cell down (***Fn Key 1 Label***) allows you to change the label assigned to the function. The default label is *Function key 1* in this case. To change the label you need to press the enter key and then change the text on the bottom line, character by character. This text is displayed when a function key is accessed in the function key menu, or it can be displayed in the PSL.

```
FUNCTION KEYS
Fn Key 1 Label
Function Key 1
```

Subsequent cells allow you to carry out the same procedure as above for the other function keys.

The status of the function keys is stored in non-volatile memory. If the auxiliary supply is interrupted, the status of all the function keys is restored. The IED only recognises a single function key press at a time and a minimum key press duration of approximately 200 ms is required before the key press is recognised. This feature avoids accidental double presses.

5.4 LINE PARAMETERS

This product requires information about the circuit to which it is applied. This includes line impedance, residual compensation, and phase rotation sequence. For this reason circuit parameter information must be input using the *LINE PARAMETERS* settings. These *LINE PARAMETERS* settings are used by protection elements as well as by the fault locator.

5.4.1 TRIPPING MODE

The ***Tripping Mode*** setting selects whether the product should trip single-phase or three-phase when instantaneous protection elements detect single-phase faults.

Selecting `1 and 3 Pole` means that the product will only trip the affected phase for a single-phase fault. For faults involving more than one phase the product will always trip all three phases.

Selecting `3 Pole` means that the product will always trip all three phases.

For products controlling more than one circuit breaker, the tripping mode is independent for each circuit breaker.

The product features an autorecloser that can be used for single-phase autoreclose. In that case, if a single-phase fault evolves into a multi-phase fault during the autoreclose cycle, the product will switch to three-phase tripping.

5.4.1.1 CB TRIP CONVERSION LOGIC DIAGRAM

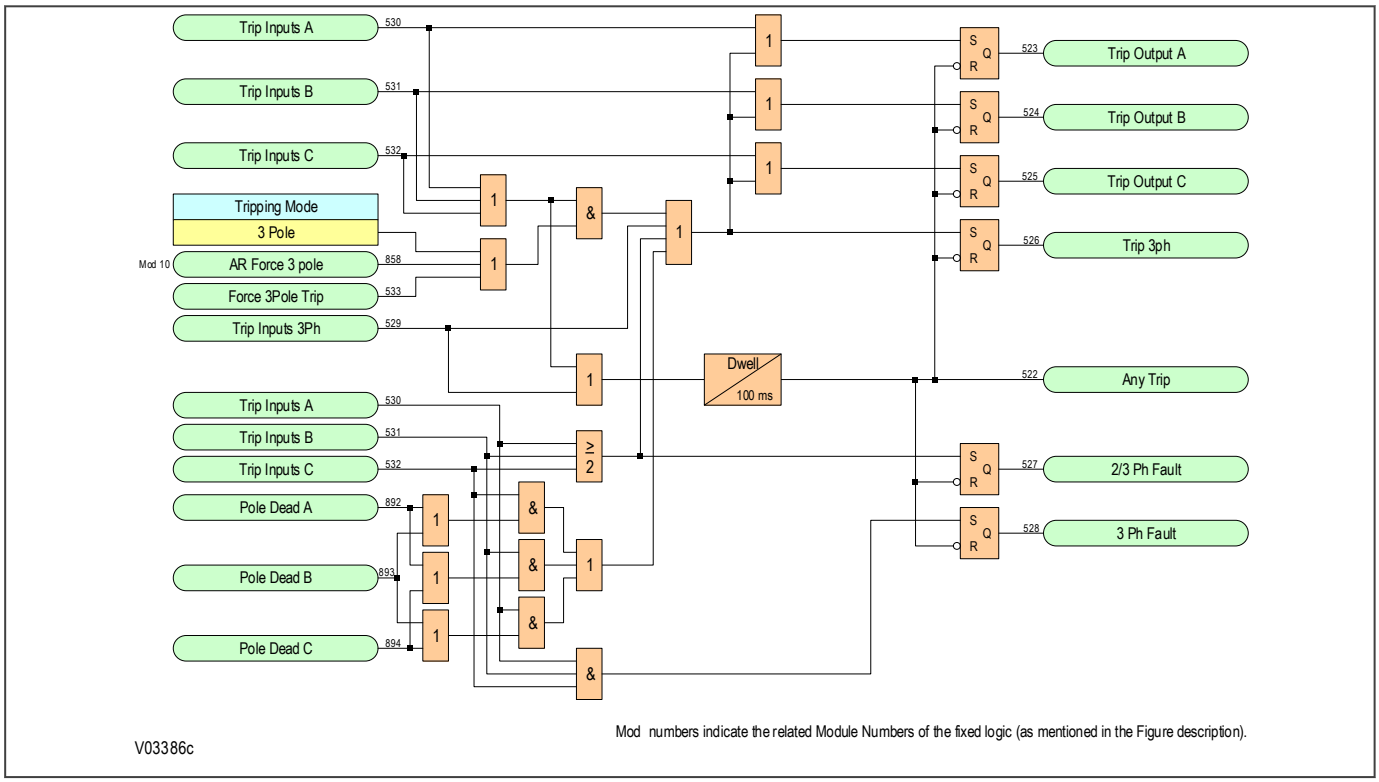


Figure 32: Circuit breaker trip conversion logic (module 63)

5.4.2 RESIDUAL COMPENSATION

To improve accuracy of impedance measuring elements such as those used in distance protection and fault locators, the total loop impedance calculation Z_{LP}/I_A can be calibrated by the positive sequence impedance between the relaying point and the fault (Z_{F1}) using the following equation:

$$\mathbf{Z}_{F1} = \frac{\mathbf{V}_A}{\mathbf{I}_A + \mathbf{k}_{ZN} \cdot \mathbf{I}_N}$$

where:

- V_A is the phase A voltage
- I_A is the phase A current
- I_N is the residual current, derived from the phase currents by the equation:

$$\mathbf{I}_N = \mathbf{I}_A + \mathbf{I}_B + \mathbf{I}_C$$

- k_{ZN} is the residual compensation coefficient given by the complex equation:

$$\mathbf{k}_{ZN} = \frac{\mathbf{Z}_{L0} - \mathbf{Z}_{L1}}{3\mathbf{Z}_{L1}}$$

where:

- Z_{L0} is the total zero sequence impedance of the line (a complex value)
- Z_{L1} is the total positive sequence impedance of the protected line (a complex value)

The complex residual compensation coefficient is defined by two settings: ***kZN Res Comp*** (the absolute value) and ***kZN Res Angle*** (the angle in degrees).



Caution:
The *kZN Res Angle* is different to that in LFZP, SHNB, and LFZR products: If importing settings from these products, you must subtract angle $\angle Z_{L1}$

5.4.3 MUTUAL COMPENSATION

On parallel circuits, mutual flux coupling can alter the impedance seen by fault locators and distance zones. A current input (the Mutual Compensation input) is provided to compensate.

If you want to use Mutual Compensation, the connection polarity must match that shown in the connection diagram and the element must be `Enabled` in the settings.

Consider for example an A-phase to earth fault on one circuit of a parallel circuit. The positive sequence impedance between the relaying point and the fault can be calculated using the following equation:

$$\boldsymbol{Z}_{F1} = \frac{\boldsymbol{V}_A}{\boldsymbol{I}_A + \boldsymbol{k}_{ZN} \cdot \boldsymbol{I}_N + \boldsymbol{k}_{Zm} \cdot \boldsymbol{I}_M}$$

where:

- V_A is the phase A voltage
- I_A is the phase A current
- I_N is the residual current of the protected line (derived from phase currents)
- I_M is the residual current of the parallel line (measured)
- k_{ZN} is the residual compensation coefficient
- k_{Zm} is the mutual compensation coefficient

In the above equation:

$$\mathbf{I}_N = \mathbf{I}_A + \mathbf{I}_B + \mathbf{I}_C$$

$$\mathbf{k}_{ZN} = \frac{\mathbf{Z}_{L0} - \mathbf{Z}_{L1}}{3\mathbf{Z}_{L1}}$$

$$\mathbf{k}_{Zm} = \frac{\mathbf{Z}_{m0}}{3\mathbf{Z}_{L1}}$$

where:

- Z_{L0} is the total zero sequence impedance of the line (a complex value)
- Z_{L1} is the total positive sequence impedance of the protected line (complex value)
- Z_{m0} is the zero sequence mutual impedance between the two circuits (complex value).

If used, you must set the mutual compensation feature k_{Zm} using the settings:

- ***kZm Mutual Set*** (the absolute value) and
- ***kZm Mutual Angle*** (the angle in degrees).

Note:
The following paragraph applies only to distance products and so may not be applicable to your model

In applications where the Mutual Compensation is used to reduce errors in the distance elements, a third setting, ***Mutual Cut Off***, is used for a fast dynamic control. The ratio I_M/I_N is compared with the ***Mutual Cut Off*** setting. If the ratio is higher, mutual compensation is suppressed to prevent false-tripping for faults on the parallel line.

Typically a ***Mutual Cut Off*** factor of 1.5 is chosen to give a good margin of safety between the requirements of correct mutual compensation for faults on the protected circuit whilst avoiding maloperations for faults on the parallel circuit.

5.5 DATE AND TIME CONFIGURATION

The date and time setting will normally be updated automatically by the chosen UTC (Universal Time Co-ordination) time synchronisation mechanism when the device is in service. You can also set the date and time manually using the ***Date/Time*** cell in the *DATE AND TIME* column.

5.5.1 USING AN SNTP SIGNAL

When using SNTP to maintain the clock, the IED must first be connected to the SNTP server, which should be energised and functioning.

1. In the *DATE AND TIME* column, check that either the ***Primary Source*** or ***Secondary Source*** setting is set to `SNTP`.
2. Ensure that the IED is receiving valid time synchronisation messages by checking that the ***SNTP Status*** cell reads `Server 1 OK` or `Server 2 OK`.
3. Check that the ***Act. Time Source*** cell reads `SNTP`. This indicates that the IED is using PTP as the source for its time. Note that If IRIG-B or PTP have been selected as the Primary Source, these must first be disconnected before the device can switch to SNTP as the active source.
4. Once the IED is using SNTP as the active time source, adjust the time offset of the universal coordinated time on the SNTP Server equipment, so that local time is displayed.
5. Check that the time, date and month are correct in the ***Date/Time*** cell.

5.5.2 USING AN IRIG-B SIGNAL

When using IRIG-B to maintain the clock, the IED must first be connected to the timing source equipment (usually a P594/RT430), which should be energised and functioning.

1. In the *DATE AND TIME* column, check that either the ***Primary Source*** or ***Secondary Source*** setting is set to `IRIG-B`.
2. Ensure the IED is receiving the IRIG-B signal by checking that ***IRIG-B Status*** cell reads `Active`
3. Check that the ***Act. Time Source*** cell reads `IRIG-B.` This indicates that the IED is using IRIG-B as the source for its time. Note that If SNTP or PTP have been selected as the Primary Source, these must first be disconnected before the device can switch to IRIG-B as the active source.
4. Once the IED is using IRIG-B as the active time source, adjust the time offset of the universal coordinated time (satellite clock time) on the satellite clock equipment, so that local time is displayed.
5. Check that the time, date and month are correct in the ***Date/Time*** cell. The IRIG-B signal does not contain the current year so this also needs to be set manually in this cell.
6. If the auxiliary supply fails, the time and date are maintained by the supercapacitor. Therefore, when the auxiliary supply is restored, you should not have to set the time and date again. To test this, remove the IRIG-B signal, and then remove the auxiliary supply. Leave the device de-energised for approximately 30 seconds. On re-energisation, the time should be correct.
7. Reconnect the IRIG-B signal.

5.5.3 USING AN IEEE 1588 PTP SIGNAL

When using IEEE 1588 PTP to maintain the clock, the IED must first be connected to the PTP Grandmaster, which should be energised and functioning.

1. In the *DATE AND TIME* column, check that either the ***Primary Source*** or ***Secondary Source*** setting is set to `PTP`.
2. Set the ***Domain Number*** setting. The domain defines which clocks the IED will use for synchronisation. Therefore this number must match the domain used by the other clocks on the network.

3. Ensure that the IED is receiving valid time synchronisation messages by checking that the ***PTP Status*** cell reads `Valid Master`.
4. Check that ***Act. Time Source*** cell reads `PTP`. This indicates that the IED is using PTP as the source for its time. Note that If IRIG-B or SNTP have been selected as the Primary Source, these must first be disconnected before the device can switch to PTP as the active source.
5. Once the IED is using PTP as the active time source, adjust the time offset of the universal coordinated time on the Master Clock equipment, so that local time is displayed.
6. Check that the time, date and month are correct in the ***Date/Time*** cell.

5.5.4 WITHOUT A TIMING SOURCE SIGNAL

If the time and date is not being maintained by an IRIG-B, PTP or SNTP signal, in the *DATE AND TIME* column, ensure that both the ***Primary Source*** and ***Secondary Source*** are set to `NONE`.

1. Check that ***Act. Time Source*** cell reads `Free Running`.
2. Set the date and time to the correct local time and date using the Date/Time cell or the serial protocol.
3. If the auxiliary supply fails, the time and date are maintained by the supercapacitor. Therefore, when the auxiliary supply is restored, you should not have to set the time and date again. To test this, remove the auxiliary supply. Leave the device de-energised for approximately 30 seconds. On re-energisation, the time should be correct.

5.5.5 TIME ZONE COMPENSATION

The UTC time standard uses Greenwich Mean Time as its standard. Without compensation, the date and time would be displayed on the device irrespective of its location.

You may wish to display the local time corresponding to its geographical location. You can do this with the settings ***LocalTime Enable*** and ***LocalTime Offset***.

The ***LocalTime Enable*** has three setting options; `Disabled`, `Fixed`, and `Flexible`.

With `Disabled`, no local time zone is maintained. Time synchronisation from any interface will be used to directly set the master clock. All times displayed on all interfaces will be based on the master clock with no adjustment.

With `Fixed`, a local time zone adjustment is defined using the ***LocalTime Offset*** setting and all non-IEC 61850 interfaces, which uses the Simple Network Time Protocol (SNTP), are compensated to display the local time.

With `Flexible`, a local time zone adjustment is defined using the ***LocalTime Offset*** setting. The non-local and non-IEC 61850 interfaces can be set to either the UTC zone or the local time zone. The local interfaces are always set to the local time zone and the Ethernet interface is always set to the UTC zone.

The interfaces where you can select between UTC and Local Time are the serial interfaces RP1, RP2, DNP over Ethernet (if applicable) and Tunnelled Courier (if applicable). This is achieved by means of the following settings, each of which can be set to UTC or Local.:

- RP1 Time Zone
- RP2 Time Zone
- DNPOE Time Zone
- Tunnel Time Zone

The ***LocalTime Offset*** setting allows you to enter the local time zone compensation from -12 to + 12 hours at 15 minute intervals.

5.5.6 DAYLIGHT SAVING TIME COMPENSATION

It is possible to compensate for Daylight Saving time using the following settings

- DST Enable
- DST Offset
- DST Start
- DST Start Day
- DST Start Month
- DST Start Mins
- DST End
- DST End Day
- DST End Month
- DST End Mins

These settings are described in the *DATE AND TIME* settings table in the configuration chapter.

5.6 SETTINGS GROUP SELECTION

You can select the setting group using opto inputs, a menu selection, and for some models the hotkey menu or function keys. You choose which method using the Setting Group setting in the *CONFIGURATION* column. There are two possibilities; Select via Menu, or Select via PSL. If you choose ***Select via Menu***, you set the settings group using the ***Active Settings*** setting or with the hotkeys. If you choose ***Select via PSL*** , you set the settings group with DDB signals according to the following table:

SG Select 1X	SG Select X1	Selected Setting Group
0	0	1
0	1	2
1	0	3
1	1	4

Each setting group has its own PSL. Once a PSL configuration has been designed it can be allocated to any one of the 4 setting groups. When downloading or extracting a PSL configuration, you will be prompted to enter the required setting group to which it will allocated.

CHAPTER 6

CURRENT DIFFERENTIAL PROTECTION

6.1 CHAPTER OVERVIEW

This product is used in combination with other similar devices to protect multi-terminal transmission and distribution lines and feeder circuits. The main protection type is numerical, phase-segregated, low-impedance, biased current differential. One product is needed at each terminal, and suitable communications are required to interconnect the devices. The maximum number of terminals that can be supported in a scheme is six.

Back-up protection is also included in this product. By default, the current differential protection is enabled, but it can be disabled if you don't want to use it. In contrast, most other protections are disabled by default, so you will need to enable them if you want to use them.

This chapter describes the functionality of the biased current differential protection. It outlines what the device does and how it does it, covering the following:

This chapter contains the following sections:

Chapter Overview 90
Current Differential Protection Principle 91
Implementation of Numerical Current Differential Protection for Multi-Termnial Applications 92
Current Differential Protection-Auxiliary Functions 121
Differential IED compatibility with previous versions 124
Communications Interfacing 125
Application Notes 127

6.2 CURRENT DIFFERENTIAL PROTECTION PRINCIPLE

Current differential protection is based on Kirchhoff's Law. It generally uses the Merz-Price principle in which the sum of the currents entering the protected zone should equal the sum of the currents leaving the protected zone. A difference between these currents is known as Differential Current. If the Differential Current exceeds a threshold, then a protection device may be required to operate (trip). If the Differential Current is below the threshold, then it is expected to restrain.

Errors caused by mismatch of the current transformers at the different terminals, or saturation of the current transformers during external faults could lead to unwanted tripping. To avoid this, a Restrain quantity is normally applied so that when the Current values in the system rise, so the levels of Differential Current necessary to cause tripping rise. The restraint applied is called Bias Current and its relationship with the Operate quantity is called a Biased Differential characteristic.

Current differential protection does not need voltage transformer inputs, but they can be employed to enhance capacitive charging, protection, control, automation, and supervision features of this product for certain applications.

To provide current differential protection of transmission lines and distribution feeders, it is normal practice to have similar devices at each terminal, with interconnecting communications links to exchange values of currents between terminals.

When applying numerical current differential to protection of transmission lines and distribution feeders, as well as communicating details of Current values, the product also communicates timing, status, and control data to remote terminals. The Current values, timing, status, and control data are encapsulated into messages (sometimes referred to as telegrams) which are transmitted frequently and regularly. The timing data is used to align local and remote current values. The control and status data is used for purposes such as intertripping. Messages are secured by an address field as well as a cyclic redundancy check code (CRC code). The use of the address field ensures that only the intended receiving device will respond to the message. Corruption of the data in the messages could potentially cause the product to trip incorrectly. The use of the CRC code together with other error checking prevents this.

6.2.1 NUMERICAL CURRENT DIFFERENTIAL PROTECTION

At each terminal in the scheme the power system Current values are acquired, converted into numerical equivalents, filtered, and compared with those from the other terminal(s) in the scheme.

For each phase, and at each terminal, the differences between the Current values flowing into the protected zone is calculated. This is known as the Differential current and provides an Operate quantity. Also calculated is the sum of the same current values and a proportion of the sum is used as a restrain quantity. This is known as the Bias Current. To determine whether tripping should occur, the Differential Current is compared with a percentage of the Bias Current.

If it is exceeded, then a trip can be initiated. The Differential and Bias currents are calculated on a per phase basis, and the tripping decision is made on a per phase basis. However, the Bias current used in the calculation is the same for all three phases and is based on the highest of the Bias currents calculated for each phase. This is called Maximum Bias and improves discrimination for single phase faults.

Line differential protection requires the comparison of Current values taken at the different line terminals. For a meaningful comparison, synchronisation of the Current values is needed so that they are related to a common time reference. Common referencing may be achieved through different methods. In numerical line differential protection devices this is usually achieved using proprietary software to implement established techniques.

6.3 IMPLEMENTATION OF NUMERICAL CURRENT DIFFERENTIAL PROTECTION FOR MULTI-TERMNIAL APPLICATIONS

The following figure illustrates the principle of current differential protection based on Kirchoff's Law. In the illustration, the protection is applied to a line connecting two terminals experiencing current flows I1 and I2 as shown. The cases represent three scenarios of interest:

- A healthy system for which the protection should not trip
- An unhealthy system with a fault applied inside the zone of protection (internal fault) for which the protection should trip
- A system with a fault applied outside of the protected zone. Since the fault is outside of the protected zone, it is referred to as an external fault for which the differential protection should not trip.

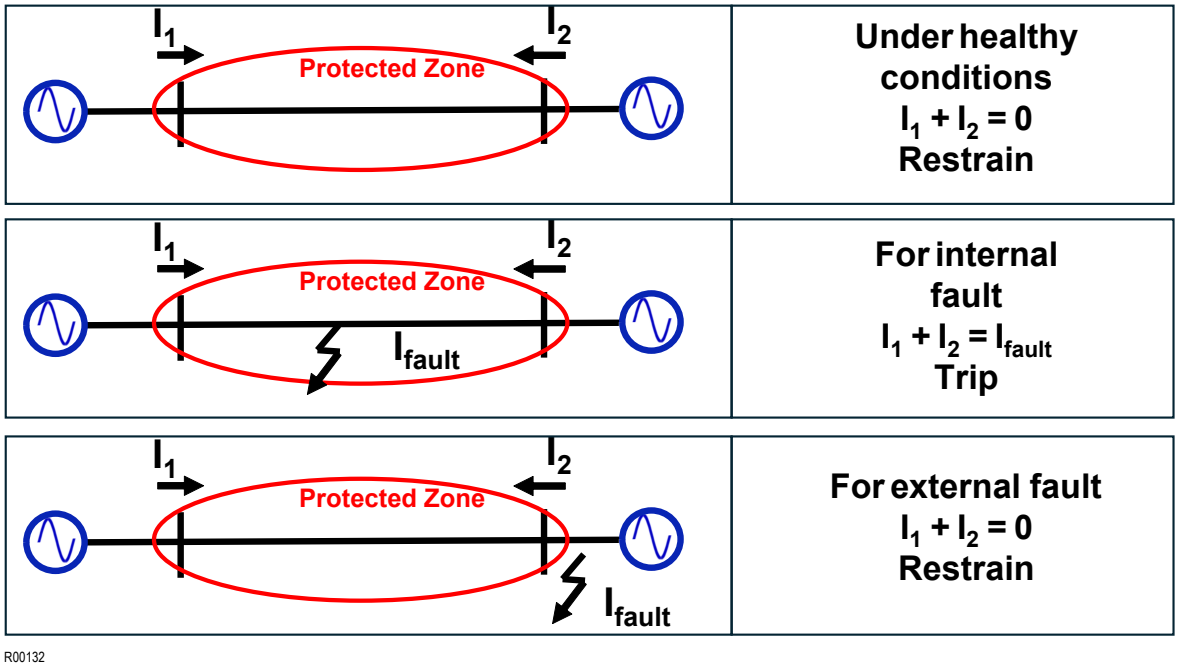


Figure 33: Illustration of principle of current differential protection applied to a transmission line

The operating principle is based on summing all the currents entering the protected zone and comparing them with a threshold which, in a perfect scenario should be 0A. For the ideal cases shown in the figure, the protection response is correct.

The principle can be easily extended to multi-terminal networks (such as that shown in the following figure) by extending the summation to include currents flowing at all terminals in the protected scheme.

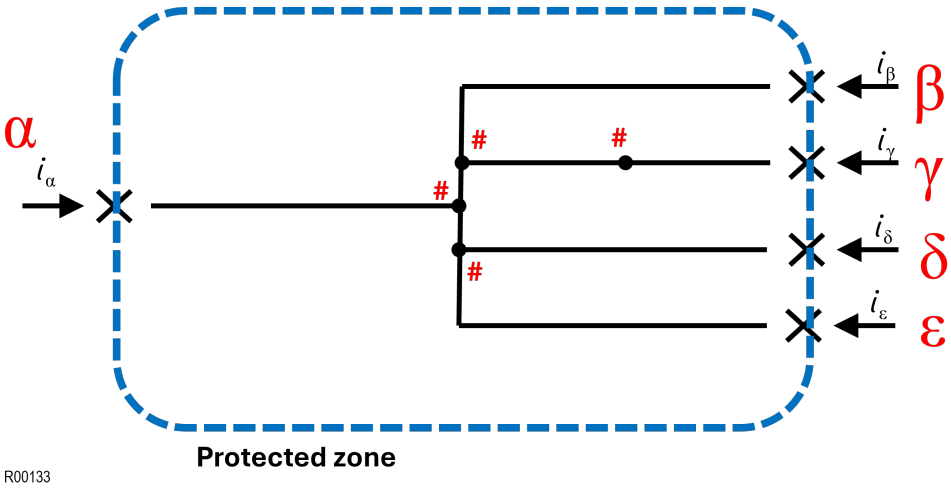


Figure 34: Multi-terminal network suitable for protection using current differential principles

To protect multi-terminal networks such as the one shown in the previous figure using this product, a scheme must be created using one device from this product range at each terminal in the network. The maximum number of terminals in a network that can be protected by this product is six; the minimum number is two. Internal junctions (or nodes) within the network connect the terminals together and the maximum number of junctions (nodes) is limited to four. The example shown represents a network having five terminals (labelled α, β, γ, δ, & ε) connected via four internal junctions/nodes (identified by #). This configuration is considered typical and is chosen for demonstration purposes only.

For each phase, and at each terminal, the protection device calculates the differences between all the currents entering the protected zone. This is known as the Differential Current and it provides an Operate quantity for the protection. Also calculated in the same devices are the sums of the rms (root mean square) magnitudes of all the currents entering the protected zone. A proportion of the sum of the rms magnitudes is used as a quantity to restrain operation of the protection. This restraining quantity is referred to as the Bias Current. To determine whether tripping should occur, the Differential and Bias Currents are compared against a tripping characteristic threshold. If the Differential Current exceeds the threshold, then the devices would be expected to operate (trip). Otherwise, the devices would be expected to restrain. The tripping characteristic is critical to ensure reliable operation of the protection as the magnitudes of the currents experienced on the network varies.

Current differential protection generally connects using conventional protection current transformers (CTs) which are prone to errors. These errors affect the accuracy (and hence reliability) of current differential performance. The CT errors which most affect the accuracy of current differential protection are caused either by mismatch of the CT transformation ratios or by waveform distortion caused by saturation of the magnetic cores. The latter is particularly important since there are multiple CTs in the scheme, and saturation will affect them all differently. The distorted output currents from CTs will result in incorrect differential currents being calculated. The result can be either unwanted operation for external faults (unwanted tripping), or failure to trip for internal faults. Inclusion of bias current quantities into the comparison helps to stabilise the protection against these unwanted effects. Operation of this product is based on a dual slope biased differential characteristic to determine tripping as presented in the following figure.

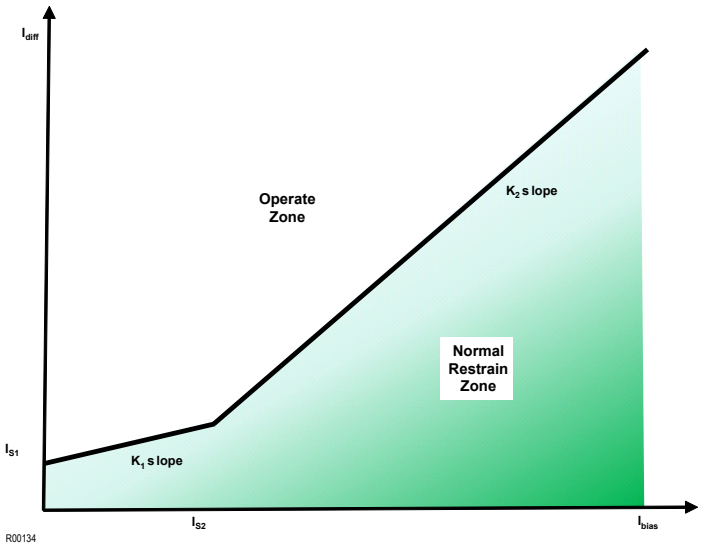


Figure 35: Basic biased differential characteristic

The differential and bias currents are calculated on a per-phase basis. Tripping decisions are also made on a per phase basis but, to aid stability, the differential comparison is made between each individually calculated phase differential current, and the maximum value of bias current calculated on any of the phases. This technique is referred to as Maximum Bias and is adopted since it provides improved discrimination for single-phase faults.

6.3.1 MULTI-TERMINAL NUMERICAL CURRENT DIFFERENTIAL PROTECTION DESIGN

The following diagram shows component blocks that collectively contribute to the current differential protection functionality implemented in this product:

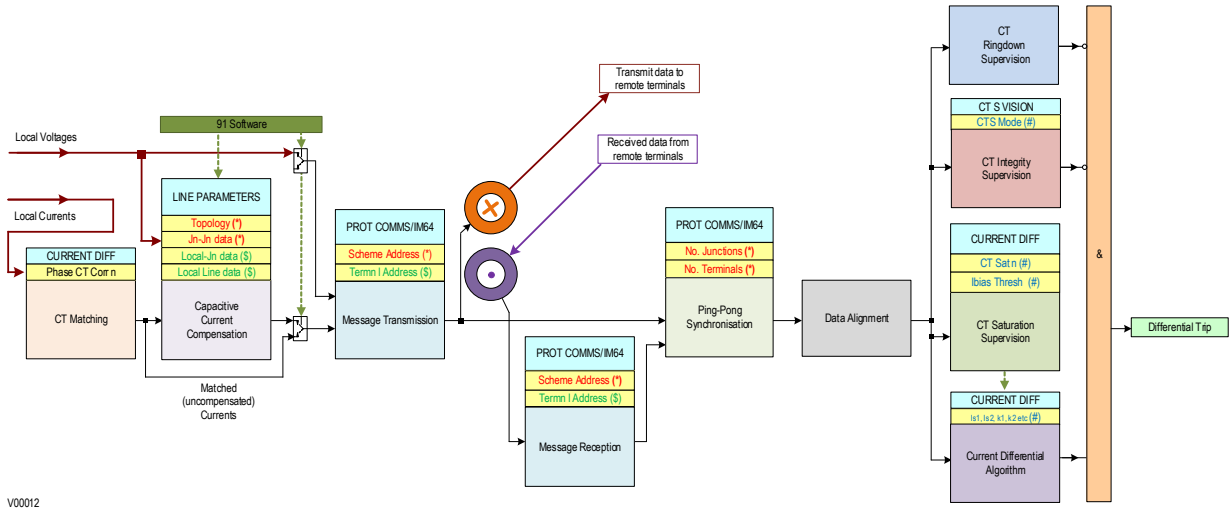


Figure 36: Functional block diagram of multi-terminal numerical current protection

The previous figure shows the functionality of one device associated with one terminal of the protection scheme. The devices fitted at the other terminals in the scheme will share similar functionality. To assure similarity of performance of the different devices and, therefore, the effectiveness of the protection scheme, a co-ordinated approach to configuring and setting the devices in the scheme is required. This requires that the network to be protected is defined, configured, and set consistently across all devices in the protection scheme. This is assured by representing the protection scheme according to strict topology definitions. Topology rules apply to both the

electrical network and the communications network. A consequence of the topologies imposed is that there is an order of precedence associated with setting the different devices in the scheme. This section presents the product design. Sub-sections explain the functionality of the design's component blocks, introduce topology, and outline an order of precedence that must be observed when configuring the protection scheme and setting the devices.

The differential protection always requires current inputs. In the case of applications that require capacitive charging current compensation, voltage inputs are also needed. These inputs are shown as Local Currents and Local Voltages in the functional diagram. The details of how these input streams are acquired are not described here. Please refer to the chapters on Hardware Design and Software Design for more detail. It is important to note here, however, that the times at which the inputs are sampled across the different devices are not synchronised. Since the current signals at each device are time varying, it is critical that, for accurate calculation of differential and bias currents, the various current signals involved are referenced to a common time base. Since sampling of the current signals at the different devices is not synchronised, a different method of synchronising current data streams is required ahead of the differential calculations and algorithms being applied. In this product the synchronisation is performed in software. There is no need for any external input (such as GPS) for the current differential synchronisation (nor indeed is there any option to apply one).

As well as not showing the raw analogue data acquisition, the functional diagram also does not show the impact of topology on the operation of the devices. In many respects, however, these are the glue that holds the different blocks together and so an introduction to topology is provided, ahead of an outline of:

- Sampling of Current Signals

and the following functional block descriptions:

- Compensating for Different CT Ratios
- Communication of Current Signals
- Synchronisation of Current Signals
- Simple Biased Current Differential Characteristic
- Capacitive Charging Current Compensation
- CT Saturation
- CT Ringdown
- Current Transformer (Circuitry) Supervision
- Switching Communications Paths Compensation
- Complete Biased Current Differential Characteristic

6.3.2 MULTI-TERMINAL CURRENT DIFFERENTIAL PROTECTION SCHEME TOPOLOGY

When designing a multi-terminal current differential protection scheme, it is important to ensure that all devices in the scheme can work together correctly and consistently. This requires that the configuration and settings of all devices are properly determined and applied. An approach based on co-ordinating the physical, electrical, and communications connections of the protected network is employed. A topology approach to consistently describe the electrical network is combined with similar for the communications arrangements to provide a methodology for designing and configuring the protection scheme and its contributing devices. It is important to recognise that the devices must be set and configured as part of a scheme design approach. Without an understanding of the electrical network arrangement and the communications network arrangement and how they combine, individual device settings associated with the multi-terminal current differential protection scheme just won't make sense.

The following two sub-sections will describe the topological approach applicable to this product.

6.3.2.1 ELECTRICAL NETWORK TOPOLOGY

The type of electrical network that this product is intended to protect will, in all but the simplest of cases[1], consist of multiple inter-connected electrical terminals and junctions (nodes). Typically, the network is presented as a single-line diagram (SLD).

Note:
[1] The simplest case is a two-terminal line in which both terminals are directly connected together with no intermediate junctions.

The SLD resembles the physicality of the network but restricts itself to showing only a single-phase conductor. An example is shown as the 'SLD Network model' in the following figure:

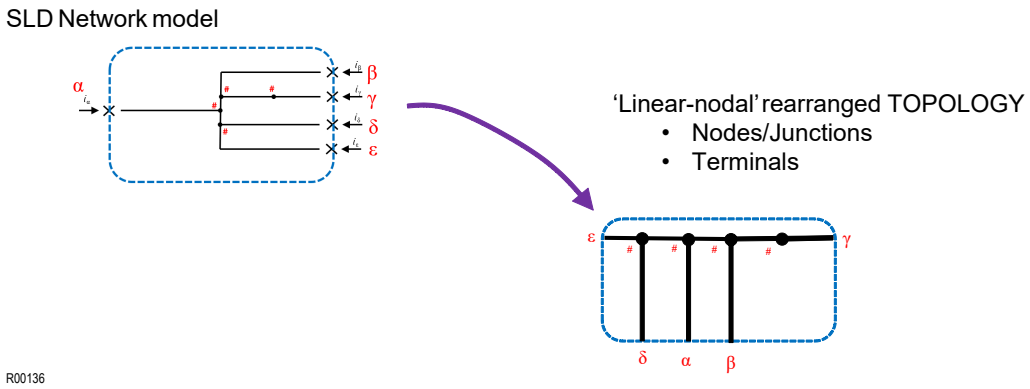


Figure 37: Electrical network rearrangement into linear-nodal presented topology

The SLD Network model (on the left of the figure) shows a multi-terminal network that is to be protected by devices at its five terminals (α, β, γ, δ, & ε). Each of the devices in the protection scheme needs information about how it and the other devices in the scheme connect into the network. But the arrangement shown does not lend itself to a simple system for uniquely and consistently identifying and referencing each specific terminal and junction across all devices in the scheme. Consider, however, rearranging the visual layout to be like the one shown on the right-hand side of the figure. Here, the internal junctions connect linearly between two opposing terminals at the edges of the network. Now the junctions can be unambiguously ordered and labelled according only to their horizontal position. The terminals are also horizontally ordered and so can also be unambiguously labelled and referenced. This linear ordering of the junctions into a 'Linear-nodal' rearranged topology allows each terminal and junction to be uniquely and unambiguously identified.

Applying the linear-nodal rearrangement to the five-terminal network example introduced previously, the layout shown in the following figure can be developed. The junctions are labelled 1 - 4 (left to right), and the terminals are labelled 1 - 5 (left to right). The junctions and terminals must be inter-connected to define the logical assignments to maintain the functionality of the network. The line sections making these connections are also shown in the figure.

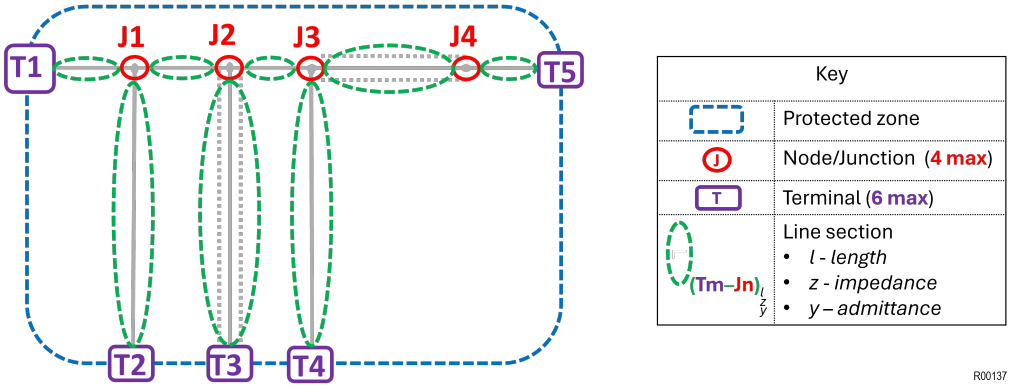


Figure 38: Terminal, junction, and line section logical assignments to electrical network topology

Within the topology shown in the previous figure, the attributes of each line section (length, unit impedance, and unit admittance) are defined. In the example, the line sections connecting to J4 are of different construction, showing

how the topology representation can accommodate different sections of line construction type (for example a composite overhead line/underground cable) section without having to add additional terminal devices.

Programming the information about the positions of the terminals and junctions, and their interconnectivity relationships and parameters, into each of the devices means that each device in the scheme can have the same consistent model of the network within its configuration and settings. The logical ordering and referencing of the terminals and junctions allows their interconnectivity relationships to be defined and presented in a bit-stream pattern referred to as the Topology matrix. An example is provided in the following figure:

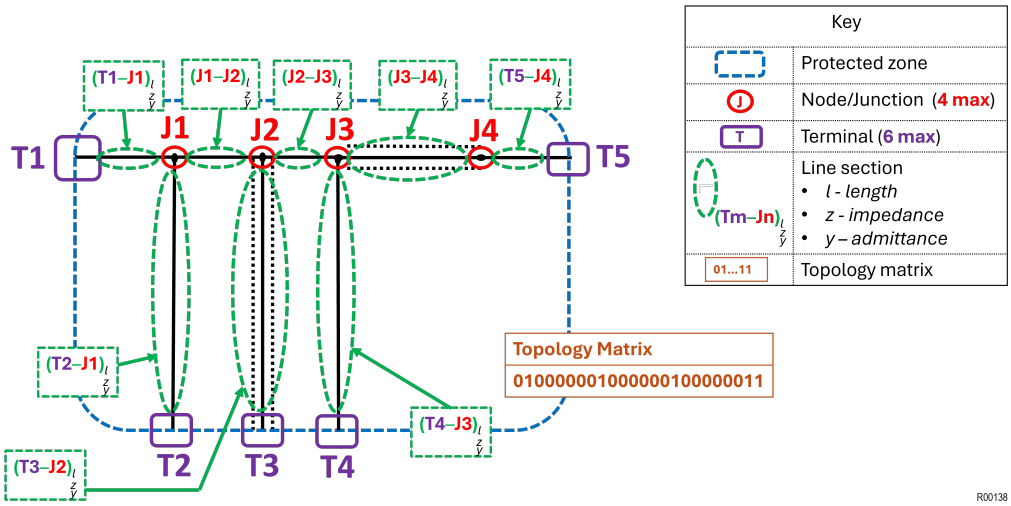


Figure 39: Electrical network topology line section parameterisation and topology matrix illustration

The figure above shows a topology example for a multi-terminal line differential scheme. The presentation of the network has been arranged to provide a linearly ordered sequence of junctions running from left to right. The terminals and junctions are numbered sequentially from left to right. The line parameters for each section (either terminal-junction or junction-junction) have been added. The model is completed by the Topology Matrix which defines the interconnectivity associations between the various junctions and terminals as a bit-stream, and which is common to every device in the scheme.

Starting from the least-significant-bit (LSB), each bit in the Topology Matrix represents an association between a terminal and a junction (for example, T1-J1 represents connection between terminal T1 and junction J1, similarly with T2-J1 for terminal T2 and junction J1, up to the maximum T6-J4). Setting the bit (1) indicates that the connection is made. Not setting the bit (0) indicates that the connection is not made. Junction-junction connections do not need defining since the topology is underpinned by a 1-to-1, junction-to-junction, linear nodal arrangement. The following figure illustrates how the Topology Matrix and the line section parameters are programmed (through MiCOM Agile S1) and includes the derivation of the Topology Matrix applied in the previous figure.

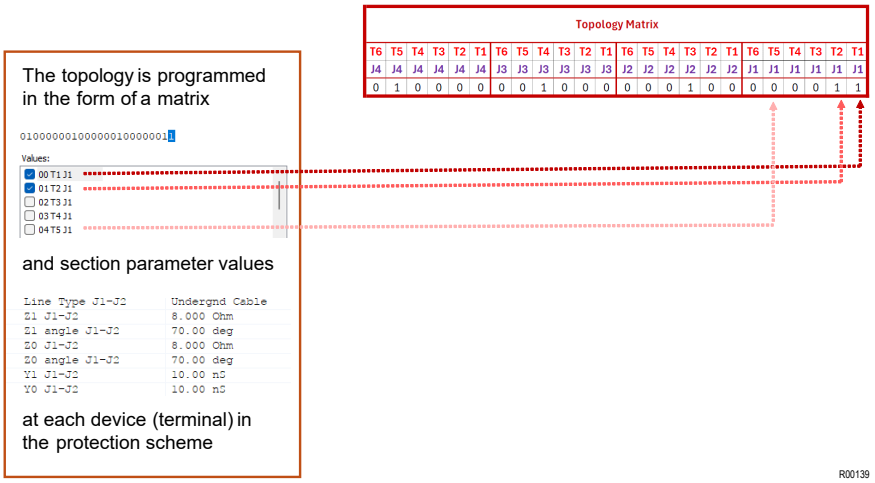


Figure 40: Protection scheme electrical network topology matrix

6.3.2.2 COMMUNICATIONS NETWORK TOPOLOGY

Multi-terminal current differential protection requires the various devices in the scheme to share information. Each device has a dual-channel PROT COMMS/IM64 communications port that is dedicated for this purpose. The physical connections and the logical connections of the communications ports need to be carefully configured to ensure that the protection scheme will operate correctly. A communications topology helps assure this. The communications topology is applicable to both the physical and the logical connections.

The PROT COMMS/IM64 interface is presented via fibre-optic media in accordance with the IEEE standard C37.94. It is suitable either for direct (dark) fibre connection between devices or using suitable C37.94 compliant network services. A two-terminal scheme is a special case that requires one device to connect only to one other device and so only point-to-point connection is needed. With more terminals in the protection scheme, and a requirement for each terminal to exchange data with every other terminal in the scheme, it is not possible to make all the data exchanges with point-to-point connections when each device has only two physical connections. To overcome the limitation on physical ports whilst satisfying the need to share all information between all devices, communications are arranged in a ring structure. As shown in the following figure, having two channels on each device enables a dual-ring structure to be implemented which can provide redundancy in the event of one of the links failing. The two channels are identified as channel 1 (Ch1) and channel 2 (Ch2). It is important to note that, with only one exception, Ch1 on one device should always be connected to Ch2 on an adjacent device. The exception is in the case of a simple two-terminal protection scheme with just a single channel of communications (i.e. no communications redundancy) for which each device connects only via Ch1. The following figure illustrates the arrangement for an example five-terminal scheme.

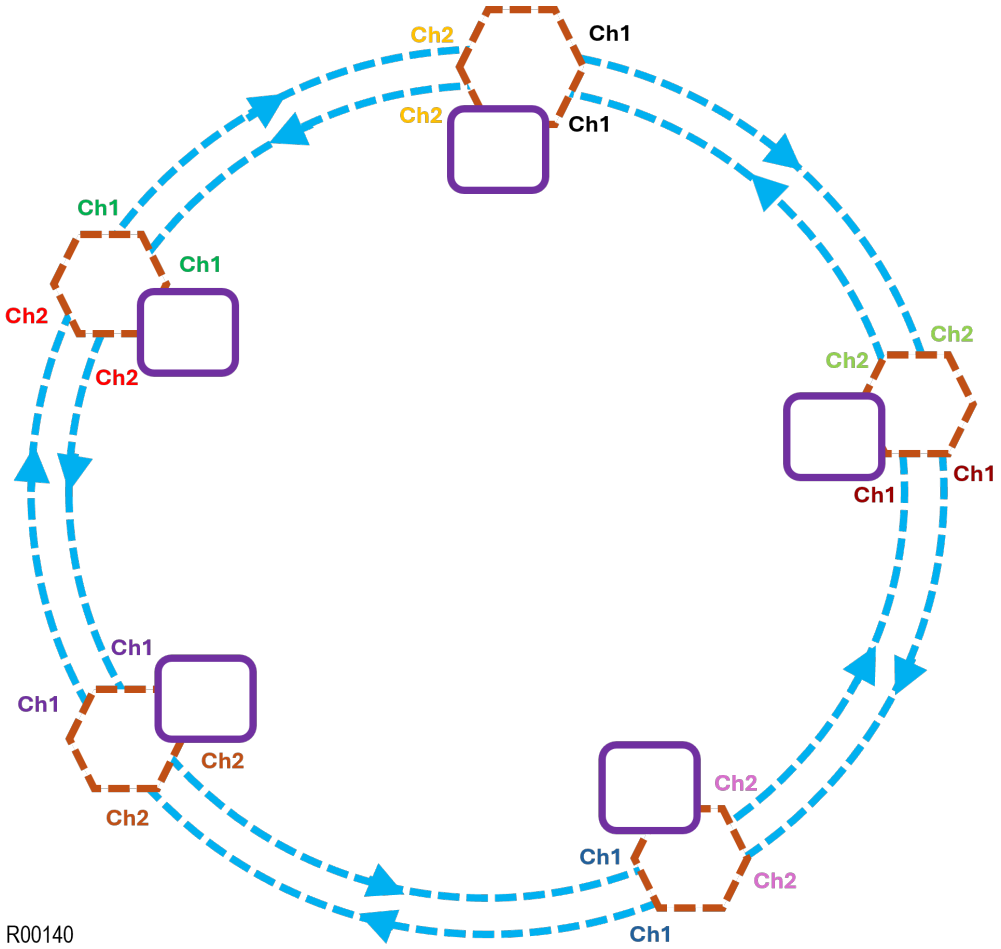


Figure 41: Dual redundant ring communications network topology

To ensure correct scheme operation, a mechanism is needed to ensure that the information conveyed over the PROT COMMS/IM64 is delivered to, and processed by, its intended destination. This is achieved by a message identification system that uses scheme and device addresses that are set in the ***PROT COMMS/IM64*** settings. To distinguish between devices in one scheme from those in another, they should be set to have different schemes. The scheme addresses are set by assigning an integer number value between 0 and 15 (the default is 1) to the ***Scheme Address*** setting in the *PROT COMMS/IM64* column. Different devices within a scheme should be set to have the same ***Scheme Address*** but need to be individually identified. This is achieved by setting the ***Terminal Address*** value found in the *PROT COMMS/IM64* column of each device to a different value. The ***Terminal Address*** values are set by assigning a letter from a choice provided. Up to six ***Terminal Address*** values are available. They start from A (the default), progressing sequentially according to the number of terminals in the scheme which, in the maximum case of six terminals is F.

As indicated in the previous figure, devices' communications must be connected in a ring structure. As well as the Ch1-Ch2 connectivity convention, there is also a convention for the allocation of terminal addresses in the scheme. This requires that the physical connections of the devices align with the sequencing of terminal addresses. To ensure this, device with ***Terminal Address*** set to *A* must connect with device with ***Terminal Address*** set to *B*. With more devices in the ring, the convention must continue so that *B* connects to *C*, and (where applicable) *C* to *D*, *D* to *E*, etc., until the last device in the ring completes it by connecting back to *A*.

There is no absolute requirement that the allocation of terminal addresses in the scheme marries to the terminal numbers allocated in the electrical network topology, but adopting such an approach simplifies understanding and is recommended. The following figure illustrates the different possibilities for terminal numbering and addressing, and channel allocation and connection. **GE Vernova recommends ONLY the top 'correct' configuration**. The other

possibilities are provided since they may provide a useful reference for troubleshooting during installation and commissioning in case communications cannot be correctly established.

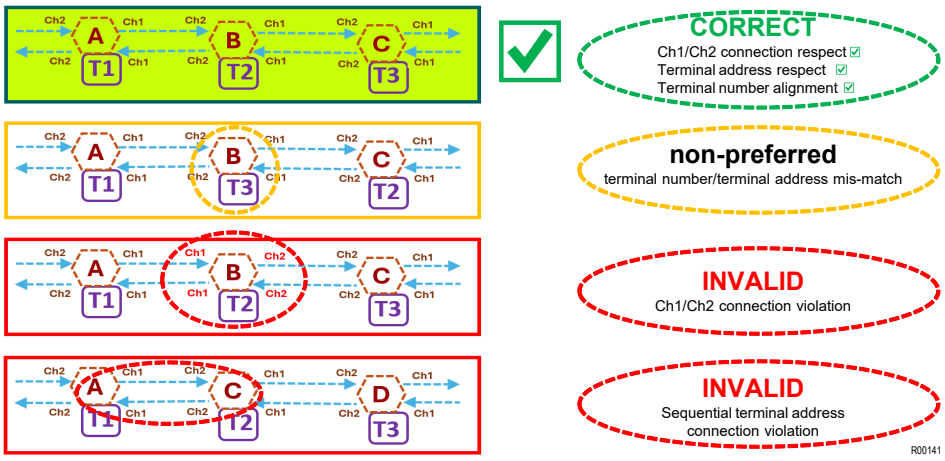


Figure 42: Communications network topology connectivity conventions showing correct, less preferred, and invalid arrangements

The following figure illustrates how the electrical network and the communication network topology approaches are recommended to be combined to simplify configuration of devices in the example five-terminal protection scheme.

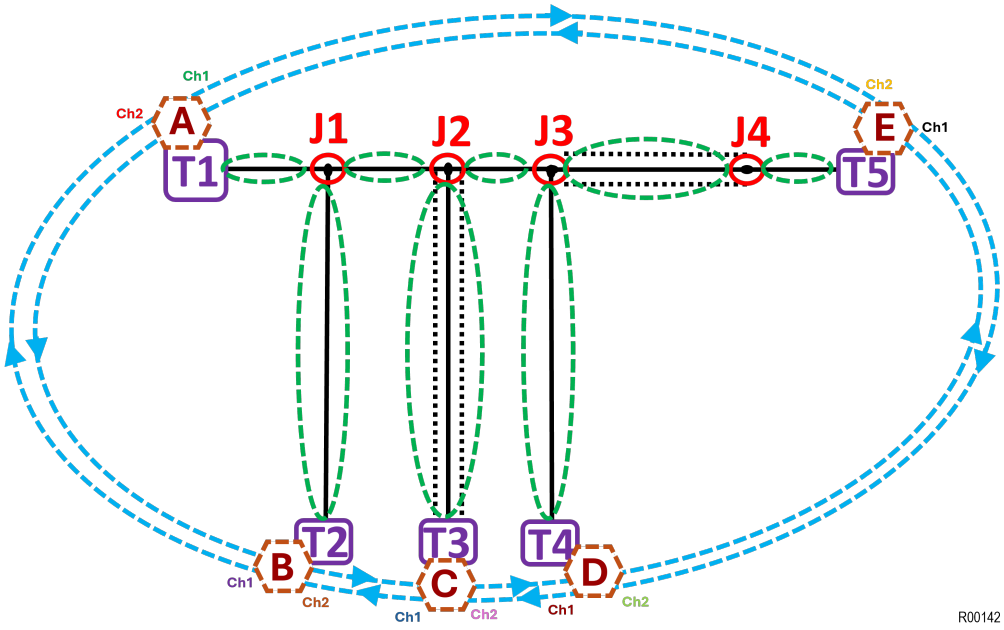


Figure 43: Combined electrical and communications networks topology

All configuration and settings associated with the electrical network and communications topologies must be confirmed before the other functional blocks associated with the differential protection are attended to.

To summarise: An holistic approach is required to determine the necessary configuration and settings which must be deployed across all devices for them to function correctly together as a multi-terminal current differential protection scheme. Application of the topology conventions according to the following list should ensure this:

In the *PROT COMMS IM64* settings:

- ***No of Junctions***
- ***No of Terminals***
- ***Scheme Address***
- ***Terminal Address***

In the *GROUP N LINE PARAMETERS* settings:

- ***Topology***
- *LENGTH LOCAL* (the length of the line from the terminal to the connected junction) together with the following data for this line section:
  - ***Line Type Local***
  - ***Z1Local***
  - ***Z1LocalAngle***
  - ***Z0Local***
  - ***Z0LocalAngle***
  - ***Y1Local***
  - ***Y1Local***

and in the case of more than one junction in the network topology, for each connected pair of junctions:

- ***Line Type Jm - Jn*** (where m and n are the (sequential) junction numbers) together with the following data for this line section:
  - ***Line Type Jm - Jn***
  - ***Z1 Jm - Jn***
  - ***Z1 angle Jm - Jn***
  - ***Z0 Jm - Jn***
  - ***Z0 angle Jm - Jn***
  - ***Y1 Jm - Jn***
  - ***Y0 Jm - Jn***

Thereafter other settings should be deployed to tailor the differential protection functional blocks according to the application needs. Engaging with the following subsections to guide the process.

6.3.3 SAMPLING OF CURRENT SIGNALS

Before applying current differential algorithms, numerical values of the current signals involved must be obtained. The analogue-to-digital conversion process that provides this service involves continually sampling the input waveforms at regular intervals before representing the instantaneous magnitudes of the signals in digital form as numbers. The times at which the current inputs are sampled in this product are not synchronised to a common clock reference - neither internal, nor external (for example in the form of GPS or PTP). The acquisition processes run independently, and asynchronously, in each device. Current differential algorithms require comparisons of current signals taken from all terminals in the scheme. For the comparison to be accurate, the comparison must be made using signals that are correct at the time at which the comparison is made. But, since the sampling process occurs at different times across all phases and across all terminals in the scheme, some form of signal alignment is required before the differential algorithm can be applied.

In this product, the alignment of samples before the current differential algorithms are executed is performed in software. Even though there is no common clock reference, by time-tagging the sampled inputs signal streams at each of the devices at the point of acquisition, and by measuring and compensating for the time taken to execute certain critical actions, necessary alignment can be achieved. To support this, at each terminal, when current signals are acquired, they are qualified with a local time tag (Ttag) as illustrated in the following figure:

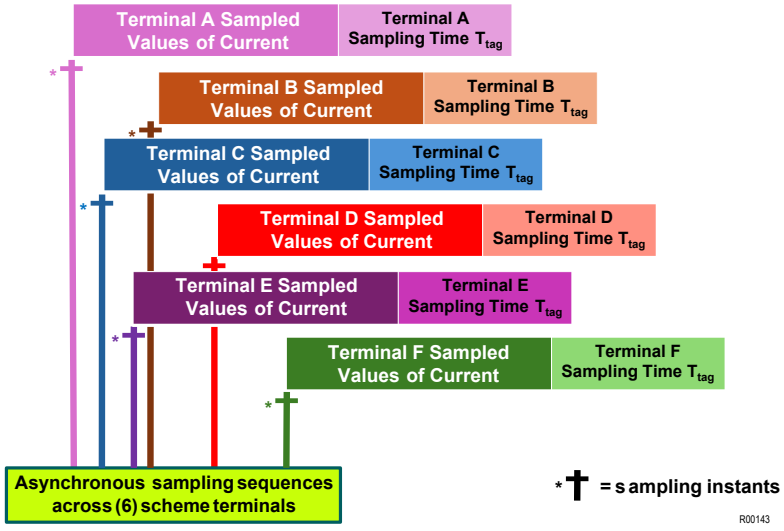


Figure 44: Illustration of non-synchronised acquisition of current signals across six-device multi-terminal differential scheme

6.3.4 COMPENSATING FOR DIFFERENT CT RATIOS

The *primary* and *secondary* ratios for the phase current transformers are set in the *CT AND VT RATIOS* column. These settings are used to display the phase current quantities in the *MEASUREMENTS 1* column. The device can be set to display the input current either in *primary* values or in *secondary* values.

To prevent incorrect operation of the differential elements, when there is no internal fault present, the currents into the differential elements of the devices balance. If the CTs have different ratios this will not be the case. This product can apply ratio (magnitude) compensation to the phase CT input signals to overcome this problem. Compensation is achieved by applying a magnitude correction factor to the CT secondary outputs to ensure that the scaled currents used in the calculations of differential and bias currents correctly balance.

When calculating differential and bias currents, the devices use compensated per-unit (p.u.) quantities. If needed, CT ratio compensation is used to scale-up the local p.u. current signals to match the scaled equivalent currents received from remote terminals. Because of dynamic range limitations, scaled-up values are limited (clipped). The limit above which the compensated values are clipped is 40 p.u.

Similarly compensated p.u. values are used in the calculation of the differential and bias currents.

The per-unit compensated values of local and remote currents as well as the per-unit values of differential and bias currents are scaled-down by the local CT ratio correction factor and displayed in the *MEASUREMENTS 3* column.

The following figure illustrates the necessary scaling of the current inputs so that the displayed measurement values, and the compensation of the inputs to the differential calculation, are correct.

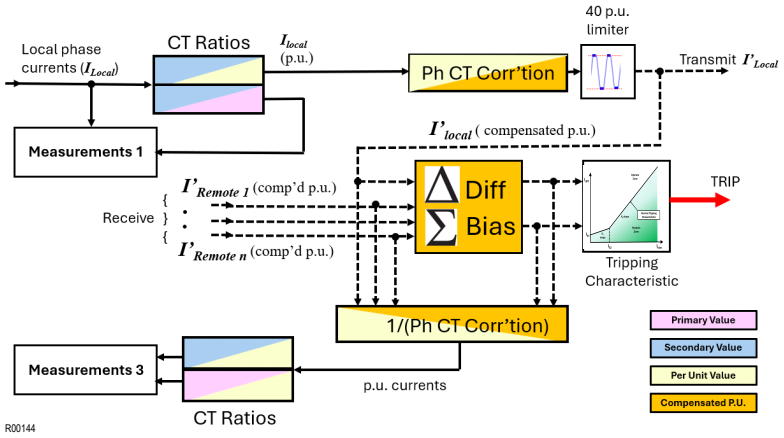


Figure 45: Current signal CT ratio compensation and scaling for differential-tripping and measurements functions

The ratios of the CTs locally associated to each device are set using the ***Phase CT Primary*** and ***Phase CT Sec'y*** settings in the *CT AND VT RATIOS* column of that device. If CT magnitude correction is needed, the compensation is applied using the ***Ph CT Corr'tion*** setting in the *GROUP N CURRENT DIFF* column of the affected device.

6.3.5 COMMUNICATION OF CURRENT SIGNALS

The compensated p.u. values of each of the current signals that are generated at each of the terminal devices need to be shared with all other devices in the scheme so that the current differential algorithm can be executed. Because of the need to time align current signals from different devices, time-tagging information also needs to be shared. The sharing of current signals is achieved using digital communications channels. Currents and time-tags are combined with other supporting data into packets of information which are then distributed according to the communications topology.

6.3.5.1 COMMUNICATION OF CURRENT SIGNALS - TRANSMISSION

Each device in the scheme needs to share locally obtained information with all other devices in the scheme. To distribute the information, a communications implementation compliant with international standard IEEE C37.94 [2] is used. To ensure correct connectivity of data between specific individual devices in the scheme, the critical device-specific data relating to terminal addresses, associated current signals and time-tagging information, data is packaged into terminal-aligned subframes of information.

Note:
[2] IEEE C37.94-2002 (R2008): IEEE Standard for N Times 64 Kilobit per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment.

An illustration of terminal-aligned subframe-encapsulated data packets is provided in the following figure:

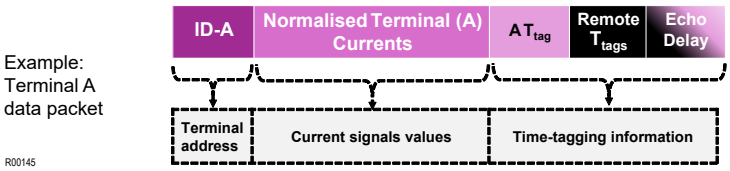


Figure 46: Terminal-aligned, subframe-encapsulated packet

The encapsulation of information into subframes is performed at each device in the scheme and is synchronised with the sampling of input data. Since the sampling is not synchronised across devices in the scheme, a snapshot across the scheme would reveal creation of similar, but non-synchronised, subframes at each device as represented in the following figure:

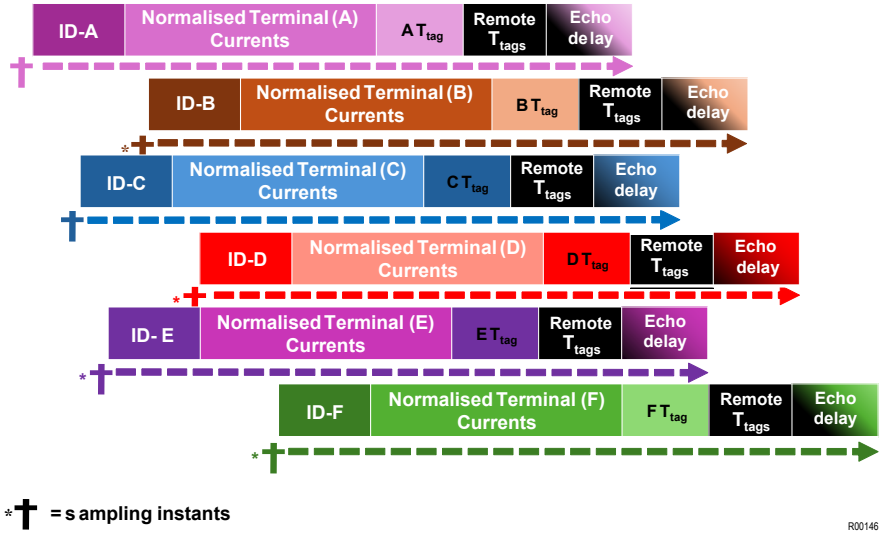


Figure 47: Creating subframes of encapsulated differential information signals for communication (between 6 terminal devices)

The encapsulated subframes need to be communicated between all devices in the scheme. For this, a ring communications architecture also based on IEEE C37.94 is used. The IEEE C37.94 implementation can be imagined as a pipelined transportation mechanism between devices as illustrated in the following figure:

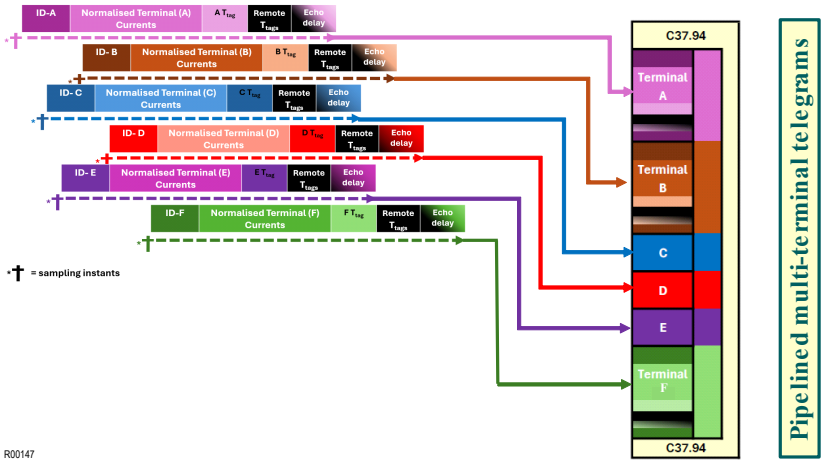


Figure 48: Pipelining of sub-framed differential information into IEEE C37.94 compliant telegram structure

At each terminal, associated subframes of information are removed from the pipeline, just as updated ones are added for distribution to service the other devices.

6.3.5.2 IEEE C37.94 REDUNDANT RING COMMUNICATIONS PRESENTATION

The packages of data transmitted on the IEEE C37.94 pipeline are referred to as telegrams. Telegrams are continually being communicated around all devices in the scheme. To improve scheme-availability in the event of failure of any single communications link, a dual-ring communications architecture is used. Within this dual-ring structure, subframes containing the differential information are constantly being uploaded to and offloaded from telegrams which, themselves, are continually being transported around the ring in both directions to provide redundancy. The concept is illustrated in the following figure:

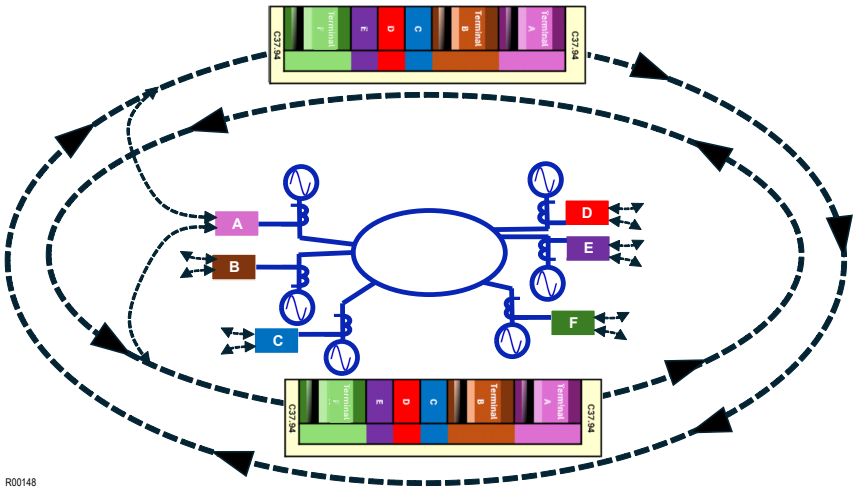


Figure 49: Communicating IEEE C37.94 compliant telegrams via dual redundant ring network

6.3.5.3 COMMUNICATION OF CURRENT SIGNALS - RECEPTION

As the pipeline of C37.94 compliant telegrams passes a connected terminal, subframes of differential information are uploaded and offloaded. Data from all remote terminals is required by the local terminal's differential protection algorithm calculations, and so the reception requires that all frames from all remote terminals be offloaded at all devices. The contents received from the telegrams are then unbundled into the separate subframes associated with each of the different specific remote terminals in the scheme. At this stage the separated frames of information contain time-tagging data, but no alignment has been implemented and so they remain 'asynchronous'. The following figure illustrates the unbundling effect performed on received communications at each terminal:

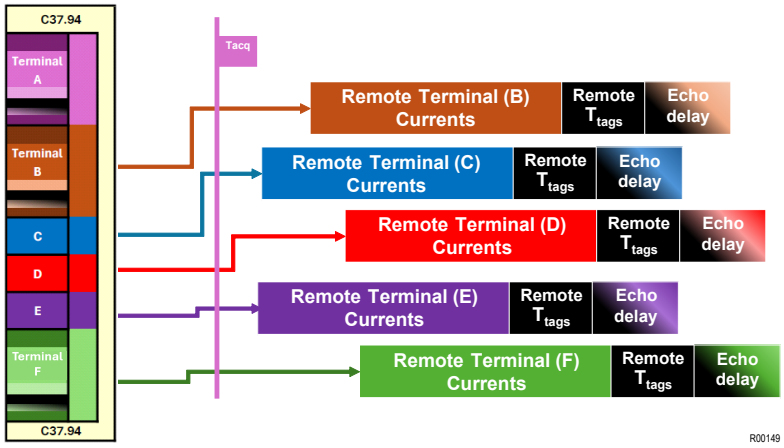


Figure 50: Multi-terminal differential protection telegrams reception and device-ordered data unbundling

6.3.6 SYNCHRONISATION OF CURRENT SIGNALS

Each device in a protection scheme provided by this product receives streams of sampled values of current inputs from all other devices in the scheme. At each terminal, this information is combined with local data for differential protection calculations. Before the calculations, however, the currents must be synchronised to a common time reference so that they will have the correct phase-relationship. This synchronisation is achieved through a two-stage process: The first stage calculates the relative time offsets of the current signal subframes created at the different terminals in the scheme. The second stage correlates the relative offsets against a fixed reference time point to deliver, at each terminal, a complete set of scheme-wise synchronised current signals.

6.3.6.1 RELATIVE TIME ALIGNMENT OF CURRENT SIGNALS

The first stage in the process to synchronise current signals from different terminals relative to each other. This method of time-alignment has been used in numerical line differential protection since the 1990s [3] and is referred to as ping-pong. The technique is based on sending and returning time tags between pairs of devices. Measuring and combining overall transmission times with the 'echo delay' time taken to reflect the signals back, coupled with an assumption that both directions of communication experience the same propagation delay time, then sampled data streams taken at both terminals can be time aligned with each other. The principle is outlined in the following figure:

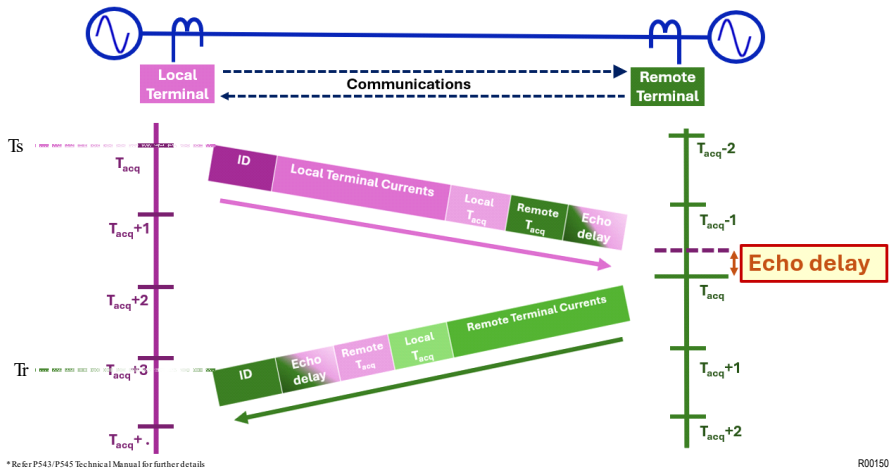


Figure 51: Illustration of 'ping-pong' method for current signal synchronisation between pairs of devices

Note:
[3] Refer to LFCB Service Manual Publication R5905 © ALSTOM T&D Protection & Control Ltd. 1998 (Pages 73, 74).

In this multi-ended differential product, the technique is applied at each terminal in a coupling between each terminal's local currents and all remote terminal currents. The output at each terminal is a data of all currents from all terminals aligned relative to each other. The principle is illustrated in the following figure:

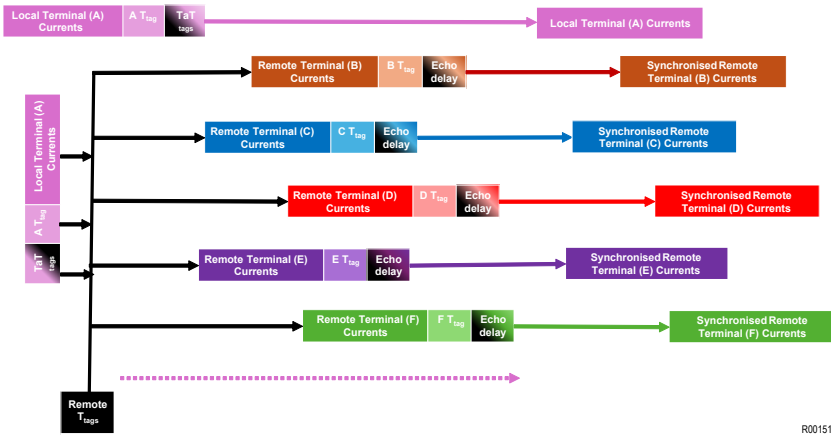


Figure 52: Relative time synchronisation between locally acquired current signals and remotely obtained equivalents

6.3.6.2 DATA FRAME ALIGNMENT OF CURRENT SIGNALS ACROSS SCHEME

The process to complete the alignment of current signals from different terminals adjusts the ping-pong aligned streams of local and remote current signals from all terminals to a common timing reference point. This is performed across all currents at each terminal and provides the time regulation for the current differential protection algorithms to be executed at each terminal. The principle is outlined in the following figure:

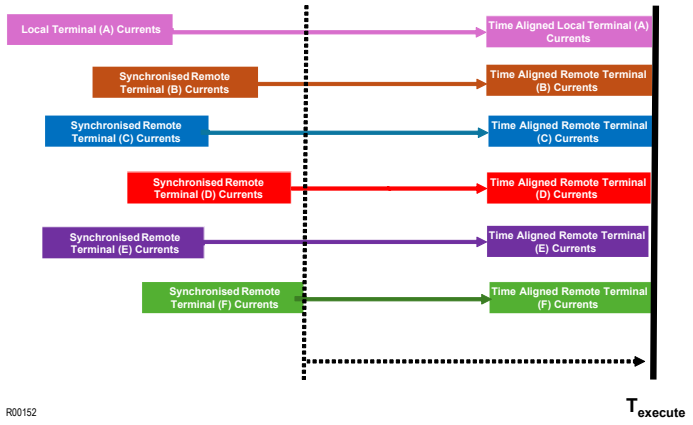


Figure 53: Multi-terminal data alignment

6.3.7 SIMPLE BIASED CURRENT DIFFERENTIAL CHARACTERISTIC

With all data streams aligned to a common time reference point, the current differential algorithm can be executed as per the following figure:

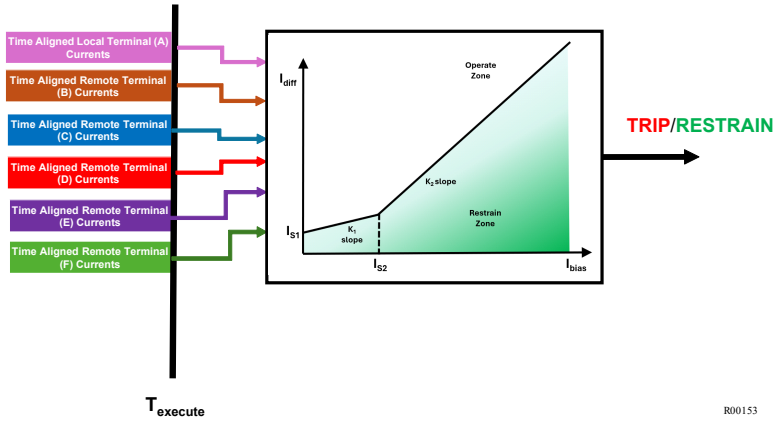


Figure 54: Processing of multi-terminal time-aligned data packets according to basic dual-slope biased current differential protection algorithm

The basic current differential algorithm requires that the differences between the currents entering the protected zone are calculated, and that the sums of the RMS (root mean square) magnitudes of all the currents entering the protected zone at all terminals are calculated. A differential (operating) current is formed from a proportion of the differences. A bias (restraining) current is formed from the sum of the magnitudes. The differential and bias currents are then compared against a dual-slope characteristic. The principle is outlined in the following figure:

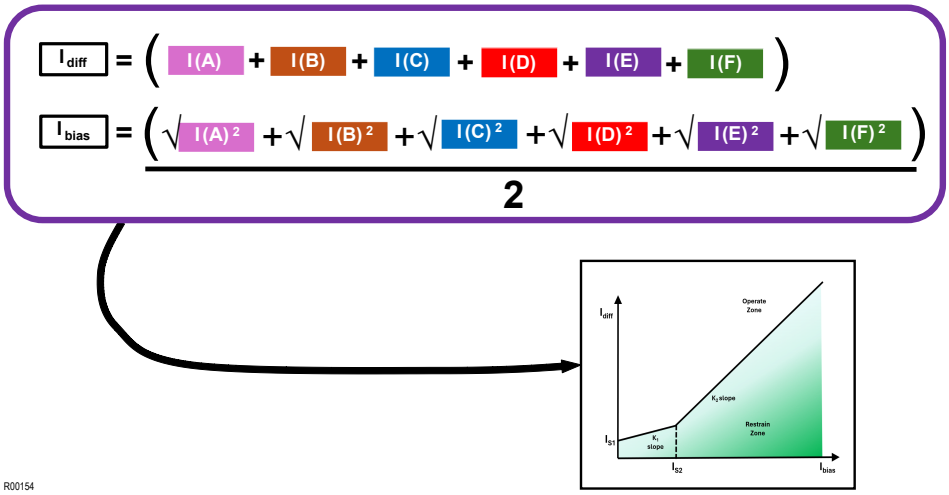


Figure 55: Outline of multi-terminal biased current differential protection implementation

6.3.7.1 CALCULATION OF DIFFERENTIAL AND BIASED CURRENTS

The multi-ended differential sample based algorithm employs the RMS value, in which the instantaneous differential current is the sum of instantaneous current of all terminals:

$$i_{diff}(n) = \sum_{m=1}^{M} i_{Tm}(n)$$

Where, i_{Tm} is the current of *m*th terminal; *M* is the number of terminals; i_{diff} is instantaneous differential current; *n* is present sample number.

The RMS value of the differential current is used for the discriminative criteria:

$$I_{diff}(n) = \sqrt{\frac{1}{N}\sum_{k=n-N+1}^{n} \left| i_{diff}(k) \right|^2}$$

Where, I_{diff} is the RMS value of i_{diff}; *N* is the window length in samples for RMS calculation, which is selected as a cycle of fundamental frequency; *n* is present sample; *k* is history sample number within the window length *N*.

Similarly, the I_{bias}, which is the sum of the RMS value of currents of all terminals:

$$I_{Tm}(n) = \sqrt{\frac{1}{N}\sum_{k=n-N+1}^{n} \left| i_{Tm}(k) \right|^2}$$

$$I_{bias}(n) = \frac{1}{2}\left[\sum_{m=1}^{M} I_{Tm}(n)\right]$$

Where, I_{bias} is RMS value of bias current; I_{Tm} is RMS value of i_{Tm}; *M* is the number of terminals; *N* is the window length in samples for RMS calculation, which is selected as a cycle of fundamental frequency; *n* is present sample number; *k* is the history sample number within the window length *N*.

6.3.7.2 DUAL-SLOPE BIASED DIFFERENTIAL CHARACTERISTIC

This product evaluates current differential protection against a dual-slope characteristic defined by four settings:

- ***Phase Is1***: The basic differential current setting which determines the minimum pick-up level of the protection.
- ***Phase k1***: The lower percentage bias setting used when the bias current is below the ***Phase Is2*** setting. This provides stability for small CT mismatches, while ensuring good sensitivity to resistive faults under heavy load conditions.
- ***Phase Is2***: A bias current threshold setting, above which the higher percentage bias setting ***Phase k2*** is used.
- ***Phase k2***: The higher percentage bias setting used to improve protection stability under heavy through fault current conditions.

Based on the analysis of the discriminative characteristic between internal and external faults, the discriminative criteria of the two stages of the differential protection are as defined and illustrated below:

For $I_{bias} < I_{S1}$:

$$Idiff \geq 1_{S1} + K_1 I_{bias}$$

For $I_{bias} \geq I_{S2}$:

$$Idiff \geq 1_{S1} + (K_1 - K_2) I_{S2} + K_2 I_{bias}$$

Where:

I_{diff}: The calculated differential current;

I_{bias}: The calculated bias current;

I_{S1}: The minimum threshold for differential current;

I_{S2}: The slope changing point (when the bias current is larger than this value, security is much more important than reliability for differential protection);

K_1: The slope of character when the fault is slight;

K_2: The slope of character when the fault is severe.

The settings for these parameters are in the *GROUP N CURRENT* column as follows:

- I_{S1} - ***Phase Is1***
- I_{S2} - ***Phase Is2***
- K_1 - ***Phase K1***
- K_2 - ***Phase K2***

Implementation is illustrated in the following figure:

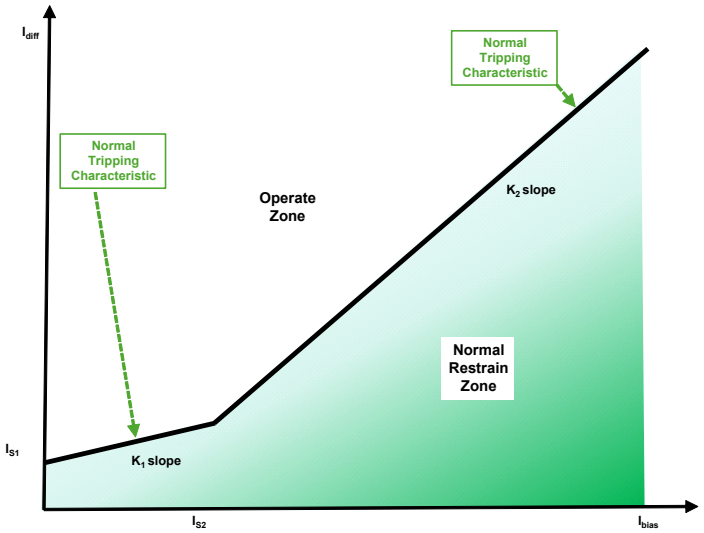


Figure 56: Basic dual-slope biased current differential protection characteristic

The value of the minimum setting threshold for differential current (I_{S1}) is required to be set higher than the maximum unbalanced current due to measurement and calculation errors. Normally, I_{S1} is set to be 0.1 ~ 0.5 p.u. to avoid unbalanced current.

When the fault is low, the bias current value will be smaller as well. In this case, reliability is more important than security, so that the slope of the character is smaller (Normally, K_1 is set to be 0.3 ~ 0.5).

On the other hand, when the fault is severe, bias current will be higher and security will become more important than reliability (in this case, the CTs could be unbalanced and saturated, which can result in much higher unbalanced current in I_{diff}), so the protection will follow the character of slope K_2, which has a much steeper slope (k_2 =1.0 ~ 1.5).

All the settings should be set following the best balance between the security and reliability.

When the phase-differential protection issues a trip command, it sends a per-phase ‘differential intertrip’ signal to the remote terminals to instruct them to trip their circuit breakers. This is to ensure that all ends of the protected line trip, even for marginal fault conditions.

For grading with other protection, the phase differential protection trip signal can be time delayed using either a definite time, or an inverse time characteristic. By default, the delay characteristic is set to definite time with a zero second delay, resulting in instantaneous tripping.

Since differential and bias current calculations are made on a per-phase basis, the values vary on a per-phase basis. For optimum stability the highest value of the three-phase bias currents is used to restrain all three phases.

6.3.7.3 CURRENT DIFFERENTIAL PROTECTION LOGIC

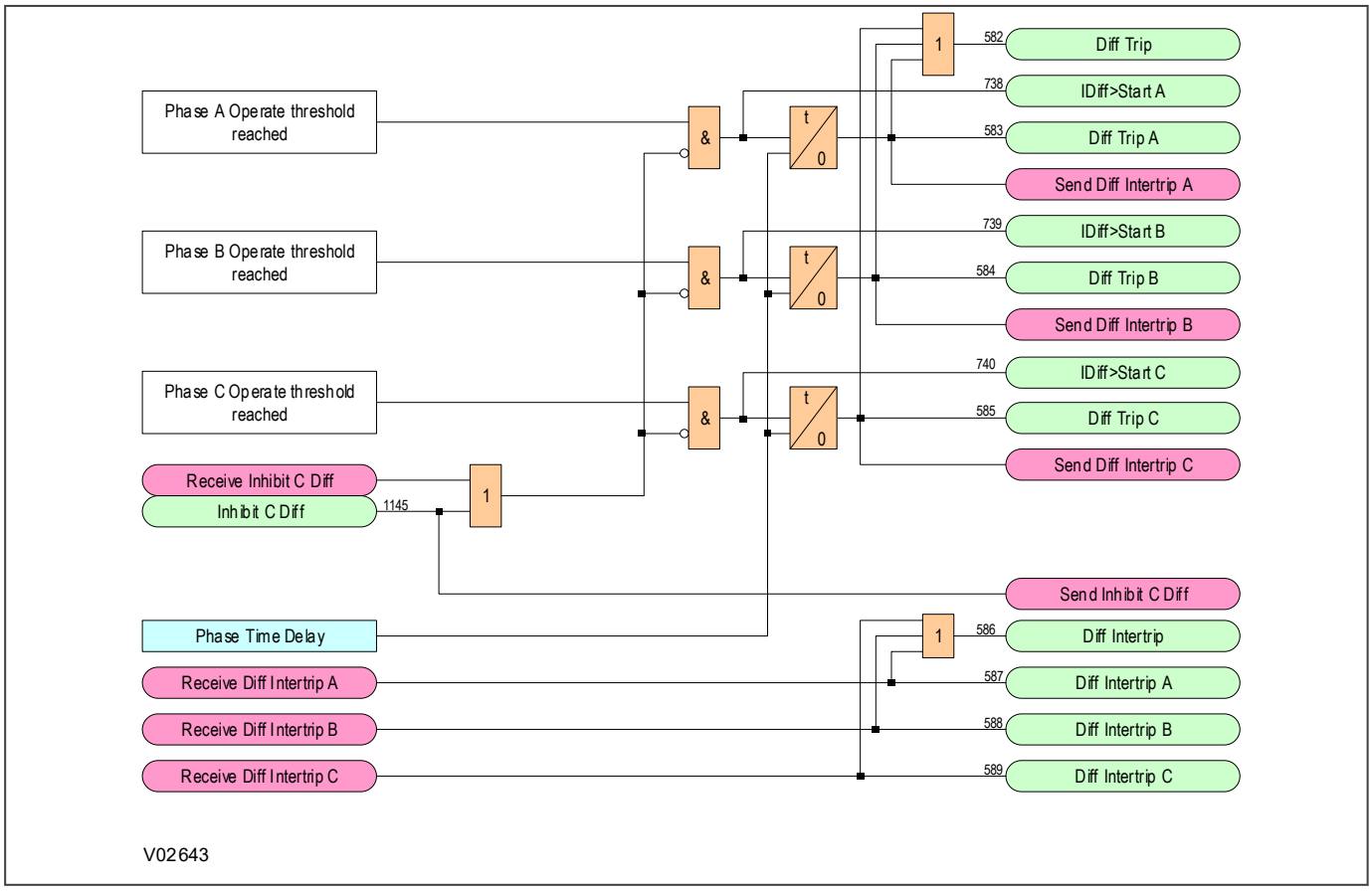


Figure 57: Current differential protection logic

6.3.8 CAPACITIVE CHARGING CURRENT COMPENSATION

All electrical conductors, including transmission lines and distribution feeders, are capacitively coupled to earth. When energised, a current flows from the conductor to earth to charge the capacitive circuit.

Both transient capacitive and steady-state capacitive charging currents exist. Transient inrush charging current consists of predominately high-order harmonics, which are generally suppressed by the high-frequency attenuating effects of the analogue current input circuits. The steady state AC charging currents, however, pass through the filters and their flow is sensed all the time that the feeder remains energised. This capacitive charging current appears as an additional differential current component when the currents at the terminals of a differential scheme are compared. On long overhead lines as well as on cable circuits, such capacitive charging currents can be sufficiently large to cause current differential elements to trip unwantedly under normal conditions. To avoid this, compensation is required.

The differential protection is most sensitive at low currents where the characteristic is dominated by the ***Phase IS1*** setting. The general guidance for setting I_{S1} is that if the minimum value should be 0.2 p.u. or 2.5 times the charging current of the circuit. As the capacitive currents increase, so too must I_{S1} if false tripping is to be avoided. This, however, reduces the sensitivity of the differential protection. With availability of phase input voltages, more effective compensation for capacitive charging current can be applied. Using voltage inputs in conjunction with details of the impedance and admittance of the circuit, the product can calculate charging currents. These can then be accounted for when calculating the differential currents.

The following figure shows a network with a mixture of overhead lines and cable circuits which could generate significant capacitive charging currents and for which compensation is required.

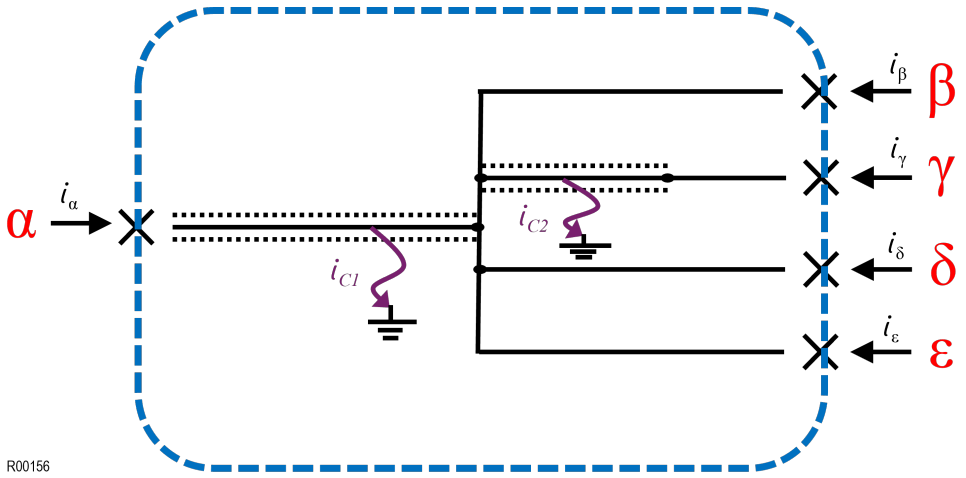


Figure 58: Illustration of capacitive charging currents in a multi-terminal electrical network

The following figure illustrates a lumped parameter model of the network demonstrating how the charging currents generate:

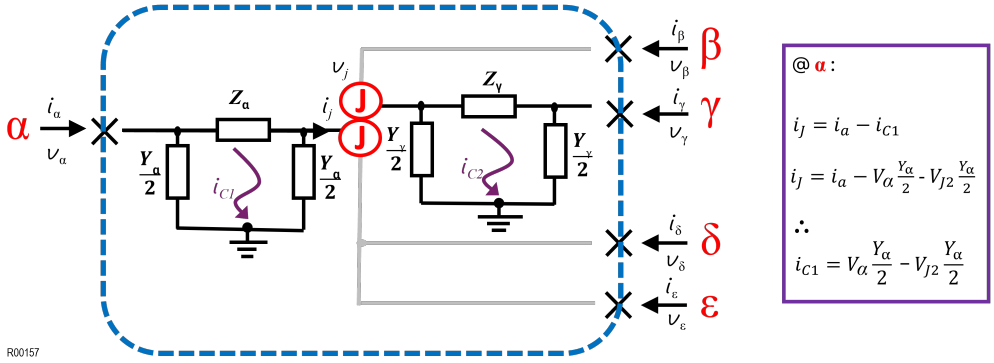


Figure 59: Simplified capacitive charging currents model for multi-terminal electrical network

With knowledge of voltage inputs and the circuit parameters at the affected terminals, and resolving across the network, the charging current components can be calculated.

By applying appropriately equipped products (i.e. with appropriate VT inputs and the capacitive charging current compensation feature) the necessary parameters can be set, and the scheme can be configured to provide appropriate compensation.

Where applicable, the feature is enabled with the ***Capacitor Comp.*** setting from the *GROUP N CURRENT DIFFERENTIAL* column. The circuit parameters required by the algorithm (admittances and impedances) are shared with those set as part of the electrical network topology configuration.

If the capacitive charging compensation is enabled, the current measurements in the *MEASUREMENTS 3* display compensated values.

Note:
For applications where capacitive charging current compensation is required, the feature should be enabled at all terminals (set ***Capacitor Comp.*** *to* `Enabled` *in the* ***GROUP n CURRENT DIFF*** *column of all devices).*

6.3.9 CT SATURATION

The basic dual slope biased current differential protection characteristic outlined previously is designed to provide restraint against errors caused by CT mismatch and mild saturation. The characteristic represents a compromise

between assuring stability for external faults whilst maintaining sensitivity for internal faults. The current differential protection in this product provides an additional layer of stability against the effects of current mismatch caused by CT saturation effects by implementing a CT saturation detector. If used, then if CT saturation is detected the tripping characteristic is modified to increase stability.

CT saturation is a phenomenon that occurs when, due to the operational state of the CT, a significant proportion of the current input is diverted to energising the magnetic core of the CT, rather than generating a replica output. It can be particularly onerous in current differential schemes when the CTs are subject to the same large through currents. Especially in the case of external fault currents with offset exponentially decaying components, the different CTs are likely to experience significantly different amounts of CT saturation. Saturation causes current to be diverted to energise the core, the output collapses to zero. With different amounts of saturation, different CTs will give different outputs - even though the inputs may be the same. The result for a differential scheme can be unwanted tripping for out of zone faults (or large loads). Outputs from saturated CTs exhibit quite distinctive characteristics. Detecting these provides an opportunity to stabilise the protection.

Compared with the output from an unsaturated CT, the output from a saturated CT is characterised by ‘gaps’ in the waveform. Considering a differential scheme with a pair of matched CTs such that, under ideal conditions, for an external fault, the difference between the outputs should be zero differential current. Now, if, with the same inputs applied, one CT saturates but the other doesn’t, then there will be a difference between the outputs. The difference between the unsaturated output, and saturated output appears as a gap. The gap would generate false differential current with the potential to cause false tripping. This product senses CT saturation by detecting such gaps. If CT saturation is detected, the tripping characteristic is modified to provide additional restraint.

The following figure outlines the recognition principle:

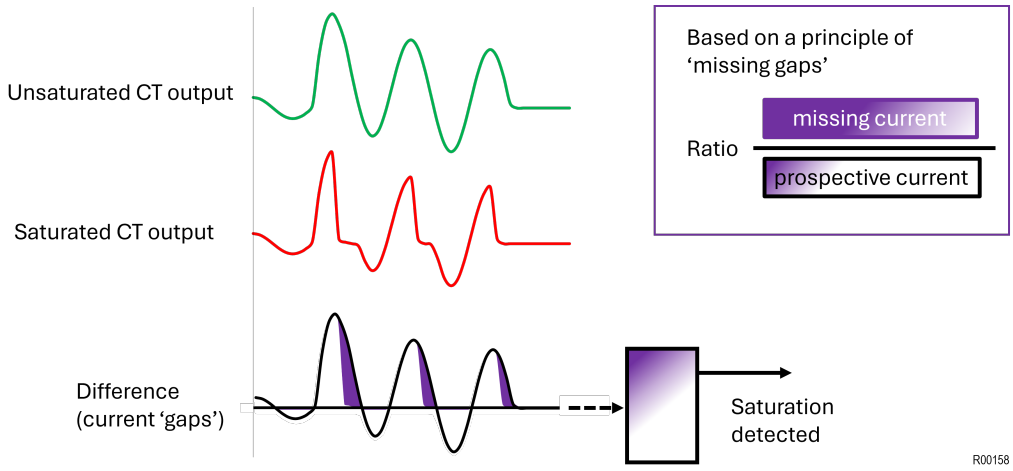


Figure 60: Principle of recognising current gaps between primary and secondary current waveforms to determine CT saturation

Implementing the CT saturation detector is based on evaluating the ratio between the missing current components and the prospective current This is implemented with rolling filters that act on the sampled input current data streams. The principle is outlined in the following figure:

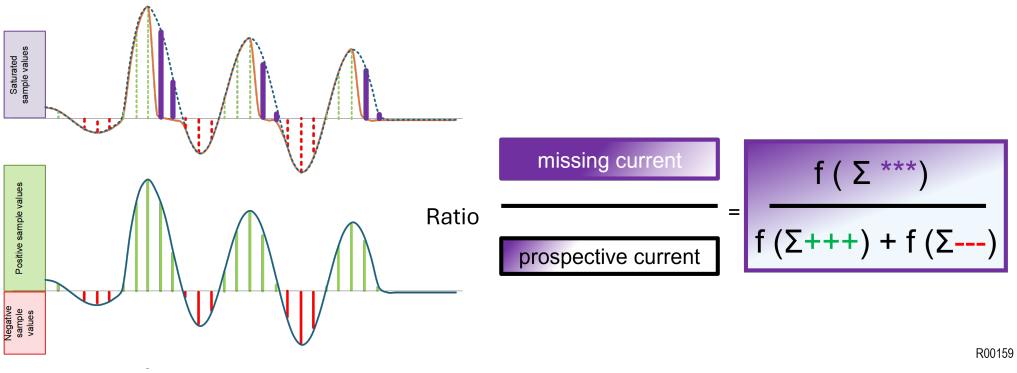


Figure 61: 'Missing-sample' principle for detecting current gaps caused by CT saturation

At each terminal in the protection scheme, the output of every phase CT is evaluated for saturation. A one-cycle rolling average of the number of positive going samples in the output is maintained, as is the rolling average of the number of negative going samples. A rolling average of the differences (Δ) and sums (Σ) of these streams are then generated. A division of the differences (missing currents) and sums (prospective currents) quantifies the asymmetry in the waveform. As the number of 'missing samples' in each cycle rises, so too does the amount of asymmetry between expected and actual signals. If the level of asymmetry exceeds a characteristic value, then the CT is considered to be saturated. An output indicating that CT saturation has been detected is made available to control the differential protection. The implementation of the missing samples CT saturation detection principle is shown in the following figure:

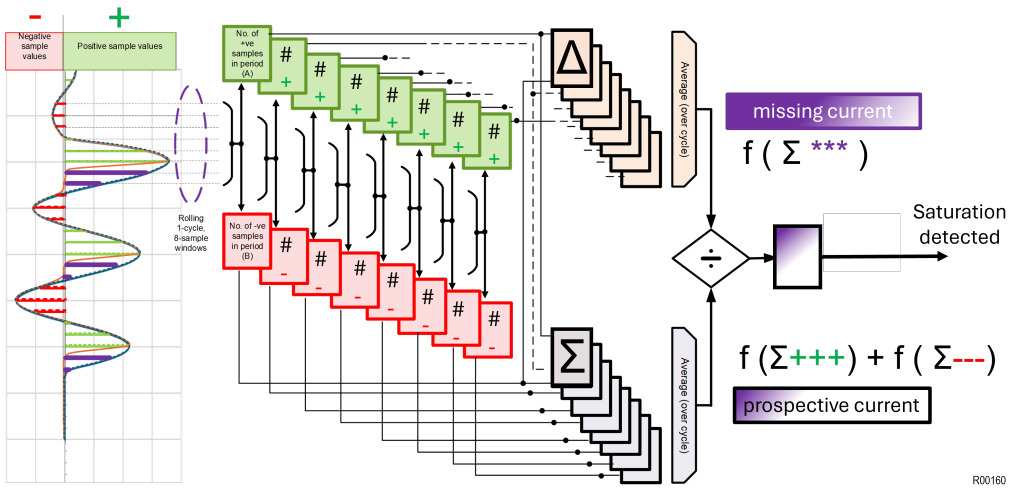


Figure 62: 'Missing'-samples algorithm to implement CT saturation detection

The following figure illustrates the operation and output of the missing samples principle:

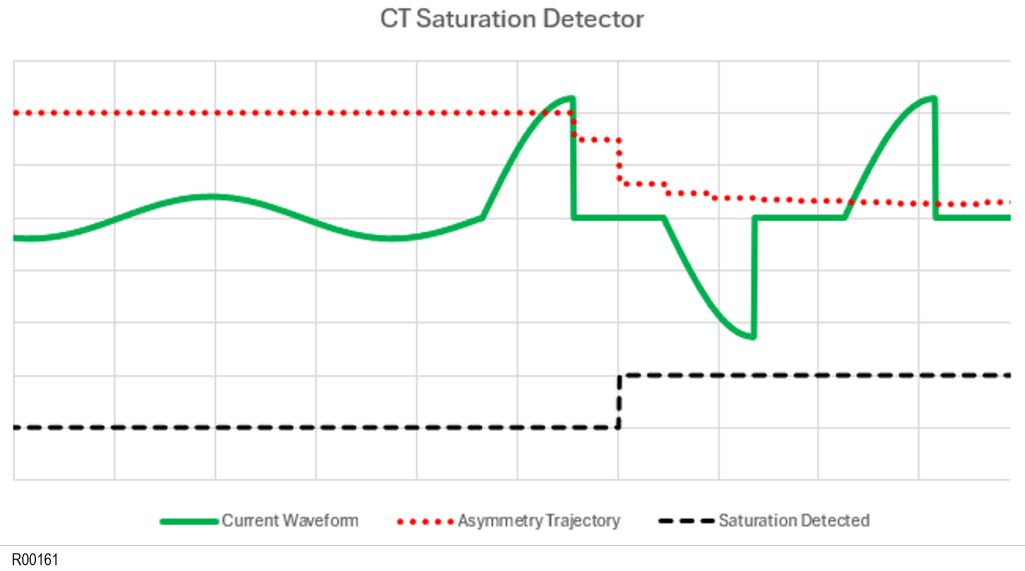


Figure 63: Illustration of CT saturation detection by 'missing samples' algorithm

The example of CT saturation being detected is based on a hypothetical case chosen for illustration purposes only. It demonstrates how, as the output collapses, the gaps change the trajectory of asymmetry and, when a threshold is crossed, the output is asserted.

The influence of the CT saturation detector with the current differential algorithm is managed by two settings. There are two settings, both found in the *GROUP N CURRENT DIFFERENTIAL* column, that affect operation.

If you want to use the feature you must set ***CT Saturation*** to `Enabled`. If you enable the feature, then the ***Ibias Thresh.*** setting becomes visible. If the feature is enabled and if CT saturation is detected, then the protection will block differential tripping if the calculated bias current exceeds the value set in ***Ibias Thresh.***

The default value for the ***Ibias Thresh.*** setting is 4 p.u. which we recommend.

The influence on the current differential characteristic is illustrated in the following figure:

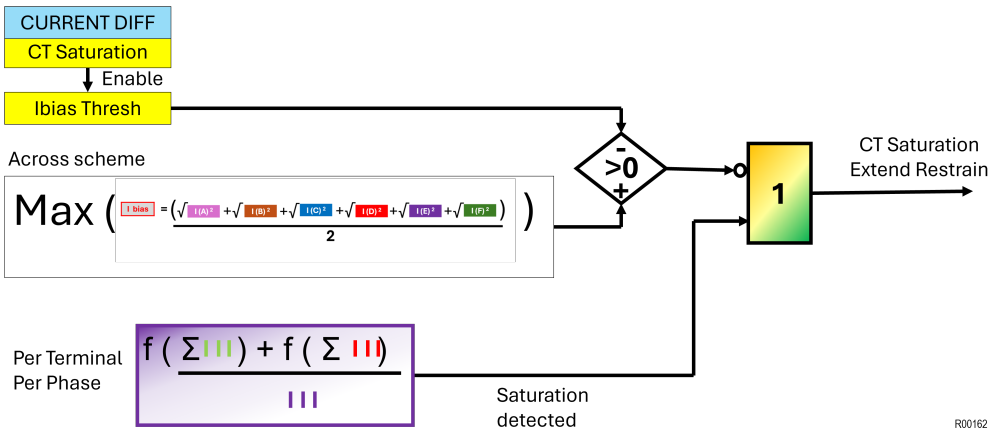


Figure 64: Using CT saturation detection to extend restraining influence on biased differential protection

The output of the CT saturation detector influences the basic biased current differential protection characteristic as shown in the following figure:

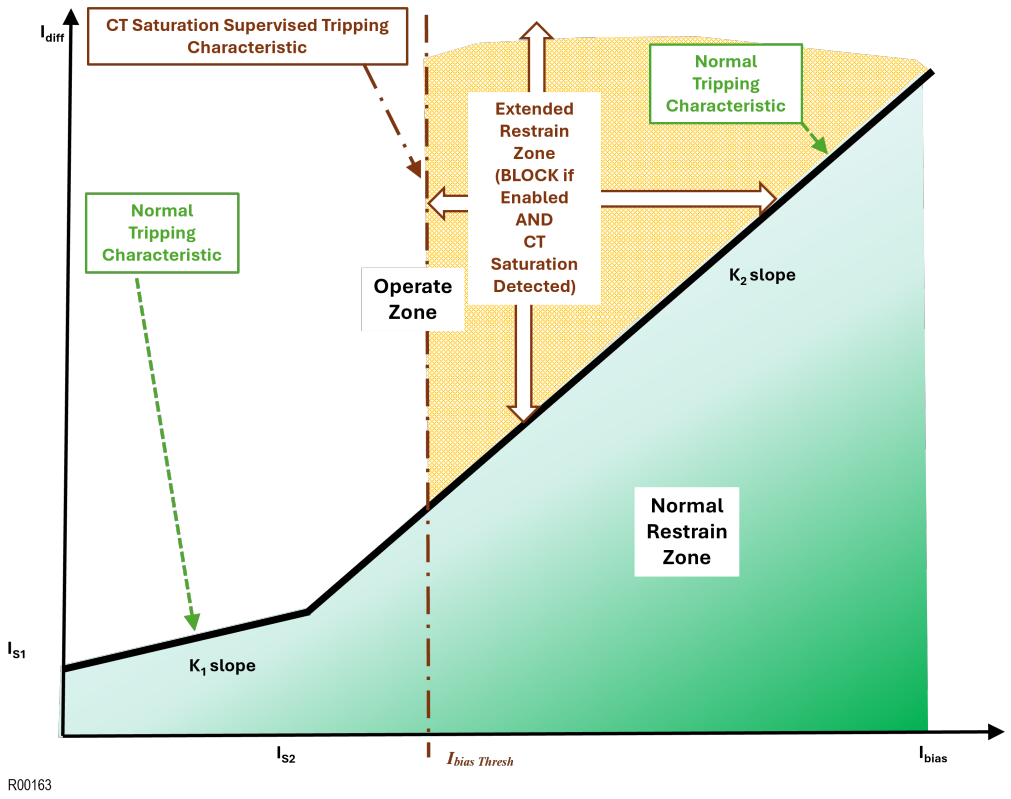


Figure 65: Modifying biased differential protection characteristic according to CT saturation conditions

If, either the feature is disabled, or if the feature is enabled but saturation is not detected, then there is no change to the basic biased differential operating characteristic.

6.3.10 CT RINGDOWN

If a fault on a power network causes the magnetic core of a CT to saturate, it makes correct fault detection difficult due to the distortion in the secondary current outputs of the CT. When the fault is cleared, core flux remains, and this can continue to distort the secondary output even when the input current is removed. Rather than collapsing to zero, the secondary output decays at the natural discharge rate of the circuit from an initial value affected by the remanent flux level and pre-switching current magnitude. This phenomenon is known as CT ringdown and can cause problems for differential protection. Although all CT outputs will decay at the same rate, since the different phases at the different terminals may all potentially switch the currents at different points-on-wave, the differential calculations will use erroneous values leading to potential false tripping. The following figures show a typical (single phase) CT ringdown waveform:



R00164

Figure 66: Example of CT ringdown

A feature to detect ringdown can be used to stabilise the protection under such conditions.

The implementation of CT ringdown detection in this product is similar to the detection of CT saturation. The condition is detected by comparing a function of rolling-averaged sums of current samples against a function of rolling-averaged differences between current samples. The following diagram illustrates the implementation of CT ringdown in this product:

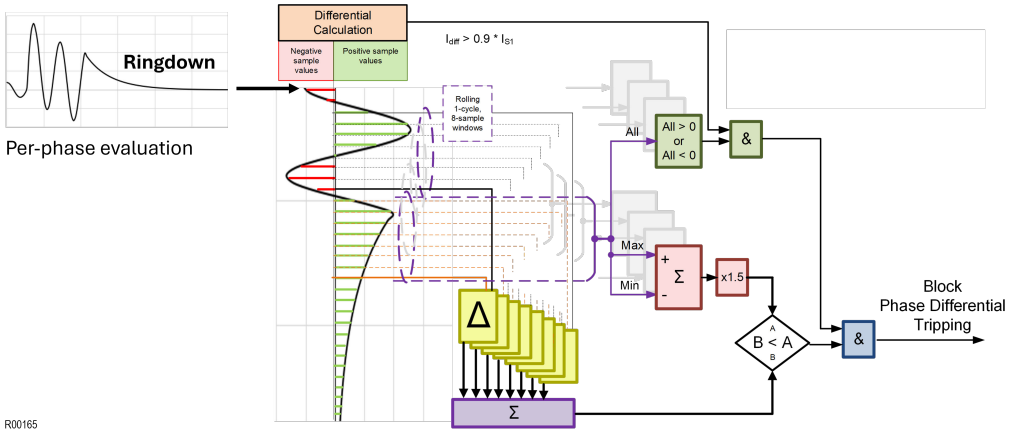


Figure 67: Implementing CT saturation ringdown detection

The feature is always operational. If a ringdown condition is detected, then the phase current differential protection is blocked until the condition clears.

6.3.11 SWITCHED COMMUNICATION PATH SUPERVISION

A feature is included in this product to supervise the operation of the Current Differential protection in the event of communications paths being switched. The Ping-Pong method of time alignment requires symmetry of communications paths. The absolute value of propagation delay is not important, but the symmetry is. Many telecommunication systems feature self-healing mechanisms so that if a particular link fails, the integrity of the system can be maintained by the re-routing of traffic via unaffected links. Careful system management can ensure that the reconfiguration of the system to bypass the failed link can respect the communications symmetry requirements.

Whilst the reconfiguration is in progress, however, there may be a temporary violation of the symmetry requirements. The Switched Communications Paths Supervision function protects against incorrect tripping during the period of transient symmetry violation by dynamically adapting the current differential operate/restrain characteristic.

The Current Differential protection continually monitors the communications propagation delay time. With reference to the following figure, if the differences between 2 successive calculated propagation times exceed the ***Comm Delay Tol*** setting in the *PROT COMMS/IM64* column, then the operating characteristic is modified from the 'Normal Tripping Characteristic' to the 'Switched-Communications Supervised Tripping Characteristic' as illustrated in the following figure:

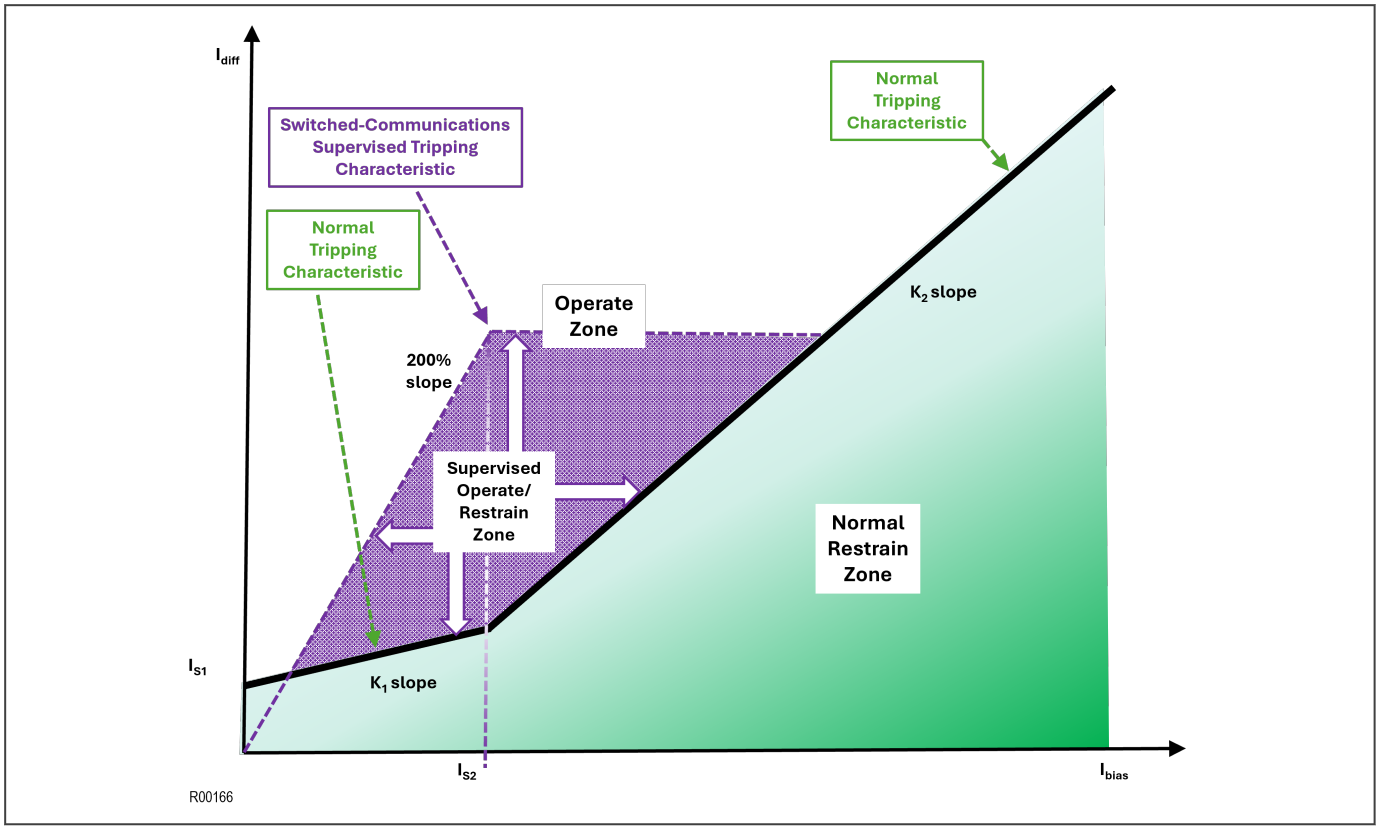


Figure 68: Biased differential protection supervision during communication path switching

When the ***Comm Delay Tol*** setting has been exceeded for two consecutive calculations, as shown in the figure, the lower slope of the characteristic is increased from K1 to 200%. When this 200% slope reaches the *IS2* setting value, the characteristic tracks a horizontal line until it meets with the original K2 slope which the characteristic then follows.

The change to the characteristic is determined by two timers (***Char Mod Time***, and ***Char Mod RstTime***) found separately located in the *PROT COMMS/IM64* column. These timers start when the switched communication path condition is recognised. These timers define how long the modification to the tripping characteristics is applied for. A communications delay alarm (***Comm Delay Alarm)*** is also raised at the same time.

To adequately stabilise the current differential protection during unfavourable communications switching actions, the ***Char Mod Time*** should be set higher than the maximum one-way communications propagation delay time that may be expected between any pair of devices in the differential protection scheme. The ***Char Mod Time*** setting value must include provision for all delays that may be incurred in any one direction in the communication of messages between pairs of devices. The setting value should include any additional time delays that may arise if communications are re-routed to provide redundancy via back-up paths. Setting above this minimum value will ensure that all messages that may have been impacted by switching of the communications paths will be processed in accordance with the desensitised characteristic. If the ***Char Mod Time*** is set below this maximum possible value,

then affected messages may be processed without qualification, creating phantom differential currents and potentially resulting in unwanted tripping and/or unexpected intertripping.

The characteristic normally returns to normal when the ***Char Mod Time*** expires, but a mechanism is provided to accelerate the reset if system conditions permit by using an additional timer ***Char Mod RstTime*** which is set to a value less than the ***Char Mod Time.***

The ***Char Mod RstTime*** can be enabled or disabled. If it is enabled, then the timer controlling the reset characteristics starts when the ***Char Mod Time*** starts. If the ***Char Mod RstTime*** expires whilst the ***Char Mod Time*** is still running, AND IF the bias current is above 5% In, AND IF the differential current is below 10% of bias current on all phases, then the ***Char Mod Time*** is reset and the characteristic returns to normal. If these conditions are not met, then the Switched-Communications Supervised Tripping Characteristic remains in force for the duration of the ***Char Mod Time***. The ***Char Mod RstTime*** should be set greater than the minimum switching delay expected, and less than the ***Char Mod Time***.

We don't recommend it, but if you don't want the tripping characteristic to be changed during communications switching operations, you should set ***Char Mod Time*** to `0`.

6.3.12 OVERALL BIASED CURRENT DIFFERENTIAL CHARACTERISTIC

According to the current differential supervision features applied, the basic biased current differential characteristic in this product adapts to suit different operating conditions. The combined effects of compensating for both CT saturation and communication path switching are shown in the following figure:

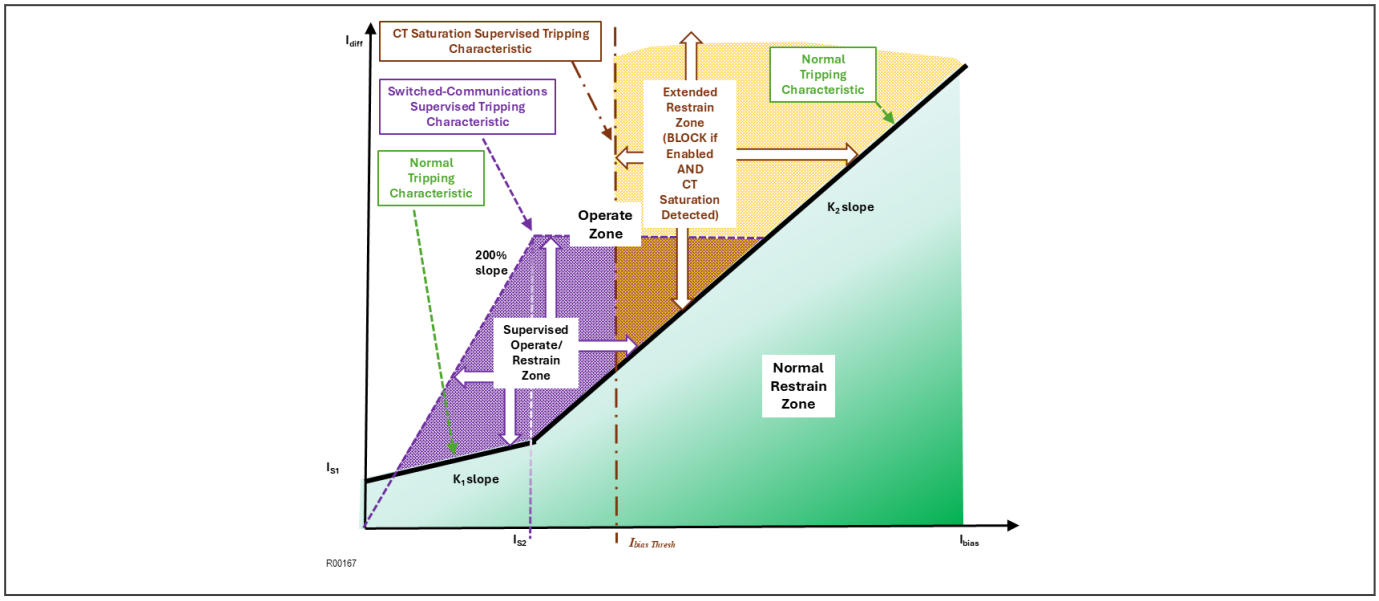


Figure 69: Complete biased differential protection characteristic including compensation for CT saturation conditions and switched communications conditions

Note:
This figure does not show the impact of the CT circuitry supervision outlined in the SUPERVISON chapter of this manual which, should also be considered when deploying this protection.

6.4 CURRENT DIFFERENTIAL PROTECTION-AUXILIARY FUNCTIONS

6.4.1 CURRENT DIFFERENTIAL INTERTRIPPING

Eight freely assignable intertripping signals are provided by a facility called InterMICOM64, which is described in the chapter on Fibre Teleprotection. In addition there are two intertripping functions associated directly with the Current Differential protection. Both are operational when the phase current differential is enabled:

The first is a differential intertripping function whereby if one terminal sees a differential fault, as well as issuing a local trip command it will also send a command to trip to remote terminals to ensure that the fault is isolated at all terminals.

The second is a permissive intertripping function. A Permissive Intertripping function (PIT) is associated with the current differential protection and is visible and active if the phase current differential protection is enabled.

Note:
The term "permissive intertripping" associated with this current differential protection is not the same as that commonly used in teleprotection schemes. It is specific to this type of Current Differential protection implementation.

A device can be configured to send a permissive intertrip command over the protection communication channel. To use this function you need to map the ***Perm Intertrip*** DDB signal to one of the opto-inputs using the PSL.

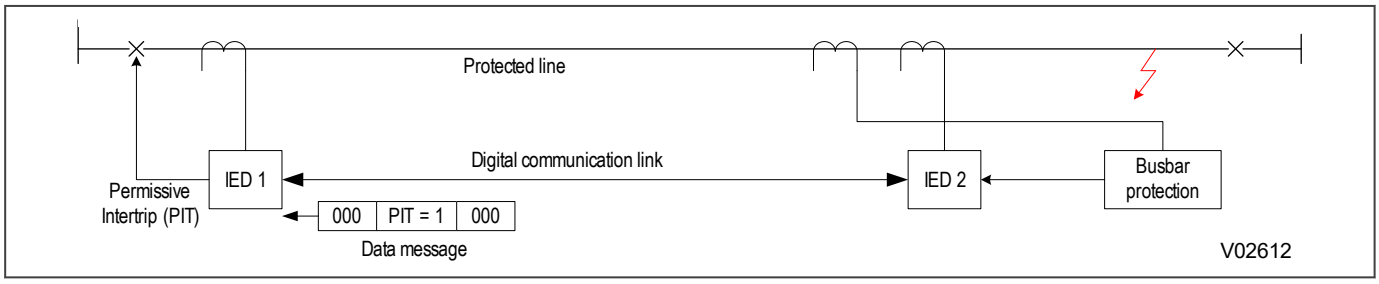


Figure 70: Permissive intertripping example

Consider the above diagram. If a fault occurs as shown, it will be seen by the busbar protection which can trip its local circuit breaker. The fault will not be seen by the differential protection, however, so the fault will continue to be fed. An input signal from the busbar protection at the faulted end can be sent as a permissive intertrip (PIT) command to a remote terminal to cause it to permissively trip the remote circuit breaker to clear the fault.

Tripping occurs if the current remains above the ***Phase Is1*** setting of the phase current differential elements while the PIT command is received. The condition must remain satisfied for a minimum time setting. The time is set in the ***PIT Time*** setting in the *CURRENT DIFF* column. The permissive intertrip (PIT) timer can be set between 0 and 200 ms. This time should be set to provide discrimination with other protection devices. For example, if there is a genuine busbar fault, the time delay should be set to allow busbar protection to clear the fault. A typical setting may be 100 to 150 ms.

You can choose whether to use the local current value sent with the PIT command to make the decision at the remote end, or whether to use the remote current value at the receiving end for the decision. This choice is made using the ***PIT I selection*** setting in the *CURRENT DIFF* column.

Note:
The permissive intertripping function always trips three-phase.

6.4.2 STUB BUS DIFFERENTIAL PROTECTION

This product can provide stub-bus protection associated with the differential protection.

If you wish to use this feature you must ensure that the current differential protection is enabled. You will need to map one of the opto-isolated inputs to the DDB ***Stub Bus Enabled*** using the programmable scheme logic and you will need to enable the feature by setting ***Ph Diff Stub Bus*** in the *CURRENT DIFF* column to `Enabled`.

When the stub bus protection is enabled and activated by energisation of the opto-isolated input, all current values transmitted to the remote relays, and all those received from remote relays are set to zero. The Stub bus protection then provides differential protection for the stub zone. No differential intertrip or permissive intertrip signals will be issued, or acted upon by the affected terminal. Intertripping signals mapped via IM64 will be acted upon, and the affected terminal remains active to protect the isolated stub bus.

For products having two sets of CT inputs, the stub bus protection takes the two sets of current inputs and uses them as inputs to the phase differential current protection. The values are compared against the dual slope characteristics to determine whether tripping should occur or not.

For products having a single set of CT inputs, an additional setting (***Ph Is1 StubBus***) is provided. In these applications, if the stub-bus feature is enabled and activated, the protection will trip if the measured current exceeds the ***Ph Is1 StubBus*** setting.

Tripping due to the operation of the stub-bus protection is always three-phase.

The principle is outlined in the figure below:

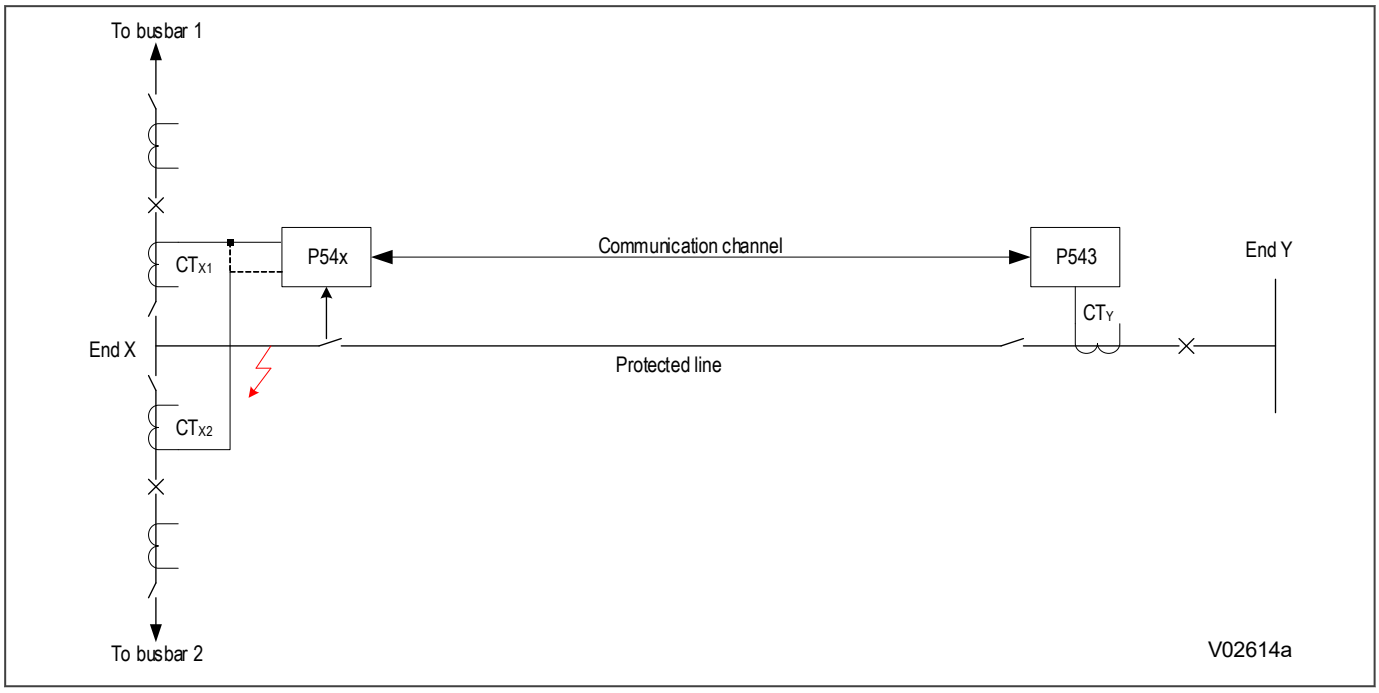


Figure 71: Stub bus protection

Note:
Models having distance protection feature a phase segregated stub bus protection associated with the distance protection elements. Where applicable these are described along with the distance elements.

6.4.3 CT REQUIREMENTS

Please refer to Appendix D for a full compatibility matrix for MiCOM P54A - P54E Line Differential Protection Relays.

The matrix can be used to check communications compatibility between related devices.

6.4.3.1 RECOMMENDED CT CLASSES

You can use Class X current transformers with a knee point voltage greater or equal to that calculated. You can also use class 5P protection CT. These have a knee-point voltage equivalent, which can be approximated from the following calculations:

$$V_k = (VA \times ALF)/I_n + (R_{CT} \times ALF \times I_n)$$

where:

- V_k = Knee-point voltage
- VA = Voltampere burden rating
- ALF = Accuracy limit factor
- I_n = CT nominal secondary current
- R_{CT} = CT resistance

6.4.3.2 CURRENT DIFFERENTIAL REQUIREMENTS

The CT knee point voltage for current differential protection using either non-air gapped and air gapped CTs should comply with the spreadsheet, attached as an embedded resource.

Note:
The CT knee point calculations in the embedded spreadsheet are based upon the following default settings: Phase Is1 set to 0.2In, Phase Is2 set to 2.0In, Phase k1 set to 30%, Phase k2 set to 150%, Ktransient set to 200%, Is1 Restraint set to 4.0In and Phase Time Delay set to 0 seconds.

If using Adobe Acrobat Reader, click on the button below to open the spreadsheet.

This manual must be opened with a PDF viewer capable of opening attachments, such as Adobe Acrobat Reader or Nitro PDF. If using Nitro PDF, attachments are shown in the attachment pane. To show or hide the attachments pane, look in the sidebar and click the attachments tab.

Note:
An Open File dialogue box may open with a warning message about potential harm from programs, macros or viruses. The file supplied does not contain any harmful content, and may be safely opened.

CT Knee-point Calculations

6.5 DIFFERENTIAL IED COMPATIBILITY WITH PREVIOUS VERSIONS

Please refer to Appendix D for a full compatibility matrix for MiCOM P54A - P54E Line Differential Protection Relays.

The matrix can be used to check communications compatibility between related devices.

6.5 DIFFERENTIAL IED COMPATIBILITY WITH PREVIOUS VERSIONS

Please refer to Appendix D for a full compatibility matrix for MiCOM P54A - P54E Line Differential Protection Relays.

The matrix can be used to check communications compatibility between related devices.

6.6 COMMUNICATIONS INTERFACING

Products in this range need to communicate power system information (phase current values, timing values, commands, etc.) between devices. Dedicated bidirectional ports are provided for this teleprotection communication. Each device has either one or two teleprotection ports enabling it to communicate with either one, or two other similar devices. For a two-terminal application only one channel is required to implement the necessary teleprotection communications to realise a scheme, but adding the second channel can be used to provide a redundant back-up. In multi-terminal applications, both channels are needed. Each of the two channels is connected to a logically adjacent device to form a ring. Because each channel is bi-directional and the devices are connected in a ring, the arrangement provides redundancy, allowing the scheme to remain functional in the event of any single link failure.

The interfaces are designed only for fibre optic connection.

6.6.1 FIBRE-OPTIC TELEPROTECTION COMMUNICATION INTERFACE

The ports are presented for fibre-optic connection using ST (straight-tip, 2.5 mm ferrule, bayonet) connectors. Options are available to support either one channel, or two channels in combination, from the following list:

- 850 nm multi-mode transmission
- 1300 nm multi-mode transmission
- 1300 nm single-mode transmission
- 1550 nm multi-mode transmission

The optical budget details of the different interfaces are provided in the Technical Information chapter of this manual.

The multi-mode interfaces are suitable for use with OM3 (or similar) fibre-optic cables.

The single-mode interfaces are suitable for use with OM2 (or similar) fibre-optic cables.

The interfaces have not been designed for use on wavelength division multiplexed links. Direct connection to WDM equipment (or variants such as CWDM) is not approved.

The ports can be used either for direct fibre connection between devices or for indirect connection via intermediary equipment supporting the IEEE C37.94 standard. If you are using direct fibre connections, you need to ensure that the appropriate ***CH1 Connection*** (and/or ***CH2 Connection***) settings in the *PROT COMMS/IM64* column are set to `Direct Fibre`.

6.6.2 MULTIPLEXER-COMPATIBLE TELEPROTECTION COMMUNICATION INTERFACE ACCORDING TO IEEE C37.94

The teleprotection interface on this device has been designed to connect via interfaces conforming to the IEEE C37.94 standard.

The Teleprotection interface is designed for 2 Mbits/s connection. This connection is internally divided into 12 ‘slots’ each operating at 64 kbits/s. By default, the protection expects that all 12 slots will be made available for the application. For operational reasons there may be a requirement for some of the 64 kbits/s slots to be allocated to other duties. Where this is the case, the product can be configured to operate using reduced communications bandwidth by allocating with fewer than the maximum 12 slots available. With ***Bandwidth Ctrl*** in the *PROT COMMS/IM64* column set to `Disabled`, the protection will default to using all 12 slots. Changing ***Bandwidth Ctrl*** to `Enabled` reveals two additional settings that control the number of slots that will be used by each protection channel. These are:

- ***Ch1 N*64kbits/s***. This setting allocates the number of slots that will be dedicated to teleprotection signalling on channel 1 of the device. The maximum value is `12`.
- ***Ch2 N*64kbits/s***. This setting allocates the number of slots that will be dedicated to teleprotection signalling on channel 2 of the device. The maximum value is `12`.

Reducing the number of slots allocated for the protection can only be implemented within certain minimum limits. These minimum limits are automatically determined by the product functionality and topology applied and are reflected into the settings options. The minimum values are outlined in the following figure:

MiCOM P54M Network Topology IEEC37-94 Minimum Slot Requirements												
Application	With Capacitive Charging Current Compensation						Without Capacitive Charging Current Compensation					
Model	P54A, or P54B, or P54C, or P54E						P54A, or P54B, or P54C, or P54E					
Topology	2T	2T-R	3T	4T	5T	6T	2T	2T-R	3T	4T	5T	6T
Minimum Number of Slots	3	3	4	7	8	12	2	2	3	4	6	8

R00135

Figure 72: IEEE C37.94 minimum slot allocation requirements

In the absence of any specific restrictions, using the maximum available bandwidth afforded by allocating the maximum 12 slots is recommended.

6.7 APPLICATION NOTES

Critical to applying this product as current differential protection for multi-terminal lines is correctly understanding and designing the scheme before configuring and setting the devices at each terminal in the protected scheme. Doing this effectively requires that an order of precedence be respected. The functional description sections in this chapter are presented in the same prescriptive order, and it is strongly recommended that you refer to those relevant sections (and the overarching figure) when designing and configuring the scheme and setting the devices within it.

6.7.1 SETTING UP A SCHEME

Whilst the underlying operating principle of this product is simple, designing, configuring, and setting the terminal devices in the scheme involves cross-device co-ordination of many parameters. Undertaking this requires familiarity with the functionality of the device and so you are recommended to take time to understand this by reading the contents of this chapter before proceeding. This note elaborates the illustration in the previously presented "Functional Block Diagram of Multi-Terminal Numerical Current Protection" figure which is repeated below for convenience:

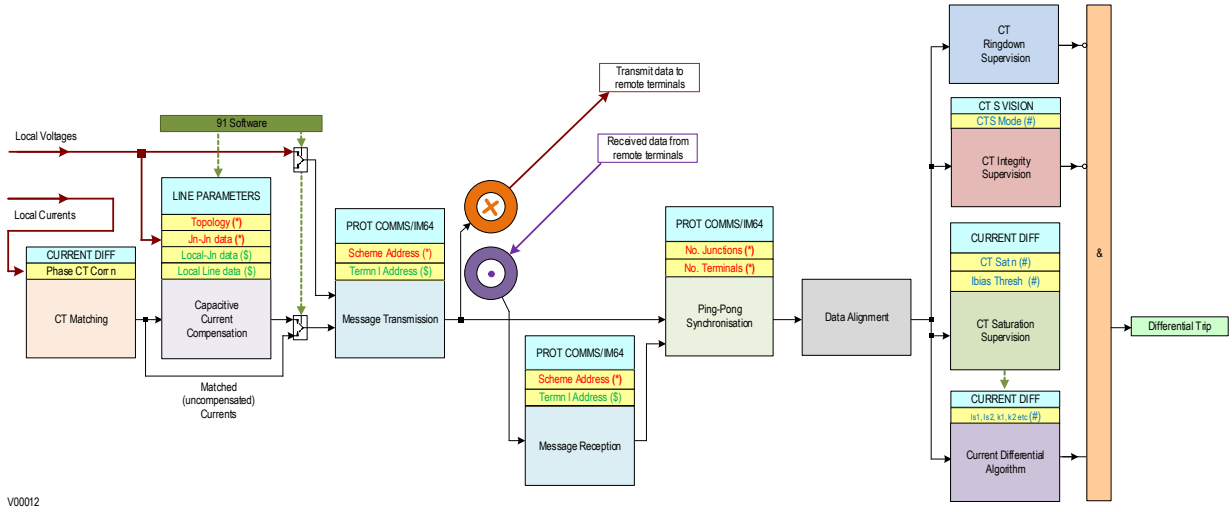


Figure 73: Functional block diagram of multi-terminal numerical current protection

In the figure, the yellow blocks indicate variables that determine the operation of associated functional blocks. These may be configuration or settings values, and the text inside the boxes represent the specific details of that variable. The text is colour coded, and the colour of the text relates to the scope of the variable (scheme-wide or device-specific), as well as the order in which it should be determined and applied.

The order of precedence to be observed is as follows:

- Confirm scheme electrical design details (number of terminals, conductor types, electrical connection arrangements).
- Realign the layout with a linearly-ordered nodal arrangement and confirm the number of junctions, the topology, and define the topology matrix.
- Overlay the communications network layout and confirm the communications topology
- Define and apply the settings at each device according to the following order of precedence:

P54 MEDiScheme Configuration and Settings Order of Precedence

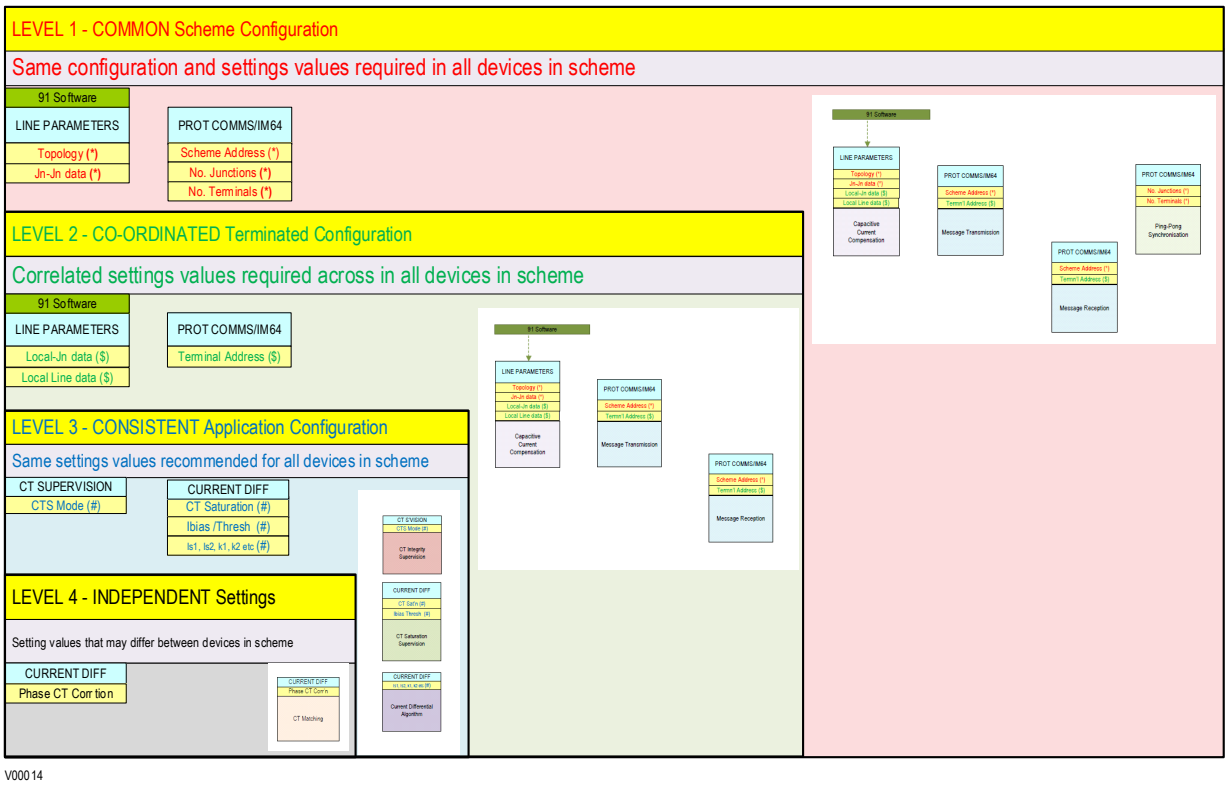


Figure 74: Multi-terminal differential protection configuration and settings - order of precedence

6.7.2 SETTING UP THE PHASE DIFFERENTIAL CHARACTERISTIC

The biased phase current differential characteristic is defined by four protection settings. Each can be set independently. This flexibility allows the characteristic to be set for particular sensitivity and current transformer requirements. To simplify setting the protection, however, we strongly recommend three of the settings be fixed as:

- ***Phase Is2*** = Set to value as recommended in section 3 Current Differential Requirements
- ***Phase k1*** = 30% (This provides stability for small CT mismatches, while ensuring good sensitivity to resistive faults under heavy load conditions
- ***Phase k2*** = 150% (For 2 terminal applications to provides stability under heavy through fault current conditions)
- ***Phase k2*** = 100% (For 3 or more terminal applications to provides stability under heavy through fault current conditions)

These settings give a characteristic suitable for most applications so that only the Phase Is1 setting needs changing from the default value.

Phase Is1 is the setting which determines the minimum pick-up of the phase current differential elements. This value should be set to account for any mismatch between the current transformers at the different terminals, as well the capacitive charging current if this is not compensated.

The table below shows some typical steady state charging currents for various lines and cables.

Voltage (kV)	Core Formation and Spacing	Conductor Size in mm2	Charging Current A/km
11 kV Cable	Three-core	120	1.2
33 kV Cable	Three-core	120	1.8
33 kV Cable	Close-trefoil	300	2.5

Voltage (kV)	Core Formation and Spacing	Conductor Size in mm2	Charging Current A/km
66 kV Cable	Flat, 127 mm	630	10
132 kV Overhead Line		175	0.22
132 kV Overhead Line		400	0.44
132 kV Cable	Three-core	500	10
132 kV Cable	Flat, 520 mm	600	20
275 kV Overhead Line		2 x 175	0.58
275 kV Overhead Line		2 x 400	0.58
275 kV Cable	Flat, 205 mm	1150	19
275 kV Cable	Flat, 260 mm	2000	24
400 kV Overhead Line		2 x 400	0.85
400 kV Overhead Line		4 x 400	0.98
400 kV Cable	Flat, 145 mm	2000	28
400 kV Cable	Tref., 585 mm	3000	33

If capacitive charging current compensation is not used, the setting of ***Phase Is1*** must be set above 2.5 times the steady state charging current. Where charging current is low or negligible, the recommended setting of 0.2 pu (factory default) should be applied.

If there is a mismatch between CTs at line ends, then the lowest primary CT rated current should be used as a reference current for p.u. calculations (assuming that the load current cannot continuously exceed this value). This means that the recommended settings ***Phase Is1*** = 0.2 pu is equal to 0.2*(the lowest primary CT rated value). The same consideration applies for other current settings such as ***Phase Is2***.

6.7.3 SENSITIVITY UNDER HEAVY LOADS

The sensitivity of the phase current differential protection is governed by its settings and also the magnitude of load current in the system. For a three-ended system, with devices LOCAL, REMOTE1 and REMOTE2, the following applies:

$$|I_{diff}| = |(\bar{I}_{LOCAL} + \bar{I}_{REMOTE1} + \bar{I}_{REMOTE2})|$$

$$|I_{bias}| = 0.5\ (|I_{LOCAL}| + |I_{REMOTE1}| + |I_{REMOTE2}|)$$

In a four-ended system, assume a load current of I_L flowing from end LOCAL to REMOTE1, REMOTE2 and REMOTE3. Assume also a high resistance single-end fault of current I_F, being fed from end LOCAL. In the worst case, we can also assume I_F to be in phase with I_L:

$$I_{LOCAL} = I_L + I_F$$

$$I_{REMOTE1} = -yI_L$$

$$I_{REMOTE2} = -xI_L$$

$$I_{REMOTE3} = -zI_L$$

$$|I_{diff}| = |I_F|$$

$$|I_{bias}| = |I_L| + 0.5\ |I_F|$$

For multi-ended current differential

$$|I_{bias}| = |I_L| + 0.5(I_L + I_{Lx} + I_{Ly} + I_{Lz} + I_F)$$

$$I_{Lx} + I_{Ly} + I_{Lz} = I_L$$

Phase current differential protection sensitivity when $|I_{bias}| <$ *Phase Is2*:

The phase current differential protection would operate if $|I_{diff}| >$ ***Phase k1*** $|I_{bias}|$ + ***Phase Is1***

therefore:

$$|I_F| > (\textit{Phase k1}\ |I_L| + \textit{Phase Is1}) / (1 - 0.5\ \textit{Phase k1})$$

For ***Phase Is1*** = 0.2 pu, ***Phase k1*** = 30% and ***Phase Is2*** =2.0 pu, then

- for $|I_L|$ = 1.0 pu, the phase current differential protection would operate if $|I_F|$ > 0.59 pu
- for $|I_L|$ = 1.59 pu, the phase current differential protection would operate if $|I_F|$ > 0.80 pu

If $|I_F|$ = 0.80 pu and |I| = 1.59 pu, then $|I_{bias}|$ = 1.99 pu, which reaches the limit of the low percentage bias curve.

Phase current differential protection sensitivity when $|_{bias}|$ > Phase Is2:

The phase current differential protection would operate if $|I_{diff}| >$ ***Phase k2*** $|I_{bias}|$ - (***Phase k2*** - ***Phase k1***) ***Phase Is2*** + ***Phase Is1***

therefore:

$$|I_F| > (\textit{Phase k2}\ |I_L| - (\textit{Phase k2} - \textit{Phase k1})\ \textit{Phase Is2} + \textit{Phase Is1}) / (1 - 0.5\ \textit{Phase k2})$$

For ***Phase Is1***= 0.2 pu, ***Phase k1*** = 30%, ***Phase Is2*** = 2.0 pu and ***Phase k2*** = 100%, then,

- for $|I_L|$ = 2.0 pu, the phase current differential protection would operate if $|I_F|$ > 1.6 pu
- for $|I_L|$ = 2.5 pu, the phase current differential protection would operate if $|I_F|$ > 2.6 pu

Fault resistance coverage

Assuming the fault resistance R_F is much higher than the line impedance and source impedance, then for a 33 kV system and 400/1 CT:

$$|I_F| = (\text{Vph-n} / R_F)(1/\text{CT ratio})\ \text{pu} = 47.63/R_F\ \text{pu}$$

Based on the analysis above, the phase current differential protection detects a fault current in excess of 0.59 pu with a load current of 1 pu flowing. The fault resistance is less than 47.63/0.59 = 81 ohms in this case.

With a short time overload current of 2.0 pu, the phase current differential protection can detect a fault resistance of 47.63/1.6 = 30 ohms or lower.

6.7.4 PERMISSIVE INTERTRIPPING

The permissive intertrip (PIT) timer can be set between 0 and 200 ms. This time should be set to provide discrimination with other protection devices. For example, if there is a genuine busbar fault, the time delay should be set to allow busbar protection to clear the fault. A typical setting may be 100 to 150 ms.

6.7.5 CT RATIO CORRECTION SETTING GUIDELINES

If there is no mismatch between current transformers at line ends, ***Ph CT Corr'tion*** should be set to *1* in all devices.

If the CTs at line ends have different primary ratings, then one of them is considered as a reference (the one with the lowest primary rating). ***Ph CT Corr'tion*** should be set to *1* in the device connected to the reference CT. For all other devices ***Ph CT Corr'tion*** is calculated as follows:

$$\textit{Ph CT Corr'tion}_{\ \text{IEDx}} = (\textit{Phase CT Primary}_{\ \text{IEDx}}) / (\textit{Phase CT Primary}_{\ \text{REFERENCE}})$$

Settings ***Phase Is1***, ***Phase Is2***, ***Diff Is1***, ***Diff Is2*** must be calculated as pu of the reference primary rating, then converted into local primary (secondary) values. For setting ***Phase Is1*** in IEDX, the equations would be:

$$\textit{Phase Is1}\ [\text{p.u.}] = (\textit{Phase Is1}\ _{\text{IABSOLUTE PRI}}\ [\text{A}]) / (\textit{Phase CT Primary}\ _{\text{REFERENCE}}\ [\text{A}])$$

$$\textit{Phase Is1}\ _{\text{IEDx PRI.}}\ [\text{A}] = (\textit{Phase Is1}\ [\text{p.u.}])\ (\textit{Phase CT Primary}\ _{\text{IEDx}})$$

$$\textit{Phase Is1}\ _{\text{IEDx SEC.}}\ [\text{A}] = (\textit{Phase Is1}\ [\text{p.u.}])\ (\textit{Phase CT Sec'y}\ _{\text{IEDx}})$$

The same considerations apply to settings ***Phase Is2***

Example:

Assume that we have a three-ended application with line ends X, Y, Z (500/5, 800/5, 200/1) and Current Differential settings in absolute primary values:

$$\textit{Phase Is1}\ _{\text{ABSOLUTE PRI.}} = 40\text{A}$$

$$\textit{Phase Is2}\ _{\text{ABSOLUTE PRI.}} = 400\text{A}$$

Setting	End X	End Y	End Z
Phase CT Primary	500A	800A	**200A**
Phase CT Sec'y	5A	5A	1A
Ph CT Corr'tion	500/**200** = 2.5	800/**200** = 4	1 (reference)
Phase Is1 [p.u.]	40/200 = 0.2	40/200 = 0.2	40/200 = 0.2
Phase Is1 (Primary)	0.2*500 = 100A	0.2*800 = 160A	0.2*200 = 40A
Phase Is1 (Secondary)	0.2*5 = 1.0A	0.2*5 = 1.0A	0.2*1 = 0.2A
Phase Is2 [p.u.]	400/200 = 2	400/200 = 2	400/200 = 2
Phase Is2 (Primary)	2*500 = 1000A	2*800 = 1600A	2*200 = 400A
Phase Is2 (Secondary)	2*5 = 10A	2*5 = 10A	2*1 = 2A

6.7.6 FEEDERS WITH SMALL TAPPED LOADS

Where transformer loads are tapped off the protected line, it is not always necessary to install CTs at this location. If the tee-off load is light, differential protection can be configured for the main line alone. The setting ***Phase Time Delay*** allows the differential element to time grade with overcurrent protection devices or fuses protecting the tap. This keeps stability of the differential protection for external faults on the tee circuit.

6.7.7 SETTING A TWO-TERMINAL PHASE CURRENT DIFFERENTIAL ELEMENT

All four settings are user adjustable. This flexibility in settings allows the phase current differential characteristic to be tailored to suit particular sensitivity and CT requirements. To simplify your task, we strongly recommend three of the settings be fixed to:

$$\textit{Phase Is2} = 2.0\ \text{pu}$$

$$\textit{Phase k1} = 30\%$$

$$\textit{Phase k2} = 150\%$$

These settings will give a characteristic suitable for most applications. It leaves only the ***Phase Is1*** setting to be decided by you. The value of this setting should be in excess of any mismatch between line ends. It should also account for line charging current, where necessary.

By considering the circuit shown below, the settings for the phase current differential element can be established.

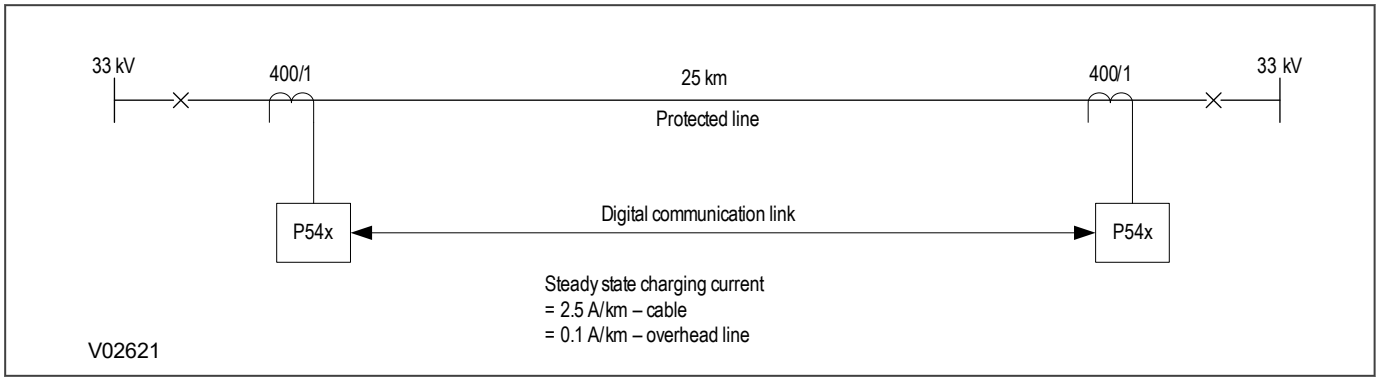


Figure 75: Typical two-terminal plain feeder circuit

In the case that voltage inputs are not in place, no facility to account for line charging current is available. The setting of ***Phase Is1*** must therefore be set above 2.5 times the steady state charging current value. In this example, assume a cable is used and there are not VT inputs connected to the device:

$$\textbf{\textit{Phase Is1}} > 2.5(\text{Ich})$$

$$\textbf{\textit{Phase Is1}} > 2.5\ (25\ \text{km x}\ 2.5\ \text{A/km})$$

$$\textbf{\textit{Phase Is1}} > 156.25\ \text{A}$$

The line CTs are rated at 400 amps primary. The setting of Phase Is1 must therefore exceed 156.25/400 = 0.391 pu.

Therefore select:

$$\textbf{\textit{Phase Is1}} = 0.4\ \text{pu}$$

If VTs are connected, a facility exists to overcome the effects of the line charging current. To use this you need to set the ***Compensation*** setting in the *CURRENT DIFF* column to `Cap Charging` and capacitive current compensation will be applied to the measured relay currents.

Phase Is1 may now be set below the value of line charging current if required, however we suggest that you choose ***Phase Is1*** only sufficiently below the charging current to offer the required fault resistance coverage. Where charging current is low or negligible, the recommended factory default setting of 0.2xIn should be applied.

6.7.8 SETTING A THREE OR MORE TERMINAL PHASE CURRENT DIFFERENTIAL ELEMENT

All four settings are user adjustable. This flexibility in settings allows the phase current differential characteristic to be tailored to suit particular sensitivity and CT requirements. To simplify your task, we strongly recommend three of the settings be fixed to:

$$\textbf{\textit{Phase Is2}} = 2.0\ \text{pu}$$

$$\textbf{\textit{Phase k1}} = 30\%$$

$$\textbf{\textit{Phase k2}} = 100\%$$

These settings will give a characteristic suitable for most applications. It leaves only the ***Phase Is1*** setting to be decided by you. The value of this setting should be in excess of any mismatch between line ends. It should also account for line charging current, where necessary.

By considering the circuit shown below, the settings for the phase current differential element can be established.

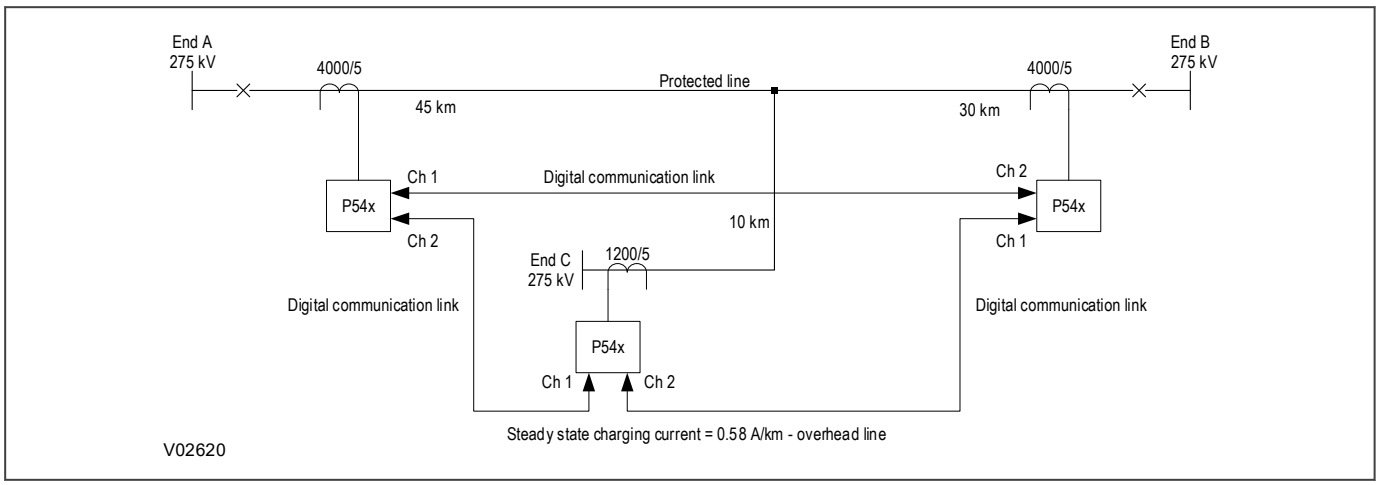


Figure 76: Typical three-terminal plain feeder circuit

If there are no VT inputs connected, the setting ***Phase Is1*** must be 2.5 times the steady state charging current suitably corrected for the different CT ratios as presented below in the calculation of charging current compensated values. For an overhead line circuit with a charging current of 0.58A/km the charging current will be:

$$Ich = 0.58\ A\ (\ 45 + 30 + 10\ ) = 49.3\ A$$

If VT inputs are connected, there is a facility to overcome the effect of charging current. To do this you need to enable the ***Capacitor Comp.*** setting.

The relay will calculate the capacitive charging currents based on the line admittance values provided in the the ***Multi-End Diff*** setting in the *LINE PARAMETERS* column.

The CT ratios on the three ends are different, so it is necessary to apply a correction factor to ensure secondary currents balance for all conditions:

To calculate the correction factor (CF), the same primary current must be used even if this current is not the expected load transfer for every branch. This will ensure secondary current balance for all conditions.

CT ratio correction input data is shown in the table below:

Setting	End A	End B	End C
Phase CT Primary	4000A	4000A	1200A
Ph CT Corr'tion	4000/1200 = 3.33	4000/1200 = 3.33	1 (reference)

We recommend the following settings:

$$\textbf{\textit{Phase Is1}} = 0.2\ \text{p.u.} = 0.2*1200A = 240A$$

$$\textbf{\textit{Phase Is2}} = 2\ \text{p.u.} = 2*1200A = 2400A$$

$$\textbf{\textit{Phase k1}} = 30\%$$

$$\textbf{\textit{Phase k2}} = 100\%$$

Therefore, settings in primary/secondary values for each device can be calculated as follows:

Setting	End A	End B	End C
Phase CT Primary	4000A	4000A	1200A
Phase CT Sec'y	5A	5A	5A
Phase Is1 [p.u.]	0.2	0.2	0.2
Phase Is1 (Primary)	0.2*4000 = 800A	0.2*4000 = 800A	0.2*1200 = 240A
Phase Is1 (Secondary)	0.2*5 = 1A	0.2*5 = 1A	0.2*5 = 1A
Phase Is2 [p.u.]	2	2	2

Setting	End A	End B	End C
Phase Is2 (Primary)	2*4000 = 8000A	2*4000 = 8000A	2*1200 = 2400A
Phase Is2 (Secondary)	2*5 = 10A	2*5 = 10A	2*5 = 10A

Note:
Settings shown in primary values at ends A and B appear different compared with end C. This is not a problem as the currents at ends A and B will be multiplied by the Correction Factor, when the differential calculation is done.

6.7.9 FAULT LOCATION

In line with other similar MiCOM Px4 products this device has an integrated fault locator. Intended primarily for use on simple 2-terminal lines and cables, the operating principle of the fault locator relies on estimating a distance to fault based on impedance values derived from measured values of voltage and current. Calculated impedance values are compared with system data to determine the location of the fault on the network. The accuracy of the fault locator and the method to determine appropriate settings have much in common with the requirements to set distance protection elements. Setting distance protection to deliver accurate reliable performance on multi-terminal lines is challenging (and underlines why current differential protection is preferred for protection of multi-terminal lines). Accordingly, whilst an impedance-based fault locator is made available within this product, we recommend that it is used for indicative purposes only on multi-terminal applications.

Note:
The single-ended fault locator integral in this product should not be relied on to provide accurate fault-location in multi-terminal scheme applications.

More credible location of faults isolated by the operation of this device can be obtained at a scheme level by combining data from all the terminals in the scheme using the Fault Locator tool provided in the MiCOM S1 Agile tool suite. This tool uses Comtrade files captured by each of the devices in the scheme together. The Fault Locator tool is launched from the MiCOM S1 Agile Start Page by first selecting the Device Configuration tile, followed by the Px40/K/L/Px20(Courier) tile at the next page, and then the Fault Locator tile. This will launch fault locator software in a separate window allowing the appropriate network description to be generated. More details about this off-line tool can be found in the MiCOM MiCOM S1 Agile user documentation (User Guide).

We don’t recommend relying on the output of the integrated fault locator to provide reliable indication of fault location for multi-terminal applications. If you chose to use it, however, then you should be aware that the impedance-based fault locator uses setting and configuration data that is shared with the current differential application. You need to ensure, therefore, that all devices in the scheme are configured and set correctly to deliver multi-terminal line differential protection. In particular, ensure that the following are correct:

- In the *PROT COMMS/IM64* column
  - ***No of Junctions***
  - ***No of Terminals***
  - ***Scheme Address***
  - ***Terminal Address***
- In the *GROUP N LINE PARAMETERS* column (as applicable according to capacitive charging functionality *)
  - ***Line Length*** *
  - ***Line Impedance*** *
  - ***Line Angle*** *
  - ***Topology***
  - ***Line Types***
  - ***Z1***

- ***Z1 Angle***
- ***Z0***
- ***Z0 Angle***
- ***Y1***
- ***Y2***

If capacitive charging current compensation is not applicable (*) then the line parameters settings apply to the fault locator only.

If capacitive charging current compensation is applicable then, at each terminal, the fault locator bases its calculations on the value of impedance between that terminal and the adjacent junction in the scheme. Beyond the adjacent junction, estimating the impedance to fault (and hence location) is affected by the values of all other conductors in the protection scheme and the source impedances of the other terminals - all of which are unavailable, and render the calculations effectively invalid.

CHAPTER 7

NON-AIDED SCHEMES

7.1 CHAPTER OVERVIEW

This chapter contains the following sections:

Chapter Overview 138
Trip On Close Schemes 139

7.2 TRIP ON CLOSE SCHEMES

Logic is provided for situations where special tripping may be necessary following closure of the associated circuit breaker. Two cases of Trip on Close (TOC) logic are catered for:

- Switch on to Fault (SOTF)
- Trip on Reclose (TOR)

SOTF and TOR are included as indication only in P54A-E products. The ***SOTF Active*** and ***TOR Active*** DDBs can be mapped to Relay outputs to derive a Trip from these functions.

SOTF provides instantaneous operation of selected elements if a fault is present when manual closure of the circuit breaker is performed.

TOR provides instantaneous operation of selected elements if a persistent fault is present when the circuit breaker attempts autoreclosure

The SOTF and TOR functions are known as Trip on Close logic. Both methods operate in parallel if mapped to the SOTF and TOR Tripping matrix in the setting file.

The settings for Switch on to Fault (SOTF) and Trip on Reclose (TOR) are located in the *TRIP ON CLOSE* section of the *SCHEME LOGIC* column.

SOTF and TOR are complemented by Current No Voltage level detectors (also known as CNV level detectors). These CNV level detectors are set using the voltage and current settings located in the *CB FAIL & P.DEAD* column. The same settings are used for pole dead logic detection. A 10ms time delay in the logic avoids a possible race between very fast overvoltage and undercurrent level detectors.

The following figures show the Trip On Close function in relation to the ***Trip On Close function*** when driven by Current No Volt level detectors.

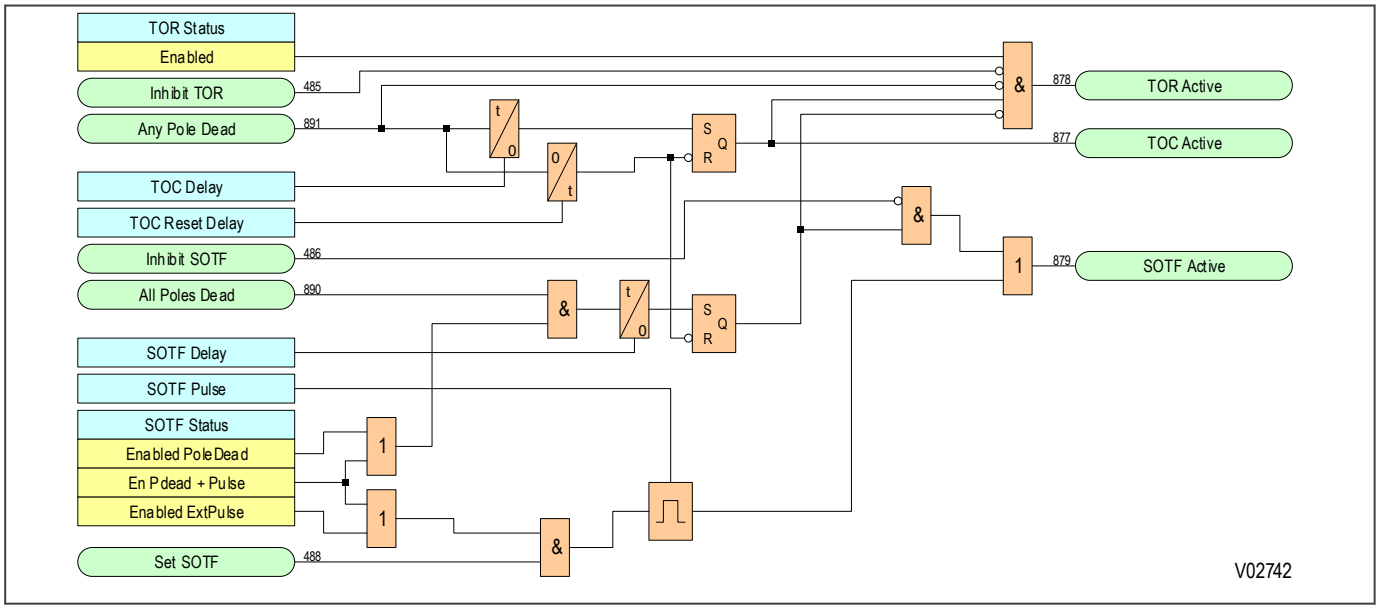


Figure 77: Trip on close logic

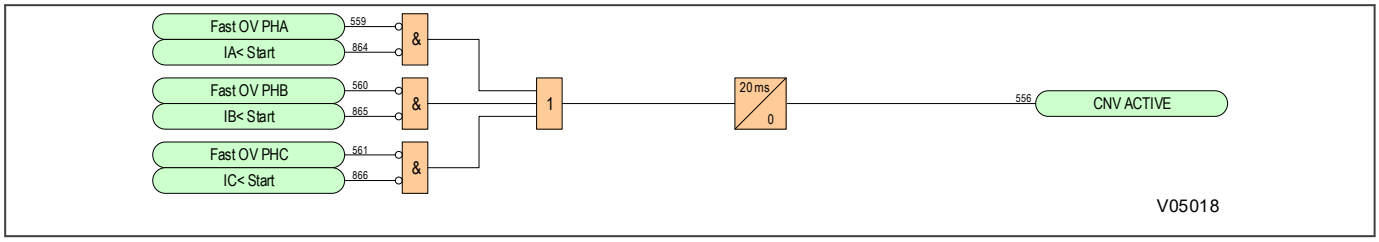


Figure 78: Trip on close based on CNV level detectors

7.2.1 SWITCH ON TO FAULT (SOTF)

You can use the ***SOTF Status*** setting to activated SOTF in in three different ways. It can be:

- Enabled using the pole dead detection logic. If an 'All Pole Dead' condition is detected, the ***SOTF Delay*** timer starts. Once this timer expires, SOTF is enabled and stays active for the period set in the ***TOC Reset Delay*** setting.
- Enabled by an external pulse. SOTF is enabled after an external pulse linked to DDB ***Set SOTF*** is ON. The external pulse could be a circuit breaker close command, for example. The function stays active for the duration of the ***SOTF Pulse*** setting.
- Enabled using both pole dead detection logic and an external pulse.

Three pole instantaneous tripping (and auto-reclose blocking) occurs for any fault detected ***or*** Current No Volt level detectors when in SOTF mode. Whether this feature is enabled or disabled, the normal time delayed elements or aided channel scheme continues to function and can trip the circuit.

The ***SOTF Delay*** is a pick up time delay that starts after opening all three poles of a circuit breaker (CB). If the CB is then closed after the set time delay has expired, SOTF protection is active. SOTF provides enhanced protection for manual closure of the breaker (not for auto-reclosure). This setting is visible only if `Enabled PoleDead` or `En Pdead + Pulse` are selected to enable SOTF.

While the Switch on to Fault Mode is active, the protection trips instantaneously for pick up of any current protection. If no elements are selected, the normal time delayed elements and current differential scheme provide the protection.

A user settable time window during which the SOTF protection is available through the ***SOTF Pulse*** setting This setting is visible only if `Enabled ExtPulse` or `En Pdead + Pulse` are selected to enable SOTF.

7.2.1.1 SWITCH ONTO FAULT MODE

To ensure fast isolation of faults (for example a closed three phase earthing switch), on energisation enable this feature with appropriate overcurrent elements or Current No Volt (CNV) level detectors, depending on utility practices.

When busbar voltage transformers are used, the ***Pole Dead*** signal is not produced. Connect circuit breaker auxiliary contacts for correct operation. This is not necessary if the SOTF is activated by an external pulse.

- ***SOTF Delay***: The time chosen should be longer than the slowest delayed-auto-reclose dead time, but shorter than the time in which the system operator might re-energise a circuit once it had opened/tripped. We recommend 110 seconds as a typical setting.
- ***SOTF Pulse***: Typically this could be set to at 500ms.
- ***TOC Reset Delay***: We recommend 500ms as a typical setting (chosen to be in excess of the 16 cycles length of memory polarising, allowing full memory charging before normal protection resumes).

7.2.2 TRIP ON RECLOSE (TOR)

Trip On Reclose (TOR) is special protection following auto-reclosure. The ***TOR status*** setting is used to enable or disable TOR. When enabled, TOR is activated after the TOC Delay expires, ready for application when an auto-reclose shot occurs.

When this feature is enabled, the protection operates in ‘Trip on Reclose mode’ for a period following circuit breaker (CB) closure. Three-phase instantaneous tripping occurs for any fault detected by the overcurrent protection or CNV level detectors. Whether this feature is enabled or disabled, the normal time-delayed elements or current differential scheme continue to function and can trip the circuit.

Note:
To map to a trip the TOR/SOTF active DDBs can be used in the PSL.

The SOTF and TOR features stay in service for the duration of the ***TOC Reset Delay*** time, once the circuit is energised. The delay timer starts on CB closure and is common for SOTF and TOR protection. Once this timer expires after successful closure, all protection reverts to normal.

A user settable time delay (***TOC Delay***) starts when the CB opens, after which TOR is enabled. The time delay must not exceed the minimum Dead Time setting of the auto-reclose because both times start simultaneously and TOR protection must be ready by the time the CB closes on potentially persistent faults.

7.2.2.1 TRIP ON RECLOSE MODE

To ensure fast isolation of all persistent faults following the circuit breaker reclosure, enable this feature.

- ***TOC Delay***: The Trip on Reclose (TOR) is activated after ***TOC Delay*** has expired. The setting must not exceed the minimum autoreclose ***Dead Time*** setting to make sure that the TOR is active immediately on reclose command.
- ***TOC Reset Delay***: We recommend 500ms as a typical setting.

CHAPTER 8

AUTORECLOSE

8.1 CHAPTER OVERVIEW

Selected models of this product provide sophisticated Autoreclose (AR) functionality. The purpose of this chapter is to describe the operation of this functionality including the principles, logic diagrams and applications.

This chapter contains the following sections:

Chapter Overview 143
Introduction to Autoreclose 144
Autoreclose Implementation 145
Autoreclose System Map 150
Logic Modules 164
Setting Guidelines 195

8.2 INTRODUCTION TO AUTORECLOSE

Approximately 80 - 90% of faults on transmission lines and distribution feeders are transient in nature. This means that most faults do not last long, and are self-clearing if isolated. A common example of a transient fault is an insulator flashover, which may be caused, for example, by lightning, clashing conductors, or wind-blown debris. Protection functions detecting the flashover will cause one or more circuit breakers to trip and may also remove the fault. If the source is removed, the fault does not recur if the line is re-energised.

The remaining 10 – 20% of faults are either semi-permanent or permanent. A small tree branch falling onto the line for example, could cause a semi-permanent fault. Here the cause of the fault would not be removed by immediate tripping of the circuit, but could possibly be burnt away during a time-delayed trip. Permanent faults could be broken conductors, transformer faults, cable faults or machine faults, which must be located and repaired before the power supply can be restored. In many fault incidents, if the faulty line is immediately tripped out, and time is allowed for the fault arc to de-ionise, reclosing the circuit breakers will result in the line being successfully re-energised.

Autoreclose schemes are used to automatically reclose a circuit breaker a set time after it has been opened due to operation of a protection element. On EHV transmission networks, Autoreclose is usually characterised by high-speed single-phase operation for the first attempt at reclosure. This is intended to help maintain system stability during a transient fault condition. On HV/MV distribution networks, Autoreclose is applied mainly to radial feeders, where system stability problems do not generally arise, and is generally characterised by delayed three-phase operation with potentially multiple reclosure attempts.

Autoreclosing provides an important benefit on circuits using time-graded protection, in that it allows the use of instantaneous protection to provide a high speed first trip. With fast tripping, the duration of the power arc resulting from an overhead line fault is reduced to a minimum. This lessens the chance of damage to the line, which might otherwise cause a transient fault to develop into a permanent fault. Using instantaneous protection also prevents blowing of fuses in teed feeders, as well as reducing circuit breaker maintenance by eliminating pre-arc heating. When instantaneous protection is used with Autoreclose, the scheme is normally arranged to block the instantaneous protection after the first trip. Therefore, if the fault persists after re-closure, the time-graded protection will provide discriminative tripping resulting in the isolation of the faulted section. However, for certain applications, where the majority of the faults are likely to be transient, it is common practise to allow more than one instantaneous trip before the instantaneous protection is blocked.

Some schemes allow a number of re-closures and time-graded trips after the first instantaneous trip, which may result in the burning out and clearance of semi-permanent faults. Such a scheme may also be used to allow fuses to operate in teed feeders where the fault current is low.

When considering feeders that are partly overhead line and partly underground cable, any decision to install Autoreclose should be subject to analysis of the data (knowledge of the frequency of transient faults). This is because this type of arrangement probably has a greater proportion of semi-permanent and permanent

faults than for purely overhead feeders. In this case, the advantages of Autoreclose are small. It can even be disadvantageous because re-closing on to a faulty cable is likely to exacerbate the damage.

8.3 AUTORECLOSE IMPLEMENTATION

Before describing this function it is first necessary to understand the following terminology:

- A **Shot** is an attempt to close a circuit breaker using the Autoreclose function.
- **Multi-shot** is where more than one **Shot** is attempted.
- **Single-shot** is where only one **Shot** is attempted.
- **Dead Time** denotes the time between initiation of the Autoreclose operation and the attempt to close the circuit breaker.
- **Reclaim time** is the time following the initiation of the circuit breaker closing and the resetting of the Autoreclose scheme should the Autoreclose attempt be successful and the protection does not detect a subsequent fault condition.
- **High-speed Autoreclose** is generally regarded as an Autoreclose application where the **Dead Time** is less than 1 second.
- **Delayed Autoreclose** is generally regarded as an Autoreclose application where the **Dead Time** is greater than 1 second.

This product features a multiple-shot Autoreclose function, which is suitable for both High-speed Autoreclose and Delayed Autoreclose.

The Autoreclose function can be set to perform a single-shot, two-shot, three-shot or four-shot cycle. Dead Times for all shots can be adjusted independently.

If a circuit breaker closes successfully at the end of the Dead Time, a Reclaim Time starts. If the circuit breaker does not trip again, the Autoreclose function resets at the end of the Reclaim Time. If the protection trips again during the Reclaim Time, the sequence advances to the next shot in the programmed cycle. If all programmed reclose attempts have been made and the circuit breaker does not remain closed, the Autoreclose function goes into Lockout, whereupon manual intervention is required.

An Autoreclose cycle can be initiated by operation of an internal or external protection element provided it is mapped correctly, and that the circuit breaker is closed when the protection operates.

You can choose to initiate the Dead Time on:

- Protection operation
- A protection reset
- A Line Dead condition
- Circuit breaker operation

At the end of the relevant Dead Time, provided system conditions are suitable, a circuit breaker close signal is given. The system conditions to be met for closing are that:

- the system voltages are in synchronism
- or that the dead line/live bus or live line/dead bus conditions exist as indicated by the internal system check synchronising element
- and that the circuit breaker closing spring, or other energy source, is fully charged as indicated by the circuit breaker healthy input.

The circuit breaker close signal is removed when the circuit breaker closes.

If the protection trips and the circuit breaker opens during the Reclaim Time, the Autoreclose function either advances to the next shot in the programmed cycle, or if all programmed reclose attempts have been made, goes into Lockout. Each time a closure is attempted, a sequence counter is incremented by 1 and the Reclaim Time starts again.

Autoreclose is configured in the *AUTORECLOSE* column of the relevant settings group. The function is disabled by default. If you wish to use it you must enable it first in the *CONFIGURATION* column.

The Autoreclose function is a logic controller implemented in software. It takes inputs and processes them according to defined logic to generates appropriate outputs. The logic is controlled by user prescribed settings and commands. The controlling logic is complex and so, in order to facilitate its design and understanding, it is decomposed into smaller logic functions which, when combined together implement the complete scheme. This section concludes with a summary of:

- the logic inputs to the Autoreclose function,
- the logic outputs from the Autoreclose function
- the Autoreclose operating sequence
- the high-level design of the system logic functionality

8.3.1 AUTORECLOSE LOGIC INPUTS FROM EXTERNAL SOURCES

Logic inputs control the operation of the Autoreclose function. The logic inputs are mapped using DDB signals in the PSL.

Generally the inputs are from external equipment connected to opto-isolated inputs. They can also come from communications inputs, and some are internally derived.

This section provides an overview of the logic inputs originating from external sources.

8.3.1.1 CIRCUIT BREAKER HEALTHY INPUT

For circuit breakers to close, it needs energy. This energy usually comes from a spring (spring-charged circuit breakers) or from gas pressure (gas pressurised circuit breakers). After closing, it is necessary to re-establish sufficient energy in the circuit breaker before it can be closed again.

DDB signal inputs to the Autoreclose function allow the health of circuit breakers to be mapped to the logic. when asserted, these signals demonstrate that there is sufficient energy available to close and trip the circuit breaker before initiating a circuit breaker close command. If the signal indicating the health of the circuit breaker is low, and remains low for a defined period set in the circuit breaker healthy timer, the circuit breaker locks out and stays open.

If the circuit breaker healthy signal is not mapped in the PSL, the DDB signal defaults to high so that Autoreclose may proceed.

8.3.1.2 INHIBIT AUTORECLOSE INPUT

A logic input can be used to inhibit the Autoreclose function. The signal is mapped to the DDB signal ***Inhibit AR*** in the PSL.

Energising the input inhibits any auto-switching of connected circuit breakers. Any Autoreclose in progress is reset and inhibited but not locked out. This function ensures that auto-switching does not interfere with any manual switching. A typical application is on a mesh-corner scheme where manual switching is being performed on the mesh, for which any Autoreclose would cause interference.

For products that are capable of single-phase tripping and Autoreclose, if a single-phase Autoreclose cycle is in progress and a single pole of the circuit breaker is tripped when the inhibit Autoreclose signal is raised, the circuit breaker is instructed to trip all phases, ensuring that all poles are in the same state (and avoiding a pole stuck condition) when subsequent closing of the circuit breaker is attempted.

8.3.1.3 BLOCK AUTORECLOSE INPUT

External inputs can be used to block the Autoreclose function. If Autoreclose is in progress when the signal is asserted, it forces a lockout.

Typically this feature is used where Autoreclose may be required for some protections functions but not required for others. An example is on a transformer feeder, where Autoreclose can be initiated from the feeder protection but blocked from the transformer protection.

It can also be used if an Autoreclose cycle is likely to fail for conditions associated with the protected circuit, such as during the Dead Time, if a circuit breaker indicates that it is not healthy to switch.

8.3.1.4 RESET LOCKOUT INPUT

If a condition that forced a lockout has been removed, the lockout can be reset by energising a logic input appropriately mapped in the PSL. Energising the input will also reset any Autoreclose alarms.

8.3.1.5 POLE DISCREPANCY INPUT

Circuit breakers with independent mechanisms for each pole (phase), normally incorporate a mechanism to cater for cases where the phases are not together. This automatically trips all three phases if they are either not all open, or not all closed.

During single-phase Autoreclosing a pole discrepancy condition is necessarily introduced, but the pole discrepancy device should not operate for this condition. This can be achieved using a delayed action pole discrepancy device with a delay longer than the single-pole Autoreclose Dead Time (***SP AR Dead Time*** setting).

Alternatively, an input can be used for external devices to indicate a pole discrepancy condition. The pole discrepancy input is activated by an external device to indicate that all three poles of a circuit breaker are not in the same position. If mapped in the PSL, energising the input forces three-phase tripping (providing there is not a single-phase Autoreclose in progress). Otherwise, a signal indicating single-phase Autoreclose in progress can be used to inhibit the external pole discrepancy device.

8.3.1.6 EXTERNAL TRIP INDICATION

Protection operation from a different device can be used to initiate the Autoreclose function. By default these external trip inputs are mapped to initiate Autoreclose and to initiate breaker failure protection (if the functions are enabled). These inputs are not mapped to the trip outputs. With appropriate mapping in the PSL however, the external device can use this product to trip connected circuit breakers.

8.3.2 AUTORECLOSE LOGIC INPUTS

This section provides an overview of the logic inputs, which are derived internally.

8.3.2.1 TRIP INITIATION SIGNALS

The phase A, phase B and phase C trip inputs are used to initiate single-phase and three-phase autoreclose. For the Autoreclose to work, you must ensure that these Trip Input signals remain appropriately mapped in the PSL.

8.3.2.2 CIRCUIT BREAKER STATUS INPUTS

Circuit breaker status information must be available as logic input(s) for Autoreclose to work. You can select whether to use CB open, CB closed, or both, as inputs. The settings are made in the *CB CONTROL* column of the menu, and you need to ensure that the PSL mapping of the chosen input(s) is correct.

8.3.2.3 SYSTEM CHECK SIGNALS

System Check and Check Synchronisation functions produce signals which are used by the Autoreclose logic ensure that the Autoreclose function is applied only when the system is in a suitable condition.

8.3.3 AUTORECLOSE LOGIC OUTPUTS

Output signals are provided to provide indication of an Autoreclose in progress (ARIP). An ARIP signal is asserted when an Autoreclose sequence starts. It remains high from initiation, either until lockout, or until successful Autoreclose.

An Autoreclose lockout condition resets any ‘Autoreclose in progress’ and associated signals. Signals are available to indicate that Autoreclose is in progress and that a circuit breakers has been successfully closed.

8.3.4 AUTORECLOSE OPERATING SEQUENCE

The Autoreclose sequence is controlled by so-called Dead Timers. Dead Time Control settings are used to select the conditions that initiate Dead Timers in the Autoreclose sequence (for example protection operate, protection reset, CB open, etc.). This section describes typical AR operation sequences in which Dead Timers start when protection operation resets.

Note:
In a multi-shot AR sequence, a number of Dead Timers are used (one for each shot). All Dead Timers are enabled when the sequence is initiated, but each timer only starts when the particular shot with which it is associated is triggered.

8.3.4.1 AR TIMING SEQUENCE - TRANSIENT FAULT

The figure below describes the operating sequence for a single-shot Autorecloser for a transient fault that clears when the faulted line is isolated.

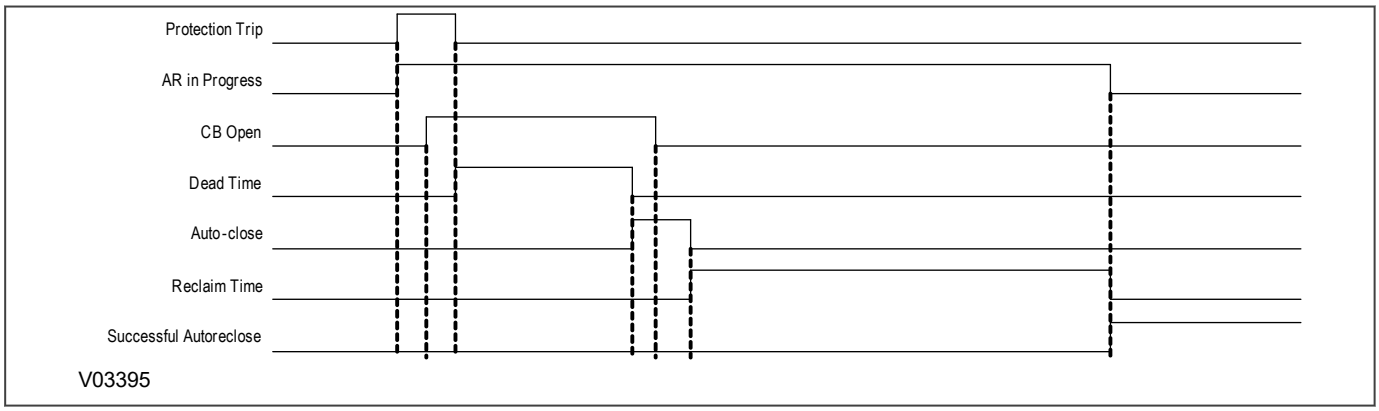


Figure 79: Autoreclose sequence for a transient fault

Following fault inception, the protection operates and issues a trip signal. At the same time the Autoreclose in Progress signal is asserted. Shortly afterwards the circuit breaker will open as indicated by the CB Open signal. Opening of the CB clears the fault and the protection resets. When this happens, the Dead Timer is started and the output remains high until the Dead Time setting expires, whereupon it resets and the Autorecloser issues the Auto-close command to close the circuit breaker. As the fault has been cleared, the circuit breaker closes and remains closed. When the Auto-close pulse is removed, the Reclaim Timer starts. If no further fault is detected before the Reclaim Timer expires, the Autoreclose is considered to be successful and this is indicated by the Successful Autoreclose signal.

8.3.4.2 AR TIMING SEQUENCE - EVOLVING/PERMANENT FAULT

The figure below shows a single-shot AR operating sequence where the fault is not cleared by the first AR cycle. The sequence starts in a similar way to that of a transient fault, but in this case the fault is not transient (it may be permanent, or it may evolve into a fault involving more than one phase). This case shows an evolving fault inception occurring before the Reclaim Time has expired. When the Autorecloser recognises that the protection has tripped, the cycle is terminated. The Autorecloser goes into Lockout, and the Autoreclose in Progress signal is reset.

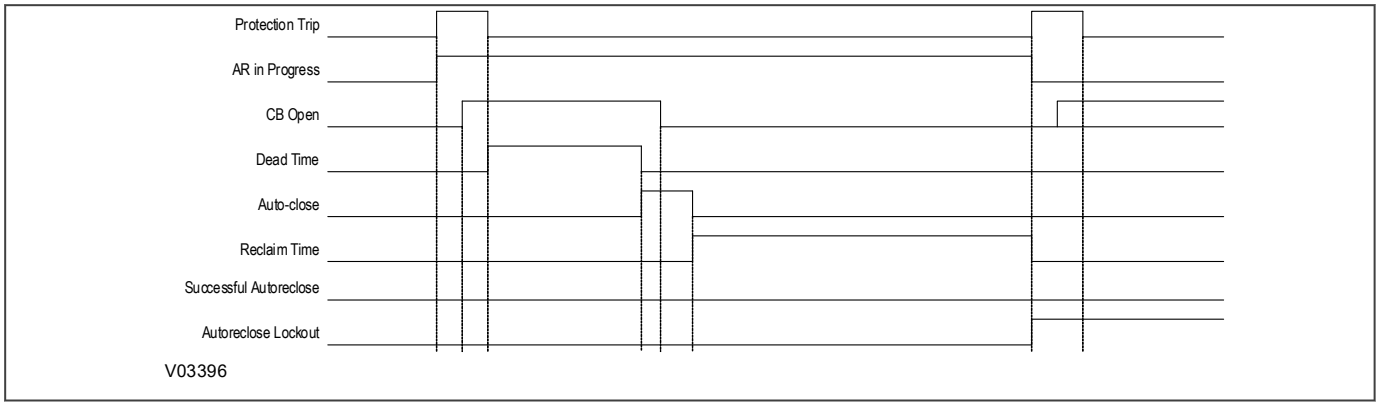


Figure 80: Autoreclose sequence for an evolving or permanent fault

8.3.4.3 AR TIMING SEQUENCE - EVOLVING/PERMANENT FAULT SINGLE-PHASE

If the Autorecloser is set for single-phase operation, then single phase operation is only allowed on the first shot. Subsequent tripping will be three-phase only until the AR has been successful or until AR has locked out as shown in the figure below.

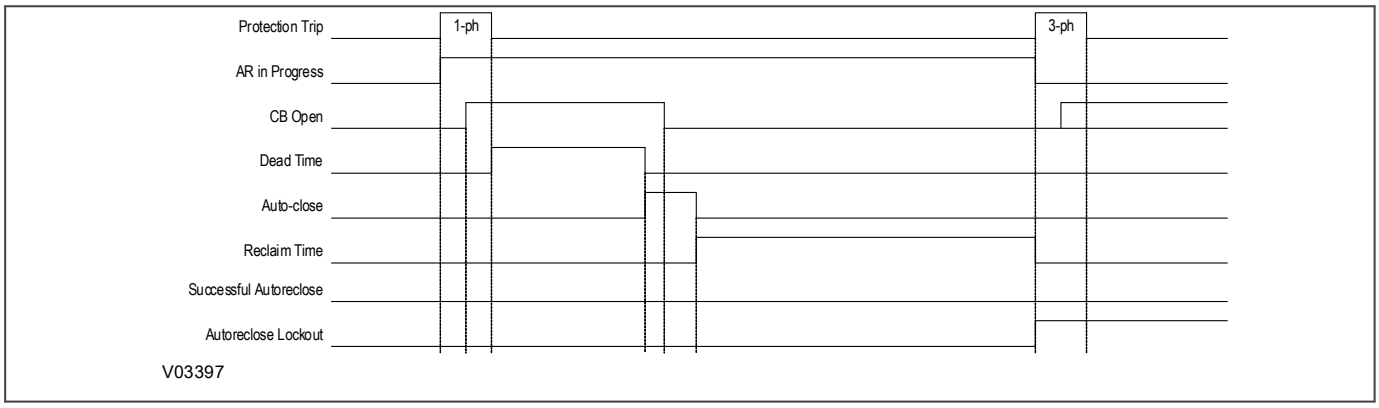


Figure 81: Autoreclose sequence for an evolving or permanent fault - single-phase operation

8.4 AUTORECLOSE SYSTEM MAP

The Autoreclose System Map describes the System Design of the Autoreclose Logic implemented in this product.

The Autoreclose is implemented in logical software modules. The logical software modules interact by exchanging signals between themselves, and with other software processes in the product. Interchange between modules is limited to digital signals which are realised as either DDB signals or so called “internal signals” (IntSigs). DDB signals are available for mapping in the PSL. Internal signals are similar to DDBs but they are self-contained within the device's functions and are not user-accessible.

The Autoreclose System Map shows the interconnection of the logic modules that are used in the Autoreclose system.

We recommend viewing the logic diagrams in colour rather than in black and white. The electronic version of the technical manual is in colour, but the printed version is not. However, coloured diagrams can be provided on request.

8.4.1 AUTORECLOSE SYSTEM MAP DIAGRAMS

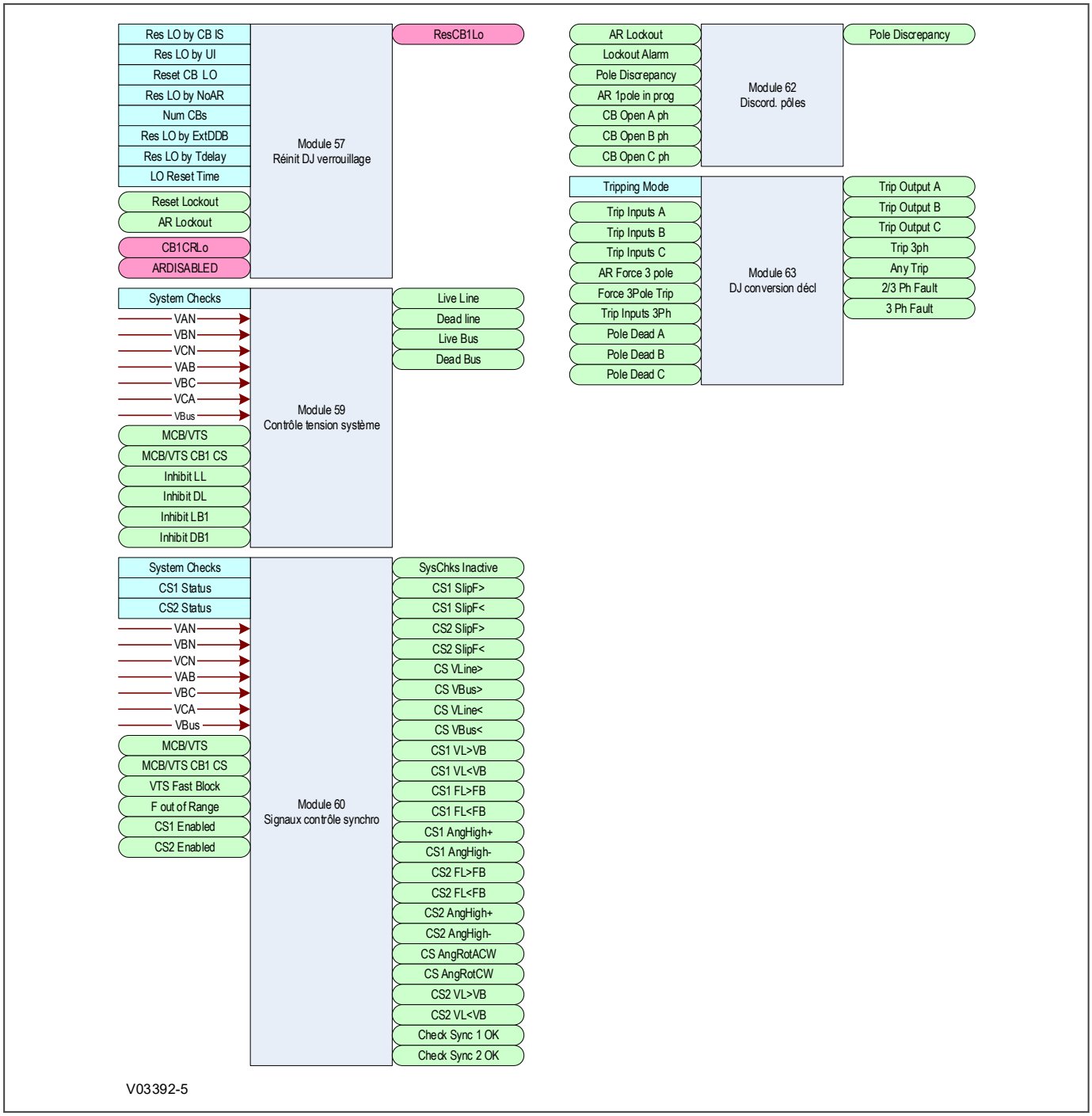


Figure 82: Autoreclose system map - part 1

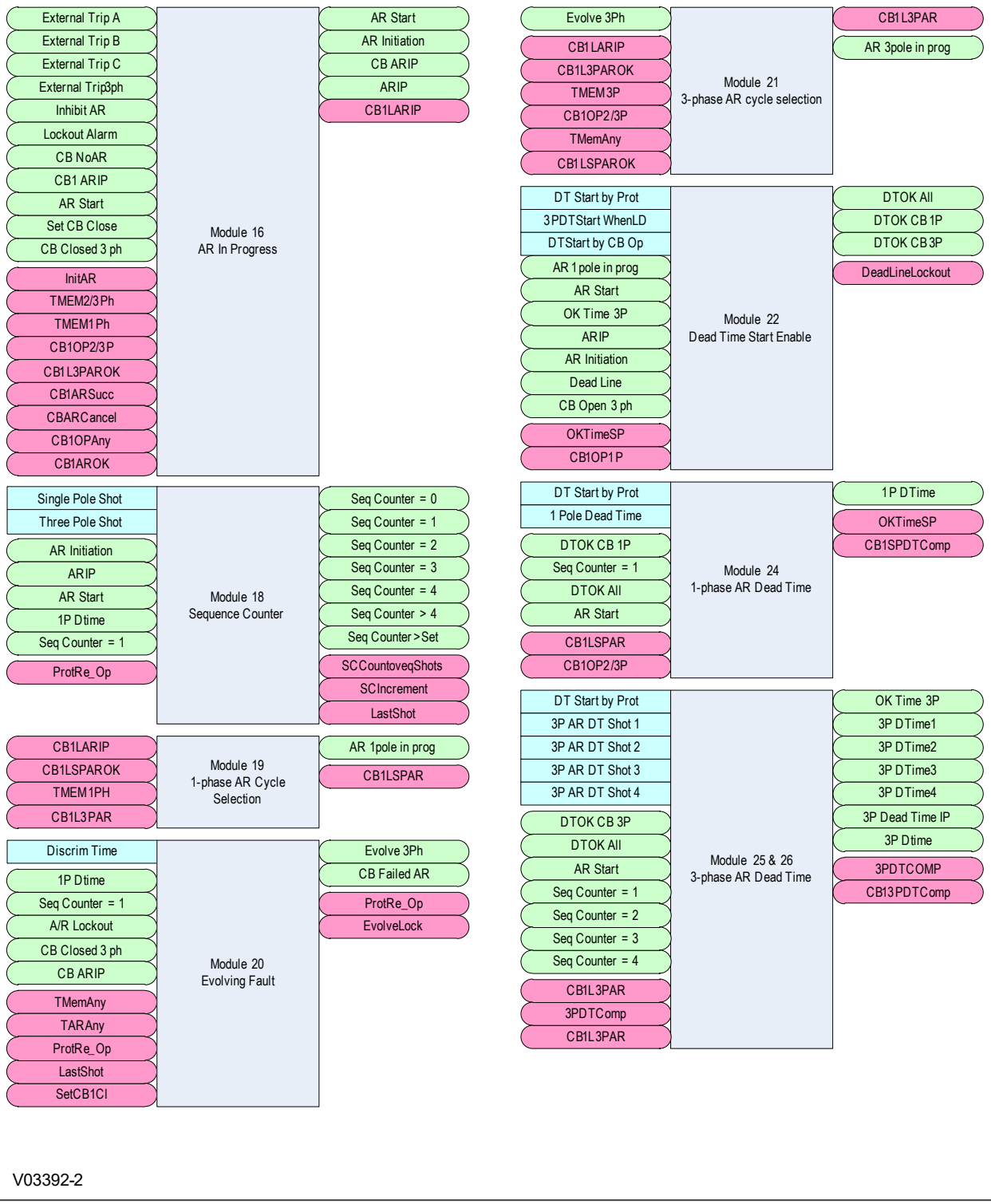


Figure 83: Autoreclose system map - part 2

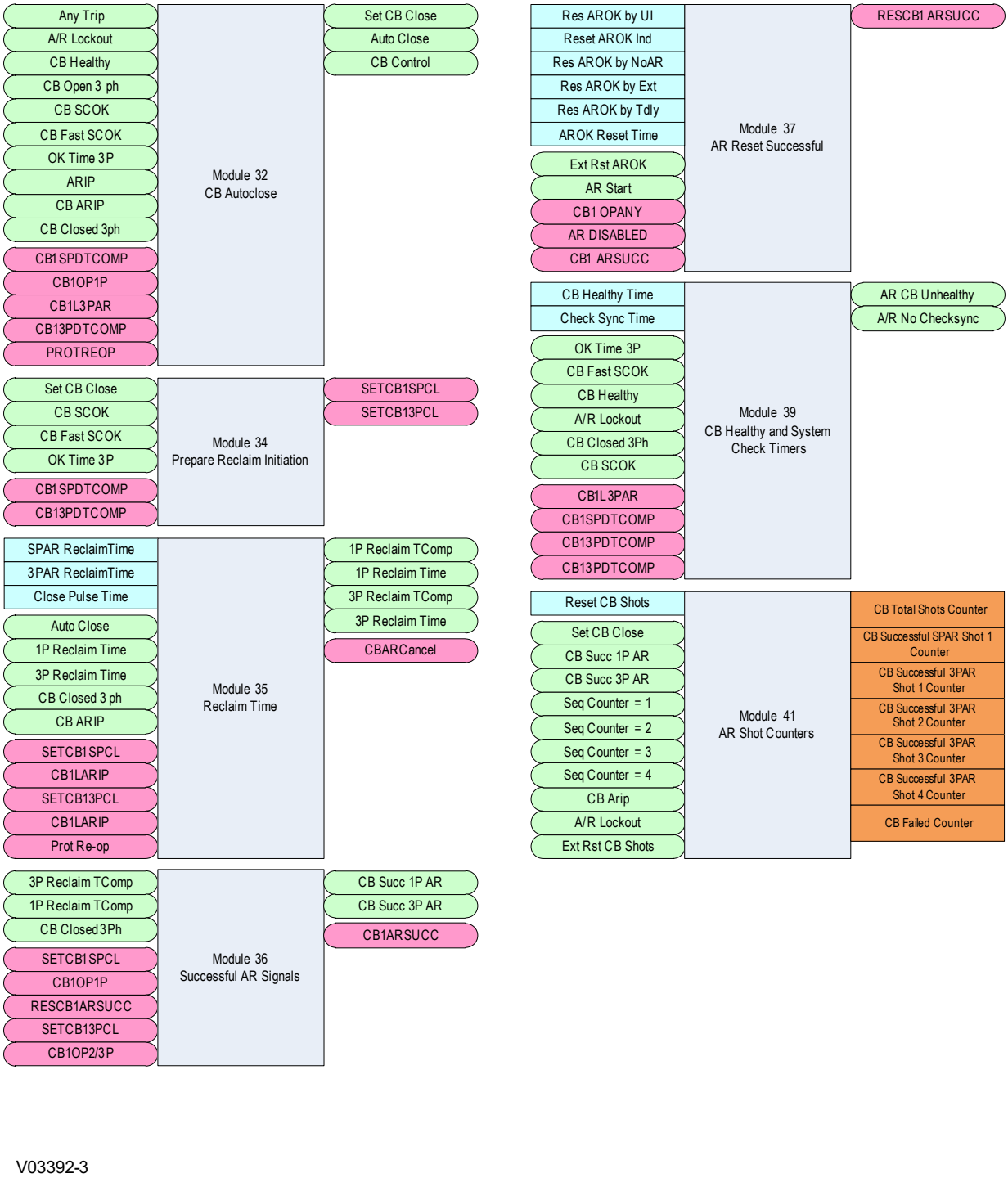


Figure 84: Autoreclose system map - part 3

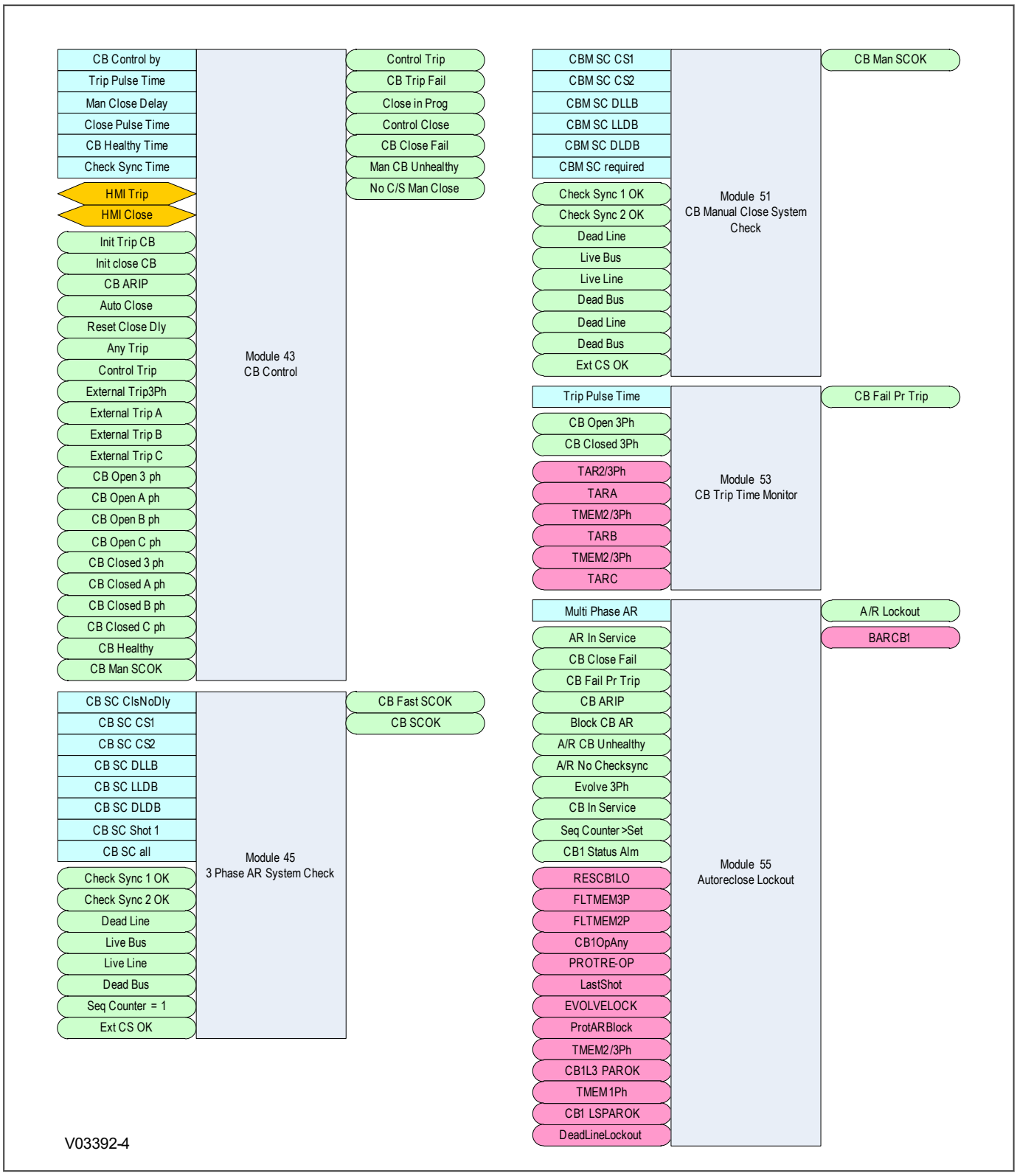


Figure 85: Autoreclose system map - part 4

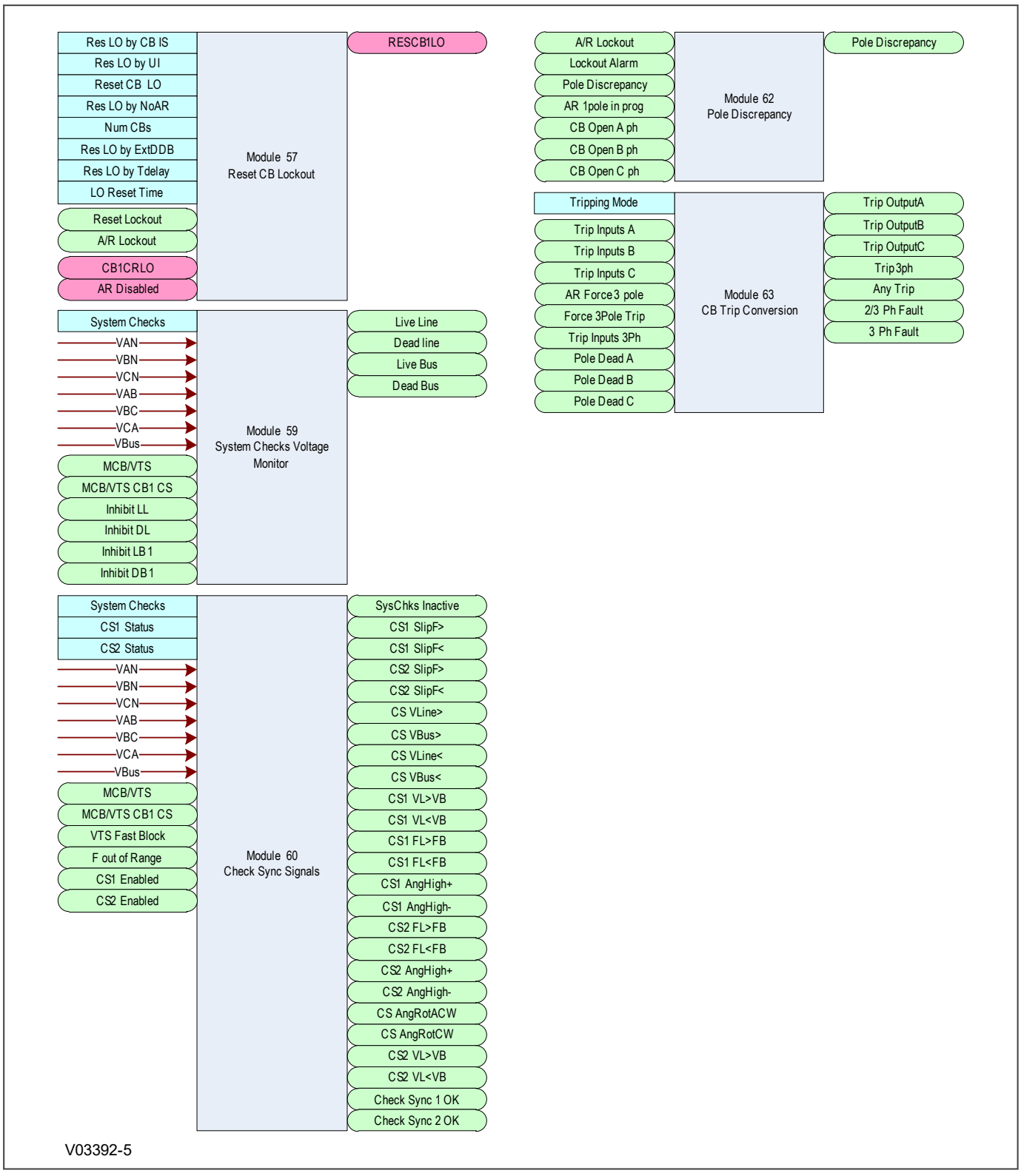


Figure 86: Autoreclose system map - part 5

8.4.2 AUTORECLOSE INTERNAL SIGNALS

The following table lists all the internal signals used in the CB control and Autoreclose logic system:

Signal Name	Source Module	Destination Module	Description
3PDTCOMP	3-phase AR Dead Time (25)	3-phase AR Dead Time (25)	Three phase dead time complete
AR DISABLED	AR Enabled (5)	Force 3-phase Trip (10) 1-pole/3-pole Trip (13) AR Reset Successful (37) Reset CB Lockout (57)	Overall Autoreclosing disabled
BAR CB	Autoreclose Lockout (55)	AR OK (8)	Block Autoreclose
CB 3PDTCOMP	3-phase AR Dead Time (25)	CB Autoclose (32) Prepare Reclaim Initiation (34) CB Healthy and System Check Timers (39)	Three-pole Autoreclose dead time is complete
CB AROK	AR OK (8)	AR In Progress (16)	CB is OK for Autoreclose
CB ARSUCC	Successful AR Signals (36)	AR In Progress (16) AR Reset Successful (37)	Autoreclose successful
CB LARIP	AR In Progress (16)	1-phase AR Cycle Selection (19) 3-phase AR Cycle Selection (21) Reclaim Time (35)	CB Autoreclose in progress
CB Op1P	CB Open (3)	Dead Time Start Enable (22) CB Autoclose (32) Successful AR Signals (36)	CB is open on 1 phase
CB Op2/3P	CB Open (3)	AR In Progress (16) 3-phase AR Cycle Selection (21) 1-phase AR Dead Time (24) Successful AR Signals (36)	CB is open on 2 or 3 phases
CB OpAny	CB Open (3)	AR In Progress (16) AR Reset Successful (37) Autoreclose Lockout (55)	CB is open on 1, 2 or 3 phases
CB SPOK	Force 3-phase Trip (10)		CB is OK for single-phase Autoreclose
CBCRLO	CB In Service (4)	Reset CB Lockout (57)	Reset CB lockout
CBL3PAR	3-phase AR Cycle Selection (21)	1-phase AR Cycle Selection (19) 3-phase AR Dead Time (25) CB Autoclose (32)	Three-phase Autoreclose is active
CBL3PAROK	AR Modes Enable (9)	AR In Progress (16) 3-phase AR Cycle Selection (21) Autoreclose Lockout (55)	CB is OK to perform three-phase Autoreclose
CBLSPAR	1-phase AR Cycle Selection (19)	1-phase AR Dead Time (24) CB Healthy and System Check Timers (39)	Single-phase Autoreclose is in progress
CBLSPAROK	AR Modes Enable (9)	Force 3-phase Trip (10) 1-phase AR Cycle Selection (19) 3-phase AR Cycle Selection (21) Autoreclose Lockout (55)	CB is OK to perform single-phase Autoreclose
CBSPDTCOMP	Dead Time Start Enable (22)	CB Autoclose (32) Prepare Reclaim Initiation (34) CB Healthy and System Check Timers (39)	CB single-phase dead time is complete
CBARCancel	Reclaim Time (35)	AR In Progress (16)	Cancel CB Autoreclose
DeadLineLockout	Dead Time Start Enable (22)	Autoreclose Lockout (55)	Signal to force the auto-reclose sequence to lockout
EVOLVE LOCK	Evolving Fault (20)	Autoreclose Lockout (55)	Lockout for 2nd trip after the "Discrim Time" has expired
FLTMEM 2P	Fault Memory (15)	Autoreclose Lockout (55)	A signal to indicate that the initiating fault involved 2 phases

Signal Name	Source Module	Destination Module	Description
FLTMEM 3P	Fault Memory (15)	Autoreclose Lockout (55)	A signal to indicate that the initiating fault involved 3 phases
INIT AR	AR Initiation (11), 1-pole/3-pole Trip (13), AR In Progress (16)		Internally derived signal to initiate Autoreclose (external triggers not included)
LastShot	Sequence Counter (18)	Evolving Fault (20) Autoreclose Lockout (55)	Idicates tha the Autoreclose sequence has reached the last shot
OKTimeSP	1-phase AR Dead Time (24)	Dead Time Start Enable (22)	The dead time for single pole Autoreclose is OK
Prot AR Block	AR Initiation (11)	Autoreclose Lockout (55)	Signal to block Autoreclose for selected host protection elements
Prot Re-op	Evolving Fault (20)	Sequence Counter (18) Evolving Fault (20) CB Autoclose (32) Reclaim Time (35) Autoreclose Lockout (55)	Signal to indicate that further protection operation has occurred during Autoreclose
RESCBARSUCC	AR Reset Successful (37)	Successful AR Signals (36)	Reset the indication of successful Autoreclose
RESCBLO	Reset CB Lockout (57)	Autoreclose Lockout (55)	Reset the indication of lockout
RESPRMEM	1-pole/3-pole Trip (13)	Fault Memory (15)	Reset the signal that indicates the faulted phases that initiated the Autoreclose
SETCB3PCL	Prepare Reclaim Initiation (34)	Reclaim Time (35) Successful AR Signals (36)	Three-phase close command to CB
SETCB1SPCL	Prepare Reclaim Initiation (34)	Reclaim Time (35) Successful AR Signals (36)	Single-phase close command to CB
Set CB Close		Evolving Fault (20)	Set CB as closed
TAR2/3Ph	1-pole/3-pole Trip (13)	1-pole/3-pole Trip (13) CB Trip Time Monitor (53)	A 2-phase or 3-phase trip has initiated Autoreclose
TARA	1-pole/3-pole Trip (13)	1-pole/3-pole trip (13) CB Trip Time Monitor (53)	An A-phase trip has initiated Autoreclose
TARANY	1-pole/3-pole Trip (13)	Force 3-phase Trip (10) 1-pole/3-pole Trip (13) Evolving Fault (20)	Any trip has initiated Autoreclose
TARB	1-pole/3-pole Trip (13)	1-pole/3-pole Trip (13) CB Trip Time Monitor (53)	A B-phase trip has initiated Autoreclose
TARC	1-pole/3-pole Trip (13)	1-pole/3-pole Trip (13) CB Trip Time Monitor (53)	A C-phase trip has initiated Autoreclose
TMEM1Ph	1-pole/3-pole Trip (13)	AR In Progress (16) 1-phase AR Cycle Selection (19) Autoreclose Lockout (55)	Signal to remember that Autoreclose was initiated by a single-phase fault
TMEM2/3Ph	1-pole/3-pole trip (13)	AR In Progress (16) CB Trip Time Monitor (53) Autoreclose Lockout (55)	Signal to remember that Autoreclose was initiated by a 2-phase fault or a 3-phase fault
TMEM3Ph	1-pole/3-pole Trip (13)	3-phase AR Cycle Selection (21)	Signal to remember that Autoreclose was initiated by a 3-phase fault
TMEMANY	1-pole/3-pole Trip (13)	Evolving Fault (20) 3-phase AR Cycle Selection (21)	Signal to remember that Autoreclose was initiated by an AnyTrip

8.4.3 AUTORECLOSE DDB SIGNALS

The following table lists all the DDB signals used in the CB control and Autoreclose logic system:

DDB Signal Name	DDB Signal Number	Source Module	Destination Module
1P DTime	1554	1-phase AR Dead Time (24)	Sequence Counter (18) Evolving Fault (20)
1P Reclaim TComp	1568	Reclaim Time (35)	Successful AR Signals
1P Reclaim Time	1567	Reclaim Time (35)	Reclaim Time Logic
2/3 Ph Fault	527	CB Trip Conversion (63)	
3 Ph Fault	528	CB Trip Conversion (63)	
3P Dead Time IP	853	3-phase AR Dead Time (25)	
3P Dtime	1560	3-phase AR Dead Time (25)	
3P DTime1	1556	3-phase AR Dead Time (25)	
3P DTime2	1557	3-phase AR Dead Time (25)	
3P DTime3	1558	3-phase AR Dead Time (25)	
3P DTime4	1559	3-phase AR Dead Time (25)	
3P Reclaim TComp	1570	Reclaim Time (35)	Successful AR Signals
3P Reclaim Time	1569	Reclaim Time (35)	Reclaim Time Logic
A/R CB Unhealthy	307	CB Healthy and System Check Timers (39)	Force 3-phase Trip Autoreclose Lockout
A/R Lockout	306	Autoreclose Lockout (55)	CB In Service AR OK Force 3-phase Trip Evolving Fault CB Autoclose Logic CB Healthy and System Check Timers Logic AR Shot Counters Reset CB Lockout Pole Discrepancy
A/R No Checksync	308	CB Healthy and System Check Timers (39)	Autoreclose Lockout
Any Trip	522	CB Trip Conversion (63)	AR Initiation CB Autoclose Logic CB Control
AR 1pole in prog	845		1-phase AR Cycle Selection Dead Time Start Enable Pole Discrepancy
AR 3pole in prog	844		3-phase AR Cycle Selection
AR Enable	1384		AR Enable
AR Enable CB	1609		AR Enable AR OK AR Modes Enable
AR Force 3 pole	858	Force 3-phase Trip (10)	CB Trip Conversion
AR In Service	1385	AR Enable (5)	AR OK AR Modes Enable Autoreclose Lockout
AR Initiation	1543	AR In Progress (16)	Sequence Counter Dead Time Start Enable
AR Mode 1P	1497		AR Modes Enable

DDB Signal Name	DDB Signal Number	Source Module	Destination Module
AR Mode 3P	1498		AR Modes Enable
AR OFF Pulse	1383		AR Enable
AR On Pulse	1382		AR Enable
AR Start	1541	AR In Progress (16)	Fault Memory AR In Progress Sequence Counter Dead Time Start Enable 1-phase AR Dead Time 3-phase AR Dead Time Enable AR Reset Successful Logic
AR Trip Test 3ph	576	Trip Test (12)	
AR Trip Test A	577	Trip Test (12)	AR Initiation
AR Trip Test B	578	Trip Test (12)	AR Initiation
AR Trip Test C	579	Trip Test (12)	AR Initiation
ARIP	1542	AR In Progress (16)	1-pole/3-pole trip Sequence Counter Dead Time Start Enable CB Autoclose Logic
Auto Close	854	CB Autoclose (32)	Reclaim Time CB Control
Block CB AR	448		Autoreclose Lockout
CB ARIP	1544	AR In Progress (16)	CB In Service Force 3-phase Trip Evolving Fault CB Autoclose AR In Progress Reclaim Time AR Shot Counters CB Control Autoreclose Lockout
CB Aux 3ph(52-A)	420		CB State Monitor
CB Aux 3ph(52-B)	424		CB State Monitor
CB Aux A(52-A)	421		CB State Monitor
CB Aux A(52-B)	425		CB State Monitor
CB Aux B(52-A)	422		CB State Monitor
CB Aux B(52-B)	426		CB State Monitor
CB Aux C(52-A)	423		CB State Monitor
CB Aux C(52-B)	427		CB State Monitor
CB Close Fail	303	CB Control (43)	Autoreclose Lockout
CB Closed 3 ph	907	CB State Monitor (1)	CB In Service CB Autoclose AR In Progress Evolving Fault Reclaim Time Successful AR Signals CB Healthy and System Check Timers CB Control CB Trip Time Monitor
CB Closed A ph	908	CB State Monitor (1)	CB Control

DDB Signal Name	DDB Signal Number	Source Module	Destination Module
CB Closed B ph	909	CB State Monitor (1)	CB Control
CB Closed C ph	910	CB State Monitor (1)	CB Control
CB Control	1566	CB Autoclose (32)	
CB Fail Pr Trip	1575	CB Trip Time Monitor (53)	Autoreclose Lockout
CB Failed AR	1550	Evolving Fault (20)	
CB Fast SCOK	1572	3 Phase AR System Check (45)	CB Autoclose Prepare Reclaim Initiation CB Healthy and System Check Timers
CB Healthy	436		CB Autoclose CB Healthy and System Check Timers CB Control
CB In Service	1526	CB In Service (4)	AR OK Autoreclose Lockout
CB Man SCOK	1574	3 Phase AR System Check (45) CB Manual Close System Check (51)	CB Control
CB NoAR	1528	AR OK (8)	AR In Progress
CB Open 3 ph	903	CB State Monitor (1)	CB Open Dead Time Start Enable CB Autoclose Logic CB Control CB Trip Time Monitor
CB Open A ph	904	CB State Monitor (1)	CB Open CB Control Pole Discrepancy
CB Open B ph	905	CB State Monitor (1)	CB Open CB Control Pole Discrepancy
CB Open C ph	906	CB State Monitor (1)	CB Open CB Control Pole Discrepancy
CB SCOK	1573	3 Phase AR System Check (45)	CB Autoclose Prepare Reclaim Initiation Logic CB Healthy and System Check Timers
CB Status Alarm	301	CB State Monitor (1)	
CB Succ 1P AR	1571	Successful AR Signals (36)	AR Shot Counters
CB Succ 3P AR	852	Successful AR Signals (36)	AR Shot Counters
CB Trip Fail	302	CB Control (43)	
Check Sync 1 OK	883	Check Sync Signals (60)	3 Phase AR System Check CB Manual Close System Check
Check Sync 2 OK	884	Check Sync Signals (60)	3 Phase AR System Check CB Manual Close System Check
Close in Prog	842	CB Control (43)	
Control Close	839	CB Control (43)	
Control Trip	838	CB Control (43)	CB Control
CS AngRotACW	1594	Check Sync Signals (60)	
CS AngRotCW	1595	Check Sync Signals (60)	
CS1 SlipF>	1578	Check Sync Signals (60)	

DDB Signal Name	DDB Signal Number	Source Module	Destination Module
CS1 SlipF<	1579	Check Sync Signals (60)	
CS VBus<	1583	Check Sync Signals (60)	
CS VBus>	1582	Check Sync Signals (60)	
CS VLine<	1580	Check Sync Signals (60)	
CS VLine>	1581	Check Sync Signals (60)	
CS1 AngHigh-	1593	Check Sync Signals (60)	
CS1 AngHigh+	1592	Check Sync Signals (60)	
CS1 FL<FB	1591	Check Sync Signals (60)	
CS1 FL>FB	1590	Check Sync Signals (60)	
CS1 VL<VB	1588	Check Sync Signals (60)	
CS1 VL>VB	1586	Check Sync Signals (60)	
CS2 AngHigh-	1496	Check Sync Signals (60)	
CS2 AngHigh+	1495	Check Sync Signals (60)	
CS2 FL<FB	1494	Check Sync Signals (60)	
CS2 FL>FB	1493	Check Sync Signals (60)	
CS2 SlipF<	1465	Check Sync Signals (60)	
CS2 VL<VB	1589	Check Sync Signals (60)	
CS2 VL>VB	1587	Check Sync Signals (60)	
Dead Bus	887	System Checks Voltage Monitor (59)	3 Phase AR System Check CB Manual Close System Check
Dead Line	889	System Checks Voltage Monitor (59)	Dead Time Start Enable 3 Phase AR System Check CB Manual Close System Check
DTOK All	1551	Dead Time Start Enable (22)	1-phase AR Dead Time 3-phase AR Dead Time Enable
DTOK CB 1P	1552	Dead Time Start Enable (22)	1-phase AR Dead Time
DTOK CB 3P	1553	Dead Time Start Enable (22)	3-phase AR Dead Time Enable
Evolve 3Ph	1547	Evolving Fault (20)	3-phase AR cycle selection Autoreclose Lockout
Ext CS OK	900		3 Phase AR System Check CB Manual Close System Check
Ext Fault Aph	1508		Fault Memory
Ext Fault BPh	1509		Fault Memory
Ext Fault CPh	1510		Fault Memory
Ext Rst AROK	1517		AR Reset Successful Logic
Ext Rst CB Shots	1518		AR Shot Counters
External Trip A	535		1-pole/3-pole trip, AR In Progress, CB Control
External Trip B	536		1-pole/3-pole trip, AR In Progress, CB Control
External Trip C	537		1-pole/3-pole trip, AR In Progress, CB Control
External Trip3ph	534		1-pole/3-pole trip, AR In Progress, CB Control
F out of Range	319		Check Sync Signals
Force 3Pole Trip	533		CB Trip Conversion
IA< Start	864		AR Initiation
IB< Start	865		AR Initiation

DDB Signal Name	DDB Signal Number	Source Module	Destination Module
IC< Start	866		AR Initiation
Inhibit AR	1420		AR In Progress, Force 3-phase Trip
Inhibit DB	1525		System Checks Voltage Monitor
Inhibit DL	1523		System Checks Voltage Monitor
Inhibit LB	1524		System Checks Voltage Monitor
Inhibit LL	1522		System Checks Voltage Monitor
Init 3P AR Test	1507		Trip Test
Init APh AR Test	1504		Trip Test
Init BPh AR Test	1505		Trip Test
Init Close CB	440		CB Control
Init CPh AR Test	1506		Trip Test
Init Trip CB	439		CB Control
Live Bus	886	System Checks Voltage Monitor (59)	3 Phase AR System Check CB Manual Close System Check
Live Line	888	System Checks Voltage Monitor (59)	3 Phase AR System Check CB Manual Close System Check
Lockout Alarm	860		AR In Progress Pole Discrepancy
Man CB Unhealthy	304	CB Control (43)	
MCB/VTS	438		System Checks Voltage Monitor
MCB/VTS CB CS	1521		System Checks Voltage Monitor
No C/S Man Close	305	CB Control (43)	
OK Time 3P	1555	3-phase AR Dead Time (25)	Dead Time Start Enable 3-phase AR Dead Time CB Autoclose Prepare Reclaim Initiation CB Healthy and System Check Timers
Pole Dead A	892		CB Trip Conversion
Pole Dead B	893		CB Trip Conversion
Pole Dead C	894		CB Trip Conversion
Pole Discrepancy	699	Pole Discrepancy (62)	Pole Discrepancy
Reset Close Dly	443		CB Control
Reset Lockout	446		Reset CB Lockout
Seq Counter = 0	846	Sequence Counter (18)	AR Modes Enable
Seq Counter = 1	847	Sequence Counter (18)	AR Modes Enable Force 3-phase Trip Sequence Counter Evolving Fault 1-phase AR Dead Time 3-phase AR Dead Time Logic AR Shot Counters 3 Phase AR System Check
Seq Counter = 2	848	Sequence Counter (18)	Force 3-phase Trip 3-phase AR Dead Time Logic AR Shot Counters

DDB Signal Name	DDB Signal Number	Source Module	Destination Module
Seq Counter = 3	849	Sequence Counter (18)	Force 3-phase Trip 3-phase AR Dead Time Logic AR Shot Counters
Seq Counter = 4	850	Sequence Counter (18)	Force 3-phase Trip 3-phase AR Dead Time Logic AR Shot Counters
Seq Counter > 4	851	Sequence Counter (18)	
Seq Counter>Set	1546	Sequence Counter (18)	Force 3-phase Trip Autoreclose Lockout
Set CB Close	1565	CB Autoclose (32)	AR In Progress Prepare Reclaim Initiation AR Shot Counters
SysChks Inactive	880	Check Sync Signals (60)	
Trip 3ph	526	CB Trip Conversion (63)	
Trip AR MemA	1535	1-pole/3-pole Trip (13)	1-pole/3-pole trip
Trip AR MemB	1536	1-pole/3-pole Trip (13)	1-pole/3-pole trip
Trip AR MemC	1537	1-pole/3-pole Trip (13)	1-pole/3-pole trip
Trip Inputs 3Ph	529		CB Trip Conversion
Trip Inputs A	530		Fault Memory CB Trip Conversion
Trip Inputs B	531		Fault Memory CB Trip Conversion
Trip Inputs C	532		Fault Memory CB Trip Conversion
Trip Output A	523	CB Trip Conversion (63)	1-pole/3-pole trip
Trip Output B	524	CB Trip Conversion (63)	1-pole/3-pole trip
Trip Output C	525	CB Trip Conversion (63)	1-pole/3-pole trip
VTS Fast Block	832		Check Sync Signals

8.5 LOGIC MODULES

This section contains a complete set of logic diagrams, which will help to explain the Autoreclose function. Most of the logic diagrams shown are logic modules that comprise the overall Autoreclose system. Some of the diagrams shown are not directly related to Autoreclose functionality, however, they may use some inputs are produce outputs that are used by the Autoreclose system. These diagrams are shown in this section for the sake of completeness.

8.5.1 CIRCUIT BREAKER STATUS MONITOR

The Circuit Breaker State Monitor logic is part of the Monitoring and Control functionality and is fully described in that chapter. The logic diagram is repeated in this section because some of the outputs of this logic module are used as inputs to some of the Autoreclose logic modules.

8.5.1.1 CB STATE MONITOR LOGIC DIAGRAM

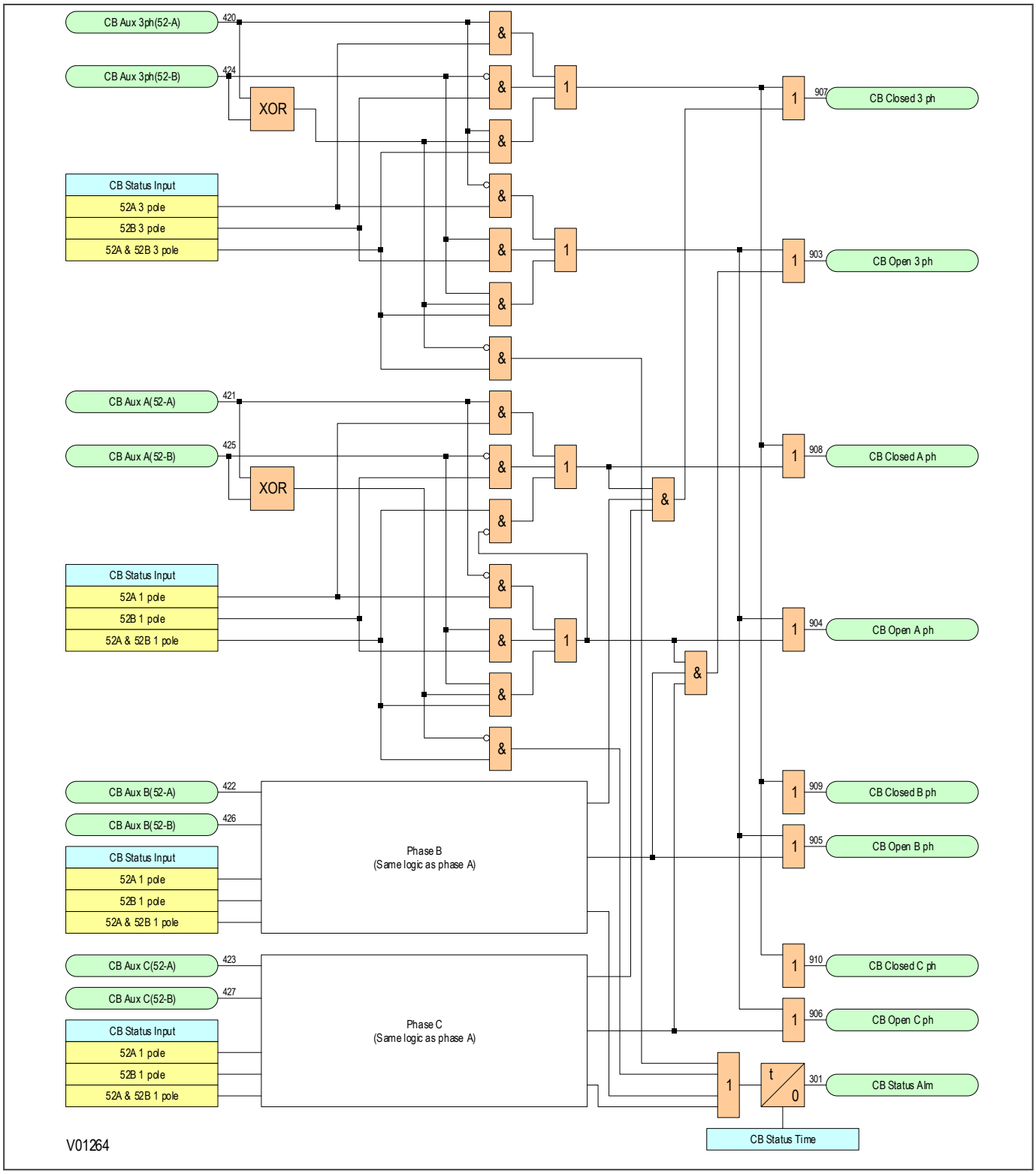


Figure 87: CB state monitor logic (module 1)

8.5.2 CIRCUIT BREAKER OPEN LOGIC

The Circuit Breaker Open logic module produces internal signals indicating the open status of one or more phases. These signals are used by some of the Autoreclose logic modules.

8.5.2.1 CIRCUIT BREAKER OPEN LOGIC DIAGRAM

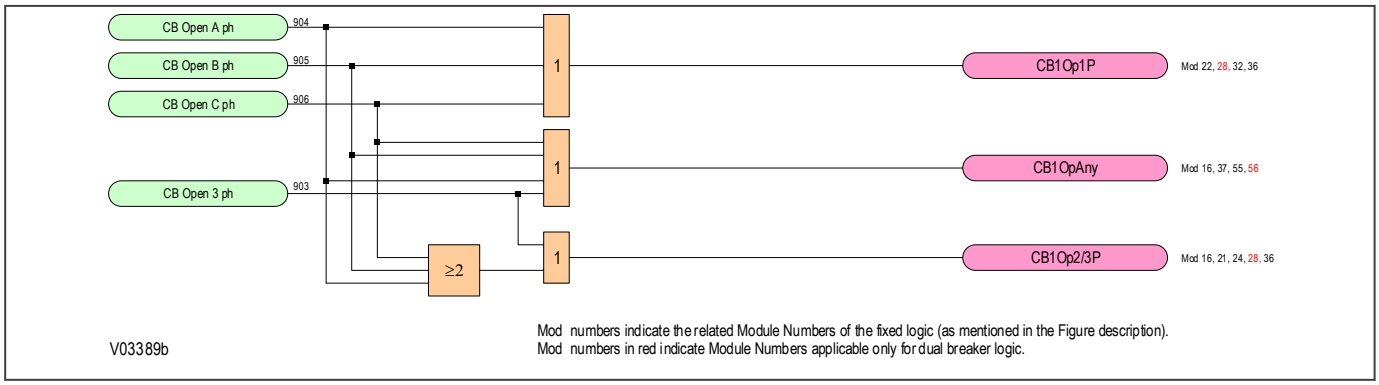


Figure 88: Circuit breaker open logic (module 3)

8.5.3 CIRCUIT BREAKER IN SERVICE LOGIC

For Autoreclose to proceed, a circuit breaker has to be in service when the Autoreclose is initiated. A circuit breaker is considered to be in service if it has been closed for more than the CB IS Time setting.

For applications with fast-acting circuit breaker auxiliary switches, a time delay setting CB IS Memory Time is provided. This is used to ensure correct operation if a delay between the circuit breaker tripping and recognition by the protection, is expected.

When an Autoreclose cycle starts, the “in service” signal for a circuit breaker stays set until the Autoreclose cycle finishes.

The circuit breaker “in service” signal resets if the circuit breaker opens, or if the corresponding Autoreclose in progress (ARIP) signal resets.

8.5.3.1 CIRCUIT BREAKER IN SERVICE LOGIC DIAGRAM

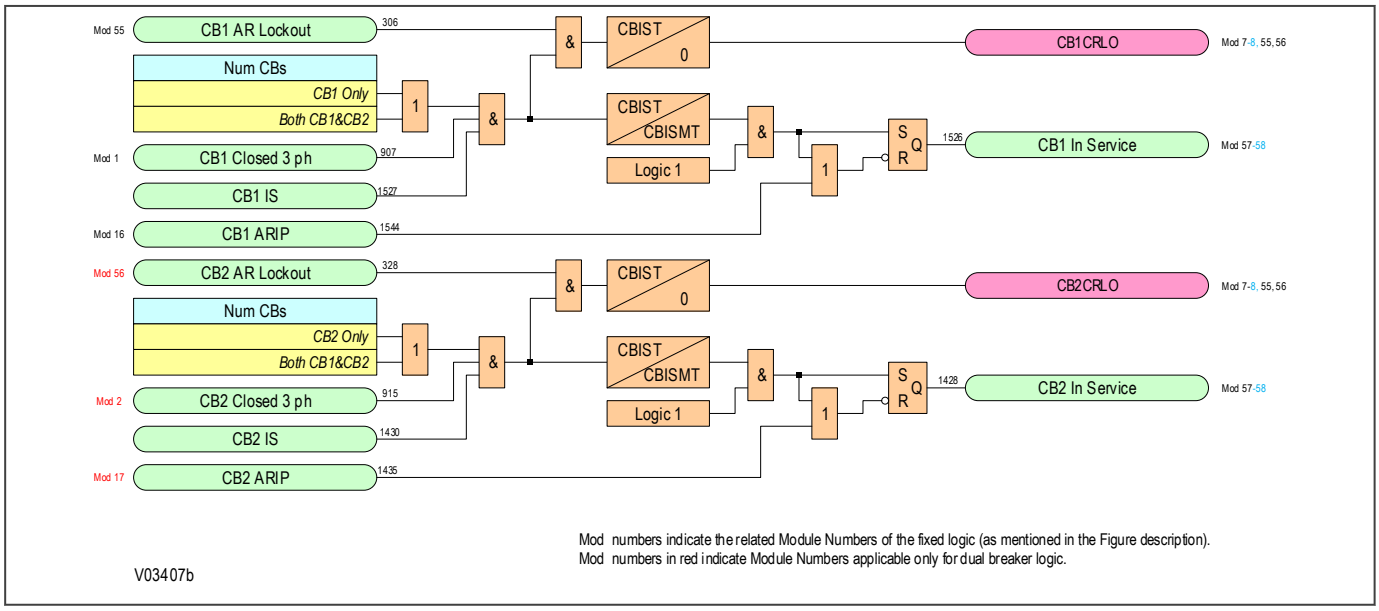


Figure 89: CB in service logic (module 4)

8.5.3.2 AUTORECLOSE OK LOGIC DIAGRAM

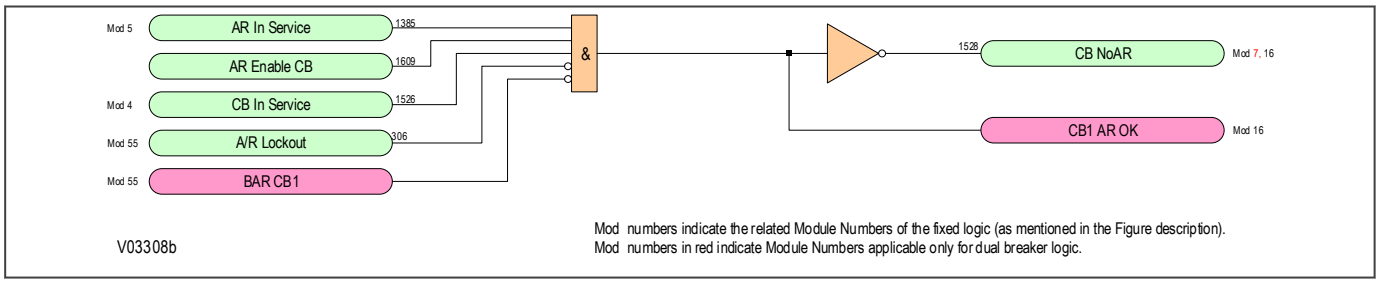


Figure 90: Autoreclose OK logic (module 8)

8.5.4 AUTORECLOSE ENABLE

The Autoreclose function must be enabled in the *CONFIGURATION* column before it can be brought into service. It can be brought into service by:

- using an opto-input mapped to the ***AR Enable*** DDB signal
- pulsing the DDB signal ***AR Pulse On*** (use ***AR Pulse Off*** to bring it out of service)
- programming a function key on the HMI.
- if applicable, using IEC 60870-5-103 communications

A further validation signal is also required to switch on Autoreclose. This is the DDB signals ***AR Enable CB***. Once Autoreclose is in service, the ***AR In Service*** DDB signal is asserted and the ***AR Status*** cell in the *CB CONTROL* column is set accordingly.

8.5.4.1 AUTORECLOSE ENABLE LOGIC DIAGRAM

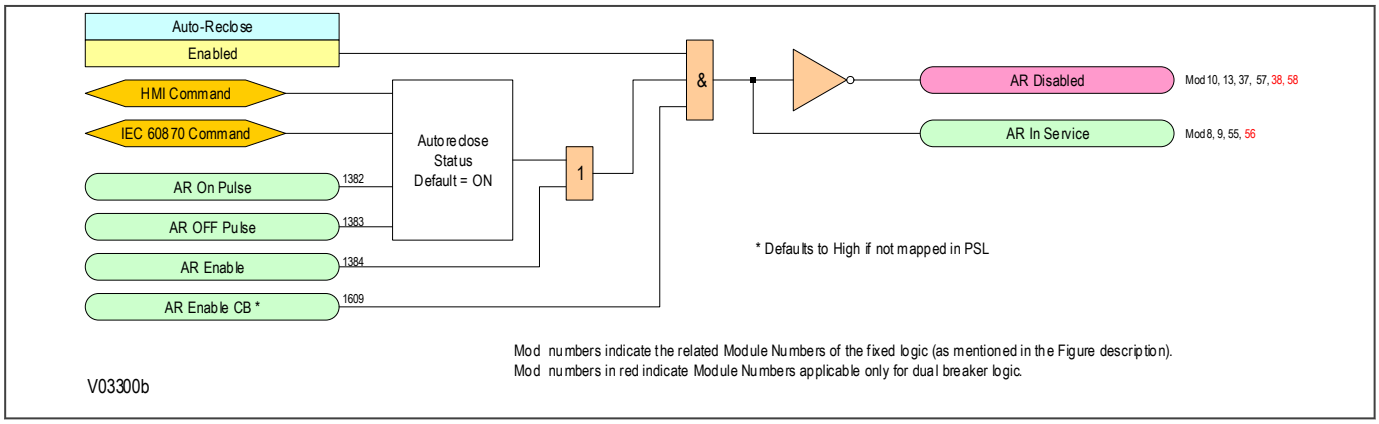


Figure 91: Autoreclose enable logic (module 5)

8.5.5 AUTORECLOSE MODES

The device can provide Single-phase and/or Three-phase Autoreclose. The Autoreclose mode is configured by the ***AR Mode*** setting in the *AUTORECLOSE* column. You can choose from:

- Single-phase (`AR 1P`)
- Three-phase (`AR 3P`)
- Single-phase and Three-phase (`AR 1/3P`)
- Controlled by commands from DDB signals that must be mapped to opto-isolated inputs in the PSL (`AR Opto`).

Single-phase Autoreclosing is permitted only for the first shot of an Autoreclose cycle. In a multi-shot Autoreclose cycle the second and subsequent trips will always be three-phase.

For multi-phase faults, you can use the ***Multi Phase AR*** setting in the *AUTORECLOSE* column to configure the following options:

- Allow Autoreclose for all fault types (`Allow Autoclose`)
- Block Autoreclose for 2-phase and 3-phase faults (`BAR 2 and 3 ph`)
- Block Autoreclose for 3-phase faults (`BAR 3 Phase`)

8.5.5.1 SINGLE-PHASE AND THREE-PHASE AUTORECLOSE

Single-phase autoreclose only

If single-phase Autoreclose is enabled, the logic allows only a single shot Autoreclose. For a single-phase fault, the single phase dead timer ***SP AR Dead Time*** starts, and the DDB signal ***CB AR 1pole in prog*** is asserted, which indicates that single-phase Autoreclose is in progress. In this case, for a multi-phase fault the logic triggers a three-phase trip and goes to lockout.

Three-phase autoreclose only

During three-phase Autoreclose, for any fault, the three-phase dead timers: ***3P AR DT Shot 1***, ***3P AR DT Shot 2***, ***3P AR DT Shot 3*** and ***3P AR DT Shot 4*** are started and the DDB signal ***CB AR 3pole in prog*** is asserted, which indicates that three-phase Autoreclose is in progress.

If three-phase only Autoreclose is enabled, the logic forces a three-phase trip by setting the DDB signal ***AR Force 3 pole*** for any single-phase fault.

Single-phase and three-phase autoreclose

With single-phase and three-phase Autoreclose enabled then, if the first fault is a single-phase fault the single-phase dead time ***SP AR Dead Time*** is started and the single-phase Autoreclose in progress signal is asserted. If the first fault is a multi-phase fault the three phase dead timer ***3P AR DT Shot 1*** is started and the three-phase Autoreclose in progress signal is asserted. If set to allow more than one reclose (***AR Shots*** >'1') then any subsequent faults are converted to three-phase trips by setting the force three-pole tripping signal. The three-phase dead times ***3P AR DT Shot 2***, ***3P AR DT Shot 3*** and ***3P AR DT Shot 4*** (Dead Times 2, 3, 4) are started for the 2nd, 3rd and 4th trips (shots) respectively. The DDB signal ***AR 3pole in prog*** is asserted. If a single-phase fault evolves to a multi-phase fault during the single-phase dead time (***SP AR Dead Time***), single-phase Autoreclose is stopped. The single-phase Autoreclose in progress signal is reset, the three-phase Autoreclose in progress signal is set, and the three-phase dead timer ***3P AR DT Shot 1*** is started.

8.5.5.2 AUTORECLOSE MODES ENABLE LOGIC DIAGRAM

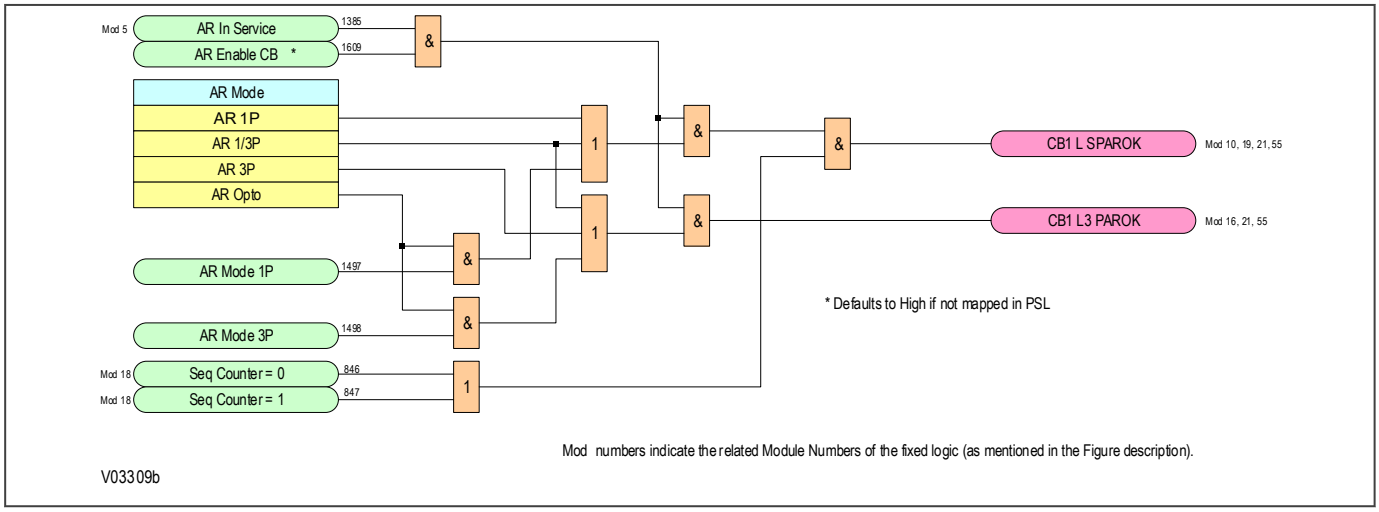


Figure 92: Autoreclose modes enable logic (module 9)

8.5.6 AR FORCE THREE-PHASE TRIP LOGIC

Following single-phase tripping, while the Autoreclose cycle is in progress, and upon resetting of the protection elements, tripping switches to three-phase.

Any protection operations that occur for subsequent faults while the Autoreclose cycle remains in progress will be tripped three-phase.

8.5.6.1 AR FORCE THREE-PHASE TRIP LOGIC DIAGRAM

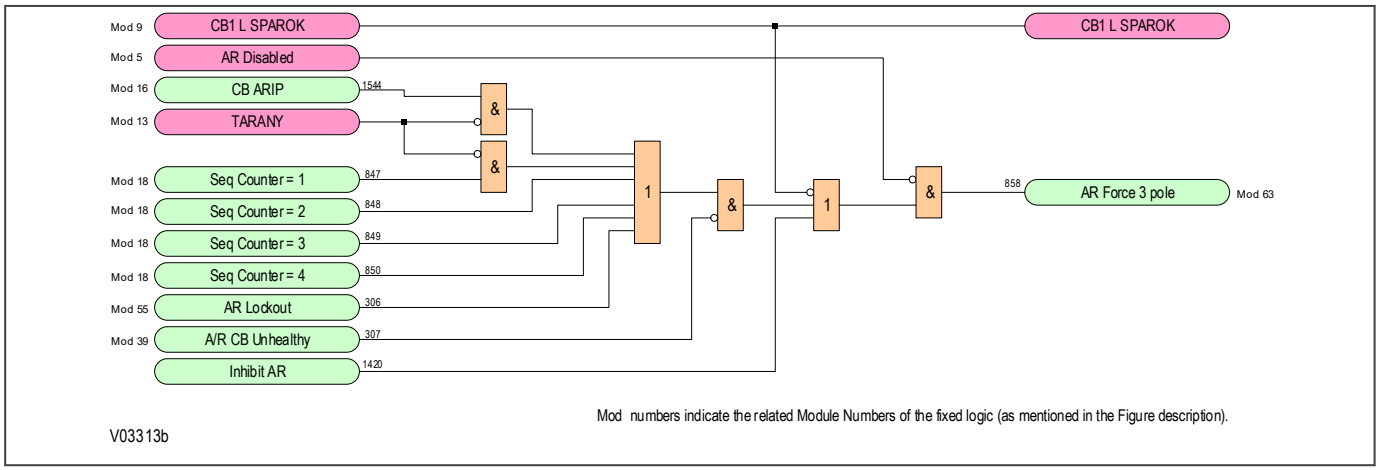


Figure 93: Force three-phase trip logic (module 10)

When a three-phase trip is forced, the DDB signal ***AR Force 3 pole*** is asserted.

8.5.7 AUTORECLOSE INITIATION LOGIC

Autoreclose initiation starts Autoreclose for a circuit breaker only if Autoreclose is enabled for the circuit breaker, and the circuit breaker is in service. When an Autoreclose cycle is started, Autoreclose in progress (ARIP) is indicated. The indication remains until the end of the cycle. The end of the cycle is signified by successful Autoreclose, or by lockout.

Autoreclose cycles can be initiated by:

- Protection functions internal to the product
- A Trip Test feature
- External protection equipment
- Evolving fault combinations

Internal protection functions

Many of the protection functions in the product can be programmed to initiate or block Autoreclose. The associated settings are found in the Autoreclose column and the available options are `No Action`, `Initiate AR`, or `Block AR`. If set to `Block AR` operation of the protection function blocks the Autoreclose function and forces a lockout.

Trip test feature

The ***Test Autoreclose*** command cell in the *COMMISSION TESTS* column can be used to initiate an Autoreclose cycle. Each option provides a 100 ms pulse output. There is also a 'No Operation' option to exit the command field without initiating a test.

External protection equipment

Protection operation from a different device can be used to initiate Autoreclose via PSL. By default these external trip input signals are mapped to initiate Autoreclose. These inputs are not mapped to the trip outputs. With appropriate mapping in the PSL, however, the external device can use this product to trip connected circuit breakers.

Evolving fault combinations

The Autoreclose function would normally be initiated by a single condition (such as a single-phase fault). If, however, the system conditions evolve such that other conditions that could initiate Autoreclose, then the dynamics

of the Autoreclose logic need to adapt. For example, if a single-phase fault evolves into a multi-phase fault, then the operation of the Autorecloser must consequently adapt. To achieve this signals are generated to indicate conditions such as evolving faults, re-operation of protection, combinations of initiation by internal protection, external protection, or test features, which control the Autoreclose sequencing.

Records of initiating conditions are stored and used to control the sequencing. Initiation can be from a protection function integrated in the product, from external protection and internal sources such as the Autoreclose test function. Initiation can be further qualified by the phases causing the initiation. These conditions are stored in signals that generally feature “MEM”- memory, or “AR” – Autoreclose, in the signal name.

8.5.7.1 AUTORECLOSE INITIATION LOGIC DIAGRAM

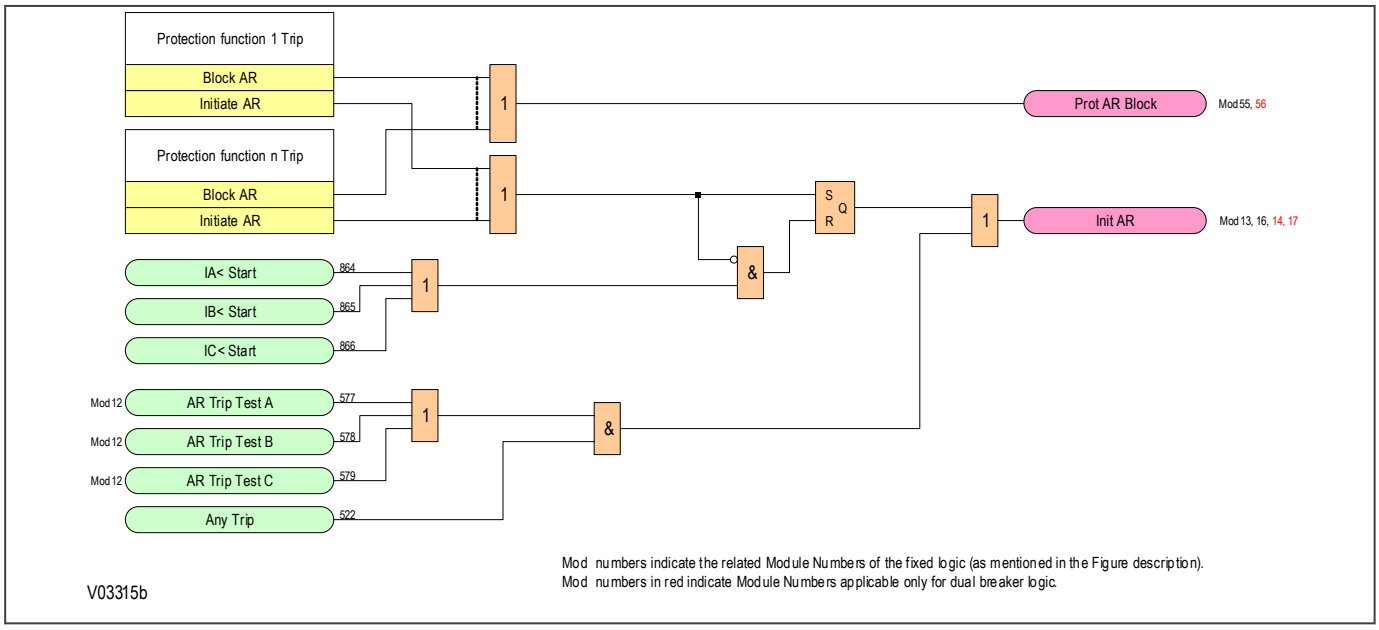


Figure 94: Autoreclose initiation logic (module 11)

8.5.7.2 AUTORECLOSE TRIP TEST LOGIC DIAGRAM

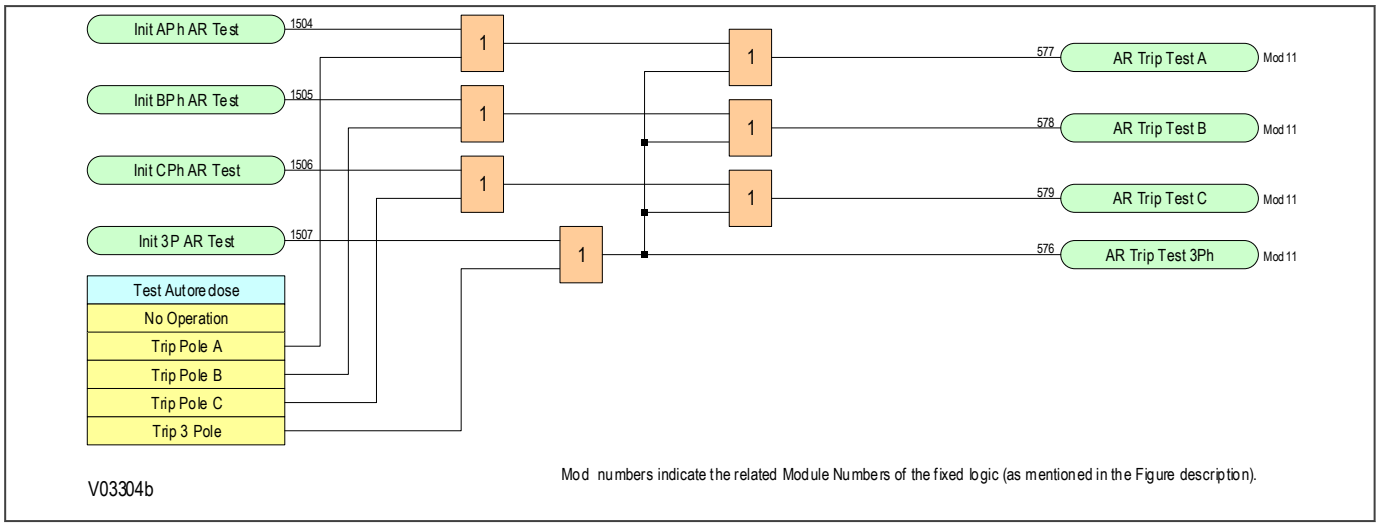


Figure 95: Autoreclose trip test logic (module 12)

8.5.7.3 AR EXTERNAL TRIP INITIATION LOGIC DIAGRAM

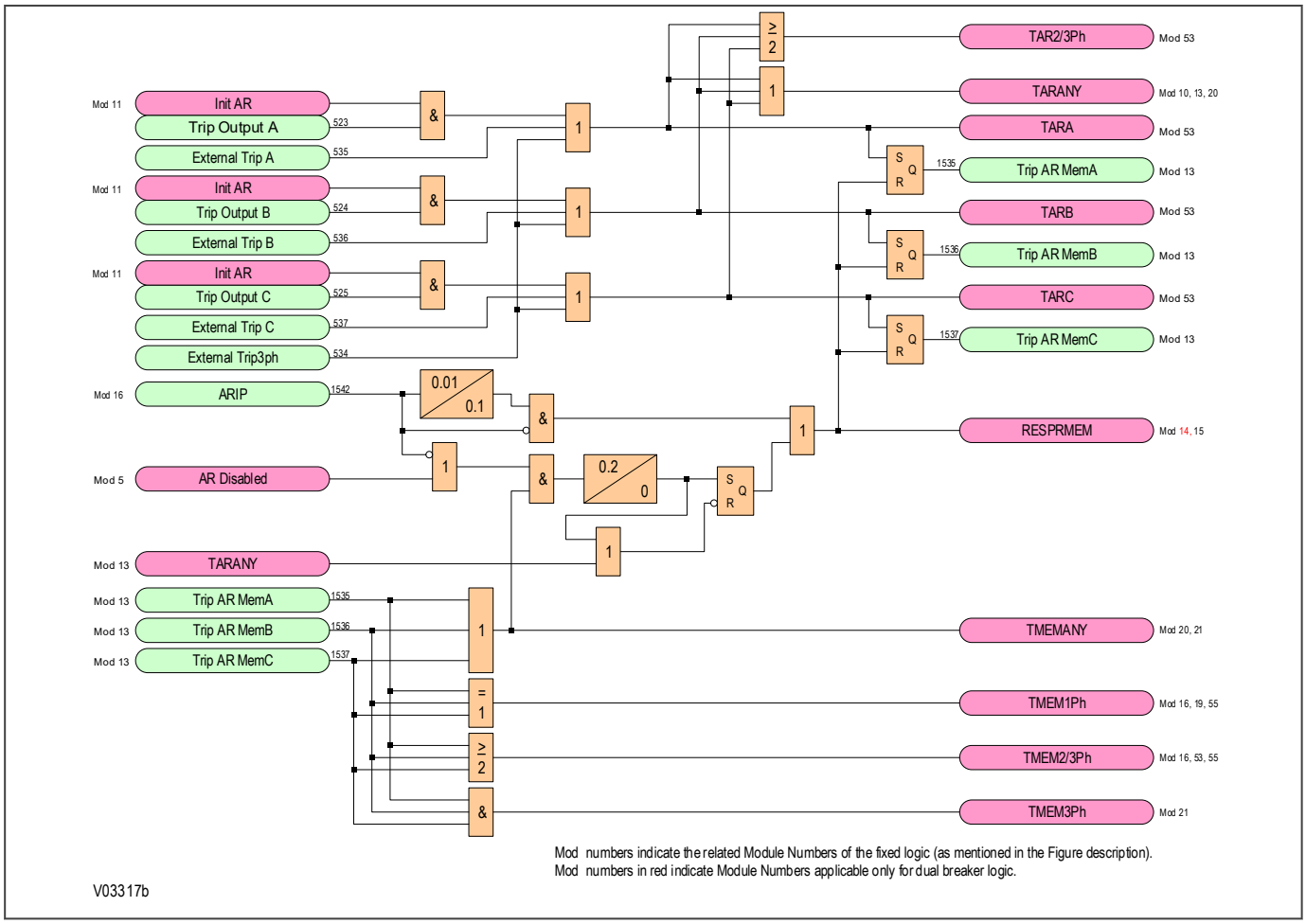


Figure 96: Autoreclose initiation by external trip or evolving conditions (module 13)

Note:
The signals must be mapped as shown in the default PSL scheme.

8.5.7.4 PROTECTION REOPERATION AND EVOLVING FAULT LOGIC DIAGRAM

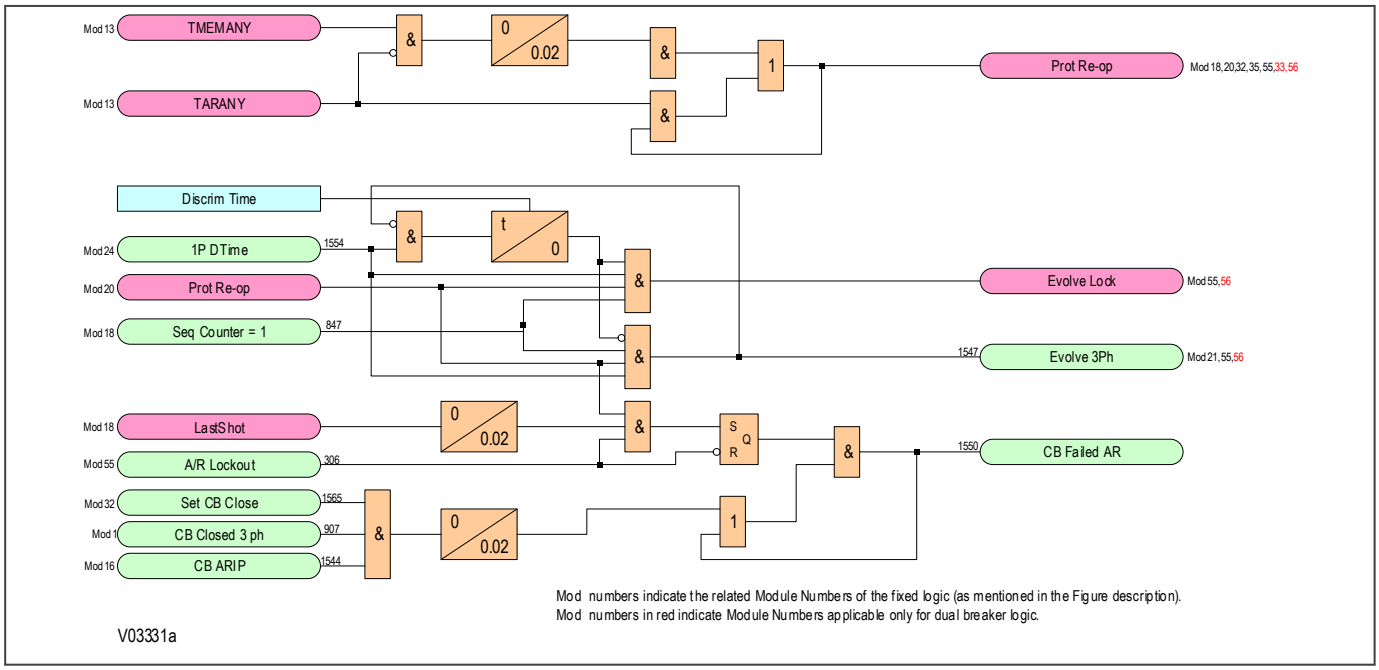


Figure 97: Protection re-operation and evolving fault logic (module 20)

8.5.7.5 FAULT MEMORY LOGIC DIAGRAM

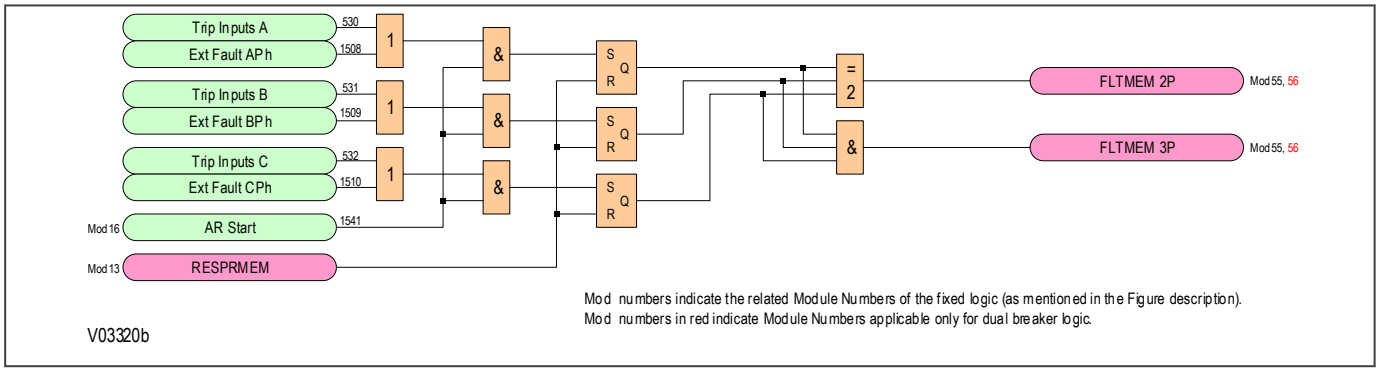


Figure 98: Fault memory logic (module 15)

8.5.8 AUTORECLOSE IN PROGRESS

The AR In Progress module produces various signals to indicate to other modules and functions that an Autoreclose operation is currently in progress.

8.5.8.1 AUTORECLOSE IN PROGRESS LOGIC DIAGRAM

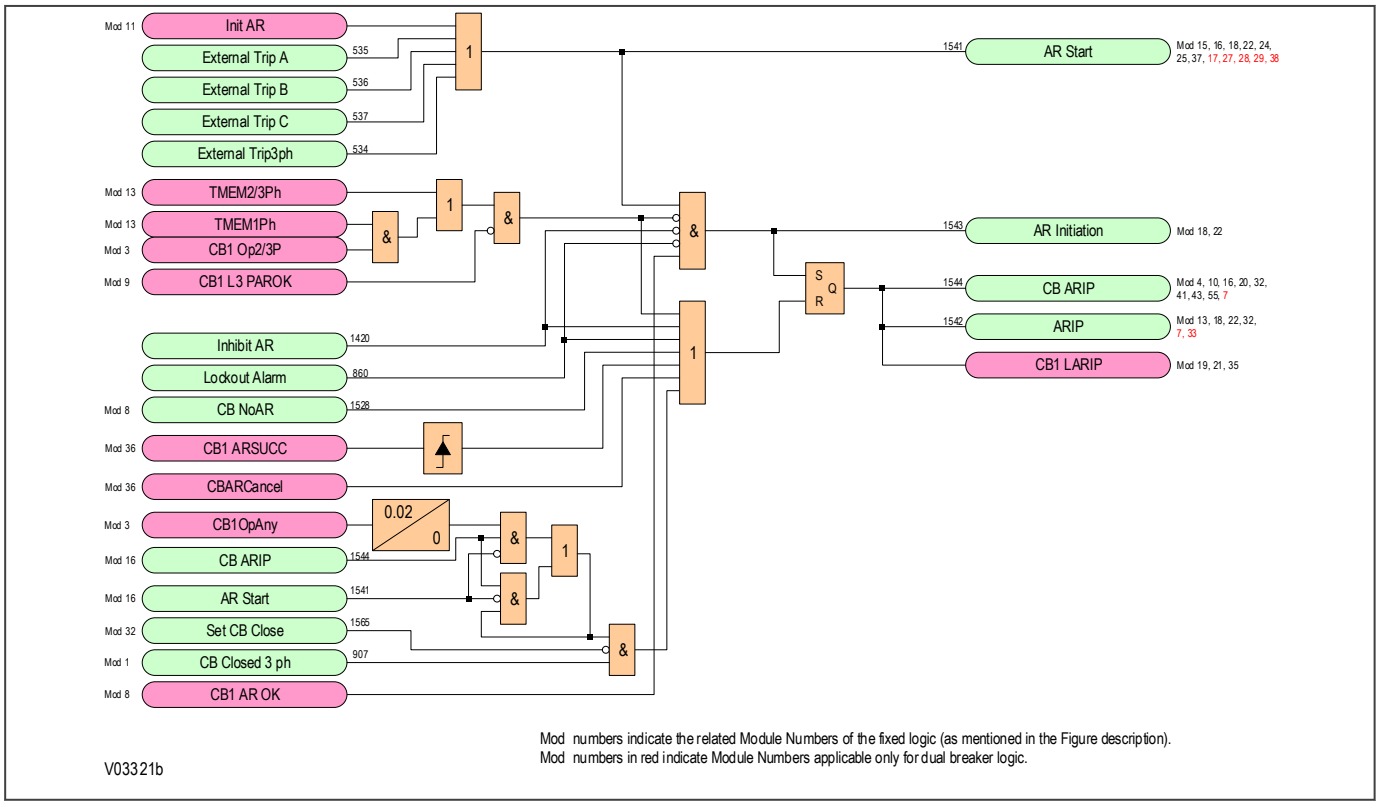


Figure 99: Autoreclose in progress logic (module 16)

8.5.9 SEQUENCE COUNTER

The Autoreclose logic includes a counter for counting the number of Autoreclose shots. This is referred to as the sequence counter. The sequence counter has a value of zero if Autoreclose is not in progress. Following a trip, and subsequent Autoreclose initiation, the sequence counter is incremented. The counter provides output signals indicating how many initiation events have occurred in any Autoreclose cycle. These signals are available as user indications and are used in the logic to select the appropriate dead times or, for a persistent fault, force a lockout.

It is possible to skip the first Autoreclose attempt by enabling the ***AR Skip Shot 1*** setting. If this is set, the sequence counter will skip the first Autoreclose attempt (Shot 1) and move to the second (Shot 2) immediately upon Autoreclose initiation. Each time the protection trips the sequence counter is incremented by 1. The Autoreclose logic compares the sequence counter value to the number of Autoreclose shots setting ***AR Shots***. If the counter value exceeds this setting then the Autoreclose is locked out. If Autoreclose is successful, the sequence counter resets to zero.

8.5.9.1 AUTORECLOSE SEQUENCE COUNTER LOGIC DIAGRAM

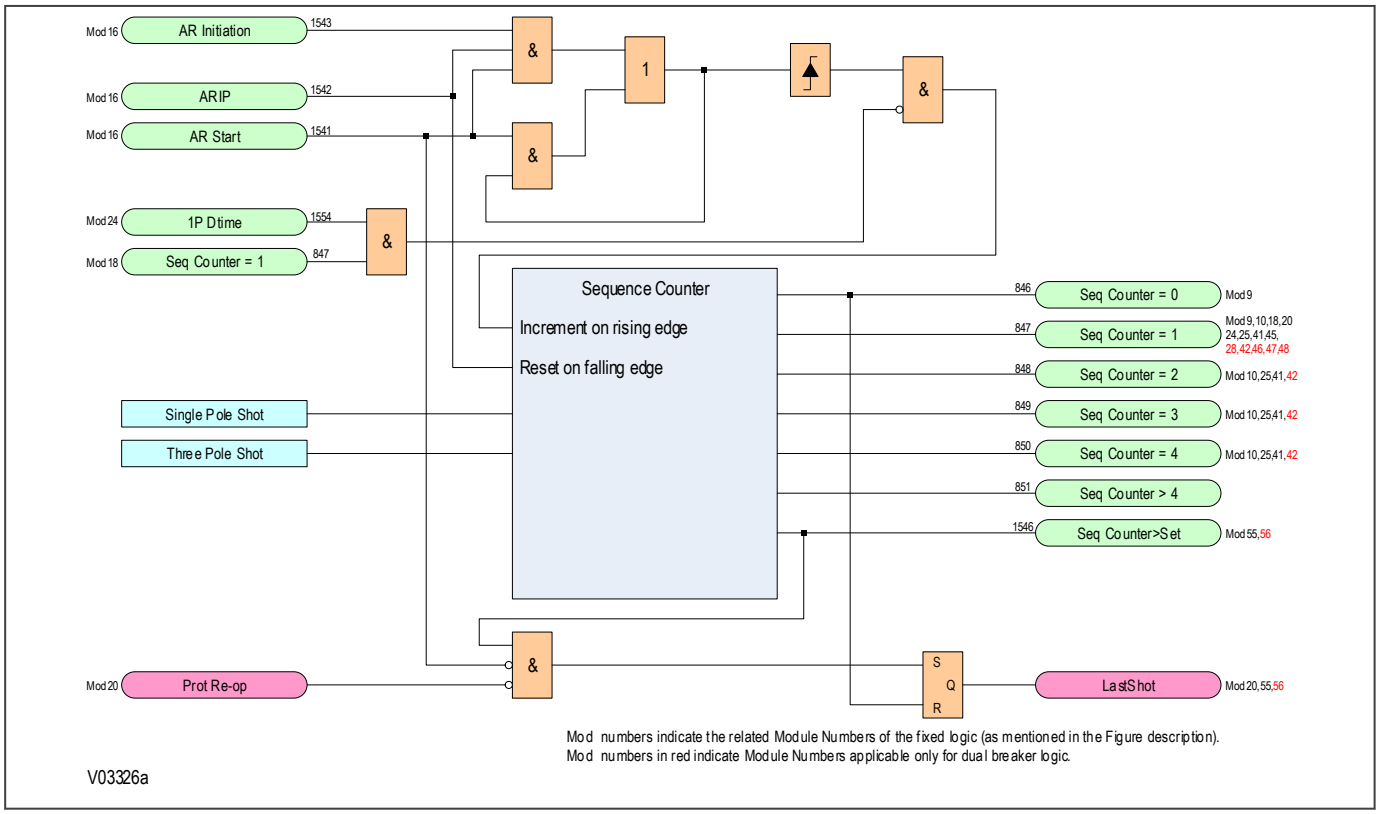


Figure 100: Autoreclose sequence counter logic (module 18)

8.5.10 AUTORECLOSE CYCLE SELECTION

The Autoreclose cycle selection logic is responsible for determining whether the Autoreclose will start as single-phase or three-phase.

8.5.10.1 SINGLE-PHASE AUTORECLOSE CYCLE SELECTION LOGIC DIAGRAM

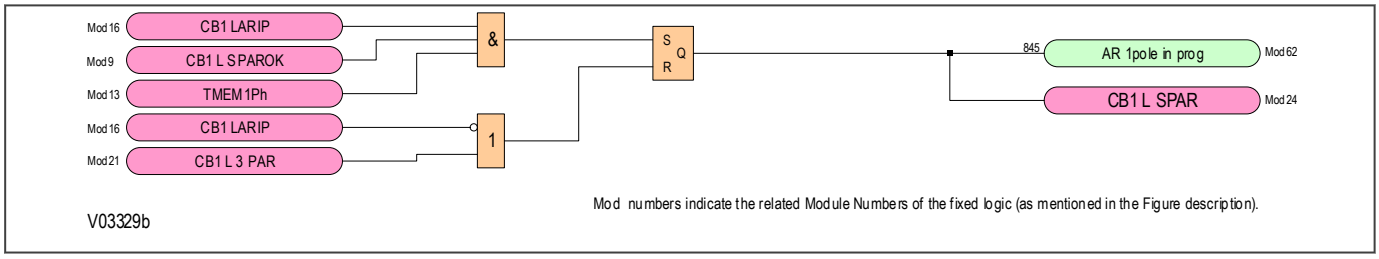


Figure 101: Single-phase autoreclose cycle selection logic (module 19)

8.5.10.2 3-PHASE AUTORECLOSE CYCLE SELECTION

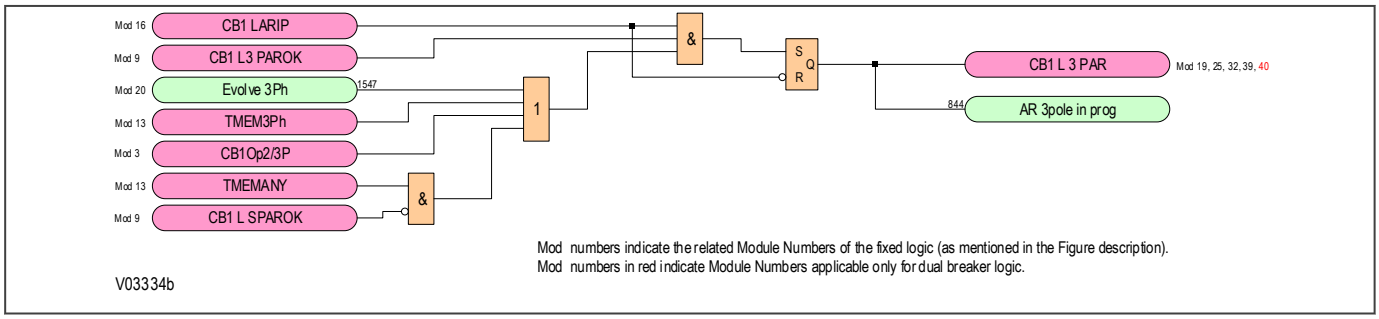


Figure 102: Three-phase autoreclose cycle selection logic (module 21)

8.5.11 DEAD TIME CONTROL

Once an Autoreclose cycle has started, the conditions to enable the dead time to run are determined by the menu settings, the circuit breaker status, the protection status, the nature of the AR cycle (single-phase or three-phase), and the opto-isolated inputs from external sources.

Three settings are involved in controlling the dead time start:

- ***DT Start by Prot***
- ***3PDTStart WhenLD***
- ***DTStart by CB Op***

The ***DT Start by Prot*** determines how the protection action will initiate a dead time. The setting is always visible and has three options `Protection Reset`, `Protection Op` (protection operation), and `Disable` which should be selected if you don't want protection action to start the dead time. These options set the basic conditions for starting the dead time.

Selecting protection operation to start the dead time can, optionally, be qualified by a check that the line is dead.

Selecting protection reset to start the dead time can, optionally, be qualified by a check, that the circuit breaker is open (***DTStart by CB Op***) before starting the dead time. For three-phase tripping applications, there is a further option to check that the line is dead (***3PDTStart WhenLD***) before starting the dead time.

If ***DT Start by Prot*** is disabled, the circuit breaker must be open for the dead time to start. For three-phase tripping applications, there is an option to check that the line is dead (***3PDTStart WhenLD***) before starting the dead time. To check that the line is dead, set ***3PDTStart WhenLD*** to `enabled`. To check that the circuit breaker is open, set ***DTStart by CB Op*** to `Enabled`.

8.5.11.1 DEAD TIME START ENABLE LOGIC DIAGRAM

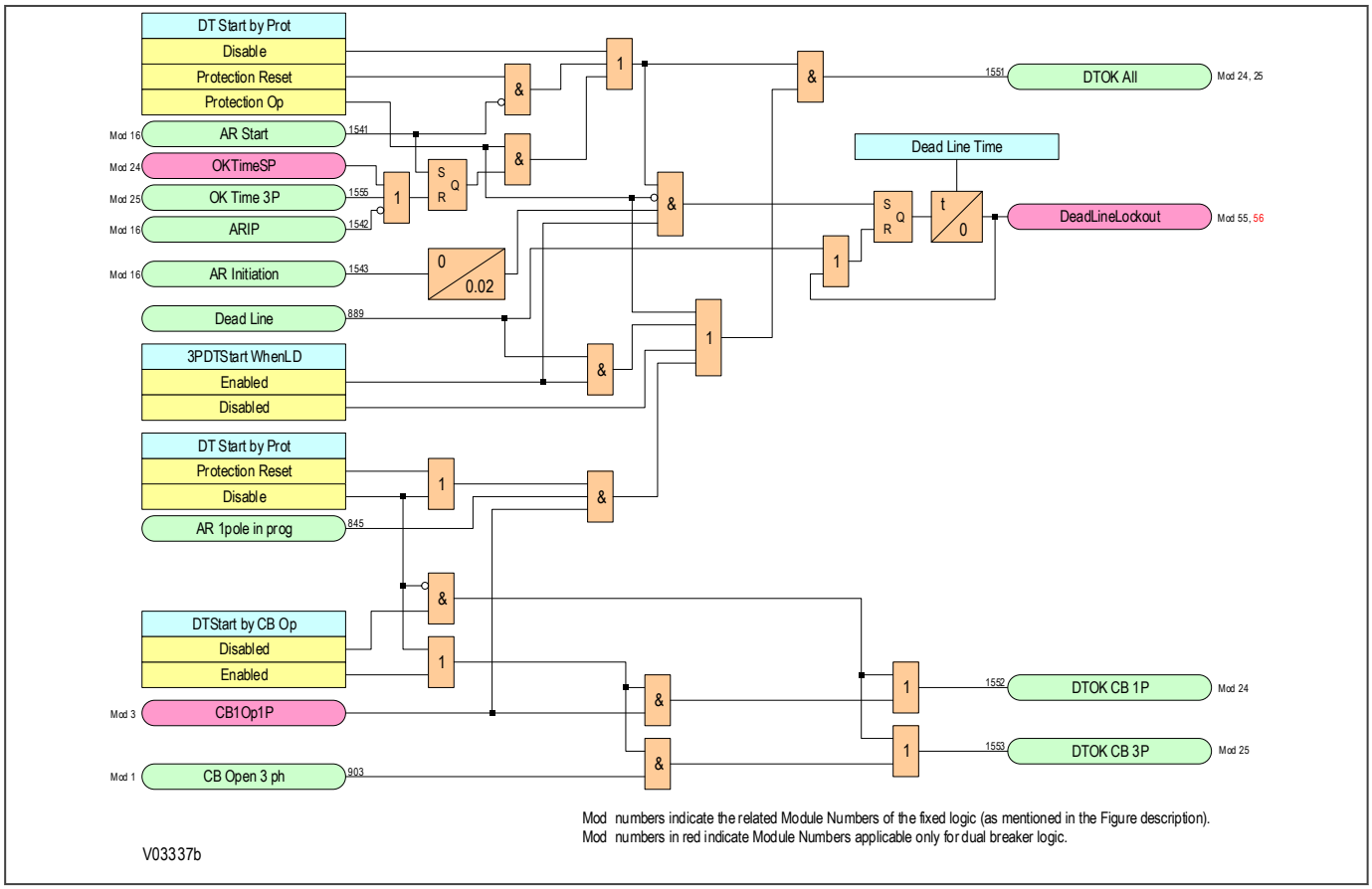


Figure 103: Dead time start enable logic (module 22)

8.5.11.2 1-PHASE DEAD TIME LOGIC DIAGRAM

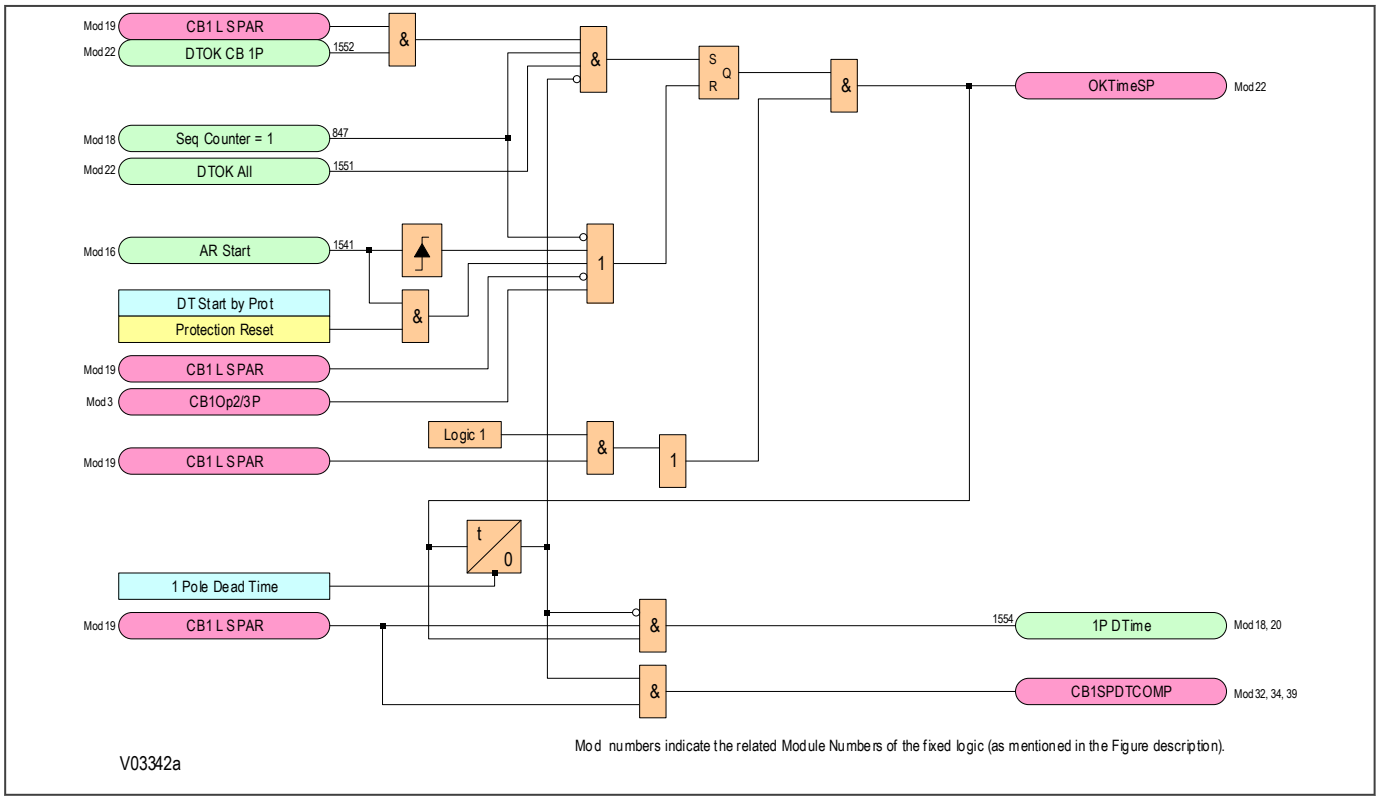


Figure 104: Single-phase dead time logic (module 24)

8.5.11.3 3-PHASE DEAD TIME LOGIC DIAGRAM

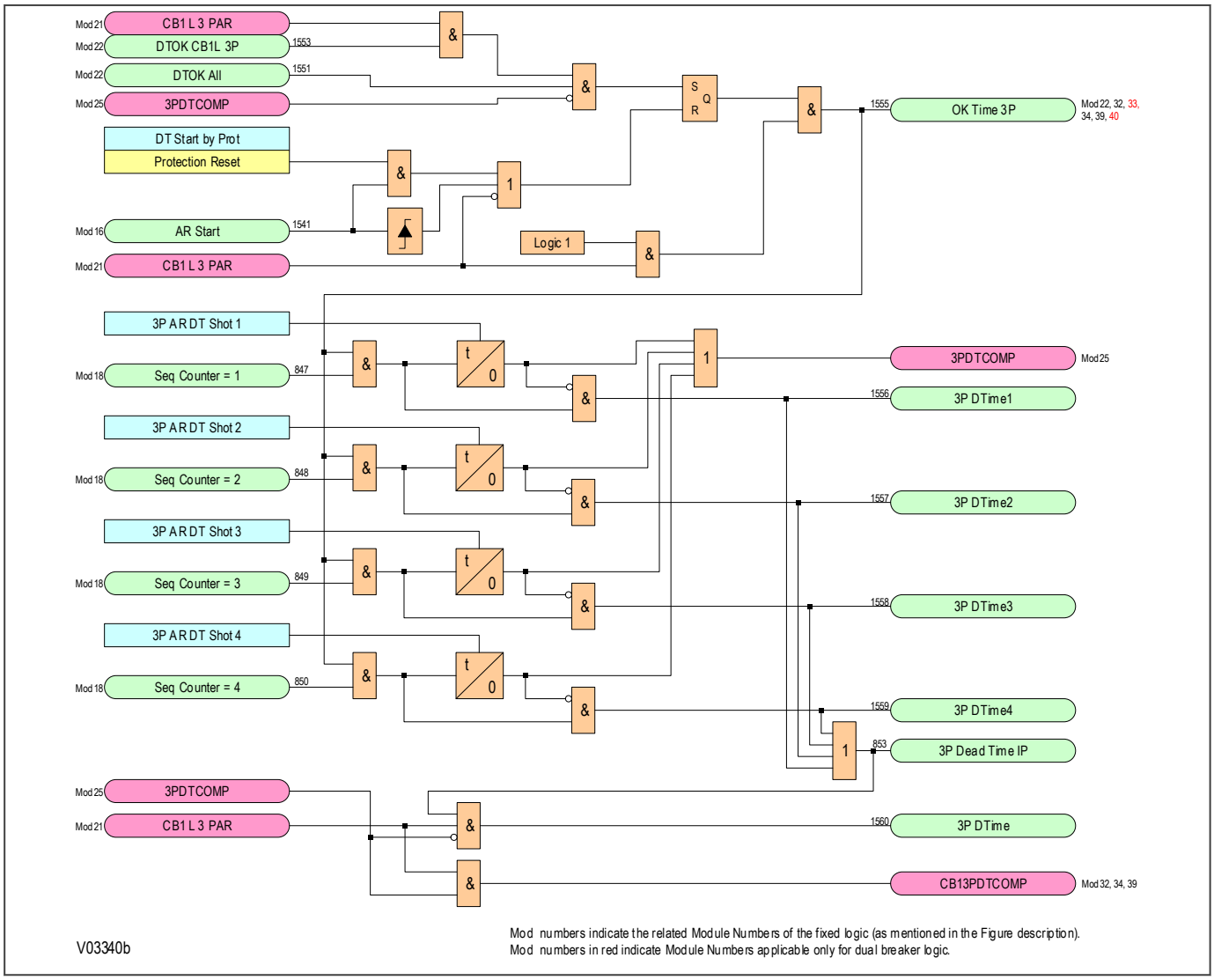


Figure 105: Three-phase dead time logic (module 25)

8.5.12 CIRCUIT BREAKER AUTOCLOSE

Autoclose logic takes effect when dead times have expired.

The Autoclose logic checks that all necessary conditions are satisfied before issuing an Autoclose command to the circuit breaker control scheme.

Before a circuit breaker can be closed, it must be healthy (sufficient energy to close, and if necessary re-trip) and it must not be in a lockout condition.

For three-phase Autoreclose, the circuit breaker must be open on all three phases and the appropriate system check conditions must be met. For single-phase Autoreclose, the circuit breaker must be open on that phase.

The Autoclose command is a pulse lasting 100 milliseconds. Another command (***Set CB Close***) to set the circuit breaker to close is asserted as well as the Autoclose command. This signal will remain set either until the end of the Autoreclose cycle, or until the next protection operation. These commands are used to initiate the Reclaim Time logic and the Autoreclose Shot Counter logic.

8.5.12.1 CIRCUIT BREAKER AUTOCLOSE LOGIC DIAGRAM

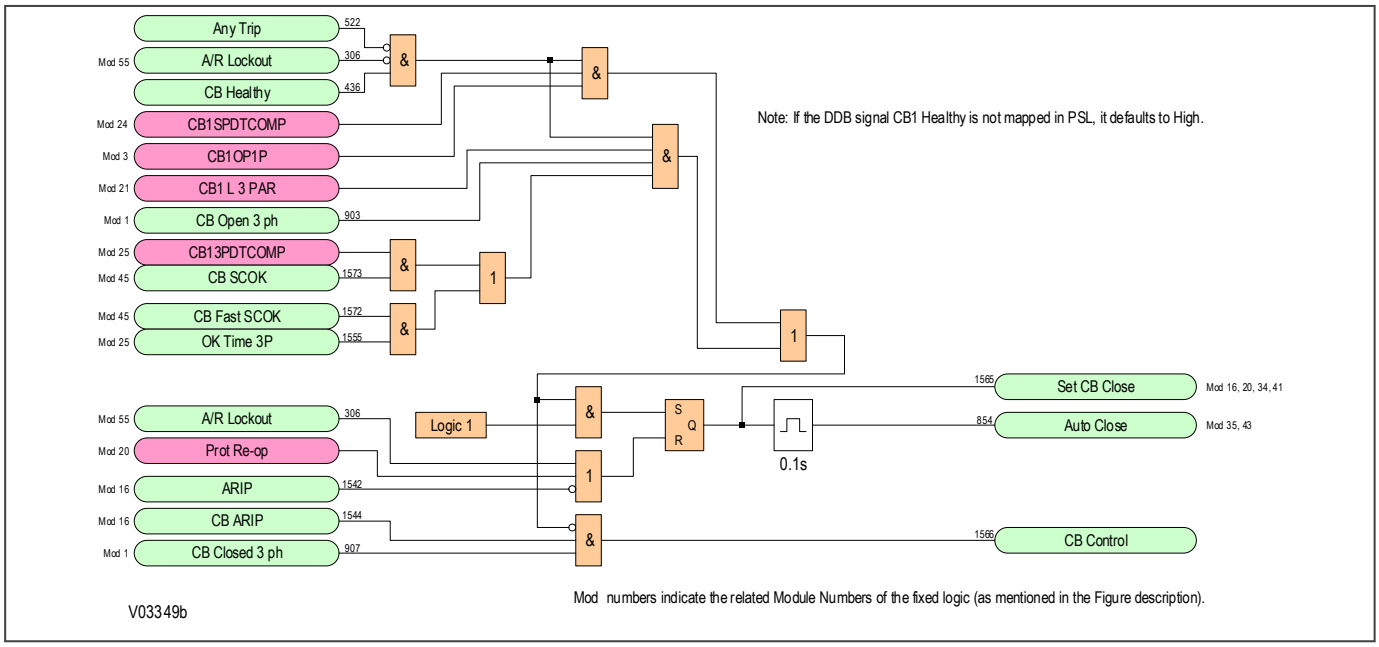


Figure 106: Circuit breaker autoclose logic (module 32)

8.5.13 RECLAIM TIME

If the protection operates again before the reclaim time has expired, the corresponding sequence counter is incremented. At the same time, any “dead time complete” (….DTCOMP) signals are reset and the logic is prepared for the next dead time to start when conditions are suitable. The operation also resets the signal that would set the circuit breaker to close, and stops and resets the reclaim timer. The reclaim time starts again if the signal to set a circuit breaker to close goes high following completion of a dead time in a subsequent Autoreclose cycle.

If the circuit breaker is closed and has not tripped again when the reclaim time expires, signals are generated to indicate successful Autoreclose. These signals increment the relevant circuit breaker successful Autoreclose shot counters and reset the relevant Autoreclose in progress signal.

The “successful Autoreclose” signals generated from the logic can be reset by various commands and settings options available under *CB CONTROL* menu settings as follows:

If ***Res AROK by UI*** is set to `Enabled`, all the signals can be reset by user interface command ***Reset AROK Ind*** from the *CB CONTROL* menu.

If ***Res AROK by NoAR*** is set to `Enabled`, the signals for each circuit breaker can be reset by temporarily generating an Autoreclose disabled signal according to the logic shown.

If ***Res AROK by Ext*** is set to `Enabled`, the signals can be reset by activation of an external input signal appropriately mapped in the PSL.

If ***Res AROK by TDly*** is set to `Enabled`, the signals are automatically reset after a time delay set in ***AROK Reset Time***.

8.5.13.1 PREPARE RECLAIM INITIATION LOGIC DIAGRAM

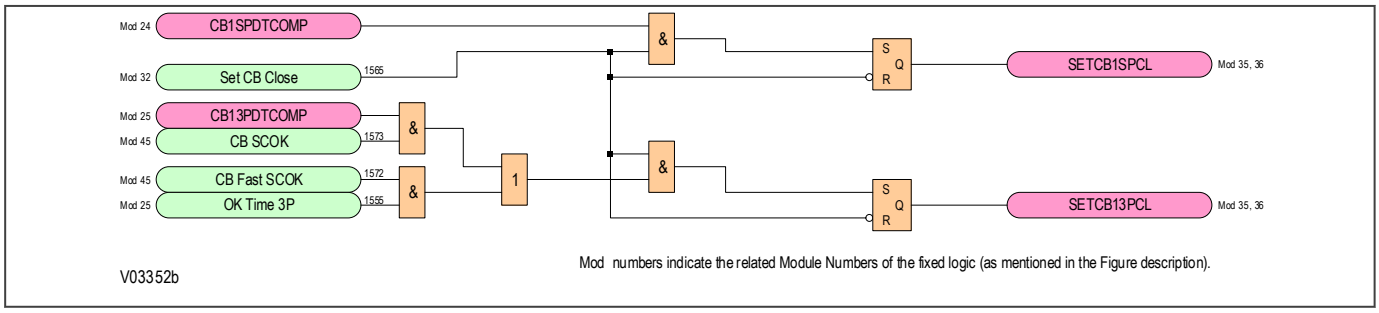


Figure 107: Prepare reclaim initiation logic (module 34)

8.5.13.2 RECLAIM TIME LOGIC DIAGRAM

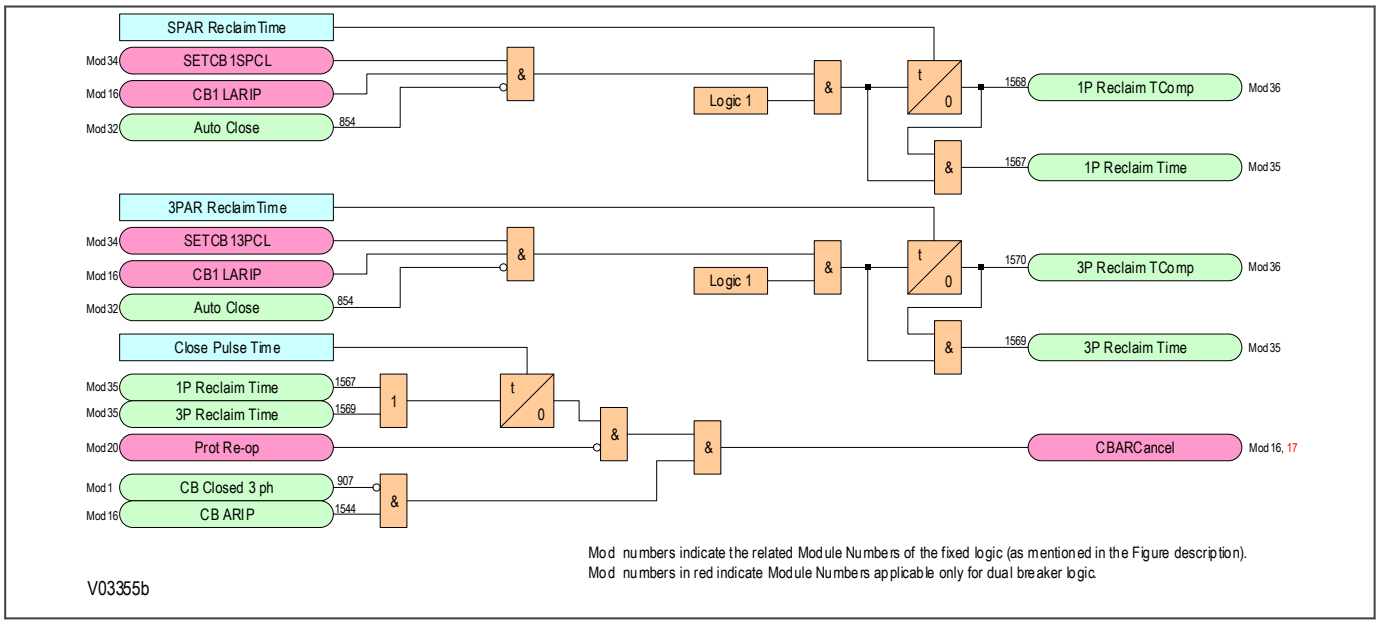


Figure 108: Reclaim time logic (module 35)

8.5.13.3 SUCCESSFUL AUTORECLOSE SIGNALS LOGIC DIAGRAM

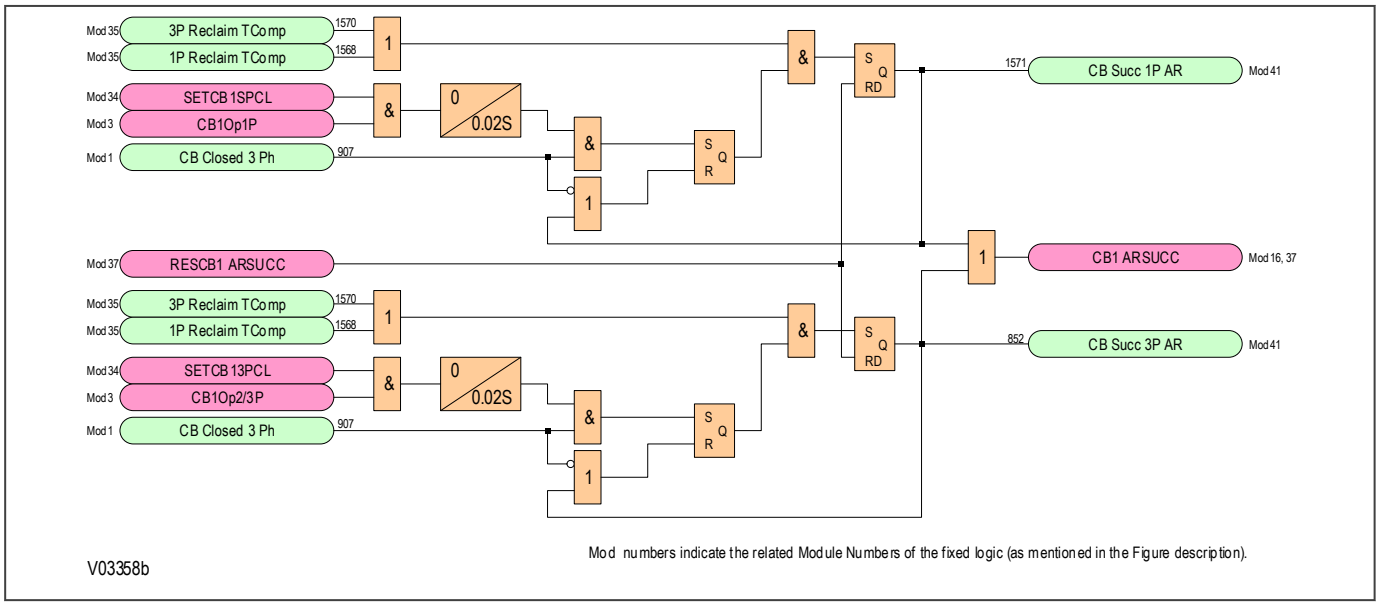


Figure 109: Successful autoreclose signals logic (module 36)

8.5.13.4 AUTORECLOSE RESET SUCCESSFUL INDICATION LOGIC DIAGRAM

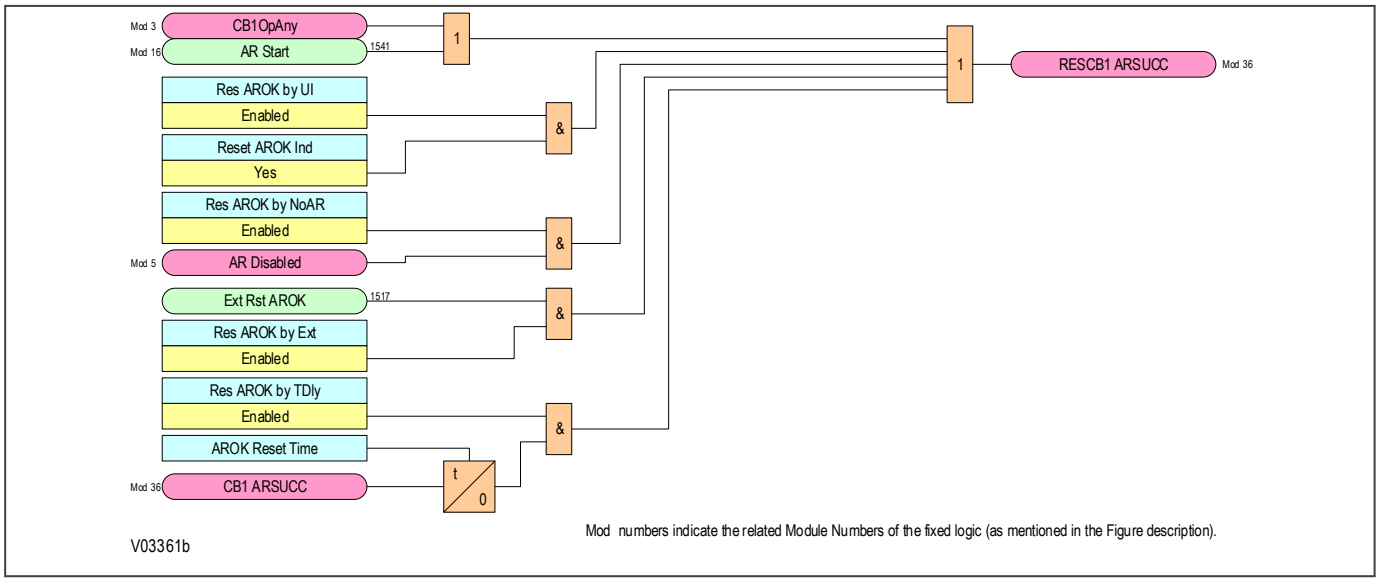


Figure 110: Autoreclose reset successful indication logic (module 37)

8.5.14 CB HEALTHY AND SYSTEM CHECK TIMERS

This logic provides signals to cancel Autoreclose if the circuit breaker is not healthy (for example low gas pressure) or system check conditions are not satisfied (for example required line & bus voltage conditions) when the scheme is ready to close the circuit breaker.

At the completion of a dead time, the logic starts an Autoreclose healthy timer. If a circuit breaker healthy signal becomes high before the Autoreclose healthy time is complete, the timer stops and, if all other relevant circuit breaker closing conditions are satisfied, the scheme issues a circuit breaker Autoclose signal. If the circuit breaker healthy signal stays low, then, at the end of the Autoreclose healthy time, a circuit breaker unhealthy alarm is raised. This forces the Autoreclose sequence to be cancelled.

Additionally, at the completion of any three-phase dead time, the logic starts an Autoreclose check synchronism timer. If the circuit breaker synchronism-check OK signal goes high before the time is complete, the timer stops and, if all other relevant circuit breaker closing conditions are satisfied, the scheme issues a circuit breaker Autoclose signal. If the circuit breaker synchronism-check OK signal stays low, then when the Autoreclose check synchronism timer expires, an alarm is set to inform that the check synchronism is not satisfied and cancels the Autoreclose cycle.

8.5.14.1 CB HEALTHY AND SYSTEM CHECK TIMERS LOGIC DIAGRAM

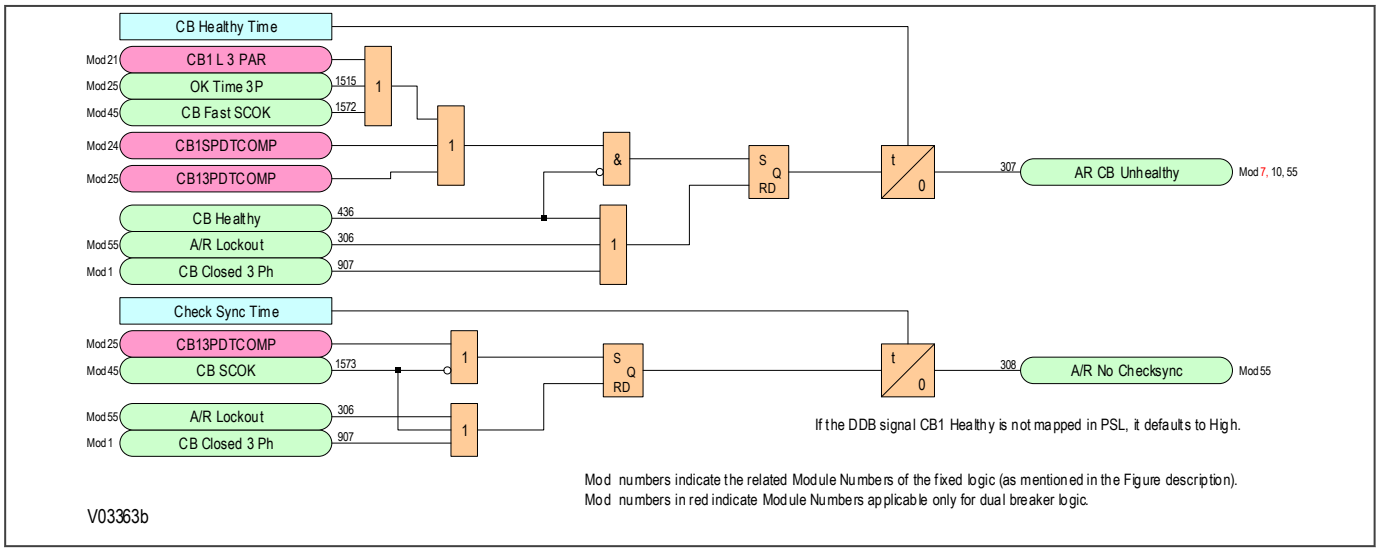


Figure 111: Circuit breaker healthy and system check timers healthy logic (module 39)

8.5.15 AUTORECLOSE SHOT COUNTERS

A number of counters are provided to enable analysis of circuit breaker Autoreclose history. The counters are stored in non-volatile memory, so that the data is maintained even in the event of a failure of the auxiliary supply. The counter values are accessible through the *CB CONTROL* column. The counters can be reset manually, or by activation of an input appropriately mapped in the PSL.

The logic provides the following summary information for each circuit breaker

- Overall total number of shots (Number of Autoreclose attempts)
- Number of successful 1st shot single-phase Autoreclose sequences
- Number of successful 1st shot three-phase Autoreclose sequences
- Number of successful 2nd shot three-phase Autoreclose sequences
- Number of successful 3rd shot three-phase Autoreclose sequences
- Number of successful 4th shot three-phase Autoreclose sequences
- Number of failed Autoreclose cycles which forced a circuit breaker to lockout

8.5.15.1 AUTORECLOSE SHOT COUNTERS LOGIC DIAGRAM

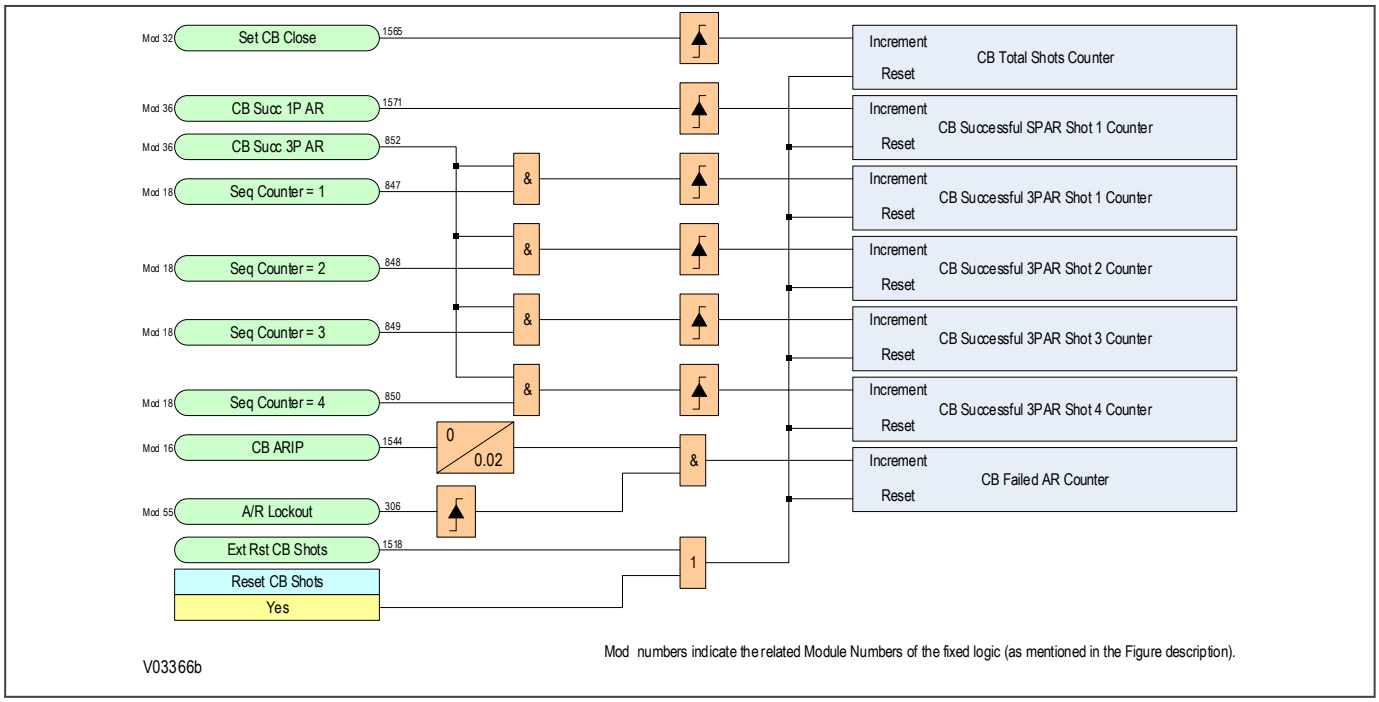


Figure 112: Autoreclose shot counters logic (module 41)

8.5.16 CIRCUIT BREAKER CONTROL

8.5.16.1 CB CONTROL LOGIC DIAGRAM

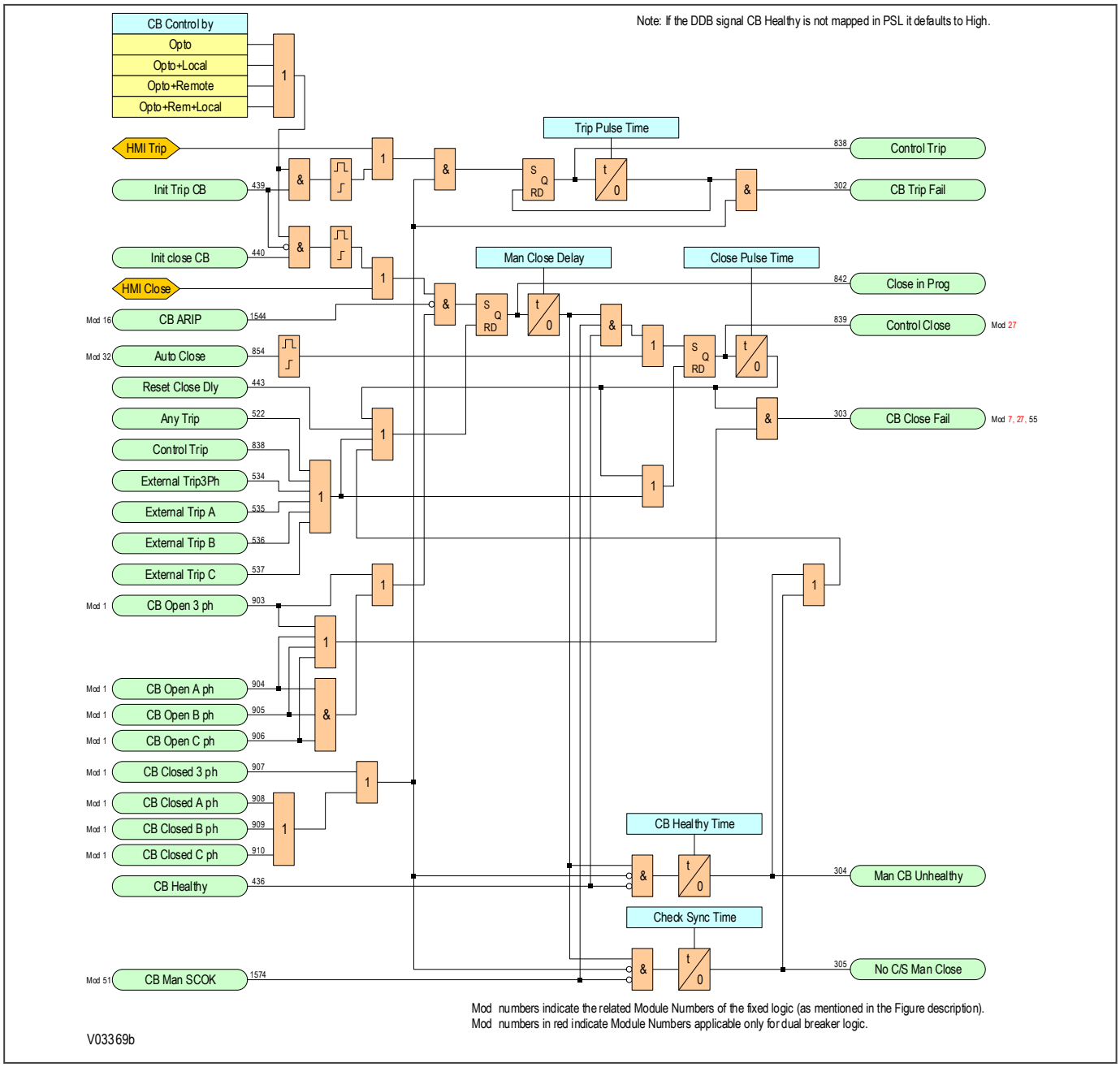


Figure 113: CB control logic (module 43)

8.5.17 CIRCUIT BREAKER TRIP TIME MONITORING

The circuit breaker trip time monitoring logic checks for correct circuit breaker tripping following the issue of a protection trip signal. When the protection trip signal is issued, a timer controlled by the ***Trip Pulse Time*** setting in the *CB CONTROL* column is started.

If the circuit breaker trips correctly the timer resets. If Autoreclose is enabled and the timer resets, the cycle continues. If the circuit breaker fails to trip correctly within the set time, the Autoreclose cycle is forced to lock out and a signal is issued indicating that the circuit breaker failed to trip in response to the protection operation.

8.5.17.1 CB TRIP TIME MONITORING LOGIC DIAGRAM

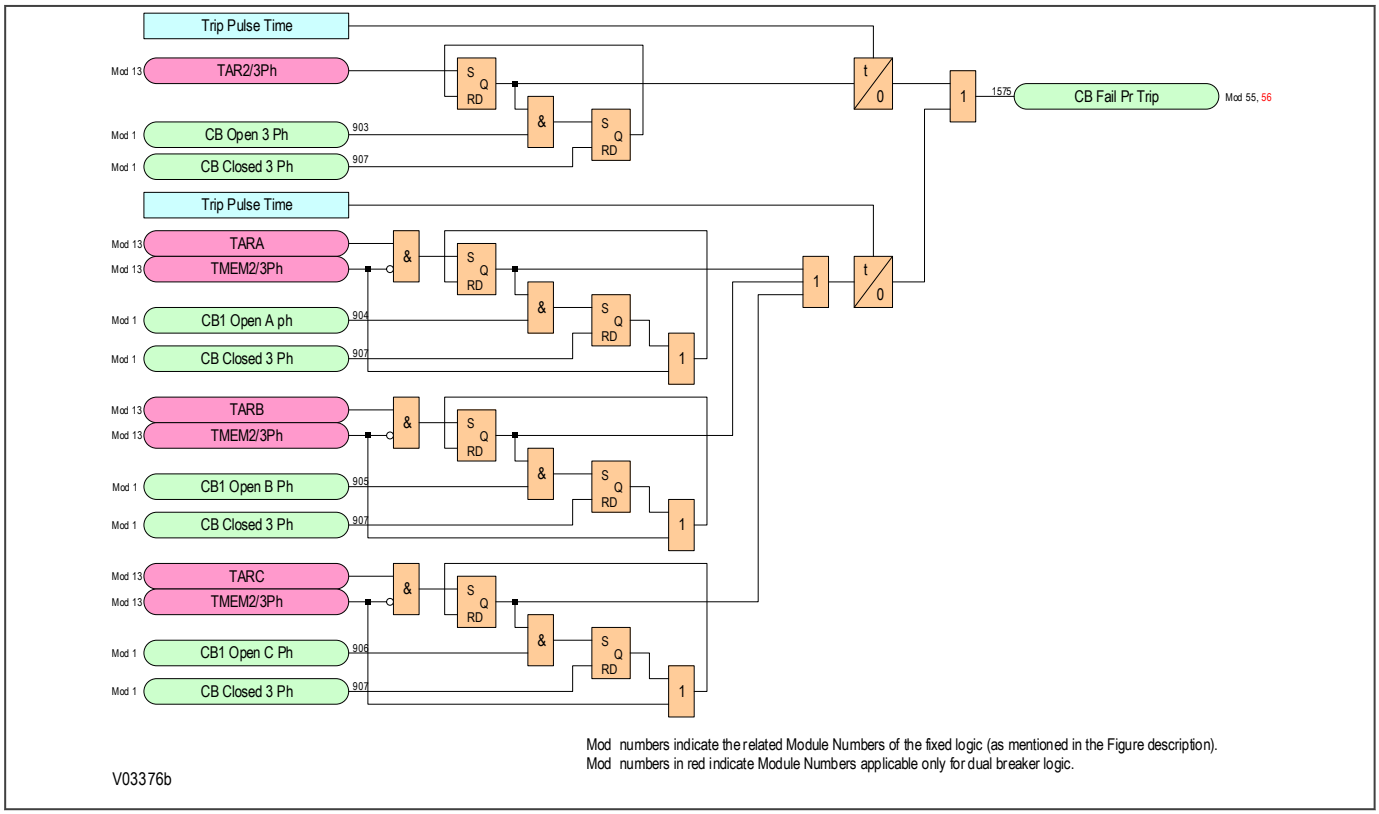


Figure 114: Circuit breaker trip time monitoring logic (module 53)

8.5.18 AUTORECLOSE LOCKOUT

A number of events will cause Autoreclose lockout. If this happens an Autoreclose lockout alarm is raised. In this condition, Autoreclose cannot be initiated until the corresponding lockout has been reset.

The following events force Autoreclose lockout:

- Protection operation during reclaim time. Following the final Autoreclose attempt, if the protection operates during the reclaim time, the AR cycle goes to AR lockout and the Autoreclose function is disabled until the AR lockout condition is reset.
- Persistent fault. A fault is considered persistent if the protection re-operates after the last permitted shot.
- Block Autoreclose. If the block Autoreclose DDB is asserted whilst Autoreclose is in progress, the cycle goes to lockout.
- Protection function selection. Setting ‘Block AR’ against a particular protection function in the AUTORECLOSE column means that operation of the protection will block Autoreclose and force lockout.
- Circuit breaker failure to close. If a circuit breaker fails to close Autoreclose is blocked and forced to lockout.
- Circuit breaker remains open at the end of the reclaim time. An Autoreclose lockout is forced if the circuit breaker is open at the end of the reclaim time.

- Circuit breaker fails to close when the close command is issued.
- Circuit breaker fails to trip correctly.
- Three-phase dead time started by 'line dead' violation. If the line does not go dead within the ***Dead Line Time*** setting, the logic forces the Autoreclose sequence to lockout. Determination of when to start the timer is made in the ***3PDTStart WhenLD*** setting.
- Multi-phase faults. The logic can be set to block Autoreclose either for two-phase or three-phase faults, or to block Autoreclose for three-phase faults only. For this, the setting ***Multi Phase AR*** in the *AUTORECLOSE* column applies.
- Single-phase evolving into multi-phase fault. A discriminating time (***Discrim Time*** in the *AUTORECLOSE* settings) is provided for this feature If, after expiry of the discriminating time, a single-phase fault evolves into a two-phase or three-phase fault, the internal signal 'Evolve Lock' is asserted and the Autoreclose is forced to lockout.

8.5.18.1 CB LOCKOUT LOGIC DIAGRAM

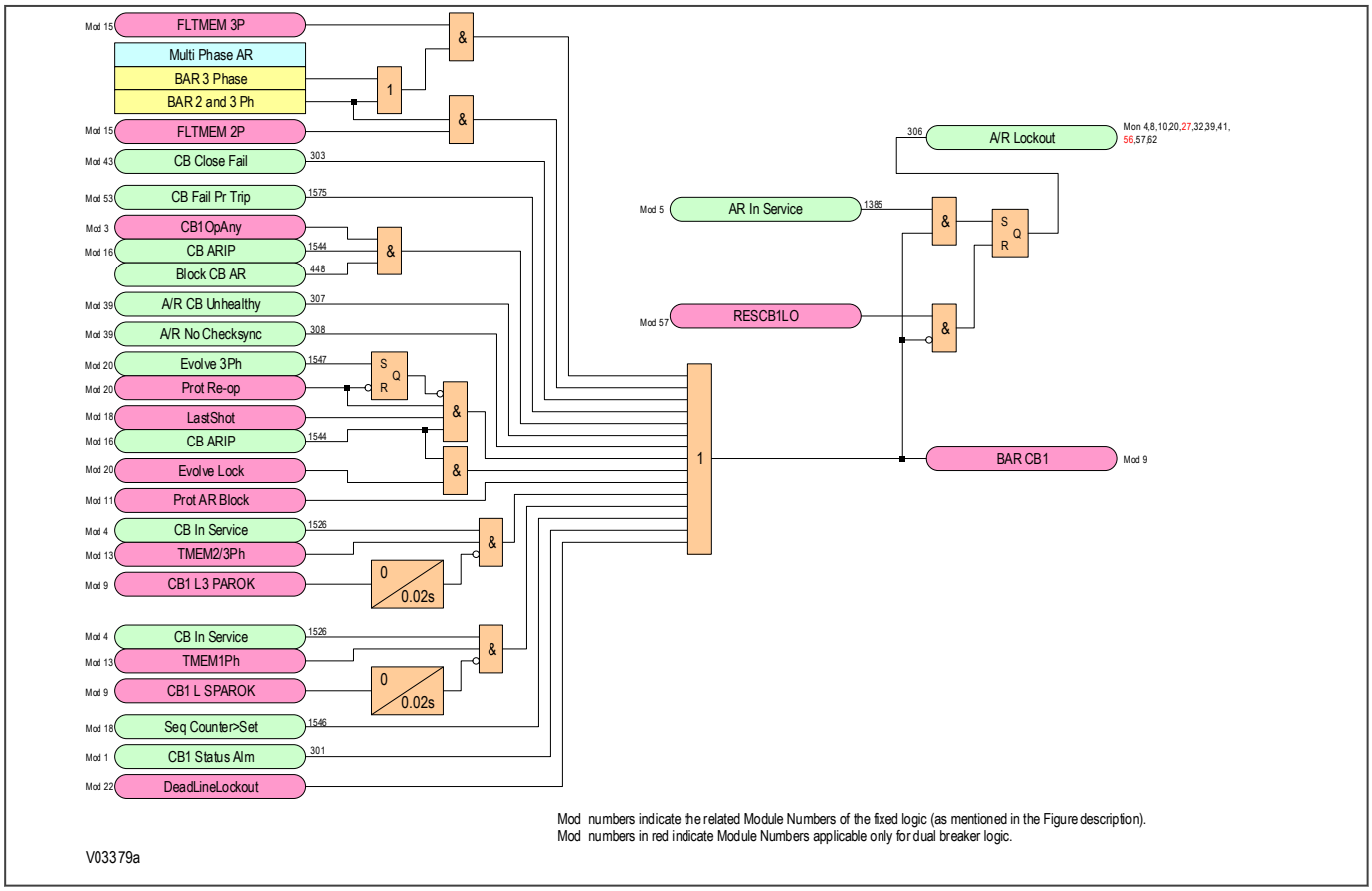


Figure 115: AR lockout logic (module 55)

8.5.19 RESET CIRCUIT BREAKER LOCKOUT

Lockout conditions caused by the circuit breaker condition monitoring functions can be reset according to the condition of the ***Rst CB mon LO*** by setting found in the *CB CONTROL* column. There are two options; `CB Close` and `User interface`.

If set to `CB Close`, a timer setting, ***CB mon LO RstDly***, becomes visible. When the circuit breaker closes, the ***CB mon LO RstDly*** time starts. The lockout is reset when the timer expires.

If set to `User Interface` then a command, ***CB mon LO reset***, becomes visible. This command can be used to reset the lockout from a user interface.

An Autoreclose lockout generates an Autoreclose lockout alarm. Autoreclose lockout conditions can be reset by various commands and setting options found under the *CB CONTROL* column.

If ***Res LO by CB IS*** is set to `Enabled`, a lockout is reset if the circuit breaker is successfully closed manually. For this, the circuit breaker must remain closed long enough so that it enters the “In Service” state.

If ***Res LO by UI*** is set to `Enabled`, the circuit breaker lockout can be reset from a user interface using the reset circuit breaker lockout command in the *CB CONTROL* column.

If ***Res LO by NoAR*** is set to `Enabled`, the circuit breaker lockout can be reset by temporarily generating an ***AR disabled*** signal.

If ***Res LO by TDelay*** is set to `Enabled`, the circuit breaker lockout is automatically reset after a time delay set in the ***LO Reset Time*** setting.

If ***Res LO by ExtDDB*** is `Enabled`, the circuit breaker lockout can be reset by activation of an external input mapped in the PSL to the relevant reset lockout DDB signal.

8.5.19.1 RESET CB LOCKOUT LOGIC DIAGRAM

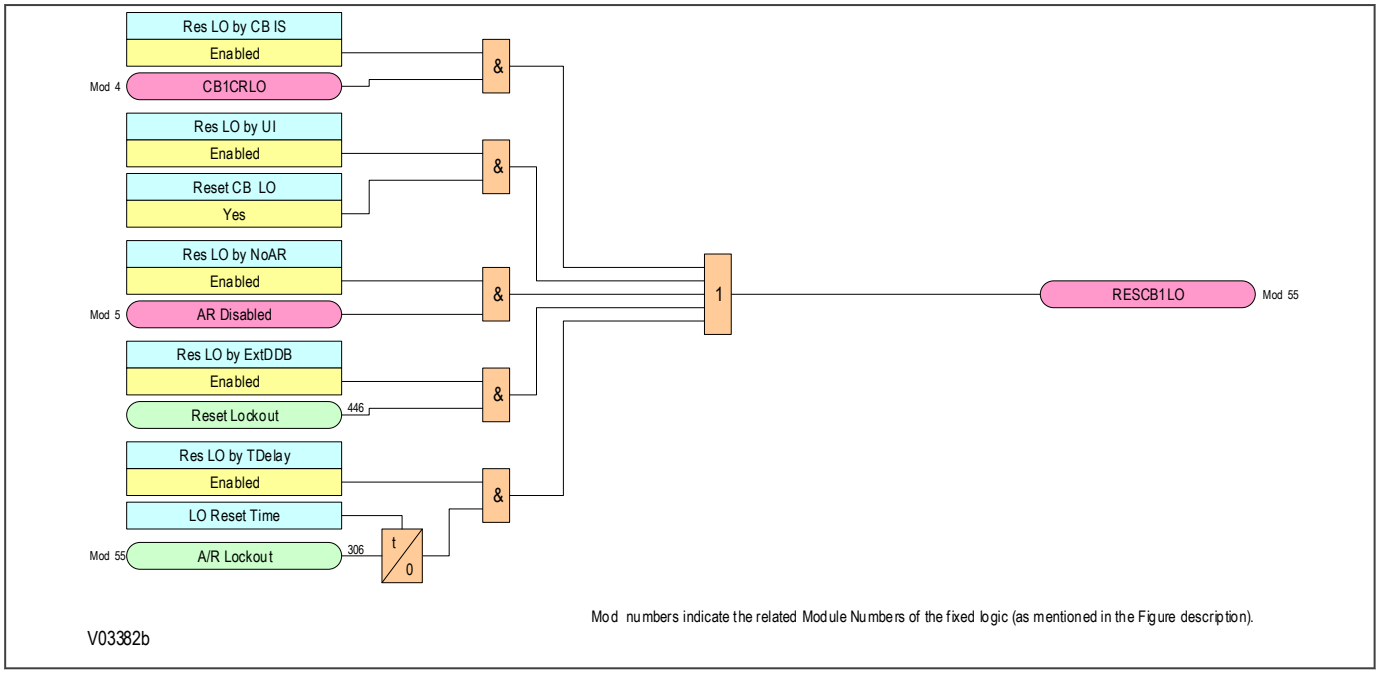


Figure 116: Reset circuit breaker lockout logic (module 57)

8.5.20 POLE DISCREPANCY

In a three-pole CB, certain combinations of poles open and closed are indicative of a problem. The Pole Discrepancy Logic combines an indication of a Pole Discrepancy condition from the CB Monitoring logic with signals from the internal Autoreclose logic to produce a combined Pole Discrepancy indication for the CB.

8.5.20.1 POLE DISCREPANCY LOGIC DIAGRAM

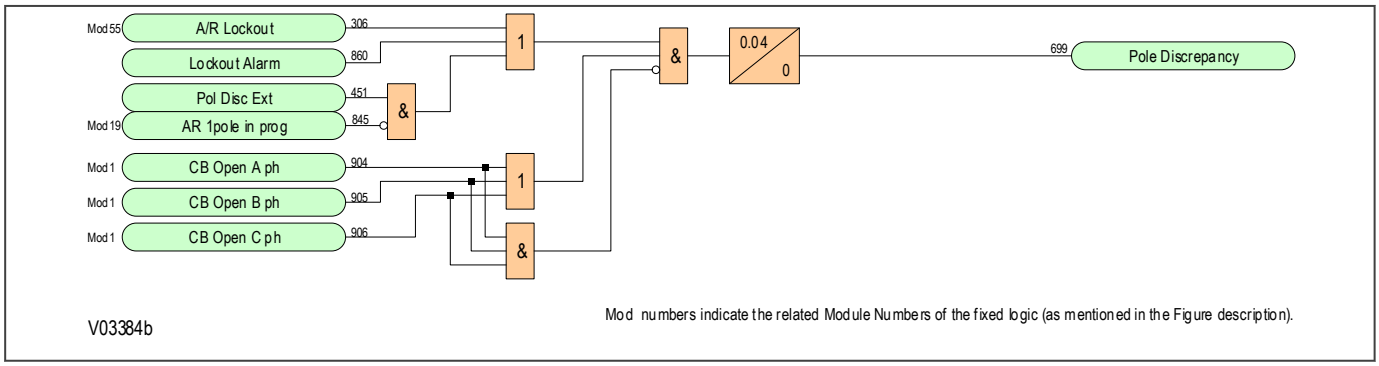


Figure 117: Pole discrepancy logic (module 62)

8.5.21 CIRCUIT BREAKER TRIP CONVERSION

Circuit breakers should only trip single-pole or three-pole. The trip conversion logic ensures that the tripping is either single-pole or three-pole. The trip conversion logic ensures that all conditions that should cause three-pole tripping do so. Indication of the number of phases that caused tripping is provided.

8.5.21.1 CB TRIP CONVERSION LOGIC DIAGRAM

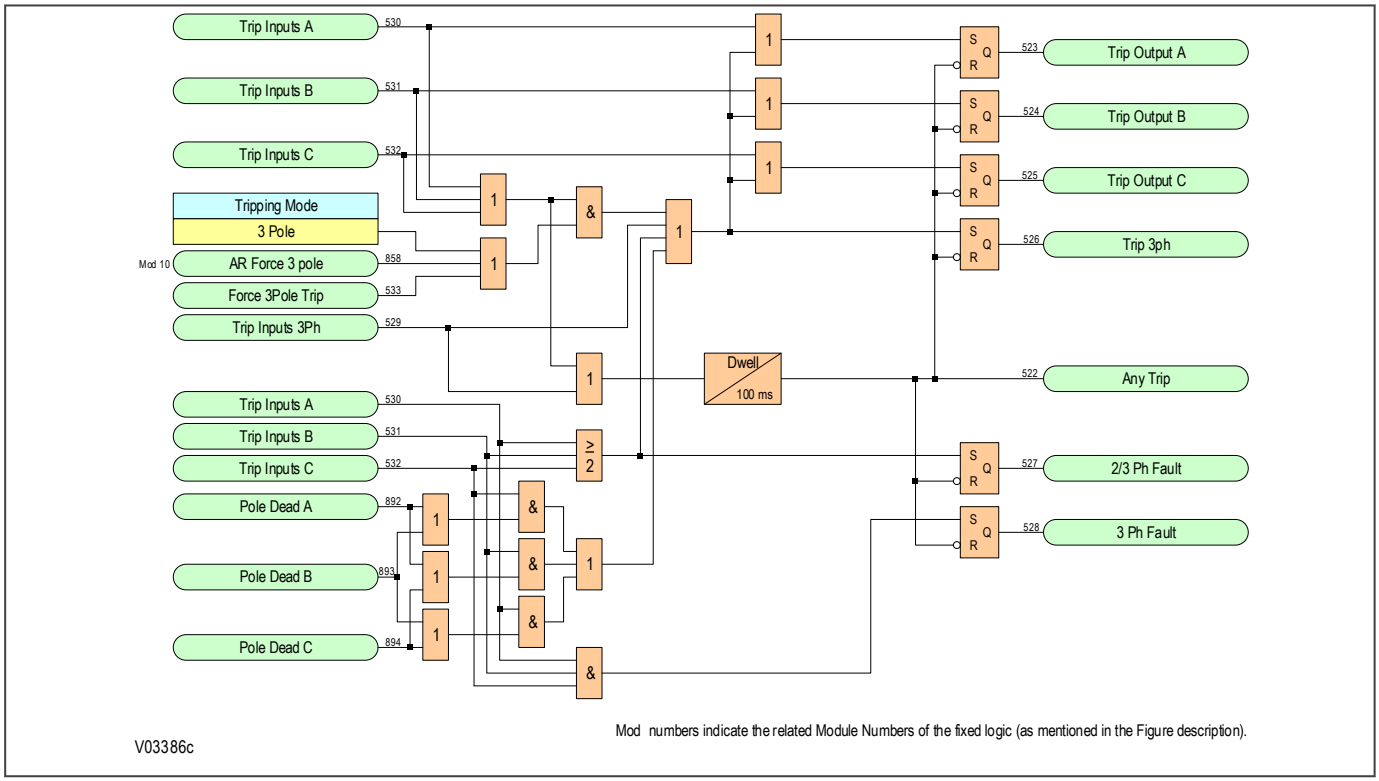


Figure 118: Circuit breaker trip conversion logic (module 63)

8.5.22 MONITOR CHECKS FOR CB CLOSURE

For single-phase Autoreclose neither voltage nor synchronisation checks are needed as synchronising power should be flowing in the two healthy phases. For three-phase Autorelcose, for the first shot (and only the first shot), you can choose to attempt reclosure without performing a synchronisation check. The setting to permit Autoreclose without checking synchronising conditions is ***CB SC Shot 1***.

Otherwise, synchronising checks on voltages, relative frequencies, and relative phase angles are needed to ensure that sympathetic conditions exist before CB closure is attempted.

The following diagrams detail the Monitor Checks for CB closure.

8.5.22.1 CHECK SYNCHRONISATION MONITOR FOR CB CLOSURE

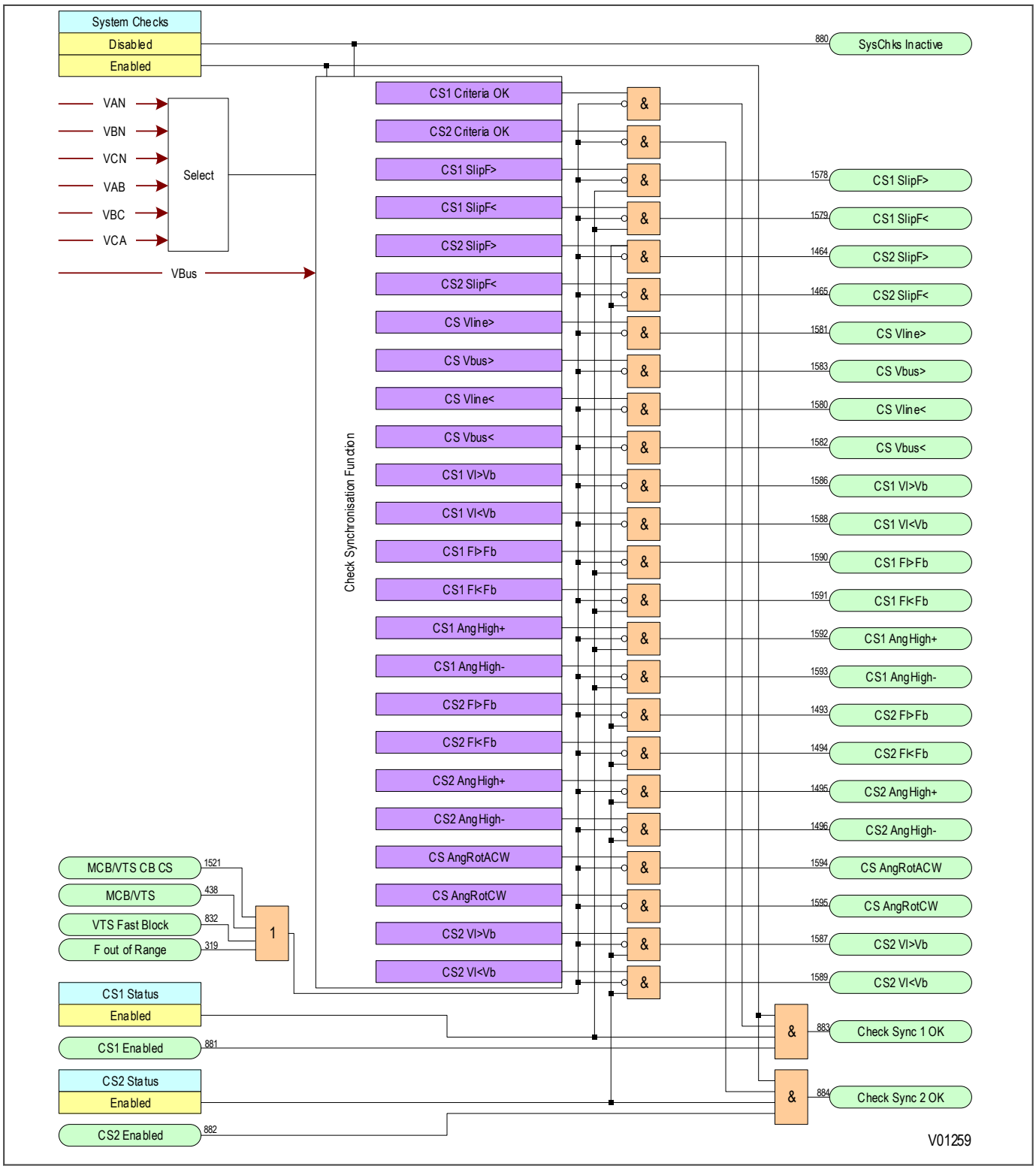


Figure 119: Check synchronisation monitor for CB closure (module 60)

8.5.22.2 VOLTAGE MONITOR FOR CB CLOSURE

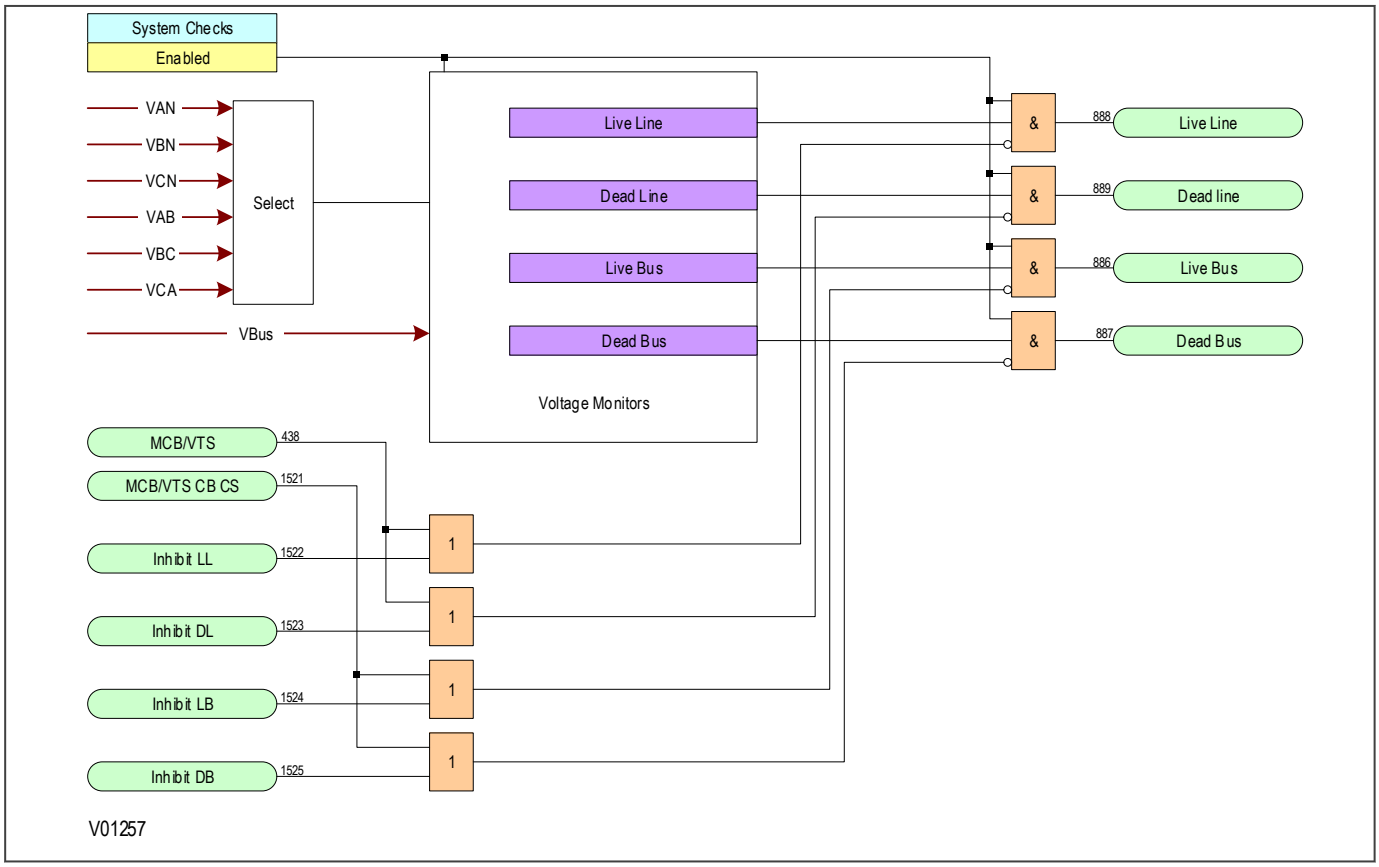


Figure 120: Voltage monitor for CB closure (module 59)

Note:
P54B, P54C, P54E models only.

8.5.23 SYNCHRONISATION CHECKS FOR CB CLOSURE

Logical checking of the outputs from the CB closure monitors is performed to generate signals to indicate that it is OK to close circuit breakers.

Signals are provided to indicate that manual CB closure conditions are OK (***CB Man SCOK***), as are signals to indicate that automatic CB closure conditions are OK (***CB SCOK*** and ***CB Fast SCOK***). The ***CB Fast SCOK*** signal allows CB autoreclosure without waiting for the Dead Time to expire.

For single-phase Autoreclose no voltage or synchronism check is required as synchronising power is flowing in the two healthy phases. Three-phase Autoreclose can be performed without checking that voltages are in synchronism for the first shot (and only the first shot). The settings to permit Autoreclose without checking voltage synchronism on the first shot are:

- ***CB1L SC Shot 1*** for circuit breaker 1 as a leader,
- ***CB1F SC Shot 1*** for circuit breaker 1 as a follower,
- ***CB2L SC Shot 1*** for circuit breaker 2 as a leader,
- ***CB2L SC Shot 1*** for circuit breaker 2 as a follower.

When the circuit breaker has closed, the Autoreclose function asserts a DDB signal ***Set CB1 Close***, which indicates that an attempt has been made to close the circuit breaker. At this point, the Reclaim Time starts. If the circuit

breaker remains closed after the reclaim timer expires, the Autoreclose cycle is complete, and signals are generated to indicate that Autoreclose was successful. These are:

- ***CB1 Succ 1P AR*** (Single-phase Autoreclose CB1)
- ***CB2 Succ 1P AR*** (Single-phase Autoreclose CB2)
- ***CB1 Succ 3P AR*** (Three-phase Autoreclose CB1)
- ***CB2 Succ 3P AR*** (Three-phase Autoreclose CB2)

These signals increment the relevant circuit breaker successful Autoreclose shot counters, as well as resetting the Autoreclose in progress signal.

The relevant circuit breaker successful Autoreclose shot counters are:

- ***CB1 SUCC SPAR*** (Single-phase Autoreclose CB1)
- CB1 SUCC 3PAR Shot1 (Three-phase Autoreclose CB1, Shot 1)
- CB1 SUCC 3PAR Shot2 (Three-phase Autoreclose CB1, Shot 2)
- CB1 SUCC 3PAR Shot3 (Three-phase Autoreclose CB1, Shot 3)
- CB1 SUCC 3PAR Shot4 (Three-phase Autoreclose CB1, Shot 4)
- ***CB2 SUCC SPAR*** (Single-phase Autoreclose CB2)
- CB2 SUCC 3PAR Shot1 (Three-phase Autoreclose CB2, Shot 1)
- CB2 SUCC 3PAR Shot2 (Three-phase Autoreclose CB2, Shot 2)
- CB2 SUCC 3PAR Shot3 (Three-phase Autoreclose CB2, Shot 3)
- CB1 SUCC 3PAR Shot4 (Three-phase Autoreclose CB2, Shot 4)

Note:
P54B, P54C, P54E models only.

8.5.23.1 THREE-PHASE AUTORECLOSE SYSTEM CHECK LOGIC DIAGRAM

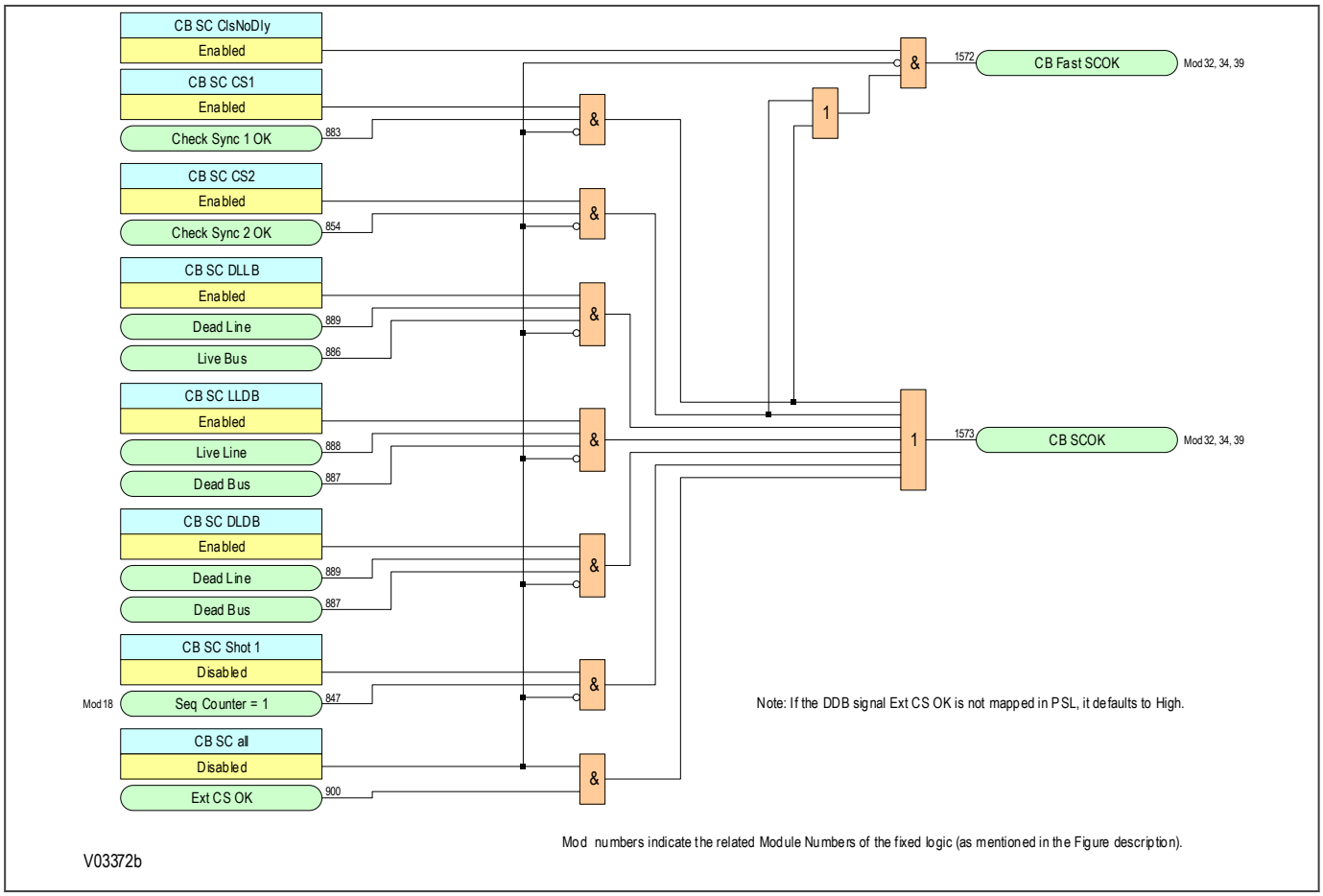


Figure 121: Three-phase autoreclose system check logic (module 45)

Note:
P54B, P54C, P54E models only.

8.5.23.2 CB MANUAL CLOSE SYSTEM CHECK LOGIC DIAGRAM

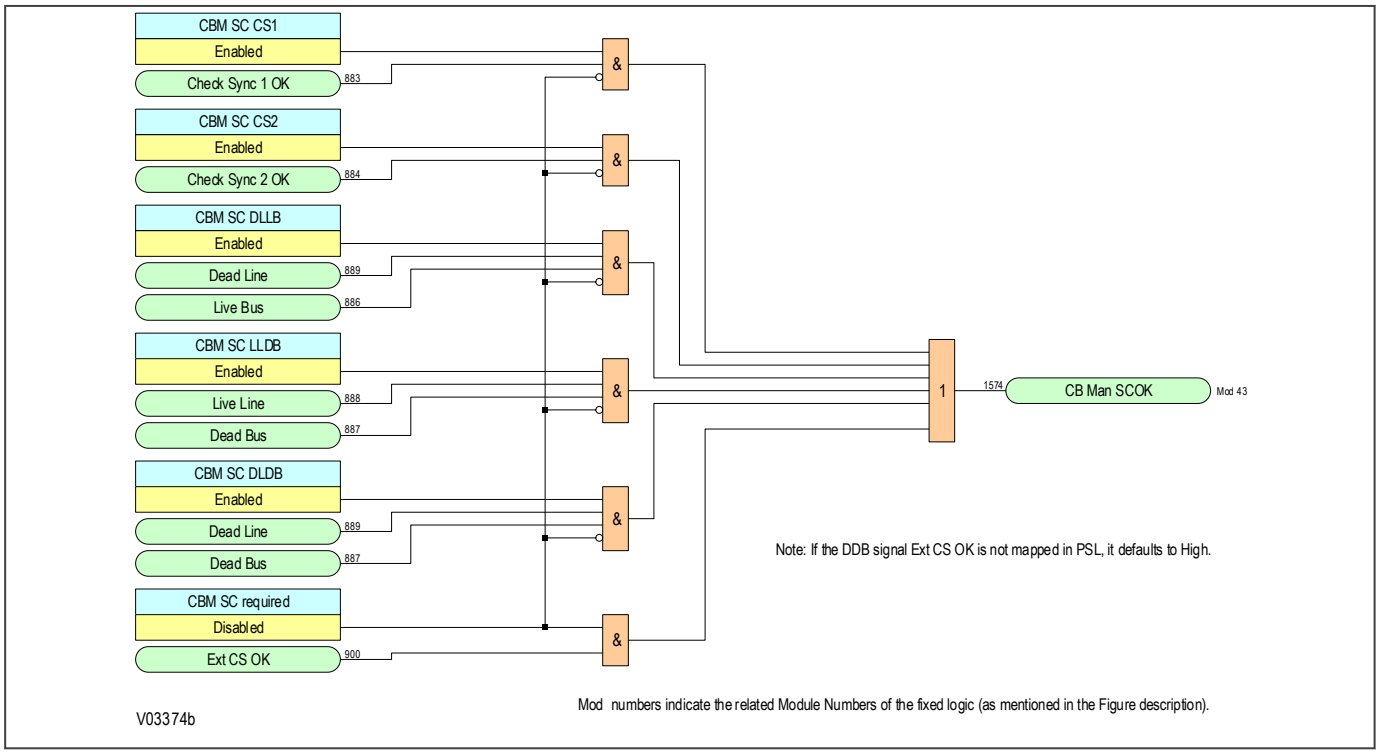


Figure 122: CB manual close system check logic (module 51)

Note:
P54B, P54C, P54E models only.

8.6 SETTING GUIDELINES

8.6.1 DE-IONISING TIME GUIDANCE

The de-ionisation time of a fault arc depends on several factors such as circuit voltage, conductor spacing, fault current and duration, atmospheric conditions, wind speed and capacitive coupling from adjacent conductors. For this reason it is difficult to estimate the de-ionisation time. Circuit voltage is, generally the most significant factor and experience tells us that typical minimum de-ionising times for a three-phase fault are as follows:

- 66 kV: 100 ms
- 110 kV: 150 ms
- 132 kV: 170 ms
- 220 kV: 280 ms
- 275 kV: 300 ms
- 400 kV: 500 ms

Where single-pole high speed Autoreclose is used, the capacitive current induced between the healthy phases and the faulty phase tends to maintain the arc. This significantly increases the de-ionisation time and hence required dead time.

Single-pole Autoreclose is generally only used at transmission voltages. A typical de-ionisation time at 220 kV may be as high as 560 ms.

8.6.2 DEAD TIMER SETTING GUIDELINES

High speed Autoreclose may need to maintain stability on a network with two or more power sources. For high speed Autoreclose the system disturbance time should be minimised by using fast protection (typically <30 ms) and fast circuit breakers (typically <60 ms). For stability between two sources a system dead time of ≤300 ms may typically be required.

The minimum system dead time (considering just the circuit breaker) is the trip mechanism reset time plus the circuit breaker closing time.

The Autoreclose minimum dead time settings are governed primarily by two factors:

- Time taken for de-ionisation of the fault path
- Circuit breaker characteristics

It is essential that the protection fully resets during the dead time, so that correct time discrimination will be maintained after Autoreclose onto a fault. For high speed Autoreclose instantaneous reset of protection is required.

For highly interconnected systems synchronism is unlikely to be lost by the tripping out of a single line. Here the best policy may be to adopt longer dead times, to allow time for power swings resulting from the fault to settle.

8.6.2.1 EXAMPLE DEAD TIME CALCULATION

The following circuit breaker and system characteristics can be used for the minimum dead time calculation:

- a) Circuit breaker Operating time (Trip coil energised to Arc interruption): 50 ms
- b) Circuit breaker Opening + Reset time (Trip coil energised to trip mechanism reset): 200 ms
- c) Protection reset time: < 80 ms
- d) Circuit breaker Closing time (Close command to Contacts make): 85 ms
- e) De-ionisation time (280 ms for 3-phase, or 560 ms for 1-phase)

Three-phase de-ionisation time for 220 kV line is typically 280 ms.

The minimum Autoreclose dead time setting is therefore the greater of:

(a) + (c) = 50 ms + 80 ms = 130 ms, to allow protection reset

(a) + (e) - (d) = 50 ms + 280 ms - 85 ms = 245 ms, to allow de-ionising

In practice a few additional cycles would be added to allow for tolerances, so Dead Time 1 could be set to 300 ms or greater. The overall system dead time is found by adding (d) to the chosen settings then subtracting (a). This gives 335 ms.

A typical de-ionising time value for single-phase trip on a 220 kV line is 560 ms, so the 1 Pole Dead Time could be chosen as 600 ms or greater. The overall system dead time is found by adding (d) to the chosen settings then subtracting (a). This gives 635 ms.

8.6.3 RECLAIM TIME SETTING GUIDELINES

Several factors influence the choice of the reclaim timer, such as:

- Fault incidence/Past experience: Small reclaim times may be required where there is a high incidence of recurrent lightning strikes to prevent unnecessary lockout for transient faults.
- Spring charging time: For high speed Autoreclose the reclaim time may be set longer than the spring charging time. A minimum reclaim time of more than 5s may be needed to allow the circuit breaker time to recover after a trip and close before it can perform another trip-close-trip cycle. This time will depend on the duty (rating) of the circuit breaker. For delayed Autoreclose this may not be needed as the dead time can be extended by an extra circuit breaker healthy check / Autoreclose Inhibit Time window time if there is insufficient energy in the circuit breaker.
- Switchgear Maintenance: Excessive operation resulting from short reclaim times can mean shorter maintenance intervals.

CHAPTER 9

CB FAIL PROTECTION

9.1 CHAPTER OVERVIEW

The device provides a Circuit Breaker Fail Protection function. This chapter describes the operation of this function including the principles, logic diagrams and applications.

This chapter contains the following sections:

Chapter Overview 198

Circuit Breaker Fail Protection 199

Circuit Breaker Fail Implementation 200

Circuit Breaker Fail Logic 202

Application Notes 206

9.2 CIRCUIT BREAKER FAIL PROTECTION

When a fault occurs, one or more protection devices will operate and issue a trip command to the relevant circuit breakers. Operation of the circuit breaker is essential to isolate the fault and prevent, or at least limit, damage to the power system. For transmission and sub-transmission systems, slow fault clearance can also threaten system stability.

For these reasons, it is common practice to install Circuit Breaker Failure protection (CBF). CBF protection monitors the circuit breaker and establishes whether it has opened within a reasonable time. If the fault current has not been interrupted following a set time delay from circuit breaker trip initiation, the CBF protection will operate, whereby the upstream circuit breakers are back-tripped to ensure that the fault is isolated.

CBF operation can also reset all start output contacts, ensuring that any blocks asserted on upstream protection are removed.

9.3 CIRCUIT BREAKER FAIL IMPLEMENTATION

Circuit Breaker Failure Protection is implemented in the *CB FAIL & P.DEAD* column of the relevant settings group.

9.3.1 CIRCUIT BREAKER FAIL TIMERS

The circuit breaker failure protection incorporates two timers, ***CB Fail 1 Timer*** and ***CB Fail 2 Timer***, allowing configuration for the following scenarios:

- Simple CBF, where only ***CB Fail 1 Timer*** is enabled. For any protection trip, the **CB Fail 1** ***Timer*** is started, and normally reset when the circuit breaker opens to isolate the fault. If breaker opening is not detected, the CB Fail 1 Timer times out and closes an output contact assigned to breaker fail (using the programmable scheme logic). This contact is used to back-trip upstream switchgear, generally tripping all infeeds connected to the same busbar section.
- A retripping scheme, plus delayed back-tripping. Here, ***CB Fail 1 Timer*** is used to issue a trip command to a second trip circuit of the same circuit breaker. This requires the circuit breaker to have duplicate circuit breaker trip coils. This mechanism is known as retripping. If retripping fails to open the circuit breaker, a back-trip may be issued following an additional time delay. The back-trip uses ***CB Fail 2 Timer***, which was also started at the instant of the initial protection element trip.

You can configure the CBF elements ***CB Fail 1 Timer*** and ***CBF Fail 2 Timer*** to operate for trips triggered by protection elements within the device. Alternatively you can use an external protection trip by allocating one of the opto-inputs to the ***External Trip*** DDB signal in the PSL.

You can reset the CBF from a breaker open indication (from the pole dead logic) or from a protection reset. In these cases resetting is only allowed if the undercurrent elements have also been reset. The resetting mechanism is determined by the settings ***Volt Prot Reset*** and ***Ext Prot Reset***.

The resetting options are summarised in the following table:

Initiation (Menu Selectable)	CB Fail Timer Reset Mechanism
Current based protection	The resetting mechanism is fixed (e.g. 50/51/46/21/87) IA< operates AND IB< operates AND IC< operates AND IN< operates
Sensitive Earth Fault element *	The resetting mechanism is fixed. ISEF< Operates
Non-current based protection (e.g. 27/59/81/32L)	Three options are available: All I< and IN< elements operate Protection element reset AND all I< and IN< elements operate CB open (all 3 poles) AND all I< and IN< elements operate
External protection	Three options are available. All I< and IN< elements operate External trip reset AND all I< and IN< elements operate CB open (all 3 poles) AND all I< and IN< elements operate

Note:
** The sensitive earth fault element is implemented in P54C and P54E models only.*

9.3.2 ZERO CROSSING DETECTION

When there is a fault and the circuit breaker interrupts the CT primary current, the flux in the CT core decays to a residual level. This decaying flux introduces a decaying DC current in the CT secondary circuit known as subsidence current. The closer the CT is to its saturation point, the higher the subsidence current.

The time constant of this subsidence current depends on the CT secondary circuit time constant and it is generally long. If the protection clears the fault, the CB Fail function should reset fast to avoid maloperation due to the

subsidence current. To compensate for this the device includes a zero-crossing detection algorithm, which ensures that the CB Fail re-trip and back-trip signals are not asserted while subsidence current is flowing. If all the samples within half a cycle are greater than or smaller than 0 A (10 mS for a 50 Hz system), then zero crossing detection is asserted, thereby blocking the operation of the CB Fail function. The zero-crossing detection algorithm is used after the circuit breaker in the primary system has opened ensuring that the only current flowing in the AC secondary circuit is the subsidence current.

9.4 CIRCUIT BREAKER FAIL LOGIC

9.4.1 CIRCUIT BREAKER FAIL LOGIC - PART 1

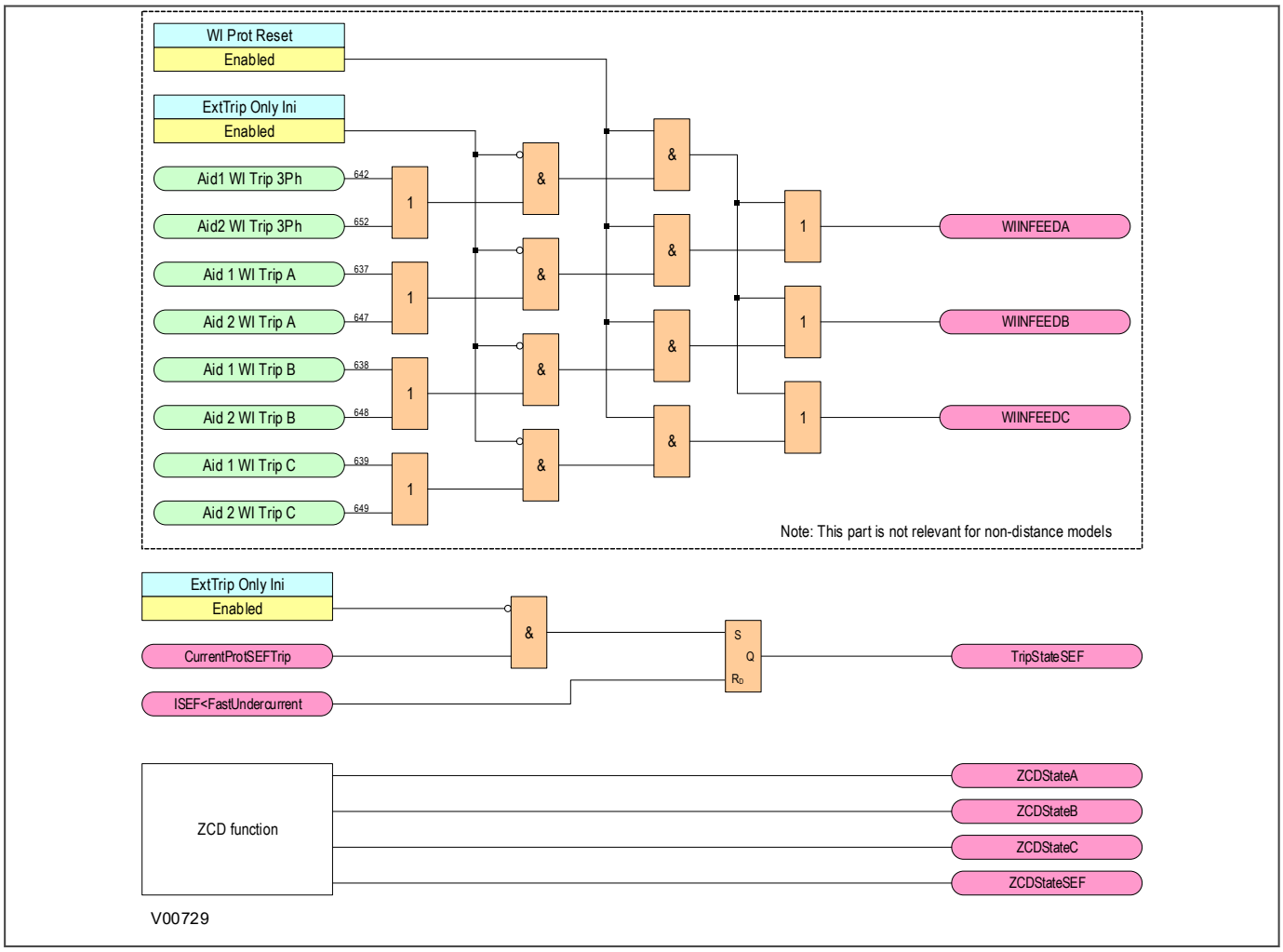


Figure 123: Circuit breaker fail logic - part 1

9.4.2 CIRCUIT BREAKER FAIL LOGIC - PART 2

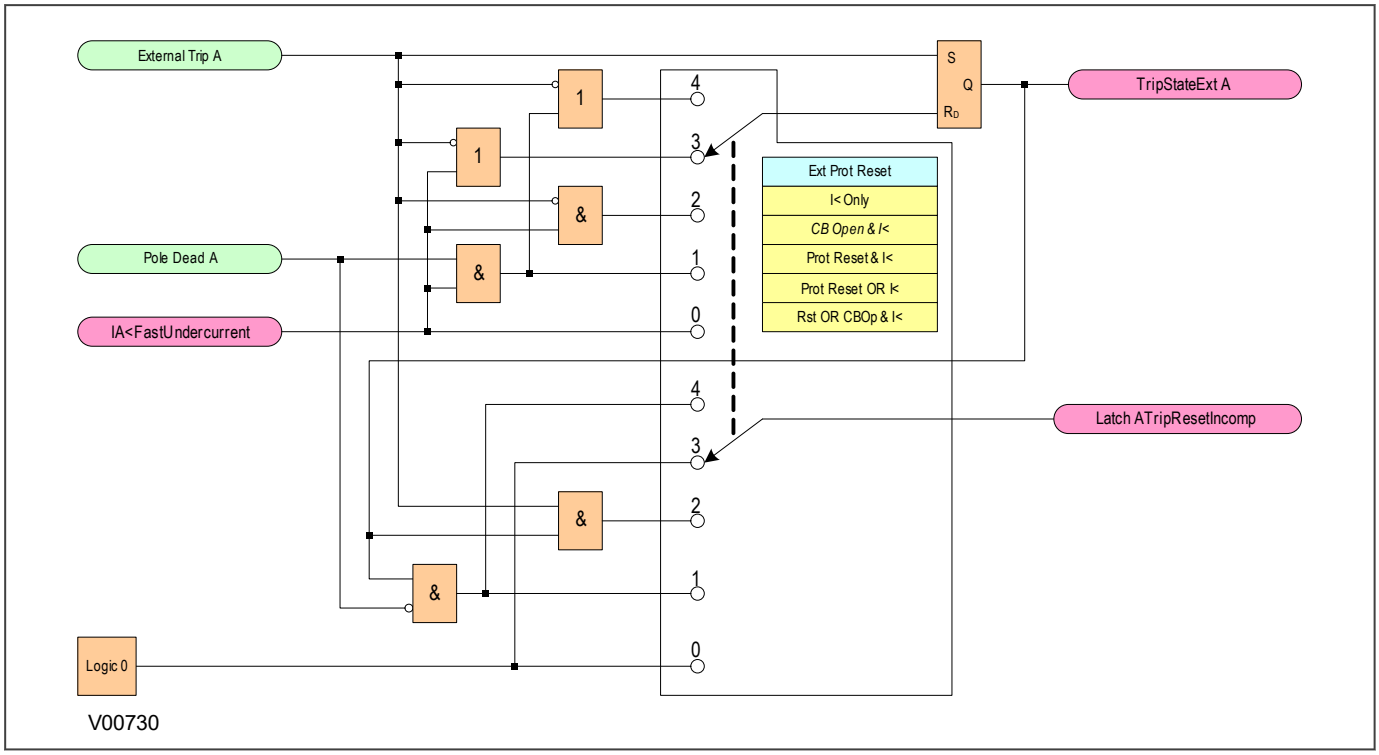


Figure 124: Circuit breaker fail logic - part 2

Note:
This diagram shows only phase-A for a single-CB device. The diagrams for phases B and C follow the same principle and are not repeated here.

9.4.3 CIRCUIT BREAKER FAIL LOGIC - PART 3

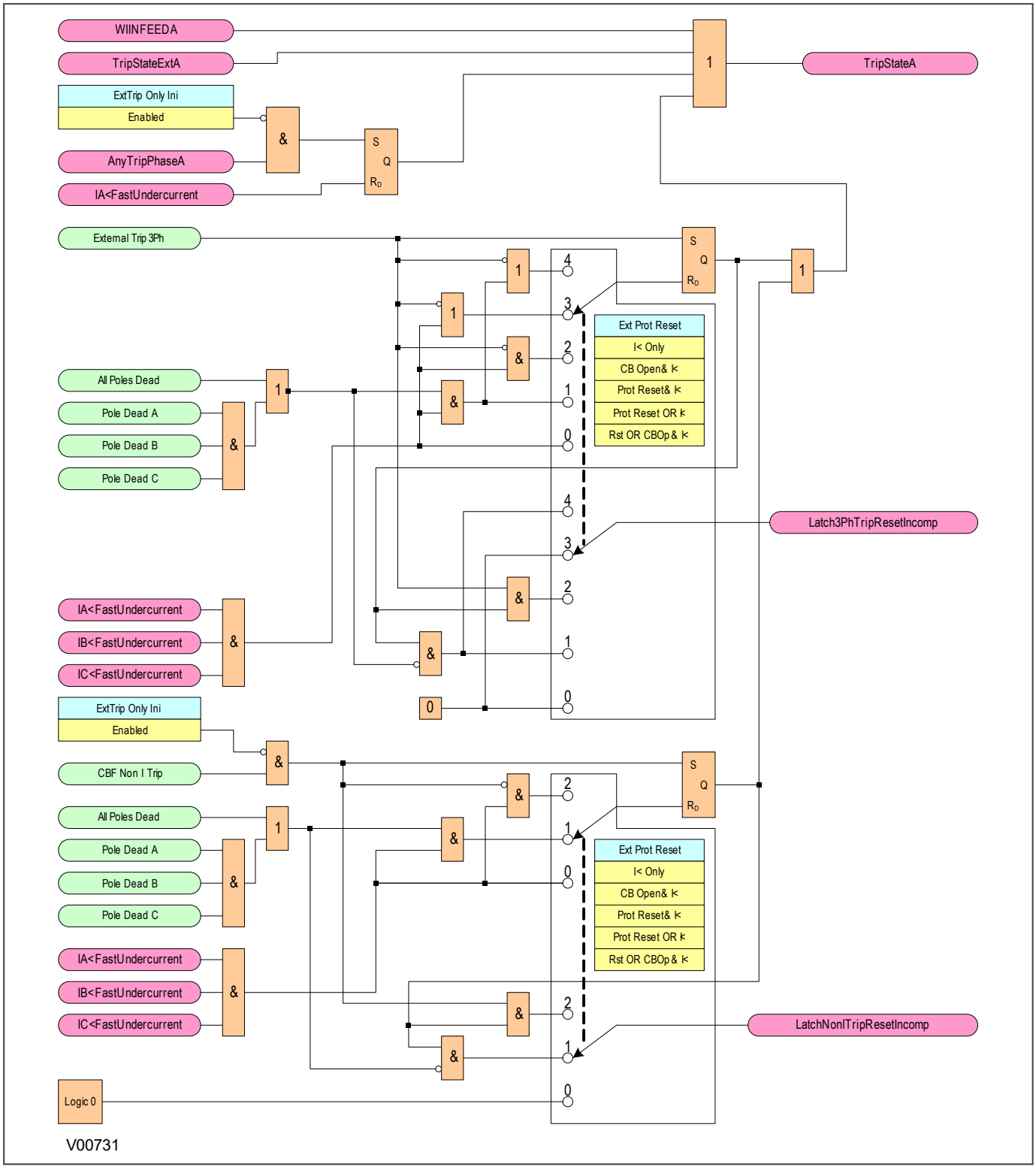


Figure 125: Circuit breaker fail logic - part 3

9.4.4 CIRCUIT BREAKER FAIL LOGIC - PART 4

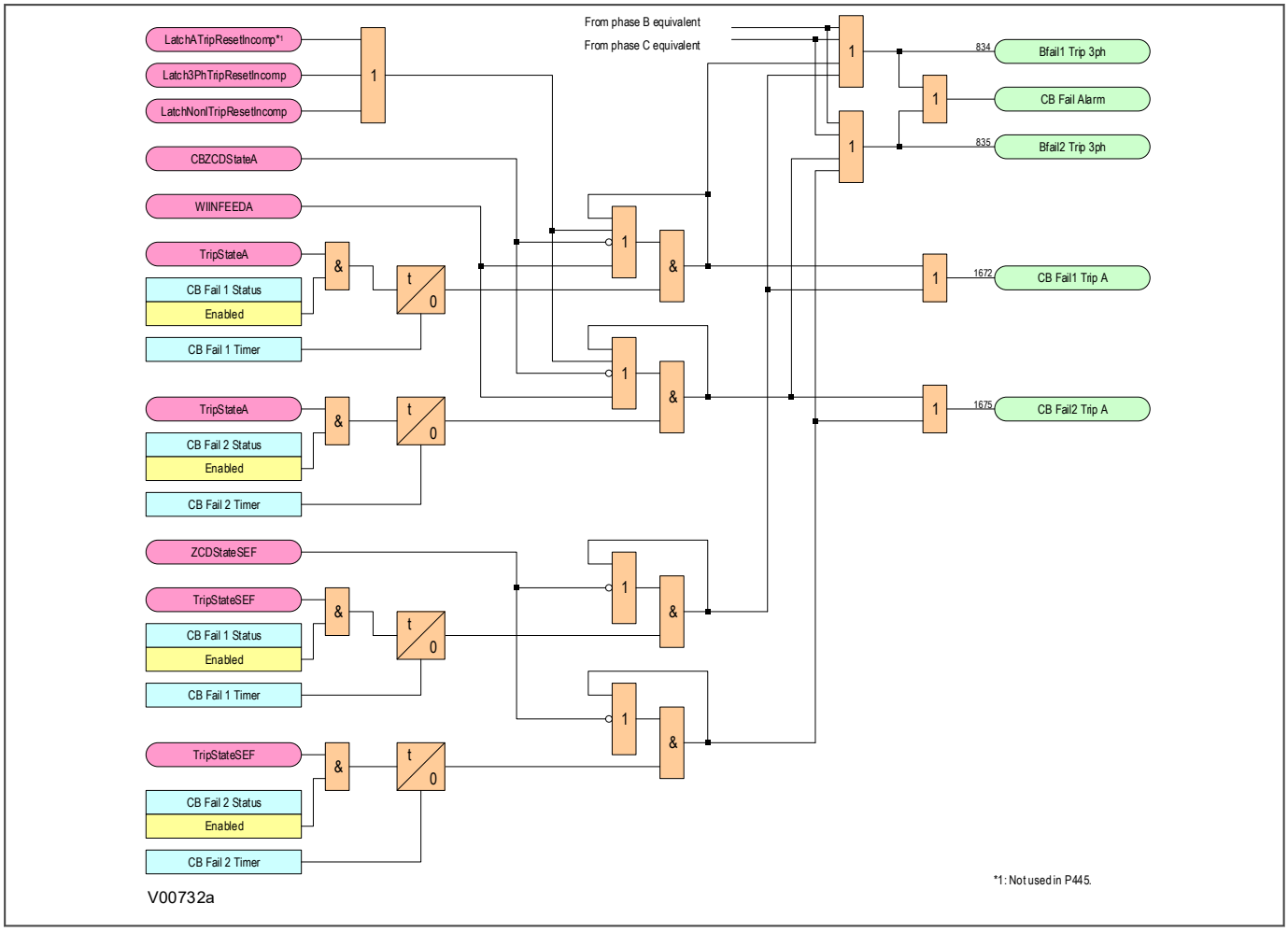


Figure 126: Circuit breaker fail logic - part 4

Note:
This diagram shows only phase-A for a single-CB device. The diagrams for phases B and C follow the same principle and are not repeated here.

9.5 APPLICATION NOTES

9.5.1 RESET MECHANISMS FOR CB FAIL TIMERS

It is common practise to use low set undercurrent elements to indicate that circuit breaker poles have interrupted the fault or load current. This covers the following situations:

- Where circuit breaker auxiliary contacts are defective, or cannot be relied on to definitely indicate that the breaker has tripped.
- Where a circuit breaker has started to open but has become jammed. This may result in continued arcing at the primary contacts, with an additional arcing resistance in the fault current path. Should this resistance severely limit fault current, the initiating protection element may reset. Therefore, reset of the element may not give a reliable indication that the circuit breaker has opened fully.

For any protection function requiring current to operate, the device uses operation of undercurrent elements to detect that the necessary circuit breaker poles have tripped and reset the CB fail timers. However, the undercurrent elements may not be reliable methods of resetting CBF in all applications. For example:

- Where non-current operated protection, such as under/overvoltage or under/overfrequency, derives measurements from a line connected voltage transformer. Here, I< only gives a reliable reset method if the protected circuit would always have load current flowing. In this case, detecting drop-off of the initiating protection element might be a more reliable method.
- Where non-current operated protection, such as under/overvoltage or under/overfrequency, derives measurements from a busbar connected voltage transformer. Again using I< would rely on the feeder normally being loaded. Also, tripping the circuit breaker may not remove the initiating condition from the busbar, and so drop-off of the protection element may not occur. In such cases, the position of the circuit breaker auxiliary contacts may give the best reset method.

9.5.2 SETTING GUIDELINES (CB FAIL TIMER)

The following timing chart shows the CB Fail timing during normal and CB Fail operation. The maximum clearing time should be less than the critical clearing time which is determined by a stability study. The CB Fail back-up trip time delay considers the maximum CB clearing time, the CB Fail reset time plus a safety margin. Typical CB clearing times are 1.5 or 3 cycles. The CB Fail reset time should be short enough to avoid CB Fail back-trip during normal operation. Phase and ground undercurrent elements must be asserted for the CB Fail to reset. The assertion of the undercurrent elements might be delayed due to the subsidence current that might be flowing through the secondary AC circuit.

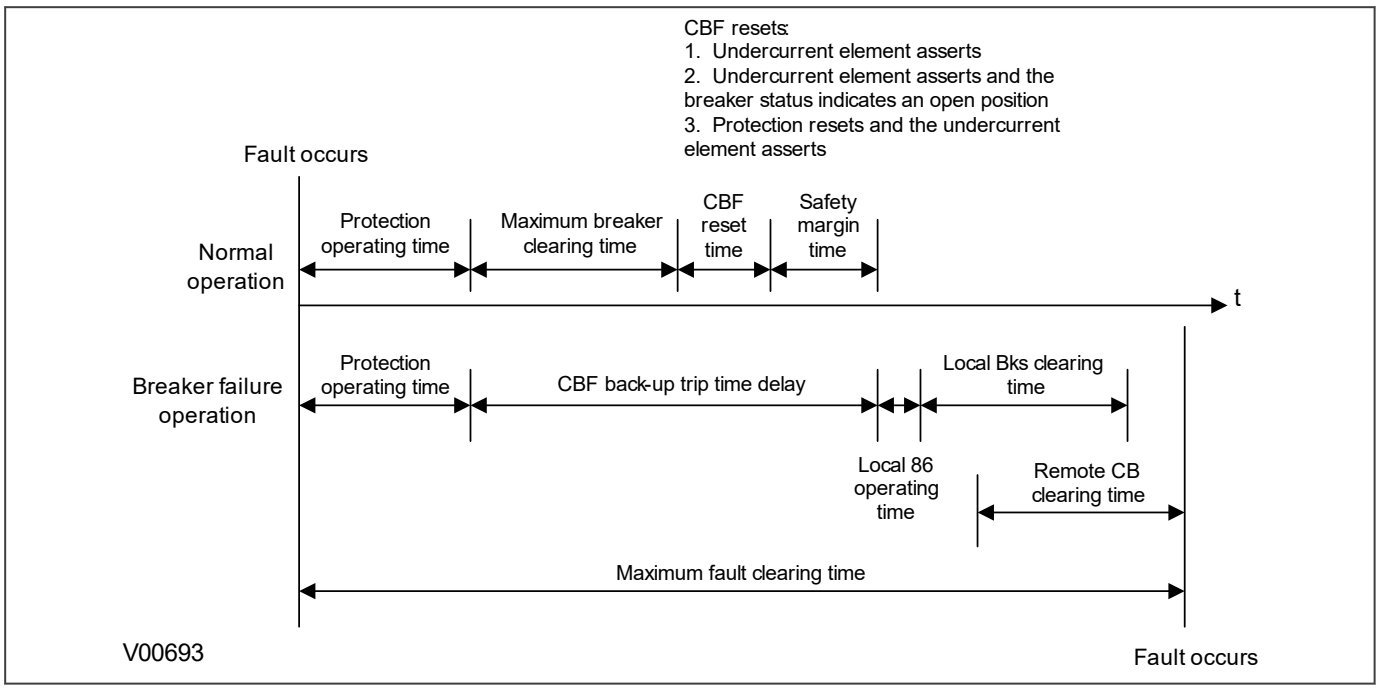


Figure 127: CB fail timing

The following examples consider direct tripping of a 2-cycle circuit breaker. Typical timer settings to use are as follows:

CB Fail Reset Mechanism	tBF Time Delay	Typical Delay For 2 Cycle Circuit Breaker
Initiating element reset	CB interrupting time + element reset time (max.) + error in tBF timer + safety margin	50 + 50 + 10 + 50 = 160 ms
CB open	CB auxiliary contacts opening/ closing time (max.) + error in tBF timer + safety margin	50 + 10 + 50 = 110 ms
Undercurrent elements	CB interrupting time + undercurrent element (max.) + safety margin operating time	50 + 25 + 50 = 125 ms

Note:
All CB Fail resetting involves the operation of the undercurrent elements. Where element resetting or CB open resetting is used, the undercurrent time setting should still be used if this proves to be the worst case.
Where auxiliary tripping relays are used, an additional 10-15 ms must be added to allow for trip relay operation.

9.5.3 SETTING GUIDELINES (UNDERCURRENT)

The phase undercurrent settings (I<) must be set less than load current to ensure that I< operation correctly indicates that the circuit breaker pole is open. A typical setting for overhead line or cable circuits is 20%In. Settings of 5% of In are common for generator CB Fail.

The earth fault undercurrent elements must be set less than the respective trip. For example:

$$IN< = (IN> trip)/2$$

CHAPTER 10

CURRENT PROTECTION FUNCTIONS

10.1 CHAPTER OVERVIEW

The primary purpose of this product is not overcurrent protection. It does however provide a range of current protection functions to be used as backup protection. This chapter assumes you are familiar with overcurrent protection principles and does not provide detailed information here. If you require further information about general overcurrent protection principles, please refer either to GE Vernova's publication, Protection and Automation Application Guide, earlier incarnations of this technical manual, or one of our technical manuals from our P40 Agile Modular distribution range of products such as the P14.

This chapter contains the following sections:

Chapter Overview 209
Overcurrent Protection Principles 210
Phase Fault Overcurrent Protection 220
Negative Sequence Overcurrent Protection 223
Earth Fault Protection 226
Sensitive Earth Fault Protection 231
High Impedance REF 236
Thermal Overload Protection 238
Broken Conductor Protection 242

10.2 OVERCURRENT PROTECTION PRINCIPLES

Most electrical power system faults result in an overcurrent of one kind or another. It is the job of protection devices, formerly known as 'relays' but now known as Intelligent Electronic Devices (IEDs) to protect the power system from faults. The general principle is to isolate the faults as quickly as possible to limit the danger and prevent fault currents flowing through systems, which can cause severe damage to equipment and systems. At the same time, we wish to switch off only the parts of the power grid that are absolutely necessary, to prevent unnecessary blackouts. The protection devices that control the tripping of the power grid's circuit breakers are highly sophisticated electronic units, providing an array of functionality to cover the different fault scenarios for a multitude of applications.

The described products offer a range of overcurrent protection functions including:

- Phase Overcurrent protection
- Earth Fault Overcurrent protection
- Negative Sequence Overcurrent protection
- Sensitive Earth Fault protection

To ensure that only the necessary circuit breakers are tripped and that these are tripped with the smallest possible delay, the IEDs in the protection scheme need to co-ordinate with each other. Various methods are available to achieve correct co-ordination between IEDs in a system. These are:

- By means of time alone
- By means of current alone
- By means of a combination of both time and current.

Grading by means of current alone is only possible where there is an appreciable difference in fault level between the two locations where the devices are situated. Grading by time is used by some utilities but can often lead to excessive fault clearance times at or near source substations where the fault level is highest.

For these reasons the most commonly applied characteristic in co-ordinating overcurrent devices is the IDMT (Inverse Definite Minimum Time) type.

10.2.1 IDMT CHARACTERISTICS

There are two basic requirements to consider when designing protection schemes:

- All faults should be cleared as quickly as possible to minimise damage to equipment
- Fault clearance should result in minimum disruption to the electrical power grid.

The second requirement means that the protection scheme should be designed such that only the circuit breaker(s) in the protection zone where the fault occurs, should trip.

These two criteria are actually in conflict with one another, because to satisfy (1), we increase the risk of shutting off healthy parts of the grid, and to satisfy (2) we purposely introduce time delays, which increase the amount of time a fault current will flow. With IDMT protection applied to radial feeders, this problem is exacerbated by the nature of faults in that the protection devices nearest the source, where the fault currents are largest, actually need the longest time delay.

IDMT characteristics are described by operating curves. Traditionally, these were defined by the performance of electromechanical devices. In numerical protection, equations are used to replicate these characteristics so that they can be used to grade with older equipment.

The old electromechanical devices countered this problem somewhat due to their natural operate time v. fault current characteristic, whereby the higher the fault current, the quicker the operate time. The characteristic typical of these electromechanical devices is called Inverse Definite Minimum Time or IDMT for short.

10.2.1.1 IEC 60255 IDMT CURVES

There are four well-known variants of this characteristic:

- Standard Inverse
- Very inverse
- Extremely inverse
- UK Long Time inverse

These equations and corresponding curves governing these characteristics are very well known in the power industry.

Standard inverse

This characteristic is commonly known as the 3/10 characteristic, i.e. at ten times setting current and TMS of 1 the device will operate in 3 seconds.

The characteristic curve can be defined by the mathematical expression:

$$t_{op} = T \frac{0.14}{\left(\frac{I}{I_s}\right)^{0.02} - 1}$$

The standard inverse time characteristic is widely applied at all system voltages – as back up protection on EHV systems and as the main protection on HV and MV distribution systems.

In general, the standard inverse characteristics are used when:

- There are no co-ordination requirements with other types of protective equipment further out on the system, e.g. Fuses, thermal characteristics of transformers, motors etc.
- The fault levels at the near and far ends of the system do not vary significantly.
- There is minimal inrush on cold load pick up. Cold load inrush is that current which occurs when a feeder is energised after a prolonged outage. In general the device cannot be set above this value but the current should decrease below the device setting before the device operates.

The Standard Inverse curve implemented in this device becomes definite time (DT) for input current values above 30 x I_s.

Very inverse

This type of characteristic is normally used to obtain greater time selectivity when the limiting overall time factor is very low, and the fault current at any point does not vary too widely with system conditions. It is particularly suitable, if there is a substantial reduction of fault current as the distance from the power source increases. The steeper inverse curve gives longer time grading intervals. Its operating time is approximately doubled for a reduction in setting from 7 to 4 times the device current setting. This permits the same time multiplier setting for several devices in series.

The characteristic curve can be defined by the mathematical expression:

$$t_{op} = T \frac{13.5}{\left(\frac{I}{I_s}\right) - 1}$$

The Very Inverse curve implemented in this device becomes definite time (DT) for input current values above 30 x I_s.

Extremely inverse

With this characteristic the operating time is approximately inversely proportional to the square of the current. The long operating time of the device at peak values of load current make the device particularly suitable for grading with fuses and also for protection of feeders which are subject to peak currents on switching in, such as feeders supplying refrigerators, pumps, water heaters etc., which remain connected even after a prolonged interruption of supply.

For cases where the generation is practically constant and discrimination with low tripping times is difficult to obtain, because of the low impedance per line section, an extremely inverse device can be very useful since only a small difference of current is necessary to obtain an adequate time difference.

Another application for this device is with auto reclosers in low voltage distribution circuits. As the majority of faults are of a transient nature, the device is set to operate before the normal operating time of the fuse, thus preventing perhaps unnecessary blowing of the fuse.

Upon reclosure, if the fault persists, the recloser locks itself in the closed position and allows the fuse to blow to clear the fault.

The Extremely Inverse curve implemented in this device becomes definite time (DT) for input current values above 20 x I_s.

This characteristic is also widely used for protecting plant against overheating since overheating is usually an I2t function.

This characteristic curve can be defined by the mathematical expression:

$$t_{op} = T \frac{80}{\left(\frac{I}{I_s}\right)^2 - 1}$$

UK long time inverse

This type of characteristic has a long time characteristic and may be used for protection of neutral earthing resistors (which normally have a 30 second rating). The device operating time at 5 times current setting is 30 seconds at a TMS of 1.

This can be defined by:

$$t_{op} = T \frac{120}{\left(\frac{I}{I_s}\right) - 1}$$

In the above equations:

- t_{op} is the operating time
- T is the time multiplier setting
- I is the measured current
- I_s is the current threshold setting

The ratio I/I_s is sometimes defined as ‘M’ or ‘PSM’ (Plug Setting Multiplier).

The Long Time Inverse curve implemented in this device becomes definite time (DT) for input current values above 30 x I_s.

These curves are plotted as follows:

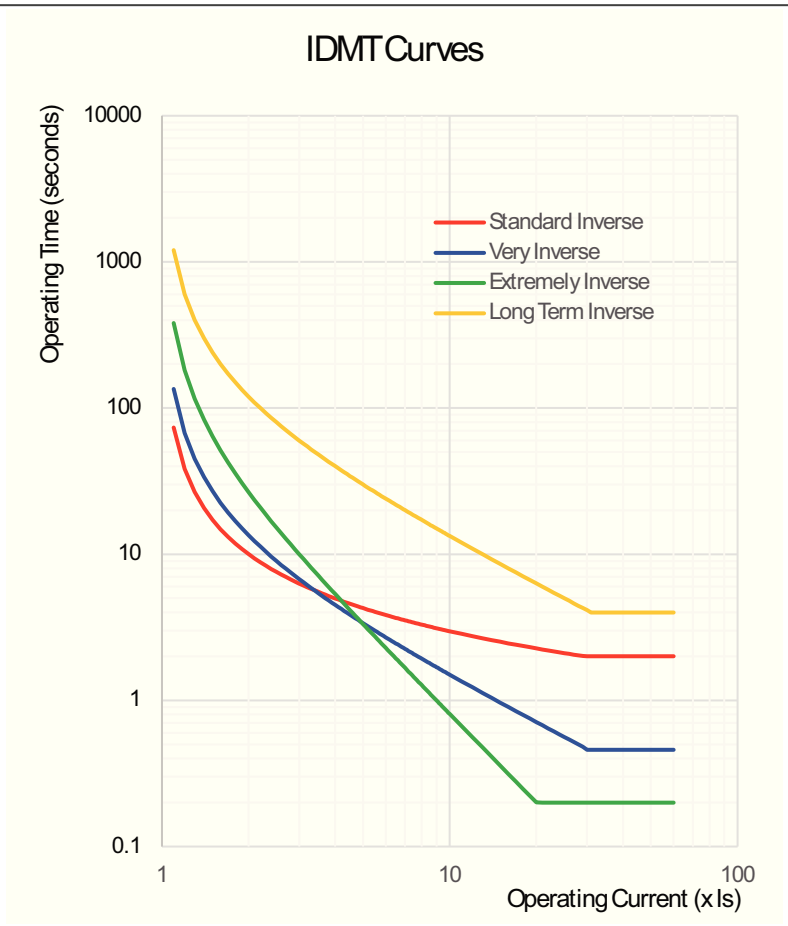


Figure 128: IEC 60255 IDMT curves

10.2.1.2 EUROPEAN STANDARDS

The IEC 60255 IDMT Operate equation is:

$$t_{op} = T\left(\frac{\beta}{M^{\alpha}-1} + L\right) + C$$

and the IEC 60255 IDMT Reset equation is:

$$t_{r} = T\left(\frac{\beta}{1-M^{\alpha}}\right)$$

where:

- t_{op} is the operating time
- t_{r} is the reset time
- T is the Time Multiplier setting
- M is the ratio of the measured current divided by the threshold current (I/Is)
- β is a constant, which can be chosen to satisfy the required curve characteristic
- α is a constant, which can be chosen to satisfy the required curve characteristic
- C is a constant for adding Definite Time (Definite Time adder)
- L is a constant (usually only used for ANSI/IEEE curves)

The constant values for the IEC IDMT curves are as follows:

Curve Description	β constant	α constant	L constant
IEC Standard Inverse Operate	0.14	0.02	0
IEC Standard Inverse Reset	8.2	6.45	0
IEC Very Inverse Operate	13.5	1	0
IEC Very Inverse Reset	50.92	2.4	0
IEC Extremely Inverse Operate	80	2	0
IEC Extremely Inverse Reset	44.1	3.03	0
UK Long Time Inverse Operate*	120	1	0
UK Rectifier Operate*	45900	5.6	0

Rapid Inverse (RI) characteristic

The RI operate curve is represented by the following equation:

$$t_{op} = K\left(\frac{1}{0.339 - \frac{0.236}{M}}\right)$$

where:

- t_{op} is the operating time
- K is the Time Multiplier setting
- M is the ratio of the measured current divided by the threshold current (I/I_S)

Note:
** When using UK Long Time Inverse, UK Rectifier or RI for the Operate characteristic, DT (Definite Time) is always used for the Reset characteristic.*

10.2.1.3 NORTH AMERICAN STANDARDS

The IEEE IDMT Operate equation is:

$$t_{op} = TD\left(\frac{\beta}{M^{\alpha} - 1} + L\right) + C$$

and the IEEE IDMT Reset equation is:

$$t_r = TD\left(\frac{\beta}{1 - M^{\alpha}}\right)$$

where:

- t_{op} is the operating time
- t_r is the reset time
- TD is the Time Dial setting
- M is the ratio of the measured current divided by the threshold current (I/I_S)

- β is a constant, which can be chosen to satisfy the required curve characteristic
- α is a constant, which can be chosen to satisfy the required curve characteristic
- C is a constant for adding Definite Time (Definite Time adder)
- L is a constant (usually only used for ANSI/IEEE curves)

The constant values for the IEEE curves are as follows:

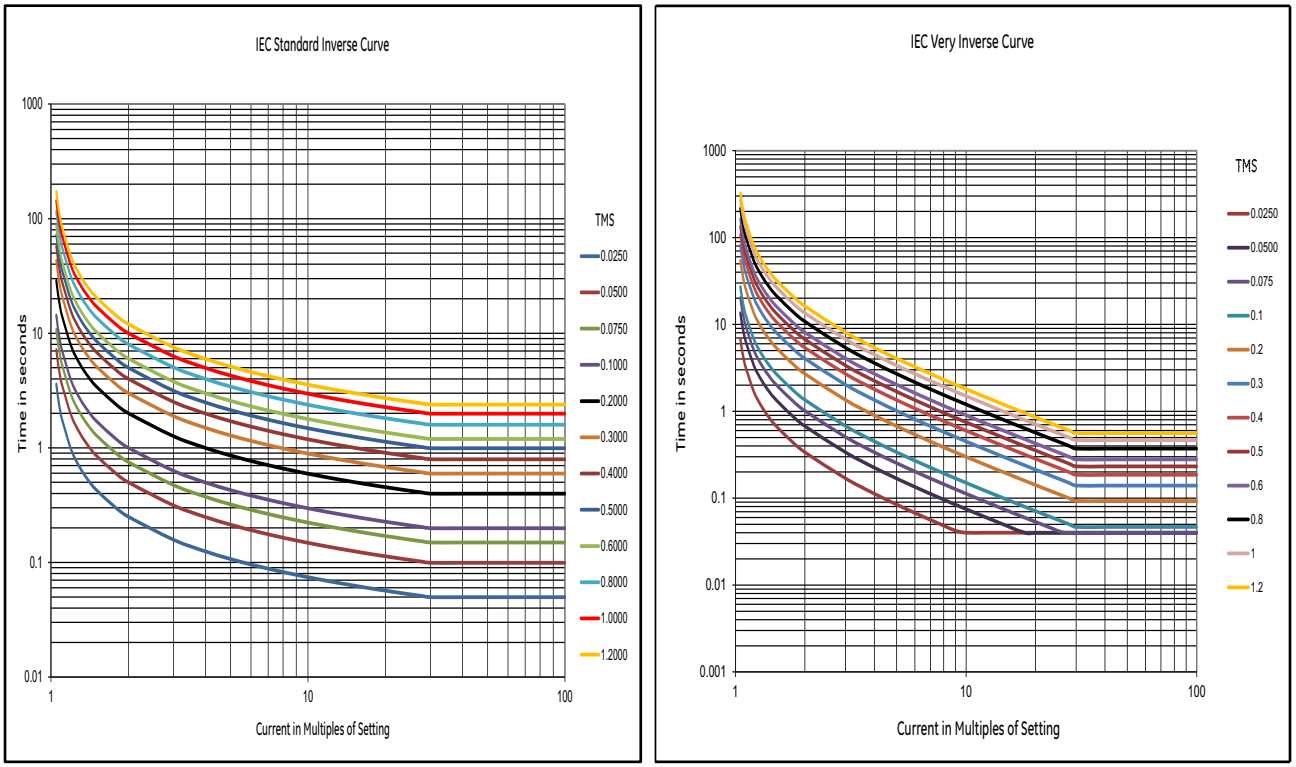
Curve Description	β constant	α constant	L constant
IEEE Moderately Inverse Operate	0.0515	0.02	0.114
IEEE Moderately Inverse Reset	4.85	2	0
IEEE Very Inverse Operate	19.61	2	0.491
IEEE Very Inverse Reset	21.6	2	0
IEEE Extremely Inverse Operate	28.2	2	0.1217
IEEE Extremely Inverse Reset	29.1	2	0
CO8 US Inverse Operate	5.95	2	0.18
CO8 US Inverse Reset	5.95	2	0
CO2 US Short Time Inverse Operate	0.16758	0.02	0.11858
CO2 US Short Time Inverse Reset	2.261	2	0

The constant values for the ANSI curves are as follows:

Curve Description	β constant	α constant	L constant
ANSI Normally Inverse Operate	8.9341	2.0938	0.17966
ANSI Normally Inverse Reset	9	2	0
ANSI Short Time Inverse Operate	0.03393	1.2969	0.2663
ANSI Short Time Inverse Reset	0.5	2	0
ANSI Long Time Inverse Operate	2.18592	1	5.6143
ANSI Long Time Inverse Reset	15.75	2	0

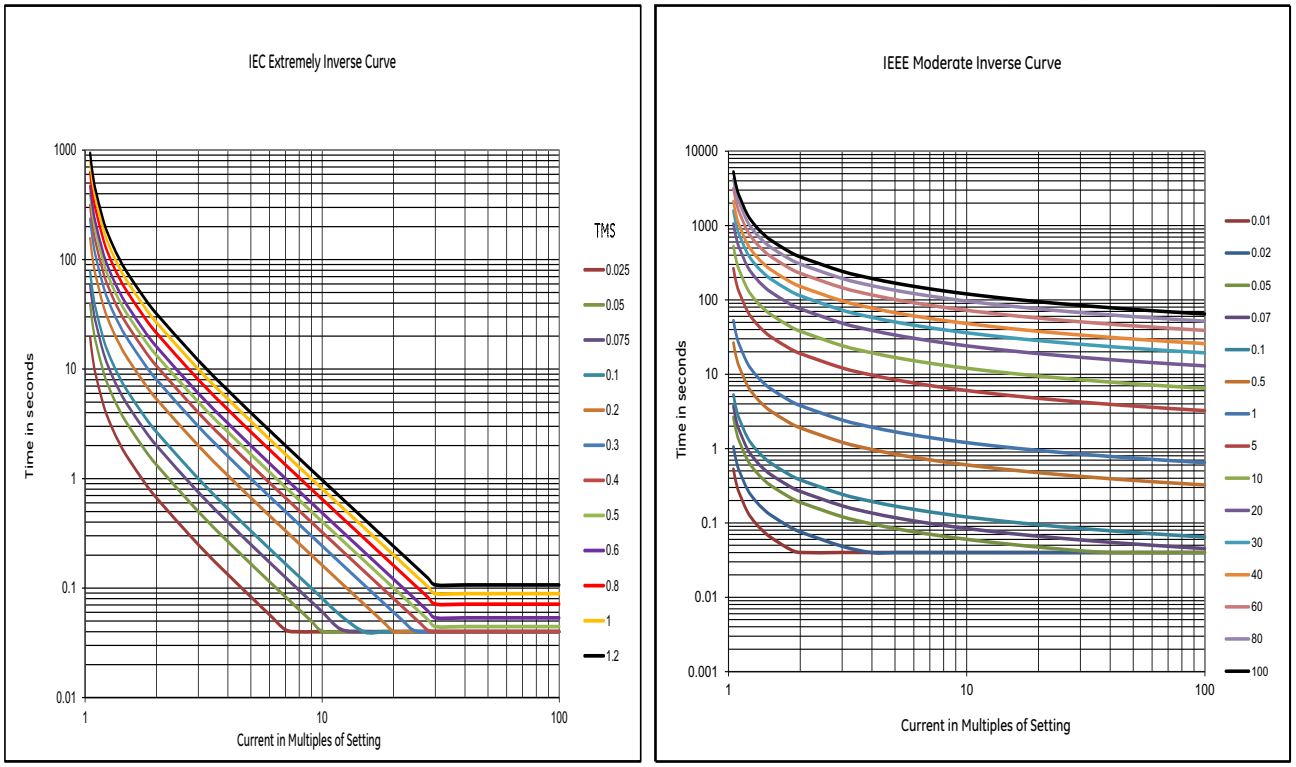
Note:
** When using UK Long Time Inverse or UK Rectifier for the Operate characteristic, DT is always used for the Reset characteristic.*

10.2.1.4 IEC AND IEEE INVERSE CURVES



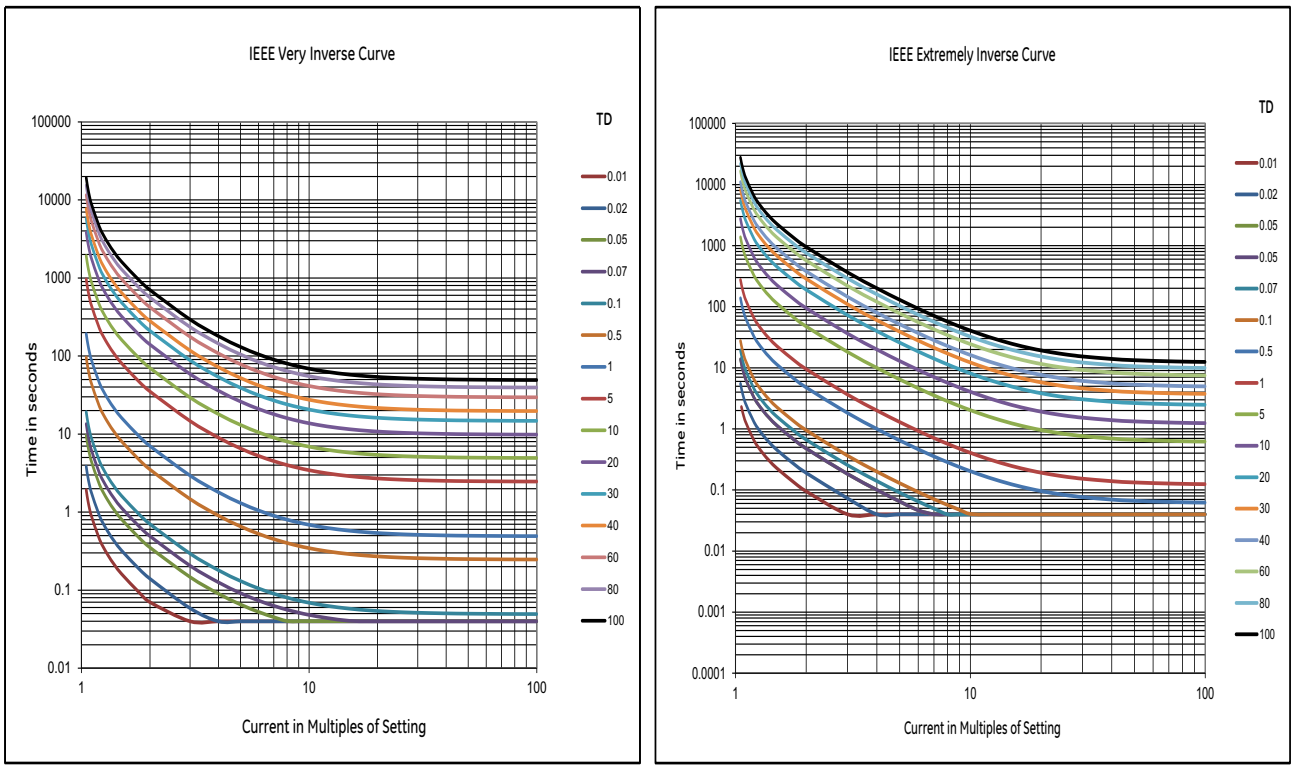
E00757

Figure 129: IEC standard and very inverse curves



E00758

Figure 130: IEC extremely inverse and IEEE moderate inverse curves



E00759

Figure 131: IEEE very and extremely inverse curves

10.2.1.5 DIFFERENCES BETWEEN THE NORTH AMERICAN AND EUROPEAN STANDARDS

The IEEE and US curves are set differently to the IEC/UK curves, with regard to the time setting. A time multiplier setting (TMS) is used to adjust the operating time of the IEC curves, whereas a time dial setting is used for the IEEE/US curves. The menu is arranged such that if an IEC/UK curve is selected, the ***I> Time Dial*** cell is not visible and vice versa for the TMS setting. For both IEC and IEEE/US type curves, a definite time adder setting is available, which will increase the operating time of the curves by the set value.

10.2.1.6 PROGRAMMABLE CURVES

As well as the standard curves as defined by various countries and standardising bodies, it is possible to program custom curves using the User Programmable Curve Tool, described in the Settings Application Software chapter. This is a user-friendly tool by which you can create curves either by formula or by entering data points. Programmable curves help you to match more closely the withstand characteristics of the electrical equipment than standard curves.

10.2.2 PRINCIPLES OF IMPLEMENTATION

The range of protection products provides a very wide range of protection functionality. Despite the diverse range of functionality provided, there is some commonality between the way many of the protection functions are implemented. It is important to describe some of these basic principles before going deeper into the individual protection functions.

A simple representation of protection functionality is shown in the following diagram:

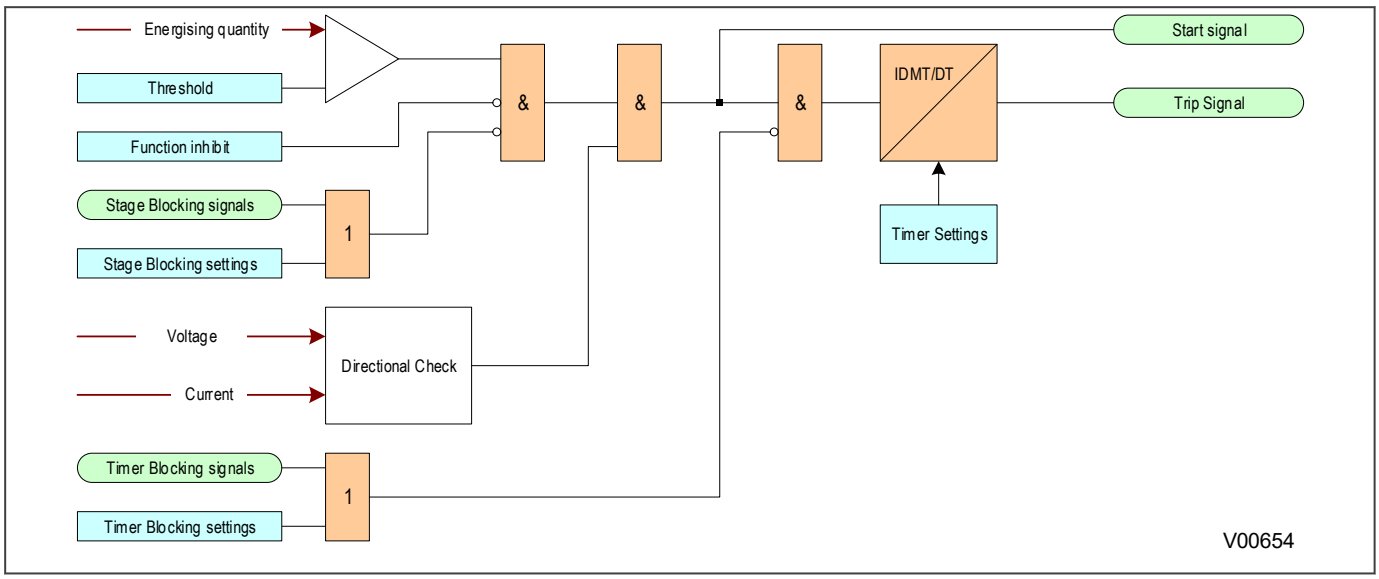


Figure 132: Principle of protection function implementation

An energising quantity is either a voltage input from a system voltage transformer, a current input from a system current transformer or another quantity derived from one or both of these. The energising quantities are extracted from the power system. The signals are converted to digital quantities where they can be processed by the IEDs internal processor.

In general, an energising quantity, be it a current, voltage, power, frequency, or phase quantity, is compared with a threshold value, which may be settable, or hard-coded depending on the function. If the quantity exceeds (for overvalues) or falls short of (for undervalues) the threshold, a signal is produced, which when gated with the various inhibit and blocking functions becomes the Start signal for that protection function. This Start signal is generally made available to Fixed Scheme Logic (FSL) and Programmable Scheme Logic (PSL) for further processing. It is also passed through a timer function to produce the Trip signal. The timer function may be an IDMT curve, or a Definite Time delay, depending on the function. This timer may also be blocked with timer blocking signals and settings. The timer can be configured by a range of settings to define such parameters as the type of curve, The Time Multiplier Setting, the IDMT constants, the Definite Time delay etc.

In GE Vernova products, there are usually several independent stages for each of the functions, and for three-phase functions, there are usually independent stages for each of the three phases.

Typically some stages use an Inverse Definite Minimum time (IDMT) timer function, and others use a Definite Time timer (DT) function. If the DT time delay is set to '0', then the function is known to be "instantaneous". In many instances, the term 'instantaneous protection" is used loosely to describe Definite Time protection stages, even when the stage may not theoretically be instantaneous.

Many protection functions require a direction-dependent decision. Such functions can only be implemented where both current and voltage inputs are available. For such functions, a directional check is required, whose output can block the Start signal should the direction of the fault be wrong.

Note:
In the logic diagrams and descriptive text, it is usually sufficient to show only the first stage, as the design principles for subsequent stages are usually the same (or at least very similar). Where there are differences between the functionality of different stages, this is clearly indicated.

10.2.2.1 TIMER HOLD FACILITY

The Timer Hold facility is available for stages with IDMT functionality , and is controlled by the timer reset settings for the relevant stages (e.g. ***I>1 tReset***, ***I>2 tReset***). These cells are not visible for the IEEE/US curves if an

inverse time reset characteristic has been selected, because in this case the reset time is determined by the time dial setting (TDS).

This feature may be useful in certain applications, such as when grading with upstream electromechanical overcurrent devices, which have inherent reset time delays. If you set the hold timer to a value other than zero, the resetting of the protection element timers will be delayed for this period. This allows the element to behave in a similar way to an electromechanical device. If you set the hold timer to zero, the overcurrent timer for that stage will reset instantaneously as soon as the current falls below a specified percentage of the current setting (typically 95%).

Another situation where the timer hold facility may be used to reduce fault clearance times is for intermittent faults. An example of this may occur in a plastic insulated cable. In this application it is possible that the fault energy melts and reseals the cable insulation, thereby extinguishing the fault. This process repeats to give a succession of fault current pulses, each of increasing duration with reducing intervals between the pulses, until the fault becomes permanent.

When the reset time is instantaneous, the device will repeatedly reset and not be able to trip until the fault becomes permanent. By using the Timer Hold facility the device will integrate the fault current pulses, thereby reducing fault clearance time.

10.3 PHASE FAULT OVERCURRENT PROTECTION

Phase fault overcurrent protection is provided as a form of back-up protection that could be:

- Permanently disabled
- Permanently enabled
- Enabled only in case of VT fuse/MCB failure
- Enabled only in case of protection communication channel failure
- Enabled if VT fuse/MCB or protection communication channel fail
- Enabled if VT fuse/MCB and protection communication channel fail

In addition, each stage may be inhibited/blocked by a DDB signal.

It should be noted that phase overcurrent protection is phase segregated, but the operation of any phase is mapped to 3 phase tripping in the default PSL.

The VTS element of the IED can be selected to either block the directional element or simply remove the directional control.

10.3.1 POC IMPLEMENTATION

Phase Overcurrent Protection is configured in the OVERCURRENT column of the relevant settings group.

The product provides four stages of three-phase overcurrent protection, each with independent time delay characteristics. The settings are independent for each stage, but for each stage, the settings apply to all phases.

Stages 1 and 2 provide a choice of operate and reset characteristics, where you can select between:

- A range of IDMT (Inverse Definite Minimum Time) curves based on IEC and IEEE standards
- A range of programmable user-defined curves
- DT (Definite Time) characteristic

This is achieved using the cells:

- ***I>(n) Function*** for the overcurrent operate characteristic
- ***I>(n) Reset Char*** for the overcurrent reset characteristic
- ***I>(n) Usr Rst Char*** for the reset characteristic for user-defined curves

where (n) is the number of the stage.

The IDMT-equipped stages, (1 and 2) also provide a Timer Hold facility. This is configured using the cells ***I>(n) tReset***, where (n) is the number of the stage. This does not apply to IEEE curves.

Stages 3 and 4 have definite time characteristics only.

10.3.2 DIRECTIONAL ELEMENT

If fault current can flow in both directions through a protected location, you will need to use a directional overcurrent element to determine the direction of the fault. Once the direction has been determined the device can decide whether to allow tripping or to block tripping. To determine the direction of a phase overcurrent fault, the device must compare the phase angle of the fault current with that of a known reference quantity. The phase angle of this known reference quantity must be independent of the faulted phase. Typically this will be the line voltage between the other two phases.

The phase fault elements of the IEDs are internally polarised by the quadrature phase-phase voltages, as shown in the table below:

Phase of Protection	Operate Current	Polarising Voltage
A Phase	IA	VBC
B Phase	IB	VCA
C Phase	IC	VAB

Under system fault conditions, the fault current vector lags its nominal phase voltage by an angle depending on the system X/R ratio. The IED must therefore operate with maximum sensitivity for currents lying in this region. This is achieved by using the IED characteristic angle (RCA). This is the is the angle by which the current applied to the IED must be displaced from the voltage applied to the IED to obtain maximum sensitivity.

The device provides a setting ***I> Char Angle***, which is set globally for all overcurrent stages. It is possible to set characteristic angles anywhere in the range –95° to +95°.

A directional check is performed based on the following criteria:

Directional forward

$$-90° < (\text{angle}(I) - \text{angle}(V) - RCA) < 90°$$

Directional reverse

$$-90° > (\text{angle}(I) - \text{angle}(V) - RCA) > 90°$$

For close up three-phase faults, all three voltages will collapse to zero and no healthy phase voltages will be present. For this reason, the device includes a synchronous polarisation feature that stores the pre-fault voltage information and continues to apply this to the directional overcurrent elements for a time period of 3.2 seconds. This ensures that either instantaneous or time-delayed directional overcurrent elements will be allowed to operate, even with a three-phase voltage collapse.

10.3.3 POC LOGIC

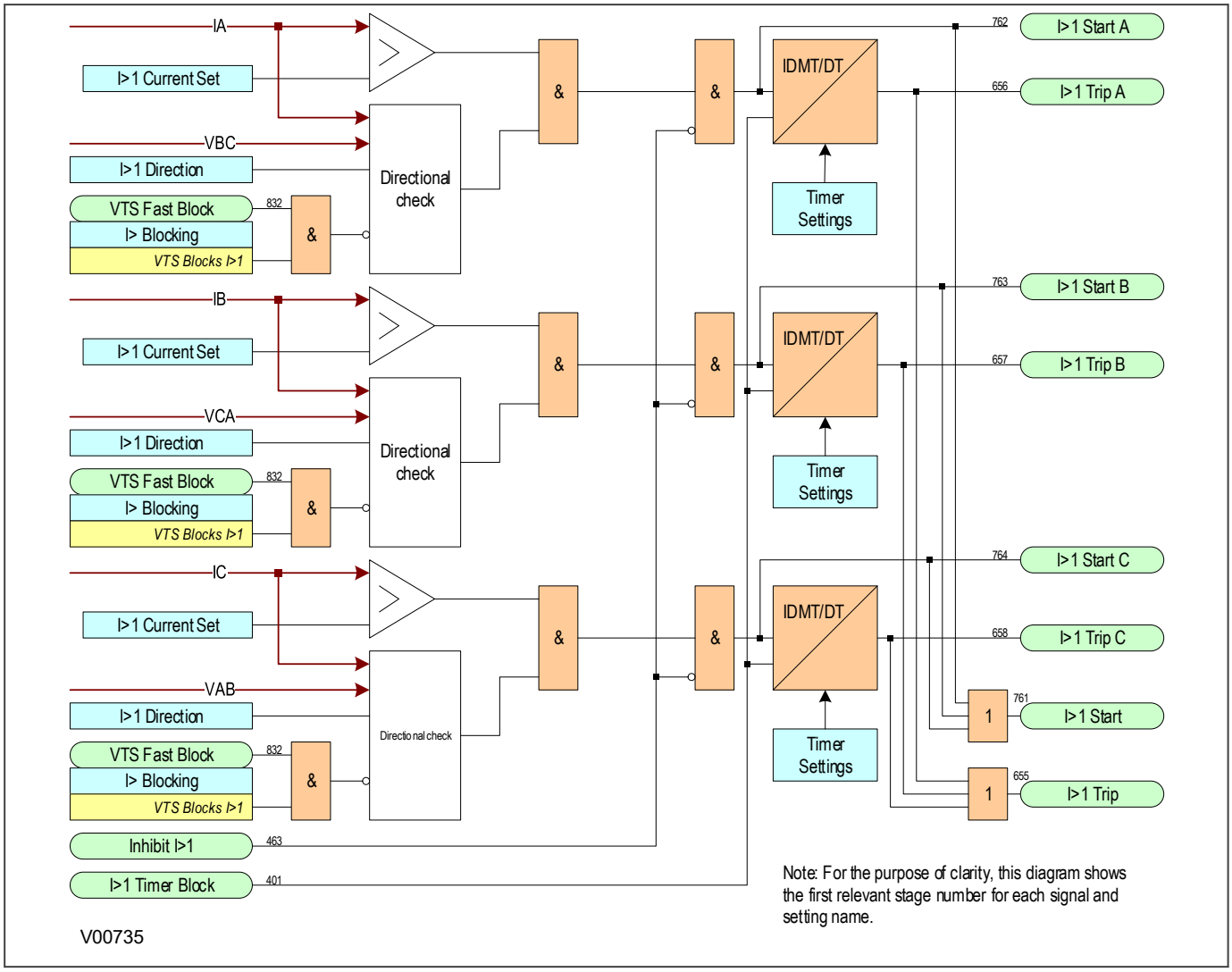


Figure 133: Phase overcurrent protection logic

10.4 NEGATIVE SEQUENCE OVERCURRENT PROTECTION

When applying standard phase overcurrent protection, the overcurrent elements must be set significantly higher than the maximum load current. This limits the element's sensitivity. Most protection schemes also use an earth fault element operating from residual current, which improves sensitivity for earth faults. However, certain faults may arise which can remain undetected by such schemes. Negative Phase Sequence Overcurrent elements can help in such cases.

Any unbalanced fault condition will produce a negative sequence current component. Therefore, a negative phase sequence overcurrent element can be used for both phase-to-phase and phase-to-earth faults. Negative Phase Sequence Overcurrent protection offers the following advantages:

- Negative phase sequence overcurrent elements are more sensitive to resistive phase-to-phase faults, where phase overcurrent elements may not operate.
- In certain applications, residual current may not be detected by an earth fault element due to the system configuration. For example, an earth fault element applied on the delta side of a delta-star transformer is unable to detect earth faults on the star side. However, negative sequence current will be present on both sides of the transformer for any fault condition, irrespective of the transformer configuration. Therefore, a negative phase sequence overcurrent element may be used to provide time-delayed back-up protection for any uncleared asymmetrical faults downstream.

10.4.1 NEGATIVE SEQUENCE OVERCURRENT PROTECTION IMPLEMENTATION

Negative Sequence Overcurrent Protection is implemented in the *NEG SEQ O/C* column of the relevant settings group.

The product provides four stages of negative sequence overcurrent protection with independent time delay characteristics.

Stages 1, 2 provide a choice of operate and reset characteristics, where you can select between:

- A range of standard IDMT (Inverse Definite Minimum Time) curves
- DT (Definite Time)

This is achieved using the cells

- ***I2>(n) Function*** for the overcurrent operate characteristic
- ***I2>(n) Reset Char*** for the overcurrent reset characteristic

where (n) is the number of the stage.

The IDMT-capable stages, (1 and 2) also provide a Timer Hold. This is configured using the cells ***I2>(n) tReset***, where (n) is the number of the stage. This is not applicable for curves based on the IEEE standard.

Stages 3 and 4 have definite time characteristics only.

10.4.2 DIRECTIONAL ELEMENT

Where negative phase sequence current may flow in either direction, directional control should be used.

Directionality is achieved by comparing the angle between the negative phase sequence voltage and the negative phase sequence current. A directional element is available for all of the negative sequence overcurrent stages. This is found in the ***I2> Direction*** cell for the relevant stage. It can be set to non-directional, directional forward, or directional reverse.

A suitable characteristic angle setting (***I2> Char Angle***) is chosen to provide optimum performance. This setting should be set equal to the phase angle of the negative sequence current with respect to the inverted negative sequence voltage (**–V2**), in order to be at the centre of the directional characteristic.

10.4.3 NPSOC LOGIC

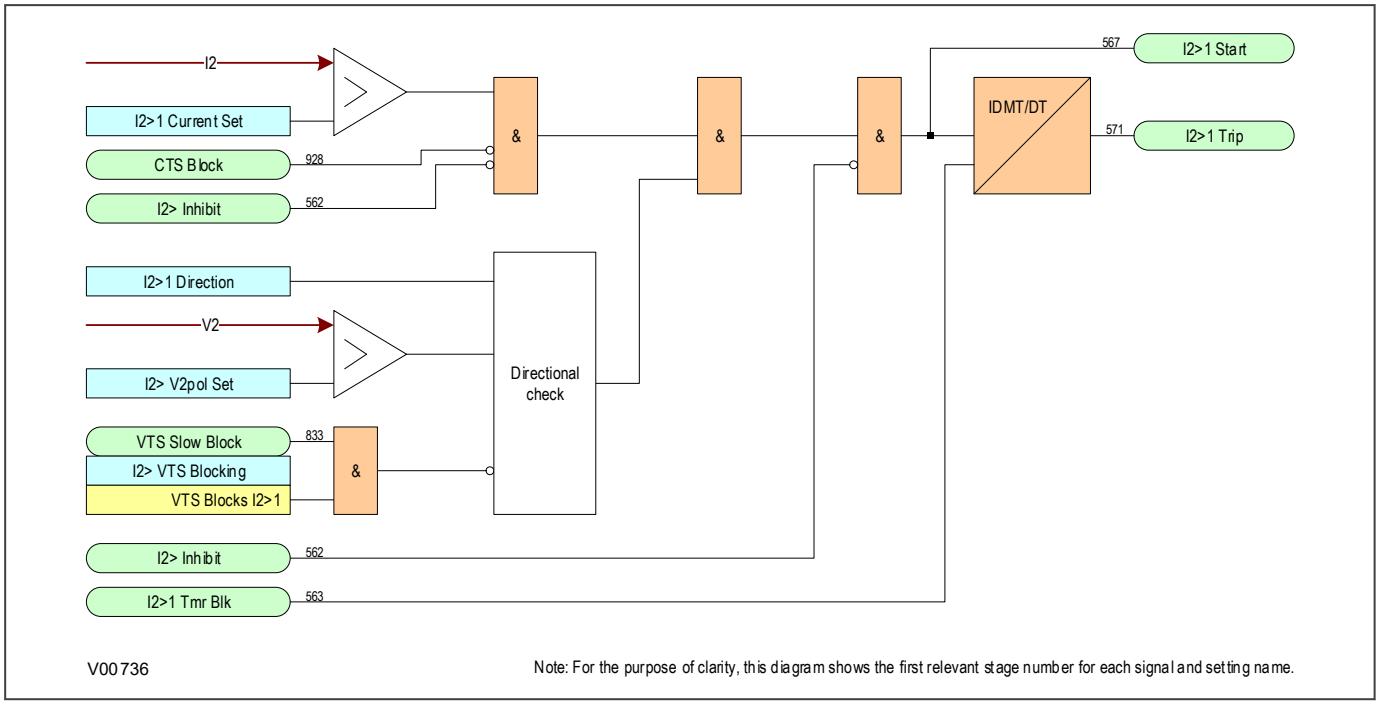


Figure 134: Negative phase sequence overcurrent protection logic

10.4.4 APPLICATION NOTES

10.4.4.1 SETTING GUIDELINES (CURRENT THRESHOLD)

A negative phase sequence element can be connected in the primary supply to the transformer and set as sensitively as required to protect for secondary phase-to-earth or phase-to-phase faults. This function will also provide better protection than the phase overcurrent function for internal transformer faults. The NPS overcurrent protection should be set to coordinate with the low-side phase and earth elements for phase-to-earth and phase-to-phase faults.

The current pick-up threshold must be set higher than the negative phase sequence current due to the maximum normal load imbalance. This can be set practically at the commissioning stage, making use of the measurement function to display the standing negative phase sequence current. The setting should be at least 20% above this figure.

Where the negative phase sequence element needs to operate for specific uncleared asymmetric faults, a precise threshold setting would have to be based on an individual fault analysis for that particular system due to the complexities involved. However, to ensure operation of the protection, the current pick-up setting must be set approximately 20% below the lowest calculated negative phase sequence fault current contribution to a specific remote fault condition.

10.4.4.2 SETTING GUIDELINES (TIME DELAY)

Correct setting of the time delay for this function is vital. You should also be very aware that this element is applied primarily to provide back-up protection to other protection devices or to provide an alarm. It would therefore normally have a long time delay.

The time delay set must be greater than the operating time of any other protection device (at minimum fault level) that may respond to unbalanced faults such as phase overcurrent elements and earth fault elements.

10.4.4.3 SETTING GUIDELINES (DIRECTIONAL ELEMENT)

Where negative phase sequence current may flow in either direction through an IED location, such as parallel lines or ring main systems, directional control of the element should be employed (VT models only).

Directionality is achieved by comparing the angle between the negative phase sequence voltage and the negative phase sequence current and the element may be selected to operate in either the forward or reverse direction. A suitable relay characteristic angle setting (***I2> Char Angle***) is chosen to provide optimum performance. This setting should be set equal to the phase angle of the negative sequence current with respect to the inverted negative sequence voltage (–V2), in order to be at the centre of the directional characteristic.

The angle that occurs between V2 and I2 under fault conditions is directly dependent on the negative sequence source impedance of the system. However, typical settings for the element are as follows:

- For a transmission system the relay characteristic angle (RCA) should be set equal to –60°
- For a distribution system the relay characteristic angle (RCA) should be set equal to –45°

For the negative phase sequence directional elements to operate, the device must detect a polarising voltage above a minimum threshold, ***I2> V2pol Set***. This must be set in excess of any steady state negative phase sequence voltage. This may be determined during the commissioning stage by viewing the negative phase sequence measurements in the device.

10.5 EARTH FAULT PROTECTION

Earth faults are overcurrent faults where the fault current flows to earth. Earth faults are the most common type of fault.

Earth faults can be measured directly from the system by means of:

- A separate current Transformer (CT) located in a power system earth connection
- A separate Core Balance Current Transformer (CBCT), usually connected to the SEF transformer input
- A residual connection of the three line CTs, where the Earth faults can be derived mathematically by summing the three measured phase currents

Depending on the device model, it will provide one or more of the above means for Earth fault protection.

10.5.1 EARTH FAULT PROTECTION IMPLEMENTATION

Earth fault protection is implemented in the *EARTH FAULT* column of the relevant settings group. The element uses quantities derived internally from summing the three-phase currents.

The product provides four stages of Earth Fault protection with independent time delay characteristics, for each *EARTH FAULT* column.

Stages 1 and 2 provide a choice of operate and reset characteristics, where you can select between:

- A range of IDMT (Inverse Definite Minimum Time) curves
- DT (Definite Time)

This is achieved using the cells:

- ***IN>(n) Function*** for the overcurrent operate characteristics
- ***IN>(n) Reset Char*** for the overcurrent reset characteristic

where (n) is the number of the stage.

Stages 1 and 2 provide a Timer Hold facility. This is configured using the cells ***IN>(n) tReset***

Stages 3 and 4 can have definite time characteristics only.

Earth fault Overcurrent IN> can be set to:

- Permanently disabled
- Permanently enabled
- Enabled only if VT fuse/MCB fails
- Enabled only if protection communication channel fails
- Enabled if VT fuse/MCB or protection communication channel fail
- Enabled if VT fuse/MCB and protection communication channel fail

Each stage can be individually inhibited with a DDB signal ***Inhibit IN>(n)***, where n is the stage number.

10.5.2 IDG CURVE

The IDG curve is commonly used for time delayed earth fault protection in the Swedish market. This curve is available in stage 1 of the Earth Fault protection.

The IDG curve is represented by the following equation:

$$t_{op} = 5.8 - 1.35 log_e \left(\frac{I}{IN > Setting} \right)$$

where:

t_{op} is the operating time

I is the measured current

IN> Setting is an adjustable setting, which defines the start point of the characteristic

Note:
Although the start point of the characteristic is defined by the "IN>" setting, the actual current threshold is a different setting called "IDG Is". The "IDG Is" setting is set as a multiple of "IN>".

Note:
When using an IDG Operate characteristic, DT is always used with a value of zero for the Rest characteristic.

An additional setting "IDG Time" is also used to set the minimum operating time at high levels of fault current.

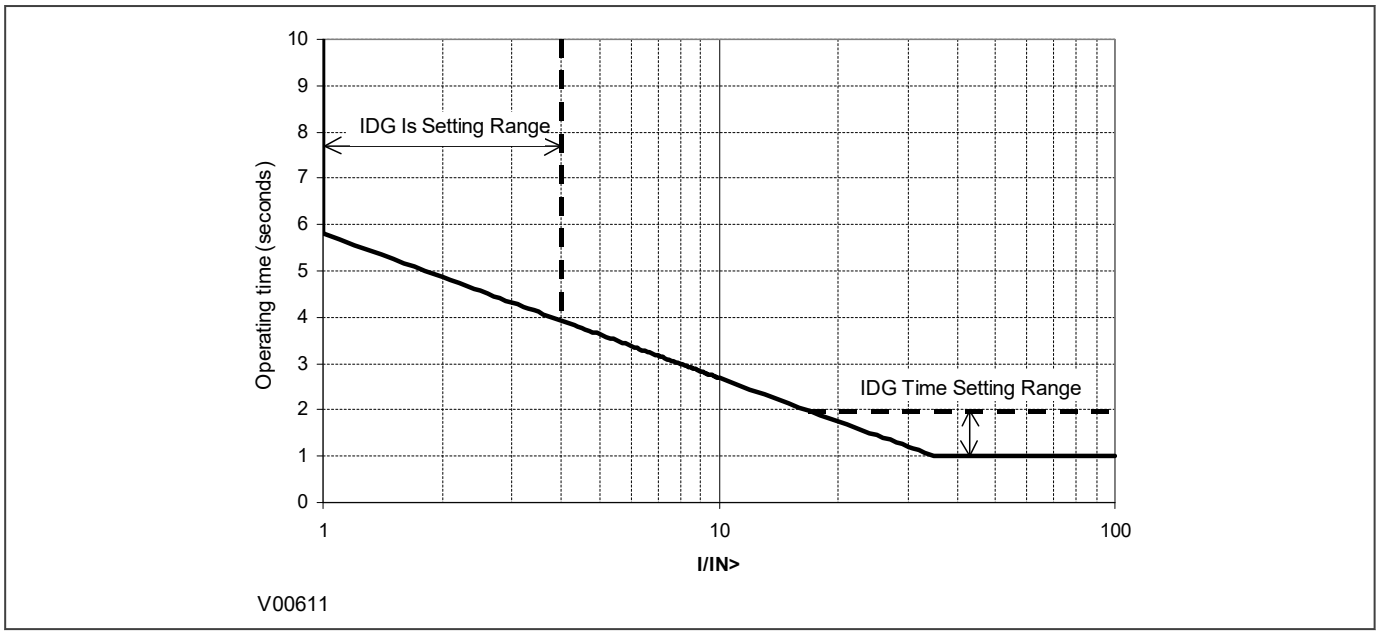


Figure 135: IDG characteristic

10.5.3 DIRECTIONAL ELEMENT

If Earth fault current can flow in both directions through a protected location, you will need to use a directional overcurrent element to determine the direction of the fault. Typical systems that require such protection are parallel feeders and ring main systems.

A directional element is available for all of the Earth Fault stages. These are found in the direction setting cells for the relevant stage. They can be set to non-directional, directional forward, or directional reverse.

Directional control can be blocked by the VTS element if required.

For standard earth fault protection, two options are available for polarisation; Residual Voltage (zero sequence) or Negative Sequence.

10.5.3.1 RESIDUAL VOLTAGE POLARISATION

With earth fault protection, the polarising signal needs to be representative of the earth fault condition. As residual voltage is generated during earth fault conditions, this quantity is commonly used to polarise directional earth fault

elements. This is known as Zero Sequence Voltage polarisation, Residual Voltage polarisation or Neutral Displacement Voltage (NVD) polarisation.

Small levels of residual voltage could be present under normal system conditions due to system imbalances, VT inaccuracies, device tolerances etc. For this reason, the device includes a user settable threshold (***IN> VNPol set***), which must be exceeded in order for the DEF function to become operational. The residual voltage measurement provided in the *MEASUREMENTS 1* column of the menu may assist in determining the required threshold setting during the commissioning stage, as this will indicate the level of standing residual voltage present.

Note:
Residual voltage is nominally 180° out of phase with residual current. Consequently, the DEF elements are polarised from the "-Vres" quantity. This 180° phase shift is automatically introduced within the device.

The directional criteria with residual voltage polarisation is given below:

- Directional forward: -90° < (angle(IN) - angle(VN + 180°) - RCA) < 90°
- Directional reverse : -90° > (angle(IN) - angle(VN + 180°) - RCA) > 90°

10.5.3.2 NEGATIVE SEQUENCE POLARISATION

In some applications, the use of residual voltage polarisation may not be possible to achieve or it can be problematic. For example, a suitable type of VT may be unavailable, or an HV/EHV parallel line application may present problems with zero sequence mutual coupling.

In such situations, the problem may be solved by using Negative Phase Sequence (NPS) quantities for polarisation. This method determines the fault direction by comparing the NPS voltage with the NPS current. The operating quantity, however, is still residual current.

This can be used for both the derived and measured standard earth fault elements. It requires a suitable voltage and current threshold to be set in cells ***IN> V2pol set*** and ***IN> I2pol set*** respectively.

Negative phase sequence polarising is not recommended for impedance earthed systems regardless of the type of VT feeding the device. This is due to the reduced earth fault current limiting the voltage drop across the negative sequence source impedance to negligible levels. If this voltage is less than 0.5 volts the device will stop providing directionalisation.

The directional criteria with negative sequence polarisation is given below:

- Directional forward: -90° < (angle(I2) - angle(V2 + 180°) - RCA) < 90°
- Directional reverse : -90° > (angle(I2) - angle(V2 + 180°) - RCA) > 90°

10.5.4 EARTH FAULT PROTECTION LOGIC

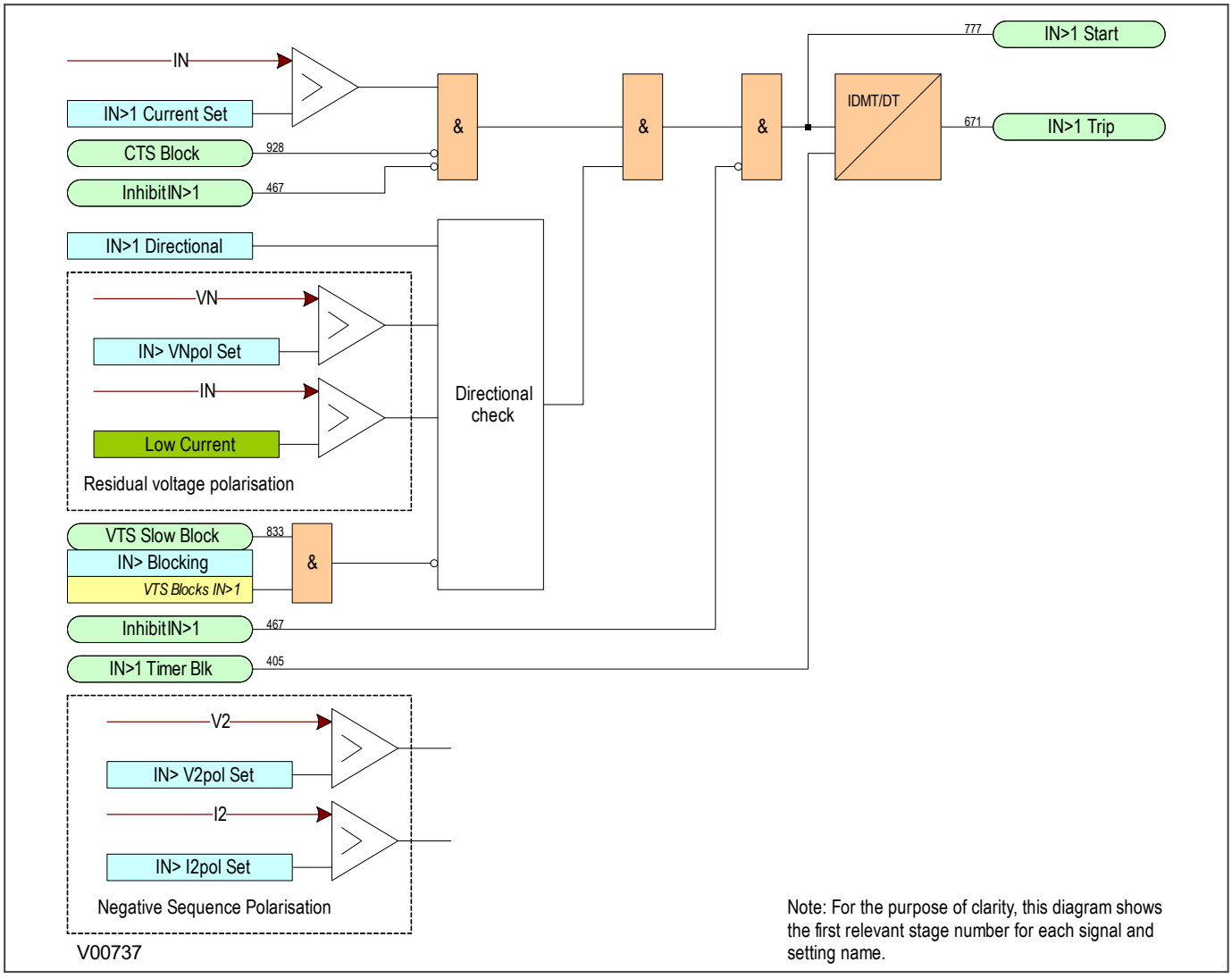


Figure 136: Earth fault protection logic

10.5.5 APPLICATION NOTES

10.5.5.1 RESIDUAL VOLTAGE POLARISATION SETTING GUIDELINES

It is possible that small levels of residual voltage will be present under normal system conditions due to system imbalances, VT inaccuracies, IED tolerances etc. Hence, the IED includes a user settable threshold (***IN> VNPol Set***) which must be exceeded in order for the DEF function to be operational. In practice, the typical zero sequence voltage on a healthy system can be as high as 1% (i.e. 3% residual), and the VT error could be 1% per phase. A setting between 1% and 4% is therefore typical. The residual voltage measurement may assist in determining the required threshold setting during commissioning, as this will indicate the level of standing residual voltage present.

10.5.5.2 SETTING GUIDELINES (DIRECTIONAL ELEMENT)

With directional earth faults, the residual current under fault conditions lies at an angle lagging the polarising voltage. Hence, negative RCA settings are required for DEF applications. This is set in the cell ***I> Char Angle*** in the relevant earth fault menu.

We recommend the following RCA settings:

- Resistance earthed systems: 0°
- Distribution systems (solidly earthed): -45°
- Transmission systems (solidly earthed): -60°

10.6 SENSITIVE EARTH FAULT PROTECTION

With some earth faults, the fault current flowing to earth is limited by either intentional resistance (as is the case with some HV systems) or unintentional resistance (e.g. in very dry conditions and where the substrate is high resistance, such as sand or rock).

To provide protection in such cases, it is necessary to provide an earth fault protection system with a setting that is considerably lower than for normal line protection. Such sensitivity cannot be provided with conventional CTs, therefore the SEF input would normally be fed from a core balance current transformer (CBCT) mounted around the three phases of the feeder cable. The SEF transformer should be a special measurement class transformer.

10.6.1 SEF PROTECTION IMPLEMENTATION

The product provides four stages of SEF protection with independent time delay characteristics.

Stages 1, 2 provide a choice of operate and reset characteristics, where you can select between:

- A range of IDMT (Inverse Definite Minimum Time) curves
- DT (Definite Time)

This is achieved using the cells

- ***ISEF>(n) Function*** for the overcurrent operate characteristic
- ***ISEF>(n) Reset Chr*** for the overcurrent reset characteristic

where (n) is the number of the stage.

Stages 1 and 2 also provide a Timer Hold facility. This is configured using the cells ***ISEF>(n) tReset***.

Stages 3 and 4 have definite time characteristics only.

Each stage can be individually inhibited with a DDB signal Inhibit ISEF>(n), where n is the stage number.

10.6.2 EPATR B CURVE

The EPATR B curve is commonly used for time-delayed Sensitive Earth Fault protection in certain markets. This curve is only available in the Sensitive Earth Fault protection stages 1 and 2. It is based on primary current settings, employing a SEF CT ratio of 100:1 A.

The EPATR_B curve has 3 separate segments defined in terms of the primary current. It is defined as follows:

Segment	Primary Current Range Based on 100A:1A CT Ratio	Current/Time Characteristic
1	ISEF = 0.5A to 6.0A	t = 432 x TMS/ISEF 0.655 secs
2	ISEF = 6.0A to 200A	t = 800 x TMS/ISEF secs
3	ISEF above 200A	t = 4 x TMS secs

where TMS (time multiplier setting) is 0.025 - 1.2 in steps of 0.025.

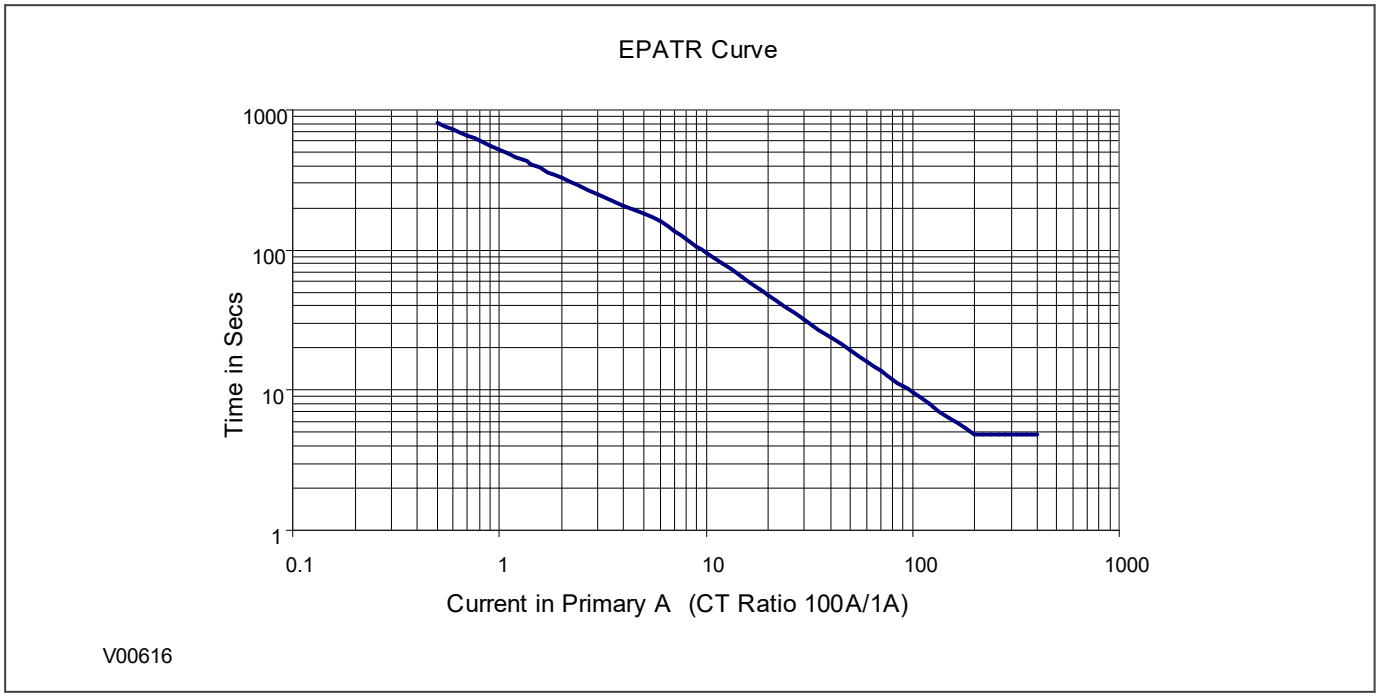


Figure 137: EPATR B characteristic shown for TMS = 1.0

10.6.3 SENSITIVE EARTH FAULT PROTECTION LOGIC

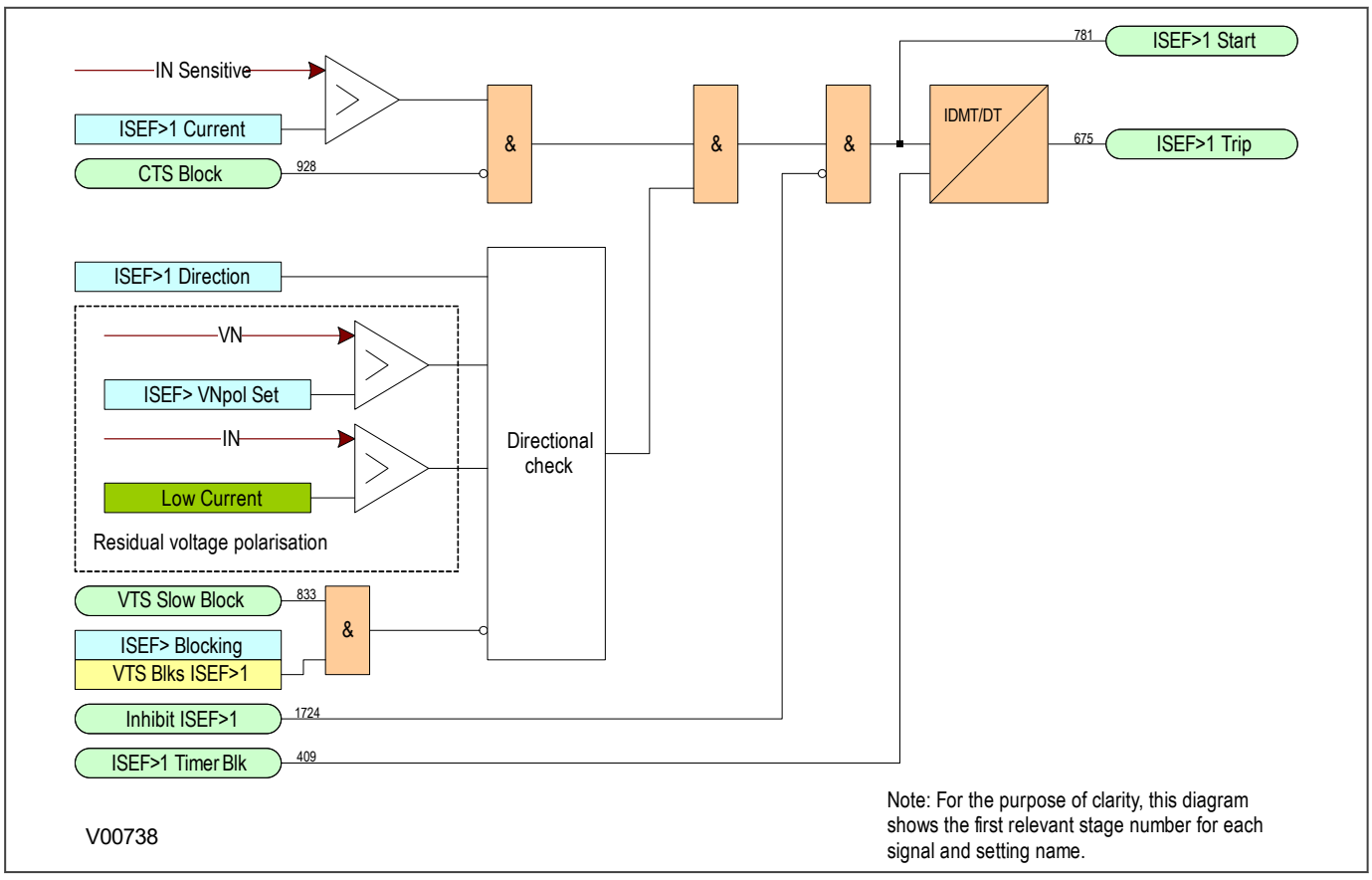


Figure 138: Sensitive earth fault protection logic

10.6.4 APPLICATION NOTES

10.6.4.1 INSULATED SYSTEMS

When insulated systems are used, it is not possible to detect faults using standard earth fault protection. It is possible to use a residual overvoltage device to achieve this, but even with this method full discrimination is not possible. Fully discriminative earth fault protection on this type of system can only be achieved by using a SEF (Sensitive Earth Fault) element. This type of protection detects the resultant imbalance in the system charging currents that occurs under earth fault conditions. A core balanced CT must be used for this application. This eliminates the possibility of spill current that may arise from slight mismatches between residually connected line CTs. It also enables a much lower CT ratio to be applied, thereby allowing the required protection sensitivity to be more easily achieved.

The following diagram shows an insulated system with a C-phase fault.

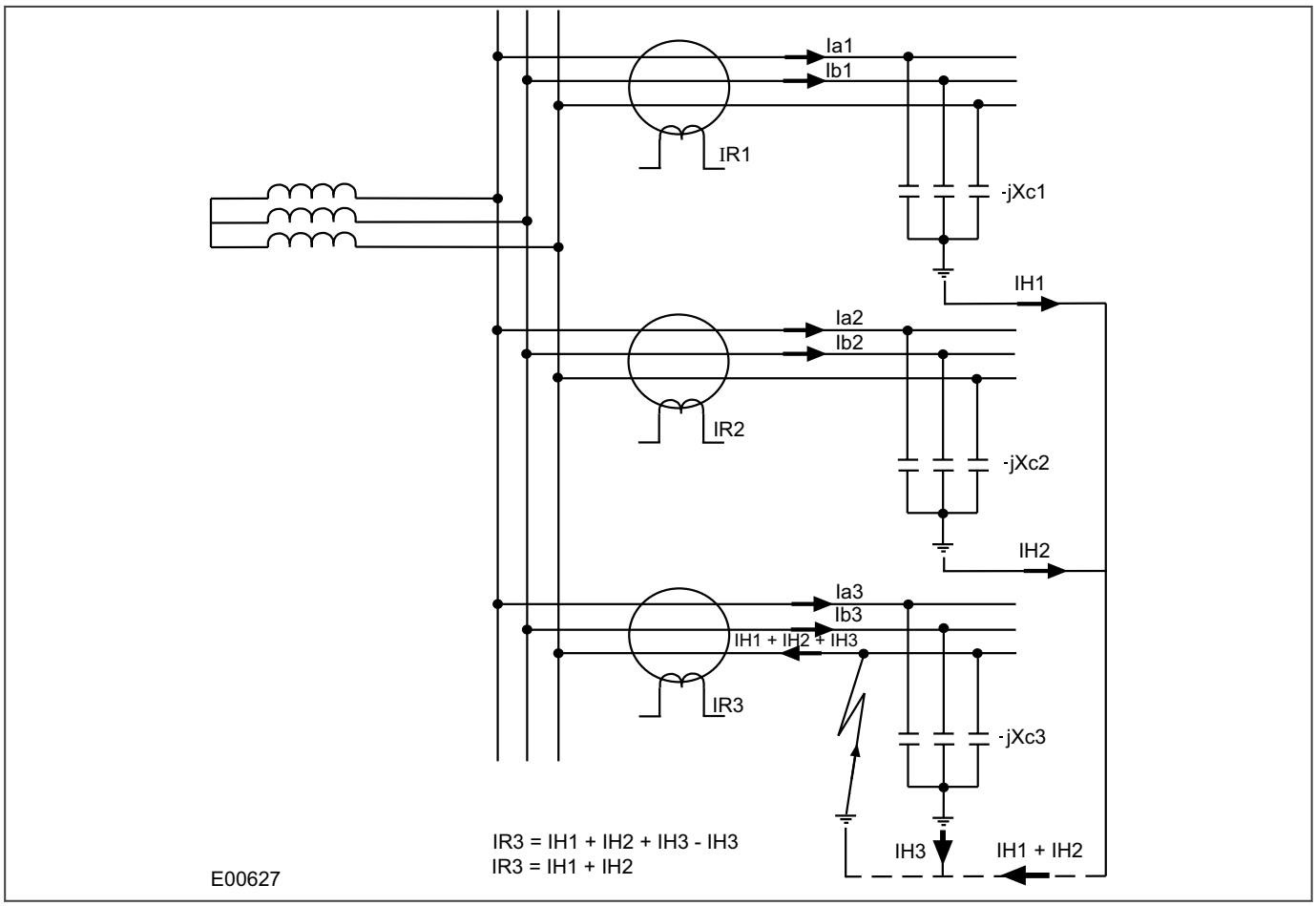


Figure 139: Current distribution in an insulated system with C phase fault

The protection elements on the healthy feeder see the charging current imbalance for their own feeder. The protection element on the faulted feeder, however, sees the charging current from the rest of the system (IH1 and IH2 in this case). Its own feeder's charging current (IH3) is cancelled out.

With reference to the associated vector diagram, it can be seen that the C-phase to earth fault causes the voltages on the healthy phases to rise by a factor of √3. The A-phase charging current (Ia1), leads the resultant A phase voltage by 90°. Likewise, the B-phase charging current leads the resultant Vb by 90°.

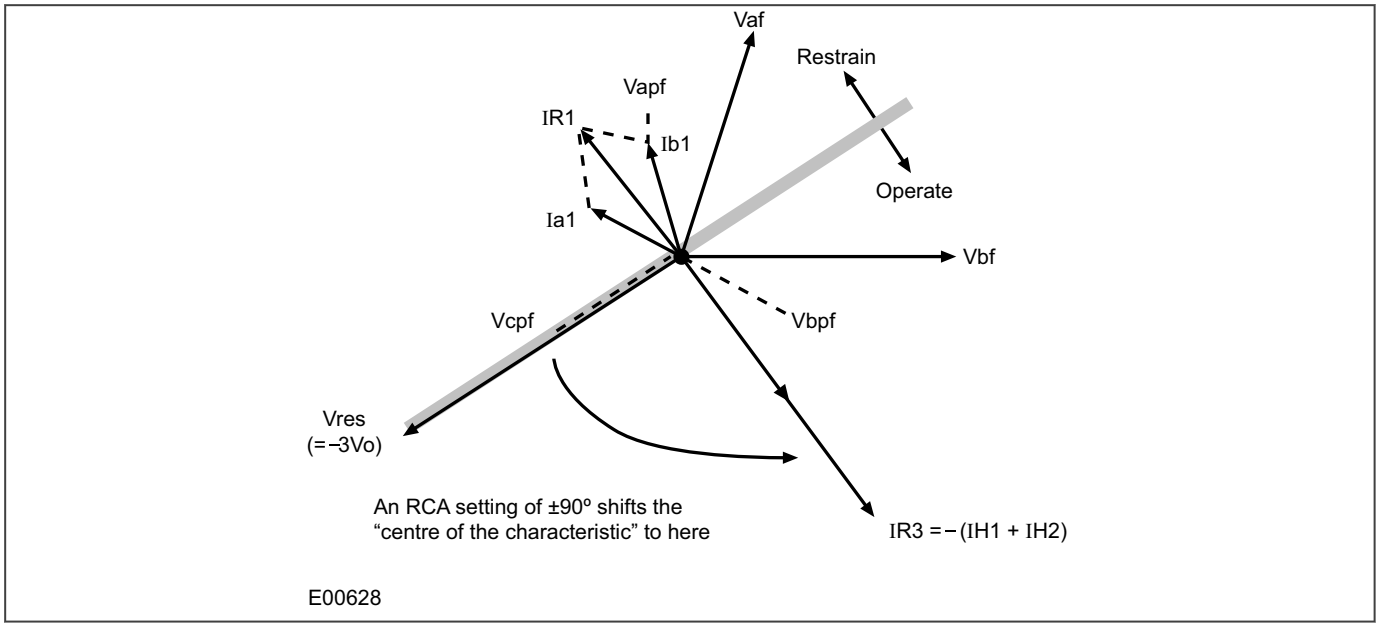


Figure 140: Phasor diagrams for insulated system with C phase fault

The current imbalance detected by a core balanced current transformer on the healthy feeders is the vector addition of Ia1 and Ib1. This gives a residual current which lags the polarising voltage (–3Vo) by 90°. As the healthy phase voltages have risen by a factor of √3, the charging currents on these phases are also √3 times larger than their steady state values. Therefore, the magnitude of the residual current IR1, is equal to 3 times the steady state per phase charging current.

The phasor diagram indicates that the residual currents on the healthy and faulted feeders (IR1 and IR3 respectively) are in anti-phase. A directional element (if available) could therefore be used to provide discriminative earth fault protection.

If the polarising is shifted through +90°, the residual current seen by the device on the faulted feeder will lie within the operate region of the directional characteristic and the current on the healthy feeders will fall within the restrain region.

The required characteristic angle setting for the SEF element when applied to insulated systems, is +90°. This is for the case when the protection is connected such that its direction of current flow for operation is from the source busbar towards the feeder. If the forward direction for operation were set such that it is from the feeder into the busbar, then a –90° RCA would be required.

Note:
Discrimination can be provided without the need for directional control. This can only be achieved, however, if it is possible to set the IED in excess of the charging current of the protected feeder and below the charging current for the rest of the system.

10.6.4.2 SETTING GUIDELINES (INSULATED SYSTEMS)

The residual current on the faulted feeder is equal to the sum of the charging currents flowing from the rest of the system. Further, the addition of the two healthy phase charging currents on each feeder gives a total charging current which has a magnitude of three times the per phase value. Therefore, the total imbalance current is equal to three times the per phase charging current of the rest of the system. A typical setting may therefore be in the order of 30% of this value, i.e. equal to the per phase charging current of the remaining system. Practically though, the required setting may well be determined on site, where suitable settings can be adopted based on practically obtained results.

When using a core-balanced transformer, care must be taken in the positioning of the CT with respect to the earthing of the cable sheath:

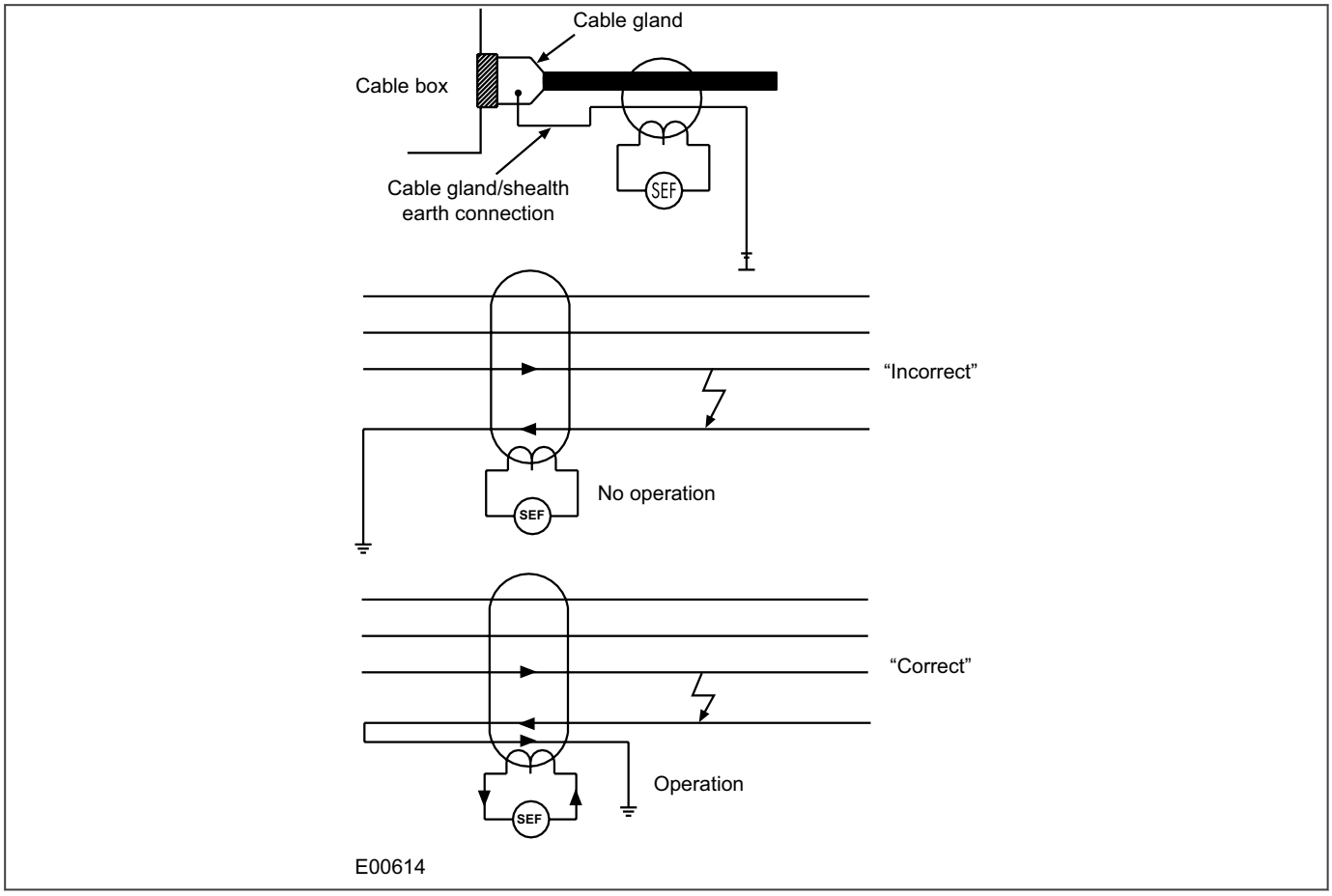


Figure 141: Positioning of core balance current transformers

If the cable sheath is terminated at the cable gland and directly earthed at that point, a cable fault (from phase to sheath) will not result in any unbalanced current in the core balance CT. Therefore, prior to earthing, the connection must be brought back through the CBCT and earthed on the feeder side. This then ensures correct device operation during earth fault conditions.

10.7 HIGH IMPEDANCE REF

The device provides a high impedance restricted earth fault protection function. An external resistor is required to provide stability in the presence of saturated line current transformers. Current transformer supervision signals do not block the high impedance REF protection. The appropriate logic must be configured in PSL to block the high impedance REF when any of the above signals is asserted.

10.7.1 HIGH IMPEDANCE REF PRINCIPLE

This scheme is very sensitive and can protect against low levels of fault current, typical of winding faults.

High Impedance REF protection is based on the differential principle. It works on the circulating current principle as shown in the following diagram.

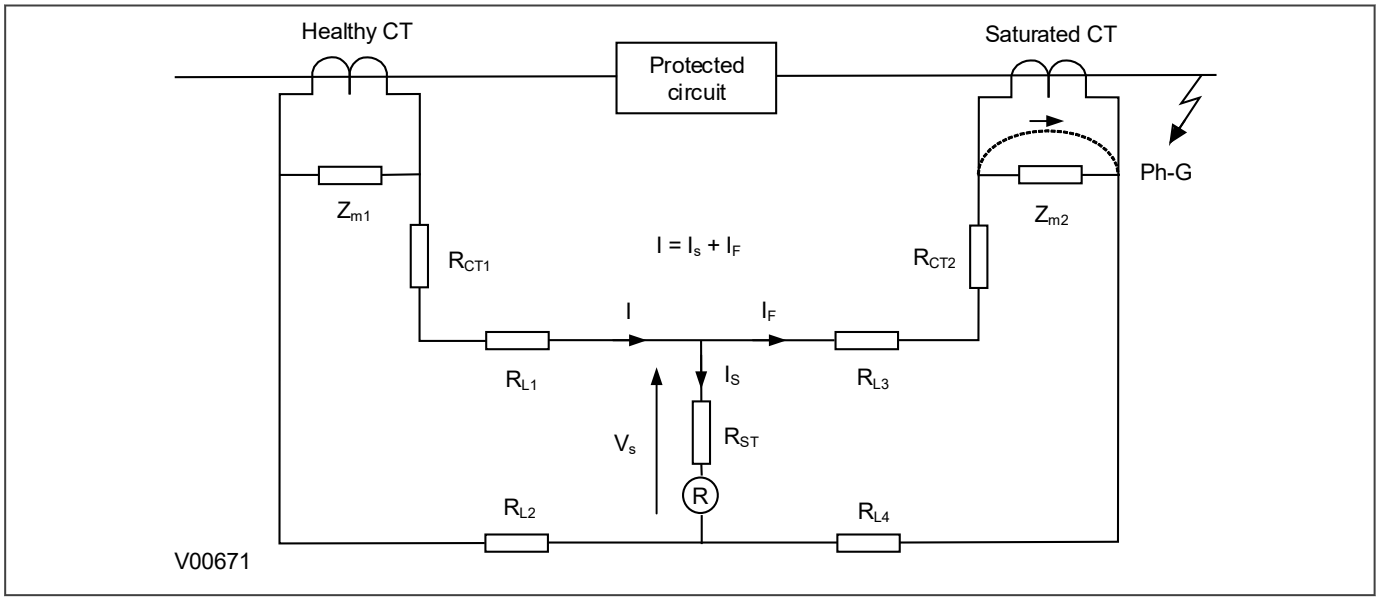


Figure 142: High impedance REF principle

When subjected to heavy through faults the line current transformer may enter saturation unevenly, resulting in imbalance. To ensure stability under these conditions a series connected external resistor is required, so that most of the unbalanced current will flow through the saturated CT. As a result, the current flowing through the device will be less than the setting, therefore maintaining stability during external faults.

Voltage across REF element $V_s = I_F (R_{CT2} + R_{L3} + R_{L4})$

Stabilising resistor $R_{ST} = V_s/I_s - R_R$

where:

- I_F = maximum secondary through fault current
- R_R = device burden
- R_{CT} = CT secondary winding resistance
- R_{L2} and R_{L3} = Resistances of leads from the device to the current transformer
- R_{ST} = Stabilising resistor

High Impedance REF can be used for either delta windings or star windings in both solidly grounded and resistance grounded systems. The connection to a modern IED are as follows:

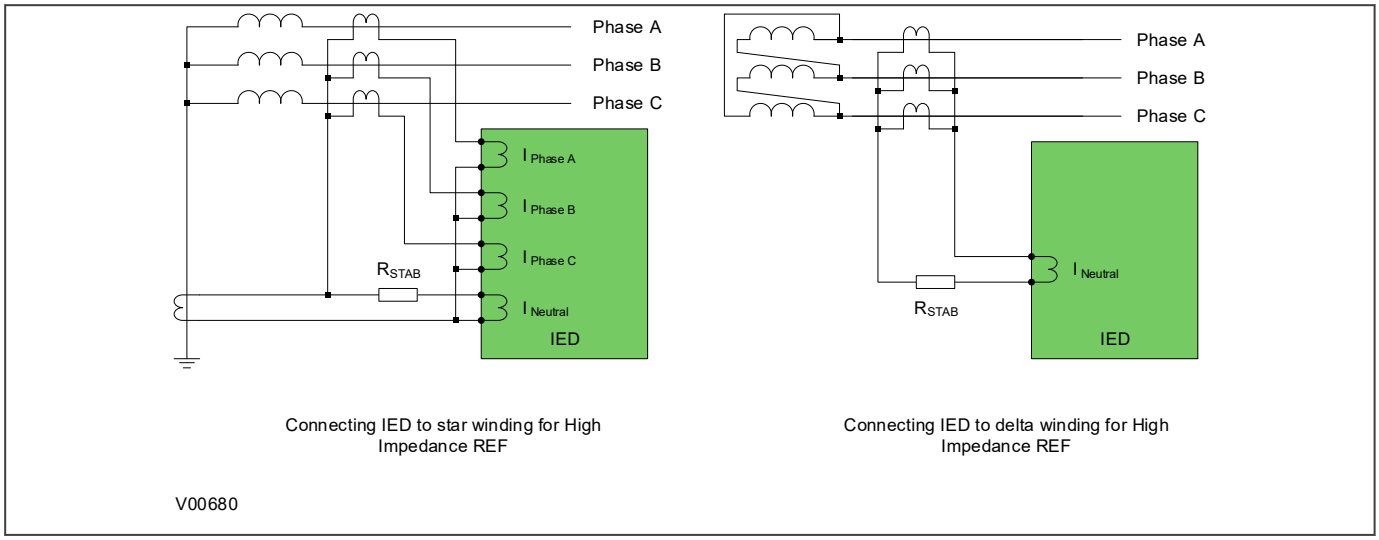


Figure 143: High impedance REF connection

10.8 THERMAL OVERLOAD PROTECTION

The heat generated within an item of plant is the resistive loss. The thermal time characteristic is therefore based on the equation I^2Rt. Over-temperature conditions occur when currents in excess of their maximum rating are allowed to flow for a period of time.

Temperature changes during heating follow exponential time constants. The device provides two characteristics for thermal overload protection; a single time constant characteristic and a dual time constant characteristic. You select these according to the application.

10.8.1 SINGLE TIME CONSTANT CHARACTERISTIC

This characteristic is used to protect cables, dry type transformers and capacitor banks.

The single constant thermal characteristic is given by the equation:

$$t = -\tau \log_e \left[\frac{I^2 - \left(KI_{FLC}\right)^2}{I^2 - I_p{}^2} \right]$$

where:

- t = time to trip, following application of the overload current I
- τ = heating and cooling time constant of the protected plant
- I = largest phase current
- I_{FLC} full load current rating (the Thermal Trip setting)
- K = a constant with the value of 1.05
- I_p = steady state pre-loading before application of the overload

10.8.2 DUAL TIME CONSTANT CHARACTERISTIC

This characteristic is used to protect equipment such as oil-filled transformers with natural air cooling. The thermal model is similar to that with the single time constant, except that two timer constants must be set.

For marginal overloading, heat will flow from the windings into the bulk of the insulating oil. Therefore, at low current, the replica curve is dominated by the long time constant for the oil. This provides protection against a general rise in oil temperature.

For severe overloading, heat accumulates in the transformer windings, with little opportunity for dissipation into the surrounding insulating oil. Therefore at high current levels, the replica curve is dominated by the short time constant for the windings. This provides protection against hot spots developing within the transformer windings.

Overall, the dual time constant characteristic serves to protect the winding insulation from ageing and to minimise gas production by overheated oil. Note however that the thermal model does not compensate for the effects of ambient temperature change.

The dual time constant thermal characteristic is given by the equation:

$$0.4e^{(-t/\tau_1)} + 0.6e^{(-t/\tau_2)} = \left[\frac{I^2 - \left(KI_{FLC}\right)^2}{I^2 - I_p{}^2} \right]$$

where:

- τ_1 = heating and cooling time constant of the transformer windings
- τ_2 = heating and cooling time constant of the insulating oil

10.8.3 THERMAL OVERLOAD PROTECTION IMPLEMENTATION

The device incorporates a current-based thermal characteristic, using Fourier based load current to model heating and cooling of the protected plant. The element can be set with both alarm and trip stages.

Thermal Overload Protection is implemented in the *THERMAL OVERLOAD* column of the relevant settings group.

This column contains the settings for the characteristic type, the alarm and trip thresholds and the time constants.

10.8.4 THERMAL OVERLOAD PROTECTION LOGIC

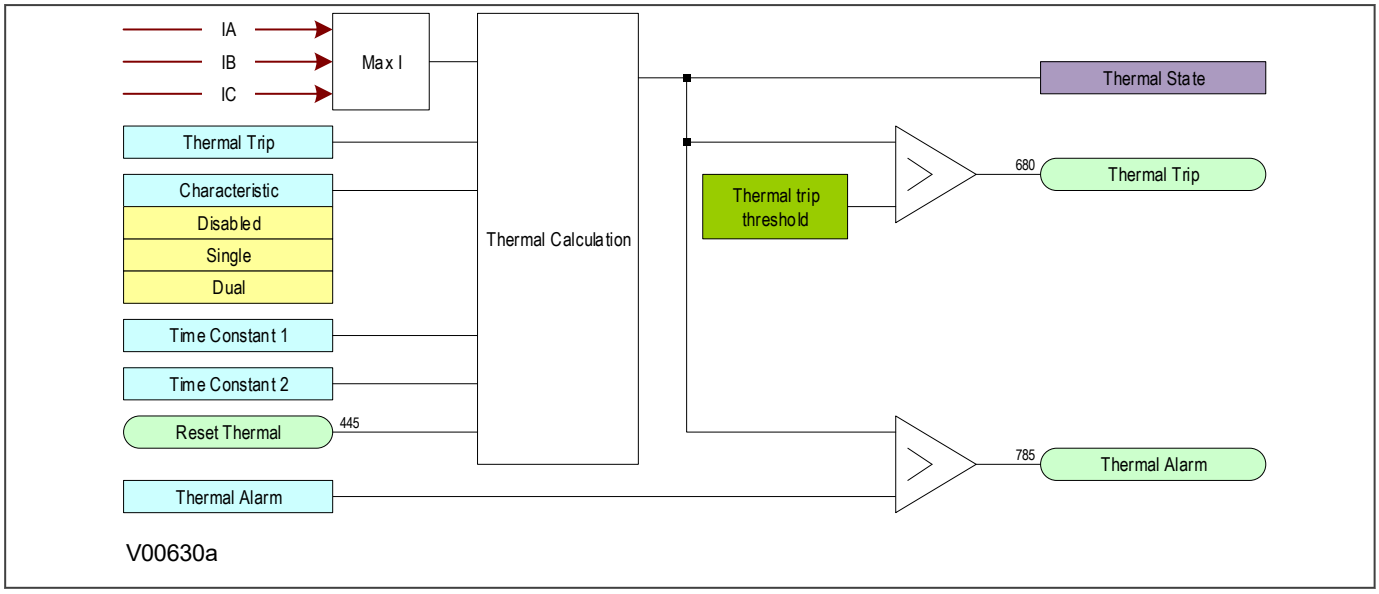


Figure 144: Thermal overload protection logic

The magnitudes of the three phase input currents are compared and the largest magnitude is taken as the input to the thermal overload function. If this current exceeds the thermal trip threshold setting a start condition is asserted.

The Start signal is applied to the chosen thermal characteristic module, which has three outputs signals; alarm trip and thermal state measurement. The thermal state measurement is made available in one of the *MEASUREMENTS* columns.

The thermal state can be reset by either a digital signal (Opto, GOOSE, InterMiCOM), if assigned to this function using programmable scheme logic or the HMI panel menu.

10.8.5 APPLICATION NOTES

10.8.5.1 SETTING GUIDELINES FOR DUAL TIME CONSTANT CHARACTERISTIC

The easiest way of solving the dual time constant thermal equation is to express the current in terms of time and to use a spreadsheet to calculate the current for a series of increasing operating times using the following equation, then plotting a graph.

$$I = \sqrt{\frac{0.4I_p^{\,2}.e^{(-t/\tau 1)} + 0.6I_p^{\,2}.e^{(-t/\tau 2)} - k^2.I_{FLC}^{\,2}}{0.4e^{(-t/\tau 1)} + 0.6e^{(-t/\tau 2)} - 1}}$$

	A	B	C	D	E	F
1						
2	**Time constant 1 =**		**300**	seconds		
3	**Time constant 2 =**		**7200**	seconds		
4	**Pre-overload current Ip =**		**0.9**	per unit		
5	**Full load current =**		**1**	Amps		
6						
7	**OP Time (t)**	**Overload current (I)**				
8	1	14.40852032				
9	1.5	11.7805774				
10	2	10.21617905				
11	2.5	9.150045407				
12	3	8.364131776				
13	3.5	7.754150044				
14	4	7.263123888				
15	4.5	6.856949012				

Figures based on equation

E00728

Figure 145: Spreadsheet calculation for dual time constant thermal characteristic

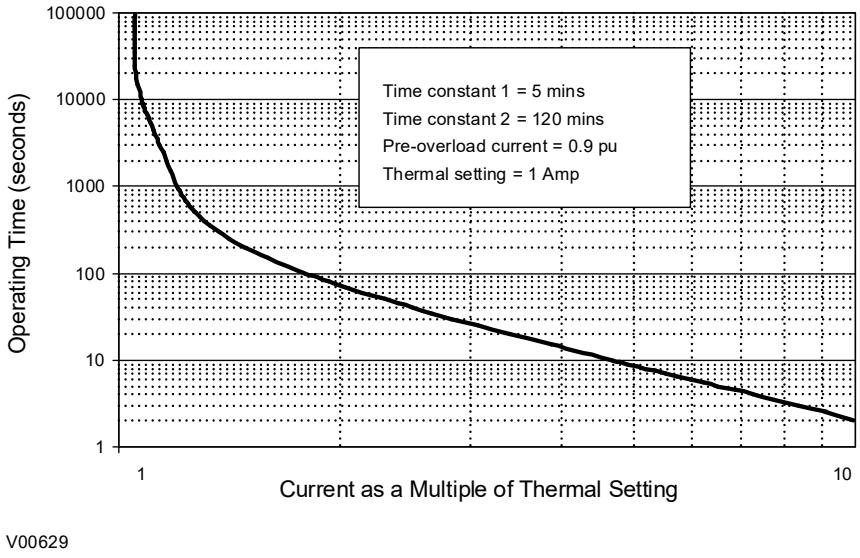


Figure 146: Dual time constant thermal characteristic

The current setting is calculated as:

Thermal Trip = Permissible continuous loading of the transformer item/CT ratio.

For an oil-filled transformer with rating 400 to 1600 kVA, the approximate time constants are:

- τ_1 = 5 minutes
- τ_2 = 120 minutes

An alarm can be raised on reaching a thermal state corresponding to a percentage of the trip threshold. A typical setting might be "Thermal Alarm" = 70% of thermal capacity.

Note:
The thermal time constants given in the above tables are typical only. Reference should always be made to the plant manufacturer for accurate information.

10.8.5.2 SETTING GUIDELINES FOR SINGLE TIME CONSTANT CHARACTERISTIC

The time to trip varies depending on the load current carried before application of the overload, i.e. whether the overload was applied from hot or cold.

The thermal time constant characteristic may be rewritten as:

$$e^{(-t/\tau)} = \left[\frac{\theta - \theta_p}{\theta - 1}\right]$$

where:

- θ = thermal state = $I^2/K^2I_{FLC}^2$
- θ_p = pre-fault thermal state = $I_p^2/K^2I_{FLC}^2$
- I_p is the pre-fault thermal state
- I_{FLC} is the full load current

Note:
A current of 105%Is (KI_{FLC}) has to be applied for several time constants to cause a thermal state measurement of 100%.

The current setting is calculated as:

Thermal Trip = Permissible continuous loading of the plant item/CT ratio.

The following tables show the approximate time constant in minutes, for different cable rated voltages with various conductor cross-sectional areas, and other plant equipment.

Area mm^2	6 - 11kV	22 kV	33 kV	66 kV
25 - 50	10 minutes	15 minutes	40 minutes	–
70 - 120	15 minutes	25 minutes	40 minutes	60 minutes
150	25 minutes	40 minutes	40 minutes	60 minutes
185	25 minutes	40 minutes	60 minutes	60 minutes
240	40 minutes	40 minutes	60 minutes	60 minutes
300	40 minutes	60 minutes	60 minutes	90 minutes

Plant Type	Time Constant (Minutes)
Dry-type transformer <400 kVA	40
Dry-type transformers 400 - 800 kVA	60 - 90
Air-core reactors	40
Capacitor banks	10
Overhead lines with cross section > 100 mm^2	10
Overhead lines	10
Busbars	60

10.9 BROKEN CONDUCTOR PROTECTION

One type of unbalanced fault is the 'Series' or 'Open Circuit' fault. This type of fault can arise from, among other things, broken conductors. Series faults do not cause an increase in phase current and so cannot be detected by overcurrent protection. However, they do produce an imbalance, resulting in negative phase sequence current, which can be detected.

It is possible to apply a negative phase sequence overcurrent element to detect broken conductors. However, on a lightly loaded line, the negative sequence current resulting from a series fault condition may be very close to, or less than, the full load steady state imbalance arising from CT errors and load imbalances, making it very difficult to distinguish. A regular negative sequence element would therefore not work at low load levels. To overcome this, the device incorporates a special Broken Conductor protection element.

The Broken Conductor element measures the ratio of negative to positive phase sequence current (I2/I1). This ratio is approximately constant with variations in load current, therefore making it more sensitive to series faults than standard negative sequence protection.

10.9.1 BROKEN CONDUCTOR PROTECTION IMPLEMENTATION

Broken Conductor protection is implemented in the *BROKEN CONDUCTOR* column of the relevant settings group.

This column contains the settings to enable the function, for the pickup threshold and the time delay.

10.9.2 BROKEN CONDUCTOR PROTECTION LOGIC

The ratio of I_2/I_1 is calculated and compared with the threshold setting. If the threshold is exceeded, the delay timer is initiated. The CTS block signal is used to block the operation of the delay timer.

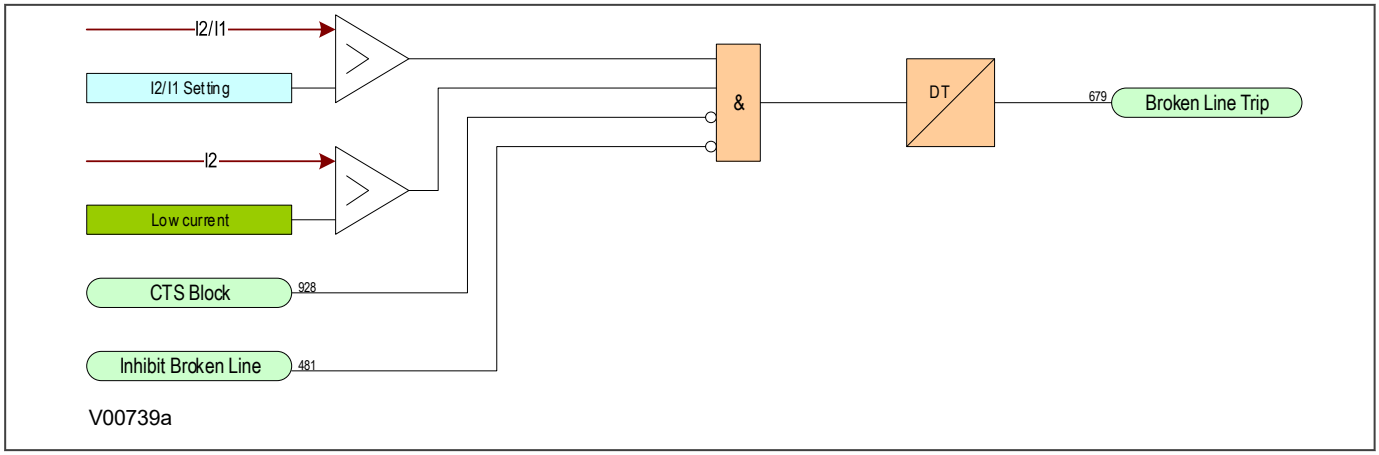


Figure 147: Broken conductor logic

10.9.3 APPLICATION NOTES

10.9.3.1 SETTING GUIDELINES

For a broken conductor affecting a single point earthed power system, there will be little zero sequence current flow and the ratio of I_2/I_1 that flows in the protected circuit will approach 100%. In the case of a multiple earthed power system (assuming equal impedance's in each sequence network), the ratio I_2/I_1 will be 50%.

In practise, the levels of standing negative phase sequence current present on the system govern this minimum setting. This can be determined from a system study, or by making use of the measurement facilities at the commissioning stage. If the latter method is adopted, it is important to take the measurements during maximum system load conditions, to ensure that all single-phase loads are accounted for.

Note:
A minimum value of 8% negative phase sequence current is required for successful operation.

Since sensitive settings have been employed, we can expect that the element will operate for any unbalanced condition occurring on the system (for example, during a single pole autoreclose cycle). For this reason, a long time delay is necessary to ensure co-ordination with other protection devices. A 60 second time delay setting may be typical.

The following example was recorded by an IED during commissioning:

$$I_{\text{full load}} = 500\text{A}$$

$$I_2 = 50\text{A}$$

therefore the quiescent I_2/I_1 ratio = 0.1

To allow for tolerances and load variations a setting of 20% of this value may be typical: Therefore set:

$$I_2/I_1 = 0.2$$

In a double circuit (parallel line) application, using a 40% setting will ensure that the broken conductor protection will operate only for the circuit that is affected. A setting of 0.4 results in no pick-up for the parallel healthy circuit.

Set I_2/I_1 Time Delay = 60 s to allow adequate time for short circuit fault clearance by time delayed protections.

CHAPTER 11

VOLTAGE PROTECTION FUNCTIONS

11.1 CHAPTER OVERVIEW

The device provides a wide range of voltage protection functions. This chapter describes the operation of these functions including the principles, logic diagrams and applications.

This chapter contains the following sections:

Chapter Overview 245
Undervoltage Setting Guidelines 246
Undervoltage Protection 247
Overvoltage Protection 250
Compensated Overvoltage 253
Residual Overvoltage Protection 254

Note:
Voltage Protection functionality is available in models P54B, P54C and P54E only.

11.2 UNDERVOLTAGE SETTING GUIDELINES

In most applications, undervoltage protection is not required to operate during system earth fault conditions. If this is the case you should select phase-to-phase voltage measurement, as this quantity is less affected by single-phase voltage dips due to earth faults.

The voltage threshold setting for the undervoltage protection should be set at some value below the voltage excursions that may be expected under normal system operating conditions. This threshold is dependent on the system in question but typical healthy system voltage excursions may be in the order of 10% of nominal value.

The same applies to the time setting. The required time delay is dependent on the time for which the system is able to withstand a reduced voltage.

If motor loads are connected, then a typical time setting may be in the order of 0.5 seconds.

11.3 UNDERVOLTAGE PROTECTION

Undervoltage conditions may occur on a power system for a variety of reasons, some of which are outlined below:

- Undervoltage conditions can be related to increased loads, whereby the supply voltage will decrease in magnitude. This situation would normally be rectified by voltage regulating equipment such as AVRs (Auto Voltage Regulators) or On Load Tap Changers. However, failure of this equipment to bring the system voltage back within permitted limits leaves the system with an undervoltage condition, which must be cleared.
- If the regulating equipment is unsuccessful in restoring healthy system voltage, then tripping by means of an undervoltage element is required.
- Faults occurring on the power system result in a reduction in voltage of the faulty phases. The proportion by which the voltage decreases is dependent on the type of fault, method of system earthing and its location. Consequently, co-ordination with other voltage and current-based protection devices is essential in order to achieve correct discrimination.
- Complete loss of busbar voltage. This may occur due to fault conditions present on the incomer or busbar itself, resulting in total isolation of the incoming power supply. For this condition, it may be necessary to isolate each of the outgoing circuits, such that when supply voltage is restored, the load is not connected. Therefore, the automatic tripping of a feeder on detection of complete loss of voltage may be required. This can be achieved by a three-phase undervoltage element.
- Where outgoing feeders from a busbar are supplying induction motor loads, excessive dips in the supply may cause the connected motors to stall, and should be tripped for voltage reductions that last longer than a pre-determined time.

11.3.1 UNDERVOLTAGE PROTECTION IMPLEMENTATION

Undervoltage Protection is implemented in the *VOLT PROTECTION* column of the relevant settings group. The Undervoltage parameters are contained within the sub-heading *UNDERVOLTAGE*.

The product provides two stages of Undervoltage protection with independent time delay characteristics.

Stage 1 provides a choice of operate characteristics, where you can select between:

- An IDMT characteristic
- DT (Definite Time)

You set this using the ***V<1 Function*** setting.

The IDMT characteristic is defined by the following formula:

$$t = K/(M-1)$$

where:

- K = Time multiplier setting
- t = Operating time in seconds
- M = Measured voltage / IED setting voltage (***V<(n) Voltage Set***)

The undervoltage stages can be configured either as phase-to-neutral or phase-to-phase voltages in the ***V< Measur't Mode*** cell.

There is no Timer Hold facility for Undervoltage.

Stage 2 can have definite time characteristics only. This is set in the ***V<2 Status*** cell.

Outputs are available for single or three-phase conditions via the ***V< Operate Mode*** cell for each stage.

11.3.2 UNDERVOLTAGE PROTECTION LOGIC

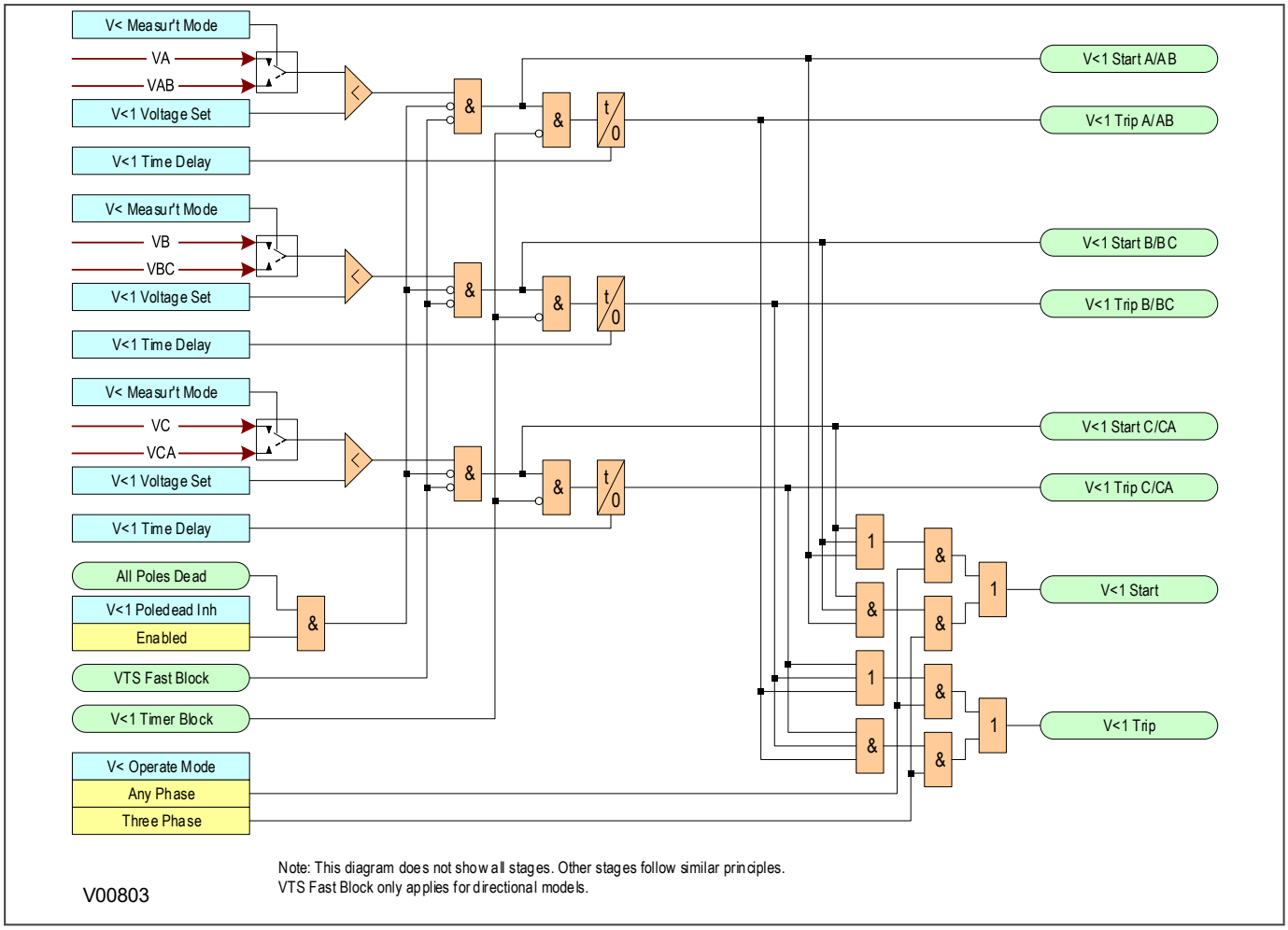


Figure 148: Undervoltage - single and three phase tripping mode (single stage)

The Undervoltage protection function detects when the voltage magnitude for a certain stage falls short of a set threshold. If this happens a ***Start*** signal, signifying the "Start of protection", is produced. This Start signal can be blocked by the ***VTS Fast Block*** signal and an ***All Poles Dead*** signal. This ***Start*** signal is applied to the timer module to produce the ***Trip*** signal, which can be blocked by the undervoltage timer block signal (***V<(n) Timer Block***). For each stage, there are three Phase undervoltage detection modules, one for each phase. The three ***Start*** signals from each of these phases are OR'd together to create a 3-phase Start signal (***V<(n) Start***), which can be be activated when any of the three phases start (Any Phase), or when all three phases start (Three Phase), depending on the chosen ***V< Operate Mode*** setting.

The outputs of the timer modules are the trip signals which are used to drive the tripping output relay. These tripping signals are also OR'd together to create a 3-phase Trip signal, which are also controlled by the ***V< Operate Mode*** setting.

If any one of the above signals is low, or goes low before the timer has counted out, the timer module is inhibited (effectively reset) until the blocking signal goes high.

In some cases, we do not want the undervoltage element to trip; for example, when the protected feeder is de-energised, or the circuit breaker is opened, an undervoltage condition would obviously be detected, but we would not want to start protection. To cater for this, an ***All Poles Dead*** signal blocks the ***Start*** signal for each phase. This is controlled by the ***V<Poledead Inh*** cell, which is included for each of the stages. If the cell is enabled, the relevant stage will be blocked by the integrated pole dead logic. This logic produces an output when it detects either an open

circuit breaker via auxiliary contacts feeding the opto-inputs or it detects a combination of both undercurrent and undervoltage on any one phase.

11.3.3 APPLICATION NOTES

11.3.3.1 UNDERVOLTAGE SETTING GUIDELINES

In most applications, undervoltage protection is not required to operate during system earth fault conditions. If this is the case you should select phase-to-phase voltage measurement, as this quantity is less affected by single-phase voltage dips due to earth faults.

The voltage threshold setting for the undervoltage protection should be set at some value below the voltage excursions that may be expected under normal system operating conditions. This threshold is dependent on the system in question but typical healthy system voltage excursions may be in the order of 10% of nominal value.

The same applies to the time setting. The required time delay is dependent on the time for which the system is able to withstand a reduced voltage.

If motor loads are connected, then a typical time setting may be in the order of 0.5 seconds.

11.4 OVERVOLTAGE PROTECTION

Overvoltage conditions are generally related to loss of load conditions, whereby the supply voltage increases in magnitude. This situation would normally be rectified by voltage regulating equipment such as AVRs (Auto Voltage Regulators) or On Load Tap Changers. However, failure of this equipment to bring the system voltage back within permitted limits leaves the system with an overvoltage condition which must be cleared.

> *Note:*
> *During earth fault conditions on a power system there may be an increase in the healthy phase voltages. Ideally, the system should be designed to withstand such overvoltages for a defined period of time.*

11.4.1 OVERVOLTAGE PROTECTION IMPLEMENTATION

Overvoltage Protection is implemented in the *VOLT PROTECTION* column of the relevant settings group. The Overvoltage parameters are contained within the sub-heading *OVERVOLTAGE*.

The product provides two stages of overvoltage protection with independent time delay characteristics.

Stage 1 provides a choice of operate characteristics, where you can select between:

- An IDMT characteristic
- DT (Definite Time)

You set this using the ***V>1 Function*** setting.

The IDMT characteristic is defined by the following formula:

$$t = K/(M - 1)$$

where:

- K = Time multiplier setting
- t = Operating time in seconds
- M = Measured voltage setting voltage (***V>(n) Voltage Set***)

The overvoltage stages can be configured either as phase-to-neutral or phase-to-phase voltages in the ***V> Measur't Mode*** cell.

There is no Timer Hold facility for Overvoltage.

Stage 2 can have definite time characteristics only. This is set in the ***V>2 Status*** cell.

Outputs are available for single or three-phase conditions via the ***V> Operate Mode*** cell for each stage.

11.4.2 OVERVOLTAGE PROTECTION LOGIC

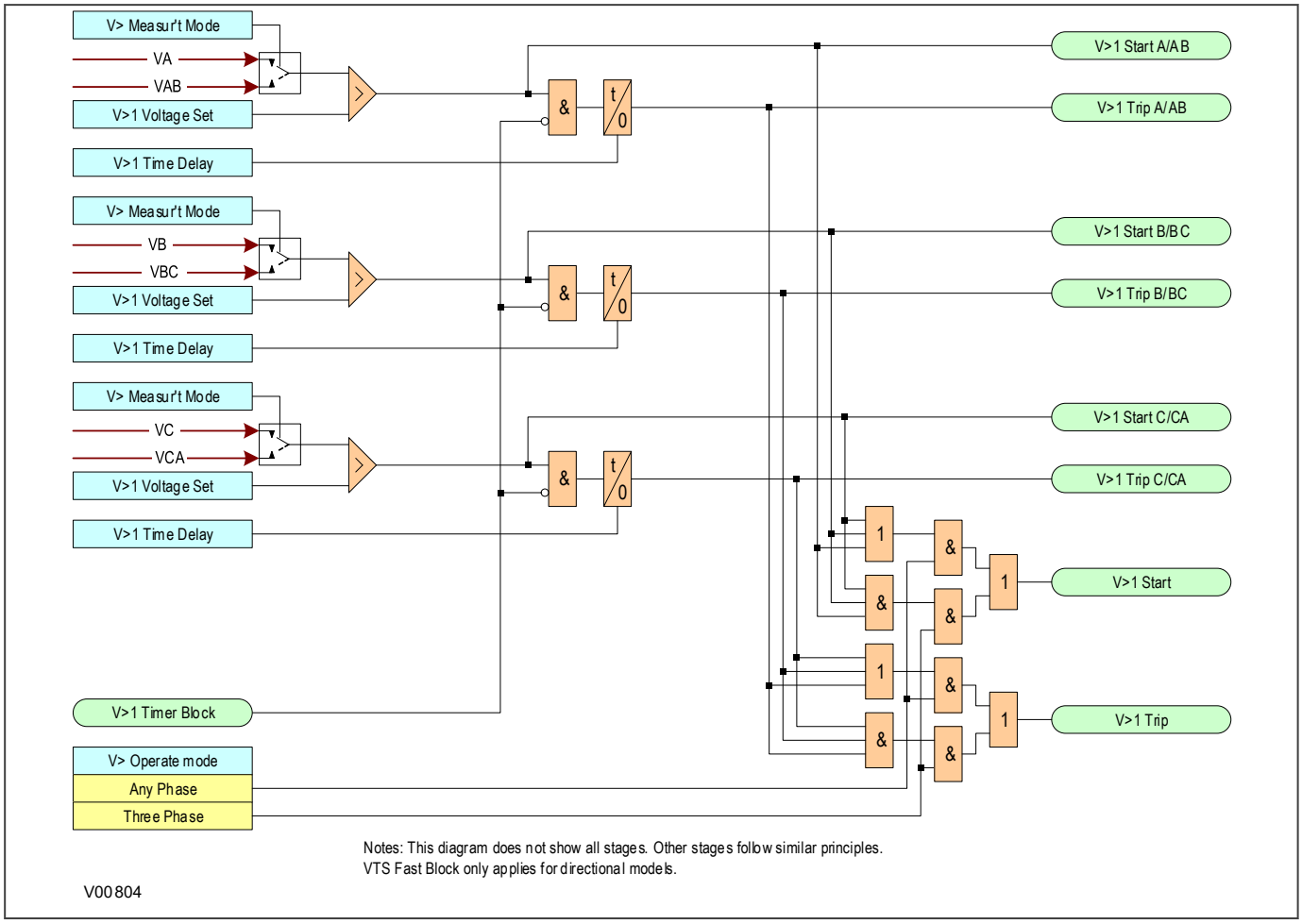


Figure 149: Overvoltage - single and three phase tripping mode (single stage)

The Overvoltage protection function detects when the voltage magnitude for a certain stage exceeds a set threshold. If this happens a ***Start*** signal, signifying the "Start of protection", is produced. This Start signal can be blocked by the ***VTS Fast Block*** signal. This start signal is applied to the timer module to produce the ***Trip*** signal, which can be blocked by the overvoltage timer block signal (***V>(n) Timer Block***). For each stage, there are three Phase overvoltage detection modules, one for each phase. The three ***Start*** signals from each of these phases are OR'd together to create a 3-phase Start signal (***V>(n) Start***), which can then be activated when any of the three phases start (Any Phase), or when all three phases start (Three Phase), depending on the chosen ***V> Operate Mode*** setting.

The outputs of the timer modules are the trip signals which are used to drive the tripping output relay. These tripping signals are also OR'd together to create a 3-phase Trip signal, which are also controlled by the ***V> Operate Mode*** setting.

If any one of the above signals is low, or goes low before the timer has counted out, the timer module is inhibited (effectively reset) until the blocking signal goes high.

11.4.3 APPLICATION NOTES

11.4.3.1 OVERVOLTAGE SETTING GUIDELINES

The provision of multiple stages and their respective operating characteristics allows for a number of possible applications:

- Definite Time can be used for both stages to provide the required alarm and trip stages.
- Use of the IDMT characteristic allows grading of the time delay according to the severity of the overvoltage. As the voltage settings for both of the stages are independent, the second stage could then be set lower than the first to provide a time-delayed alarm stage.
- If only one stage of overvoltage protection is required, or if the element is required to provide an alarm only, the remaining stage may be disabled.

This type of protection must be co-ordinated with any other overvoltage devices at other locations on the system.

11.5 COMPENSATED OVERVOLTAGE

The Compensated Overvoltage function calculates the positive sequence voltage at the remote terminal using the positive sequence local current and voltage and the line impedance and susceptance. This can be used on long transmission lines where Ferranti Overvoltages can develop under remote circuit breaker open conditions.

The Compensated overvoltage protection function can be set in the *VOLT PROTECTION* column under the sub heading COMP OVERVOLTAGE. The remote voltage is calculated using line impedance settings and the line charging admittance in the *LINE PARAMETERS* column.

The IED uses the [A,B,C,D] transmission line equivalent model given the following parameters:

- Total Impedance Z = $z\angle\theta$ ohms
- Total Susceptance Y = $y\angle -90°$
- Line Length l

The remote voltage is calculated using the following equations:

$$\begin{bmatrix} \bar{V}r \\ \bar{I}r \end{bmatrix} = \begin{bmatrix} D & -C \\ -BA & \end{bmatrix} \times \begin{bmatrix} \bar{V}s \\ \bar{I}s \end{bmatrix}$$

where

- V_r is the voltage at the receiving end
- I_r is the current at the receiving end
- V_s is the measured voltage at the sending end
- I_s is the measured current at the sending end
- A= D = cosh(y.l)
- B = Z_c.sinh(y.l)
- C = Y_c.sinh(y.l)
- y.l = $\sqrt{}$(Z.Y)
- Z_c = 1/Y_c = $\sqrt{}$(Z/Y)
- Y = total line capacitive charging susceptance
- Z_c = characteristic impedance of the line (surge impedance)

There are two stages to provide both alarm and trip stages where required. Both stages can be set independently.

Stage 1 can be set to `IDMT`, `DT` or `Disabled`, in the ***V1>1 Cmp Funct*** cell. Stage 2 is DT only and is enabled or disabled in the ***V1>2 Cmp Status*** cell.

The IDMT characteristic on the first stage is defined by the following formula:

$$t = K/(M - 1)$$

where:

- K = Time multiplier setting
- t =Operating time in seconds
- M = Remote Calculated voltage / IED setting voltage

11.6 RESIDUAL OVERVOLTAGE PROTECTION

On a healthy three-phase power system, the sum of the three-phase to earth voltages is nominally zero, as it is the vector sum of three balanced vectors displaced from each other by 120°. However, when an earth fault occurs on the primary system, this balance is upset and a residual voltage is produced. This condition causes a rise in the neutral voltage with respect to earth. Consequently this type of protection is also commonly referred to as 'Neutral Voltage Displacement' or NVD for short.

This residual voltage may be derived (from the phase voltages) or measured (from a measurement class open delta VT). Derived values will normally only be used where the model does not support measured functionality (a dedicated measurement class VT). If a measurement class VT is used to produce a measured Residual Voltage, it cannot be used for other features such as Check Synchronisation.

This offers an alternative means of earth fault detection, which does not require any measurement of current. This may be particularly advantageous in high impedance earthed or insulated systems, where the provision of core balanced current transformers on each feeder may be either impractical, or uneconomic, or for providing earth fault protection for devices with no current transformers.

11.6.1 RESIDUAL OVERVOLTAGE PROTECTION IMPLEMENTATION

Residual Overvoltage Protection is implemented in the *RESIDUAL O/V NVD* column of the relevant settings group.

Some applications require more than one stage. For example an insulated system may require an alarm stage and a trip stage. It is common in such a case for the system to be designed to withstand the associated healthy phase overvoltages for a number of hours following an earth fault. In such applications, an alarm is generated soon after the condition is detected, which serves to indicate the presence of an earth fault on the system. This gives time for system operators to locate and isolate the fault. The second stage of the protection can issue a trip signal if the fault condition persists.

The product provides two stages of Derived Residual Overvoltage protection with independent time delay characteristics.

Stage 1 provides a choice of operate characteristics, where you can select between:

- An IDMT characteristic
- DT (Definite Time)

The IDMT characteristic is defined by the following formula:

$$t = K/(M - 1)$$

where:

- K= Time multiplier setting
- t = Operating time in seconds
- M = Derived residual voltage setting voltage (***VN> Voltage Set***)

You set this using the ***VN>1 Function*** setting.

Stage 1 also provides a Timer Hold facility.

Stage 2 can have definite time characteristics only. This is set in the ***VN>2 status*** cell

The device derives the residual voltage internally from the three-phase voltage inputs supplied from either a 5-limb VT or three single-phase VTs. These types of VT design provide a path for the residual flux and consequently permit the device to derive the required residual voltage. In addition, the primary star point of the VT must be earthed. Three-limb VTs have no path for residual flux and are therefore unsuitable for this type of protection.

11.6.2 RESIDUAL OVERVOLTAGE LOGIC

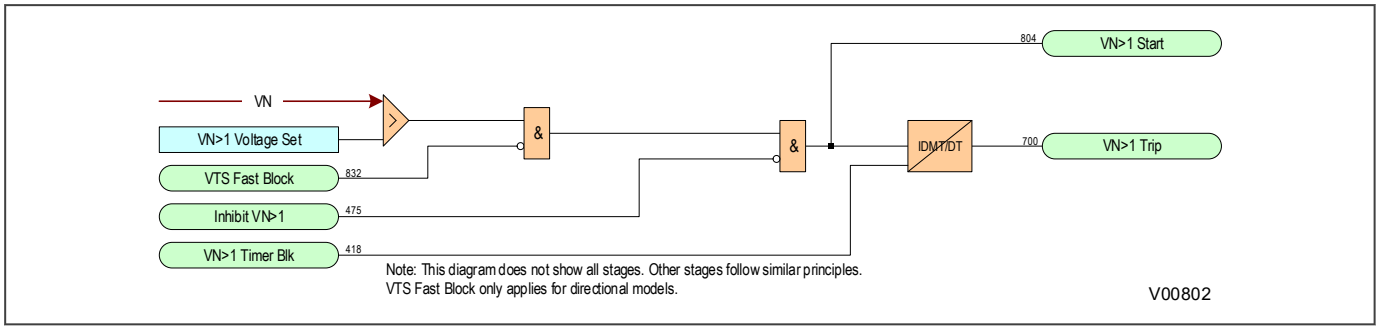


Figure 150: Residual overvoltage logic

The Residual Overvoltage module (VN>) is a level detector that detects when the voltage magnitude exceeds a set threshold, for each stage. When this happens, the comparator output produces a ***Start*** signal (***VN>(n) Start***), which signifies the "Start of protection". This can be blocked by a ***VTS Fast block*** signal. This ***Start*** signal is applied to the timer module. The output of the timer module is the ***VN> (n) Trip*** signal which is used to drive the tripping output relay.

11.6.3 APPLICATION NOTES

11.6.3.1 CALCULATION FOR SOLIDLY EARTHED SYSTEMS

Consider a Phase-A to Earth fault on a simple radial system.

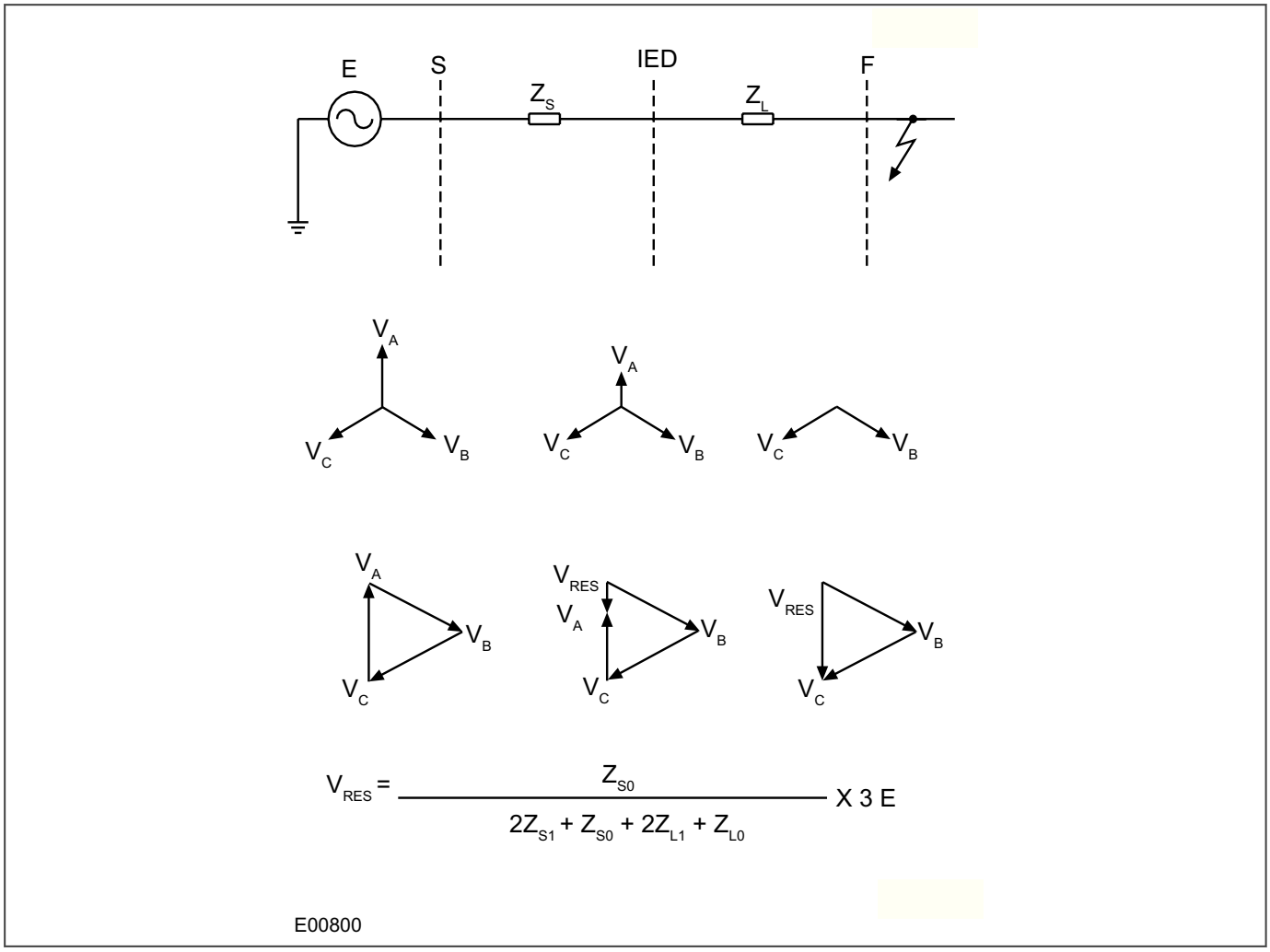


Figure 151: Residual voltage for a solidly earthed system

As can be seen from the above diagram, the residual voltage measured on a solidly earthed system is solely dependent on the ratio of source impedance behind the protection to the line impedance in front of the protection, up to the point of fault. For a remote fault far away, the Z_S/Z_L: ratio will be small, resulting in a correspondingly small residual voltage. Therefore, the protection only operates for faults up to a certain distance along the system. The maximum distance depends on the device setting.

11.6.3.2 CALCULATION FOR IMPEDANCE EARTHED SYSTEMS

Consider a Phase-A to Earth fault on a simple radial system.

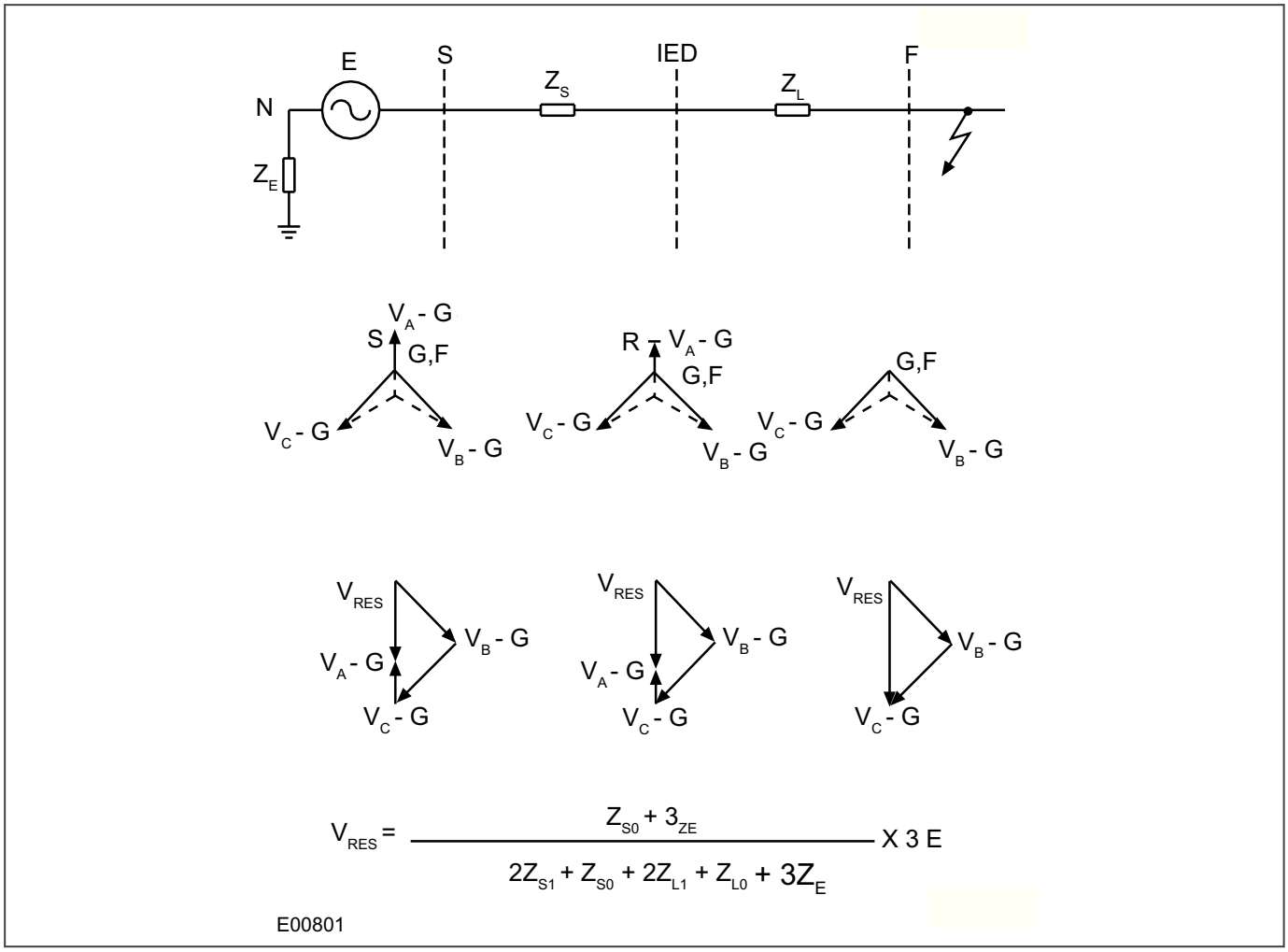


Figure 152: Residual voltage for an impedance earthed system

An impedance earthed system will always generate a relatively large degree of residual voltage, as the zero sequence source impedance now includes the earthing impedance. It follows then that the residual voltage generated by an earth fault on an insulated system will be the highest possible value (3 x phase-neutral voltage), as the zero sequence source impedance is infinite.

11.6.3.3 SETTING GUIDELINES

The voltage setting applied to the elements is dependent on the magnitude of residual voltage that is expected to occur during the earth fault condition. This in turn is dependent on the method of system earthing employed.

Also, you must ensure that the protection setting is set above any standing level of residual voltage that is present on the system.

CHAPTER 12

FREQUENCY PROTECTION FUNCTIONS

12.1 CHAPTER OVERVIEW

The device provides a range of frequency protection functions. This chapter describes the operation of these functions including the principles, logic diagrams and applications.

This chapter contains the following sections:

Chapter Overview 259

Frequency Protection 260

Independent R.O.C.O.F Protection 263

12.2 FREQUENCY PROTECTION

Power generation and utilisation needs to be well balanced in any industrial, distribution or transmission network. These electrical networks are dynamic entities, with continually varying loads and supplies, which are continually affecting the system frequency. Increased loading reduces the system frequency and generation needs to be increased to maintain the frequency of the supply. Conversely decreased loading increases the system frequency and generation needs to be reduced. Sudden fluctuations in load can cause rapid changes in frequency, which need to be dealt with quickly.

Unless corrective measures are taken at the appropriate time, frequency decay can go beyond the point of no return and cause widespread network collapse, which has dire consequences.

Normally, generators are rated for a particular band of frequency. Operation outside this band can cause mechanical damage to the turbine blades. Protection against such contingencies is required when frequency does not improve even after load shedding steps have been taken. This type of protection can be used for operator alarms or turbine trips in case of severe frequency decay.

Clearly a range of methods is required to ensure system frequency stability. The frequency protection in this device provides both underfrequency and overfrequency protection.

Frequency Protection is implemented in the *FREQ PROTECTION* column of the relevant settings group.

12.2.1 UNDERFREQUENCY PROTECTION

A reduced system frequency implies that the net load is in excess of the available generation. Such a condition can arise, when an interconnected system splits, and the load left connected to one of the subsystems is in excess of the capacity of the generators in that particular subsystem. Industrial plants that are dependent on utilities to supply part of their loads will experience underfrequency conditions when the incoming lines are lost.

Many types of industrial loads have limited tolerances on the operating frequency and running speeds (e.g. synchronous motors). Sustained underfrequency has implications on the stability of the system, whereby any subsequent disturbance may damage equipment and even lead to blackouts. It is therefore essential to provide protection for underfrequency conditions.

12.2.1.1 UNDERFREQUENCY PROTECTION IMPLEMENTATION

Simple underfrequency Protection is configured in the FREQ PROTECTION column of the relevant settings group.

The device provides 4 stages of underfrequency protection. The function uses the following settings (shown for stage 1 only - other stages follow the same principles).

- ***F<1 Status:*** enables or disables underfrequency protection for the relevant stage
- ***F<1 Setting***: defines the frequency pickup setting
- ***F<1 Time Delay***: sets the time delay

12.2.1.2 UNDERFREQUENCY PROTECTION LOGIC

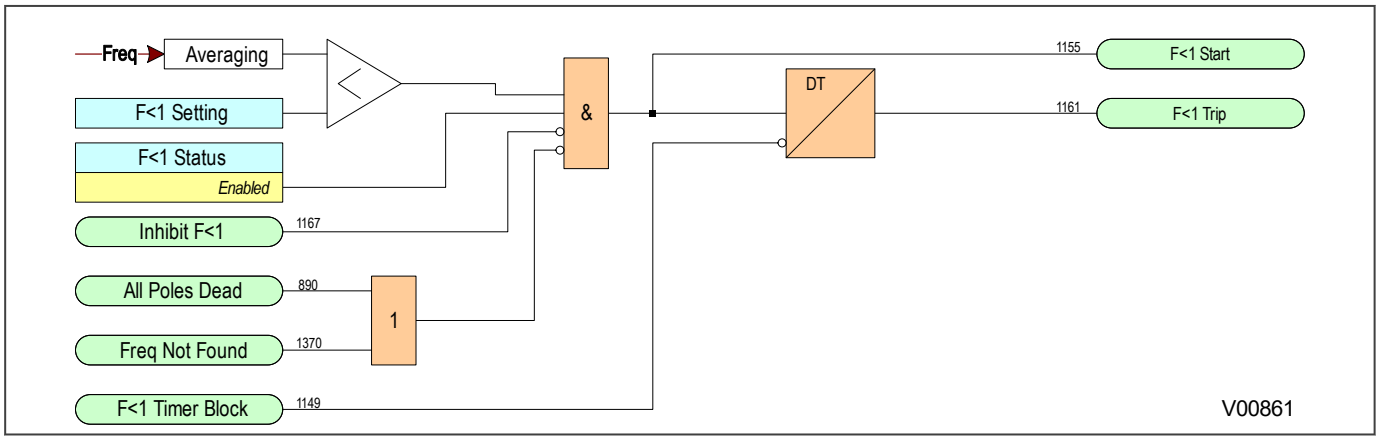


Figure 153: Underfrequency logic (single stage)

If the frequency is below the setting and not blocked the DT timer is started. If the frequency cannot be determined, the function is blocked.

12.2.1.3 APPLICATION NOTES

12.2.1.3.1 SETTING GUIDELINES

In order to minimise the effects of underfrequency, a multi-stage load shedding scheme may be used with the plant loads prioritised and grouped. During an underfrequency condition, the load groups are disconnected sequentially, with the highest priority group being the last one to be disconnected.

The effectiveness of each load shedding stage depends on the proportion of power deficiency it represents. If the load shedding stage is too small compared with the prevailing generation deficiency, then there may be no improvement in the frequency. This should be taken into account when forming the load groups.

Time delays should be sufficient to override any transient dips in frequency, as well as to provide time for the frequency controls in the system to respond. These should not be excessive as this could jeopardise system stability. Time delay settings of 5 - 20 s are typical.

The protection function should be set so that declared frequency-time limits for the generating set are not infringed. Typically, a 10% underfrequency condition should be continuously sustainable.

12.2.2 OVERFREQUENCY PROTECTION

An increased system frequency arises when the mechanical power input to a generator exceeds the electrical power output. This could happen, for instance, when there is a sudden loss of load due to tripping of an outgoing feeder from the plant to a load centre. Under such conditions, the governor would normally respond quickly to obtain a balance between the mechanical input and electrical output, thereby restoring normal frequency. Overfrequency protection is required as a backup to cater for cases where the reaction of the control equipment is too slow.

12.2.2.1 OVERFREQUENCY PROTECTION IMPLEMENTATION

Simple overfrequency Protection is configured in the *FREQ PROTECTION* column of the relevant settings group.

The device provides 2 stages of overfrequency protection. The function uses the following settings (shown for stage 1 only - other stages follow the same principles).

- ***F>1 Status:*** enables or disables underfrequency protection for the relevant stage
- ***F>1 Setting***: defines the frequency pickup setting
- ***F>1 Time Delay***: sets the time delay

12.2.2.2 OVERFREQUENCY PROTECTION LOGIC

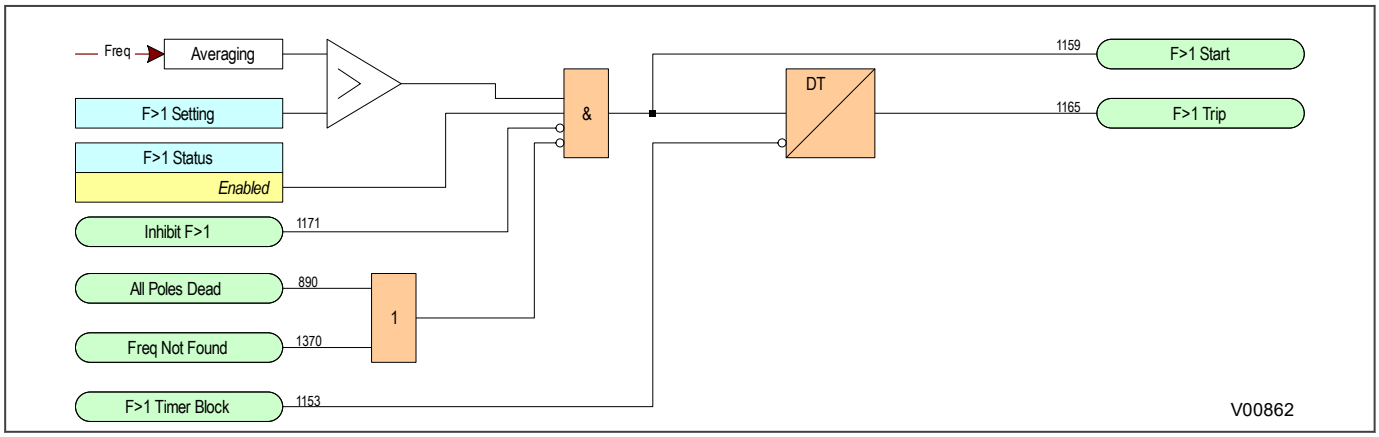


Figure 154: Overfrequency logic (single stage)

If the frequency is above the setting and not blocked, the DT timer is started and after this has timed out, the trip is produced. If the frequency cannot be determined, the function is blocked.

12.2.2.3 APPLICATION NOTES

12.2.2.3.1 SETTING GUIDELINES

Following changes on the network caused by faults or other operational requirements, it is possible that various subsystems will be formed within the power network. It is likely that these subsystems will suffer from a generation/ load imbalance. The "islands" where generation exceeds the existing load will be subject to overfrequency conditions. Severe over frequency conditions may be unacceptable to many industrial loads, since running speeds of motors will be affected. The overfrequency element can be suitably set to sense this contingency.

12.3 INDEPENDENT R.O.C.O.F PROTECTION

Where there are very large loads, imbalances may occur that result in rapid decline in system frequency. The situation could be so bad that shedding one or two stages of load is unlikely to stop this rapid frequency decline. In such a situation, standard underfrequency protection will normally have to be supplemented with protection that responds to the rate of change of frequency. An element is therefore required which identifies the high rate of decline of frequency, and adapts the load shedding scheme accordingly.

Such protection can identify frequency variations occurring close to nominal frequency thereby providing early warning of a developing frequency problem. The element can also be used as an alarm to warn operators of unusually high system frequency variations.

12.3.1 INDEPENDENT R.O.C.O.F PROTECTION IMPLEMENTATION

The device provides four independent stages of protection. Each stage can respond to either rising or falling frequency conditions. This depends on whether the frequency threshold is set above or below the system nominal frequency. For example, if the frequency threshold is set above nominal frequency, the rate of change of frequency setting is considered as positive and the element will operate for rising frequency conditions. If the frequency threshold is set below nominal frequency, the setting is considered as negative and the element will operate for falling frequency conditions.

The function uses the following settings (shown for stage 1 only - other stages follow the same principles).

- ***df/dt Avg.Cycles*** calculates the rate of change of frequency over a fixed period of several cycles.
- ***df/dt>1 Status***: determines whether the stage is for falling or rising frequency conditions
- ***df/dt>1 Setting***: defines the rate of change of frequency pickup setting
- ***df/dt>1 Time***: sets the time delay
- ***df/dt>1 Dir'n***: sets the direction of change you wish to check (positive, negative, or both)

In addition, start, trip and timer block DDB signals are available for each stage, as well as an inhibit signal to inhibit all four stages.

Note:
*It is recommended to only use **df/dt** settings <8Hz/s to maintain the claimed performance accuracy for pick-up and operating time, and to ensure the relay is within the frequency operating range, 45-65Hz.*

12.3.2 INDEPENDENT R.O.C.O.F PROTECTION LOGIC

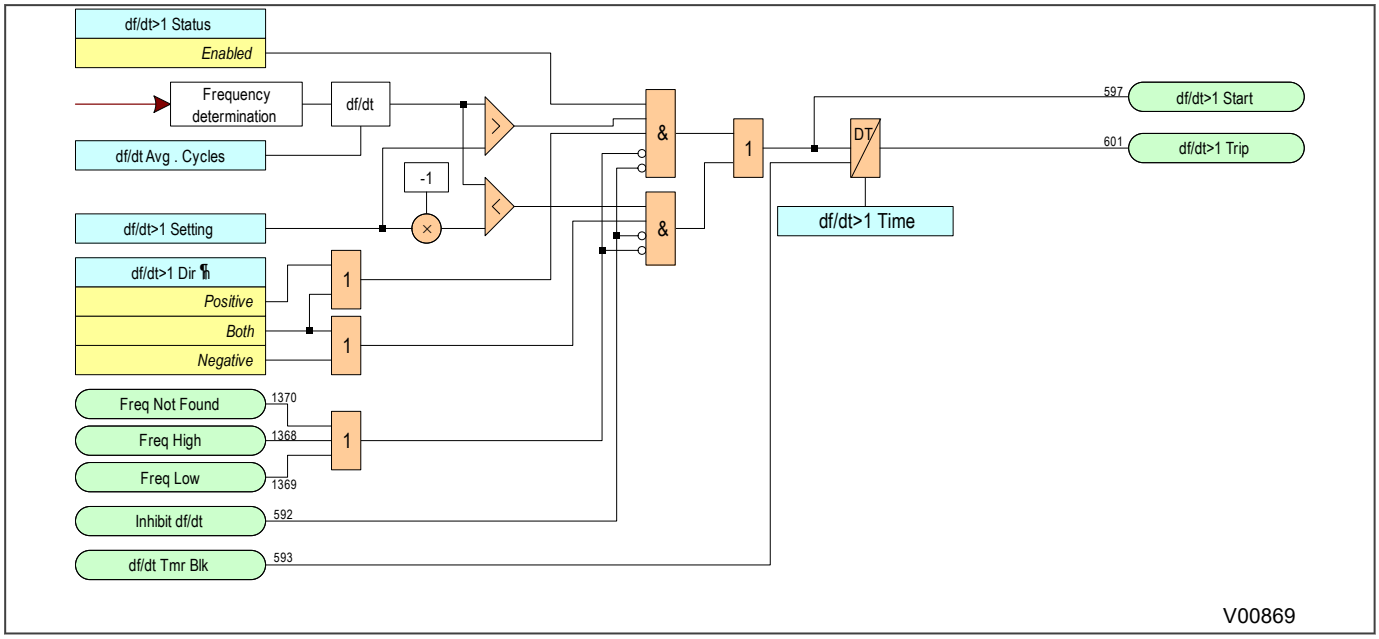


Figure 155: Rate of change of frequency logic (single stage)

CHAPTER 13

MONITORING AND CONTROL

13.1 CHAPTER OVERVIEW

As well as providing a range of protection functions, the product includes comprehensive monitoring and control functionality.

This chapter contains the following sections:

Chapter Overview 266
Event Records 267
Disturbance Recorder 271
Measurements 272
CB Condition Monitoring 273
CB State Monitoring 280
Circuit Breaker Control 282
Pole Dead Function 287
CB Condition Monitoring 289
System Checks 290

13.2 EVENT RECORDS

GE Vernova devices record events in an event log. This allows you to establish the sequence of events that led up to a particular situation. For example, a change in a digital input signal or protection element output signal would cause an event record to be created and stored in the event log. This could be used to analyse how a particular power system condition was caused. These events are stored in the IED's non-volatile memory. Each event is time tagged.

The event records can be displayed on an IED's front panel but it is easier to view them through the settings application software. This can extract the events log from the device and store it as a single .evt file for analysis on a PC.

The event records are detailed in the *VIEW RECORDS* column. The first event (0) is always the latest event. After selecting the required event, you can scroll through the menus to obtain further details.

If viewing the event with the settings application software, simply open the extracted event file. All the events are displayed chronologically. Each event is summarised with a time stamp obtained from the ***Time & Date*** cell) and a short description relating to the event obtained from the ***Event Text*** cell). You can expand the details of the event by clicking on the **+** icon to the left of the time stamp.

The following table shows the correlation between the fields in the setting application software's event viewer and the cells in the menu database.

Field in Event Viewer	Equivalent Cell in Menu DB	Cell Reference	User Settable?
Left hand column header	VIEW RECORDS → Time & Date	01 03	No
Right hand column header	VIEW RECORDS → Event Text	01 04	No
Description	SYSTEM DATA → Description	00 04	Yes
Plant reference	SYSTEM DATA → Plant Reference	00 05	Yes
Model number	SYSTEM DATA → Model Number	00 06	No
Address	Displays the Courier address relating to the event	N/A	No
Event type	VIEW RECORDS → Menu Cell Ref	01 02	No
Event Value	VIEW RECORDS → Event Value	01 05	No
Evt Unique Id	VIEW RECORDS → Evt Unique ID	01 FE	No

The device is capable of storing up to 1024 event records.

In addition to the event log, there are two logs which contain duplicates of the last 5 maintenance records and the last 5 fault records. The purpose of this is to provide convenient access to the most recent fault and maintenance events.

13.2.1 EVENT TYPES

There are several different types of event:

- Opto-input events (Change of state of opto-input)
- Contact events (Change of state of output relay contact)
- Alarm events
- Fault record events
- Standard events
- Security events

Standard events are further sub-categorised internally to include different pieces of information. These are:

- Protection events (starts and trips)
- Maintenance record events
- Platform events

Note:
The first event in the list (event 0) is the most recent event to have occurred.

13.2.1.1 OPTO-INPUT EVENTS

If one or more of the opto-inputs has changed state since the last time the protection algorithm ran (which runs at several times per cycle), a new event is created, which logs the logic states of all opto-inputs. You can tell which opto-input has changed state by comparing the new event with the previous one.

The description of this event type, as shown in the ***Event Text*** cell is always `Logic Inputs #` where # is the batch number of the opto-inputs. This is '1', for the first batch of opto-inputs and '2' for the second batch of opto-inputs (if applicable).

The event value shown in the ***Event Value*** cell for this type of event is a binary string. This shows the logical states of the opto-inputs, where the Least Significant Bit (LSB), on the right corresponds to the first opto-input `Input L1`.

The same information is also shown in the ***Opto I/P Status*** cell in the *SYSTEM DATA* column. This information is updated continuously, whereas the information in the event log is a snapshot at the time when the event was created.

13.2.1.2 CONTACT EVENTS

If one or more of the output relays (also known as output contacts) has changed state since the last time the protection algorithm ran (which runs at several times per cycle), a new event is created, which logs the logic states of all output relays. You can tell which output relay has changed state by comparing the new event with the previous one.

The description of this event type, as shown in the ***Event Text*** cell is always `Output Contacts #` where # is the batch number of the output relay contacts. This is '1', for the first batch of output contacts and '2' for the second batch of output contacts (if applicable).

The event value shown in the ***Event Value*** cell for this type of event is a binary string. This shows the logical states of the output relays, where the LSB (on the right) corresponds to the first output contact `Output R1`.

The same information is also shown in the ***Relay O/P Status*** cell in the *SYSTEM DATA* column. This information is updated continuously, whereas the information in the event log is a snapshot at the time when the event was created.

13.2.1.3 ALARM EVENTS

The IED monitors itself on power up and continually thereafter. If it notices any problems, it will register an alarm event.

The description of this event type, as shown in the ***Event Text*** cell is cell dependent on the type of alarm and will be one of those shown in the following tables, followed by `OFF` or `ON`.

The event value shown in the ***Event Value*** cell for this type of event is a 32 bit binary string. There are one or more banks 32 bit registers, depending on the device model. These contain all the alarm types and their logic states (`ON` or `OFF`).

The same information is also shown in the ***Alarm Status (n)*** cells in the *SYSTEM DATA* column. This information is updated continuously, whereas the information in the event log is a snapshot at the time when the event was created.

13.2.1.4 FAULT RECORD EVENTS

An event record is created for every fault the IED detects. This is also known as a fault record.

The event type description shown in the ***Event Text*** cell for this type of event is always `Fault Recorded`.

The IED contains a separate register containing the latest fault records. This provides a convenient way of viewing the latest fault records and saves searching through the event log. You access these fault records using the ***Select Fault*** setting, where fault number 0 is the latest fault.

A fault record is triggered by the ***Fault REC TRIG*** signal DDB, which is assigned in the PSL. The fault recorder records the values of all parameters associated with the fault for the duration of the fault. These parameters are stored in separate Courier cells, which become visible depending on the type of fault.

The fault recorder stops recording only when:

The Start signal is reset AND the undercurrent is ON OR the Trip signal is reset, as shown below:

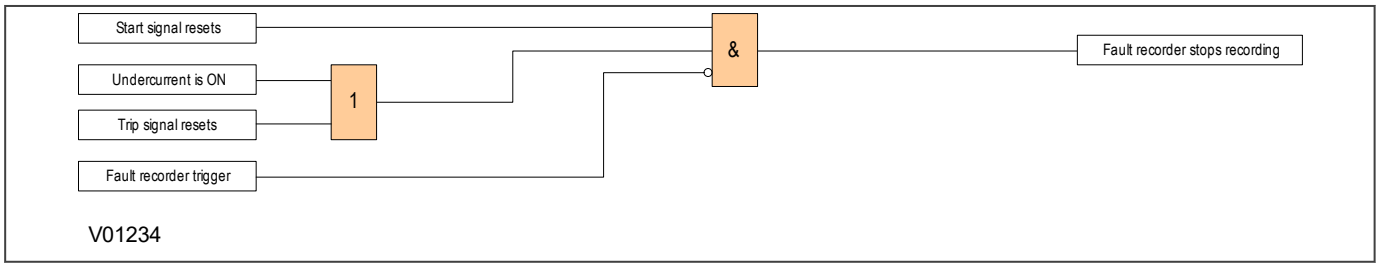


Figure 156: Fault recorder stop conditions

The event is logged as soon as the fault recorder stops. The time stamp assigned to the fault corresponds to the start of the fault. The timestamp assigned to the fault record event corresponds to the time when the fault recorder stops.

> *Note:*
> *We recommend that you do not set the triggering contact to latching. This is because if you use a latching contact, the fault record would not be generated until the contact has been fully reset.*

13.2.1.5 MAINTENANCE EVENTS

Internal failures detected by the self-test procedures are logged as maintenance records. Maintenance records are special types of standard events.

The event type description shown in the ***Event Text*** cell for this type of event is always `Maint Recorded`.

The ***Event Value*** cell also provides a unique binary code.

The IED contains a separate register containing the latest maintenance records. This provides a convenient way of viewing the latest maintenance records and saves searching through the event log. You access these fault records using the ***Select Maint*** setting.

The maintenance record has a number of extra menu cells relating to the maintenance event. These parameters are ***Maint Text***, ***Maint Type*** and ***Maint Data***. They contain details about the maintenance event selected with the ***Select Maint*** cell.

13.2.1.6 PROTECTION EVENTS

The IED logs protection starts and trips as individual events. Protection events are special types of standard events.

The event type description shown in the ***Event Text*** cell for this type of event is dependent on the protection event that occurred. Each time a protection event occurs, a DDB signal changes state. It is the name of this DDB signal followed by 'ON' or 'OFF' that appears in the ***Event Text*** cell.

The ***Event Value*** cell for this type of event is a 32 bit binary string representing the state of the relevant DDB signals. These binary strings can also be viewed in the *COMMISSION TESTS* column in the relevant DDB batch cells.

Not all DDB signals can generate an event. Those that can are listed in the *RECORD CONTROL* column. In this column, you can set which DDBs generate events.

13.2.1.7 SECURITY EVENTS

An event record is generated each time a setting that requires an access level is executed.

The event type description shown in the ***Event Text*** cell displays the type of change.

13.2.1.8 PLATFORM EVENTS

Platform events are special types of standard events.

The event type description shown in the ***Event Text*** cell displays the type of change.

13.3 DISTURBANCE RECORDER

The disturbance recorder feature allows you to record selected current and voltage inputs to the protection elements, together with selected digital signals. The digital signals may be inputs, outputs, or internal DDB signals. The disturbance records can be extracted using the disturbance record viewer in the settings application software. The disturbance record file can also be stored in the COMTRADE format. This allows the use of other packages to view the recorded data.

The integral disturbance recorder has an area of memory specifically set aside for storing disturbance records. The number of records that can be stored is dependent on the recording duration. The minimum duration is 0.1 s and the maximum duration is 10.5 s.

When the available memory is exhausted, the oldest records are overwritten by the newest ones.

Each disturbance record consists of a number of analogue data channels and digital data channels. The relevant CT and VT ratios for the analogue channels are also extracted to enable scaling to primary quantities.

The fault recording times are set by a combination of the ***Duration*** and ***Trigger Position*** cells. The ***Duration*** cell sets the overall recording time and the ***Trigger Position*** cell sets the trigger point as a percentage of the duration. For example, the default settings show that the overall recording time is set to 1.5 s with the trigger point being at 33.3% of this, giving 0.5 s pre-fault and 1 s post fault recording times.

With the ***Trigger Mode*** set to *Single*, if further triggers occurs whilst a recording is taking place, the recorder will ignore the trigger. However, with the ***Trigger Mode*** set to *Extended*, the post trigger timer will be reset to zero, extending the recording time.

You can select any of the IED's analogue inputs as analogue channels to be recorded. You can also map any of the opto-inputs output contacts to the digital channels. In addition, you may also map a number of DDB signals such as Starts and LEDs to digital channels.

You may choose any of the digital channels to trigger the disturbance recorder on either a low to high or a high to low transition, via the ***Input Trigger*** cell. The default settings are such that any dedicated trip output contacts will trigger the recorder.

It is not possible to view the disturbance records locally via the front panel LCD. You must extract these using suitable setting application software such as MiCOM S1 Agile.

13.4 MEASUREMENTS

13.4.1 MEASURED QUANTITIES

The device measures directly and calculates a number of system quantities, which are updated every second. You can view these values in the relevant MEASUREMENT columns or with the Measurement Viewer in the settings application software. Depending on the model, the device may measure and display some or more of the following quantities:

- Measured and calculated analogue current and voltage values
- Power and energy quantities
- Peak, fixed and rolling demand values
- Frequency measurements
- Thermal measurements
- Teleprotection channel measurements

13.4.2 MEASUREMENT SETUP

You can define the way measurements are set up and displayed using the *MEASURE'T SETUP* column and the measurements are shown in the relevant MEASUREMENTS tables.

13.4.3 FAULT LOCATOR

Some models provide fault location functionality. It is possible to identify the fault location by measuring the fault voltage and current magnitude and phases and presenting this information to a Fault Locator function. The fault locator is triggered whenever a fault record is generated, and the subsequent fault location data is included as part of the fault record. This information is also displayed in the ***Fault Location*** cell in the *VIEW RECORDS* column. This cell will display the fault location in metres, miles ohms or percentage, depending on the chosen units in the ***Fault Location*** cell of the *MEASURE'T SETUP* column.

The Fault Locator uses pre-fault and post-fault analogue input signals to calculate the fault location. The result is included it in the fault record. The pre-fault and post-fault voltages are also presented in the fault record.

When applied to parallel circuits, mutual flux coupling can alter the impedance seen by the fault locator. The coupling contains positive, negative and zero sequence components. In practise the positive and negative sequence coupling is insignificant. The effect on the fault locator of the zero sequence mutual coupling can be eliminated using the mutual compensation feature provided.

> *Note:*
> *Multi-ended line differential relays support fault location from the local terminal only. For this reason, the **LINE PARAMETERS** setting shall be set based on the parameters of the local to the nearest junction at each relay.*

13.4.4 OPTO-INPUT TIME STAMPING

Each opto-input sample is time stamped within a tolerance of +/- 1 ms with respect to the Real Time Clock. These time stamps are used for the opto event logs and for the disturbance recording. The device needs to be synchronised accurately to an external clock source such as an IRIG-B signal or a master clock signal provided in the relevant data protocol.

For both the filtered and unfiltered opto-inputs, the time stamp of an opto-input change event is the sampling time at which the change of state occurred. If multiple opto-inputs change state at the same sampling interval, these state changes are reported as a single event.

13.5 CB CONDITION MONITORING

The device records various statistics related to each circuit breaker trip operation, allowing an accurate assessment of the circuit breaker condition to be determined. These statistics are available in the *CB CONDITION* column. The menu cells are register values only and cannot be set directly. They may be reset, however, during maintenance. The statistics monitored are:

- Total Current Broken: A register stores the total amount of current that the CB has broken is stored in an accumulator, giving at any time a measure of the total amount of current that the CB has broken since the value was last reset.
- Number of CB operations: A counter registers the number of CB trips that have been performed for each phase, giving at any time the total number of trips that the CB has performed since the value was last reset.
- CB Operate Time: A register stores the total amount of time the CB has transitioned from closed to open is stored in an accumulator, giving at any time a measure of the total time that the CB has spent tripping since the values was last reset.
- Excessive Fault Frequency: A counter registers the number of CB trips that have been performed for all phases, giving at any time the total number of trips performed since the value was last reset.

These statistics are available in the *CB CONDITION* column. The menu cells are register values only and cannot be set directly. They may be reset, however, during maintenance.

> *Note:*
> *When in Commissioning test mode the CB condition monitoring registers are not updated.*

Circuit breaker lockout, can be caused by the following circuit breaker condition monitoring functions:

- Maintenance lockout
- Excessive fault frequency lockout
- Broken current lockout

If the circuit breaker is locked out, the logic generates a lockout alarm

13.5.1 BROKEN CURRENT ACCUMULATOR

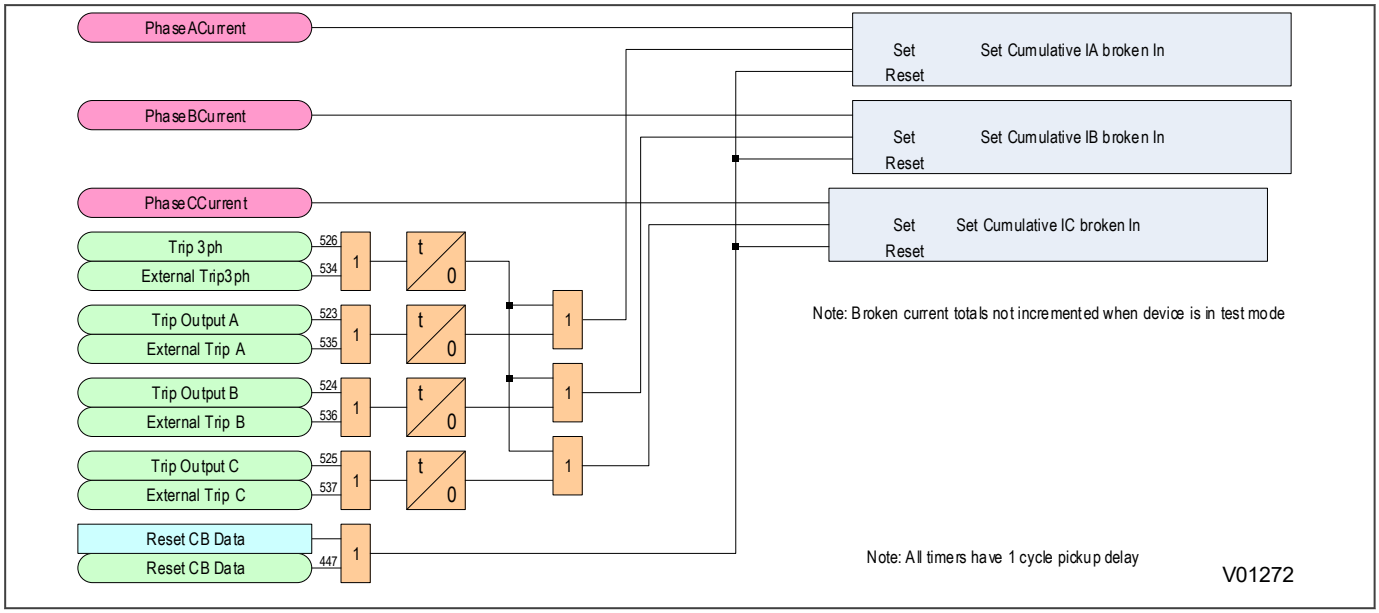


Figure 157: Broken current accumulator logic

13.5.2 CB TRIP COUNTER

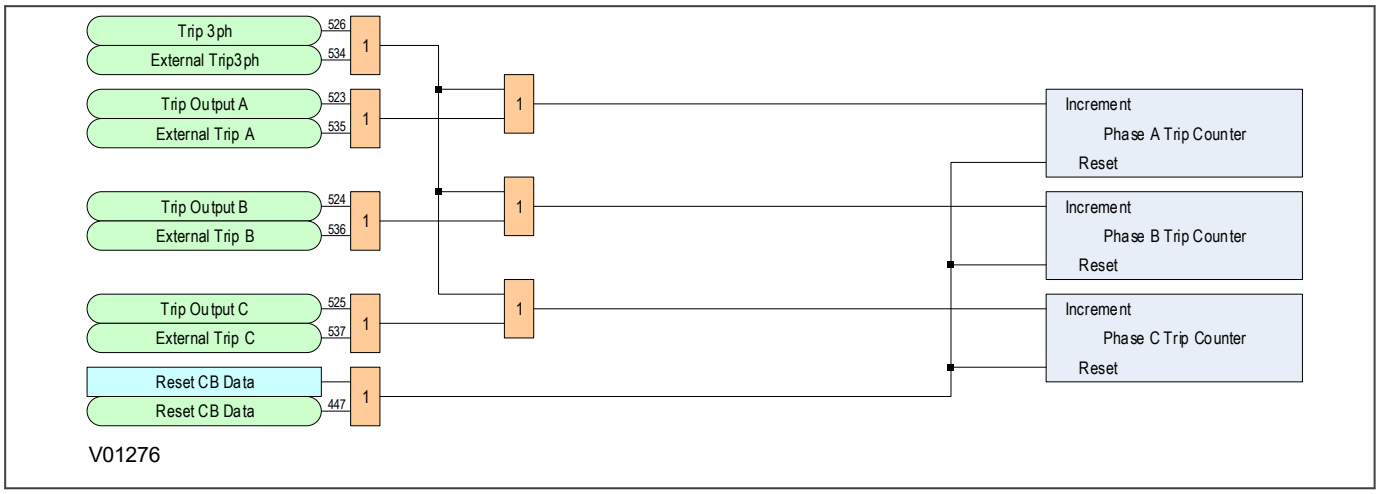


Figure 158: CB trip counter logic

13.5.3 CB OPERATING TIME ACCUMULATOR

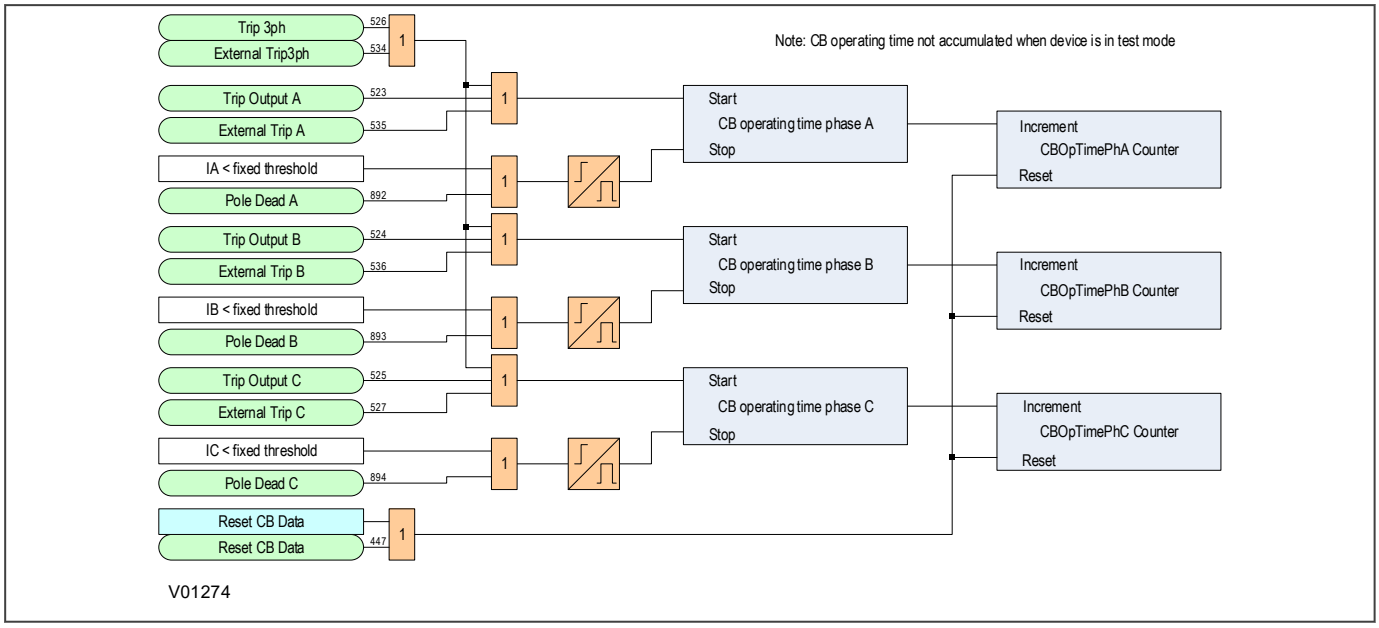


Figure 159: Operating time accumulator

13.5.4 EXCESSIVE FAULT FREQUENCY COUNTER

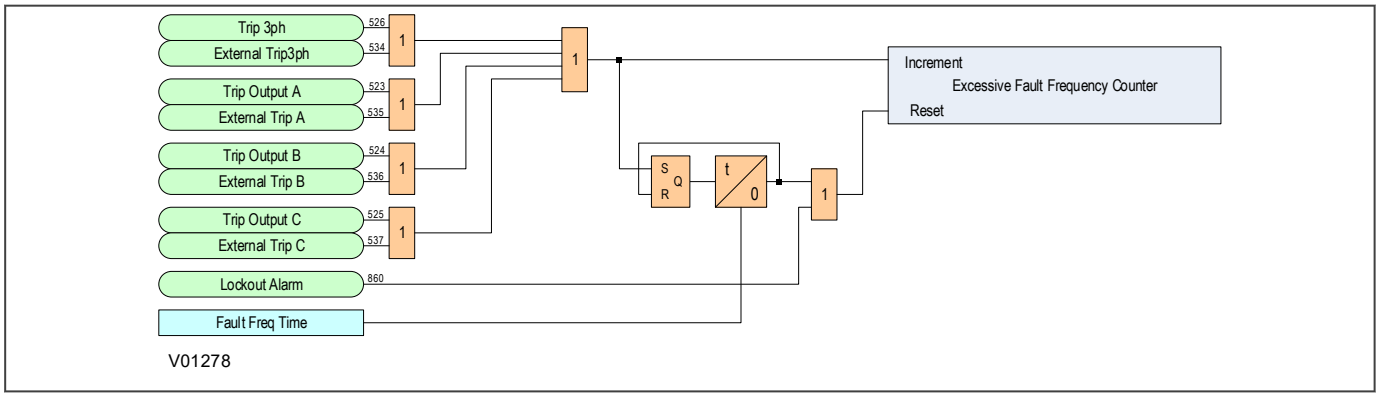


Figure 160: Excessive fault frequency logic

13.5.5 RESET LOCKOUT ALARM

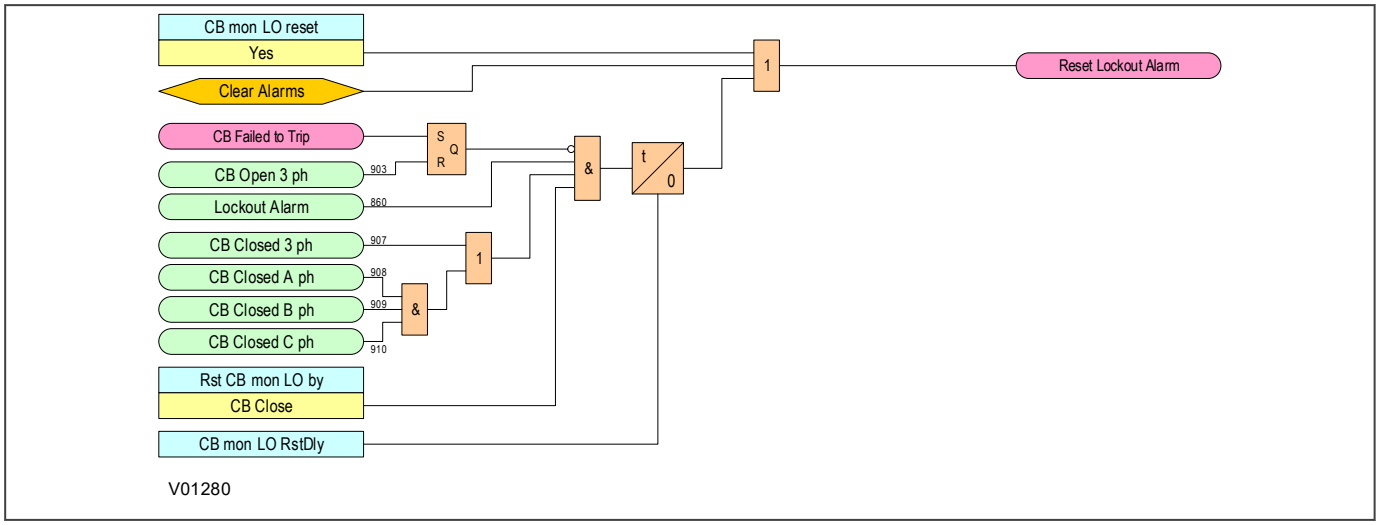


Figure 161: Reset lockout alarm logic

13.5.6 CB CONDITION MONITORING LOGIC

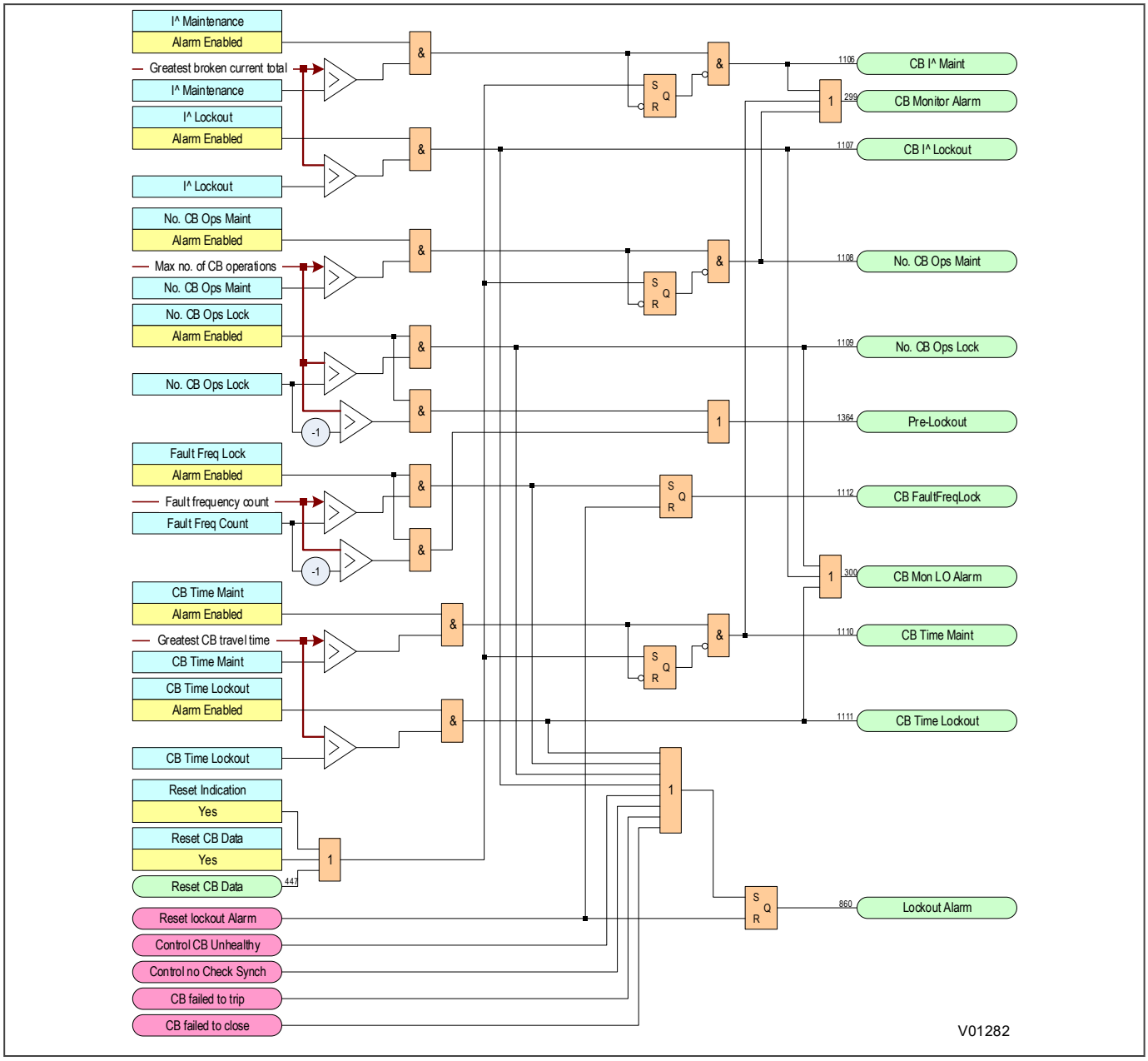


Figure 162: CB condition monitoring logic

13.5.7 RESET CIRCUIT BREAKER LOCKOUT

Lockout conditions caused by the circuit breaker condition monitoring functions can be reset according to the condition of the ***Rst CB mon LO*** by setting found in the *CB CONTROL* column. There are two options; `CB Close` and `User interface`.

If set to `CB Close`, a timer setting, ***CB mon LO RstDly***, becomes visible. When the circuit breaker closes, the ***CB mon LO RstDly*** time starts. The lockout is reset when the timer expires.

If set to `User Interface` then a command, ***CB mon LO reset***, becomes visible. This command can be used to reset the lockout from a user interface.

An Autoreclose lockout generates an Autoreclose lockout alarm. Autoreclose lockout conditions can be reset by various commands and setting options found under the *CB CONTROL* column.

If ***Res LO by CB IS*** is set to `Enabled`, a lockout is reset if the circuit breaker is successfully closed manually. For this, the circuit breaker must remain closed long enough so that it enters the “In Service” state.

If ***Res LO by UI*** is set to `Enabled`, the circuit breaker lockout can be reset from a user interface using the reset circuit breaker lockout command in the *CB CONTROL* column.

If ***Res LO by NoAR*** is set to `Enabled`, the circuit breaker lockout can be reset by temporarily generating an ***AR disabled*** signal.

If ***Res LO by TDelay*** is set to `Enabled`, the circuit breaker lockout is automatically reset after a time delay set in the ***LO Reset Time*** setting.

If ***Res LO by ExtDDB*** is `Enabled`, the circuit breaker lockout can be reset by activation of an external input mapped in the PSL to the relevant reset lockout DDB signal.

13.5.7.1 RESET CB LOCKOUT LOGIC DIAGRAM

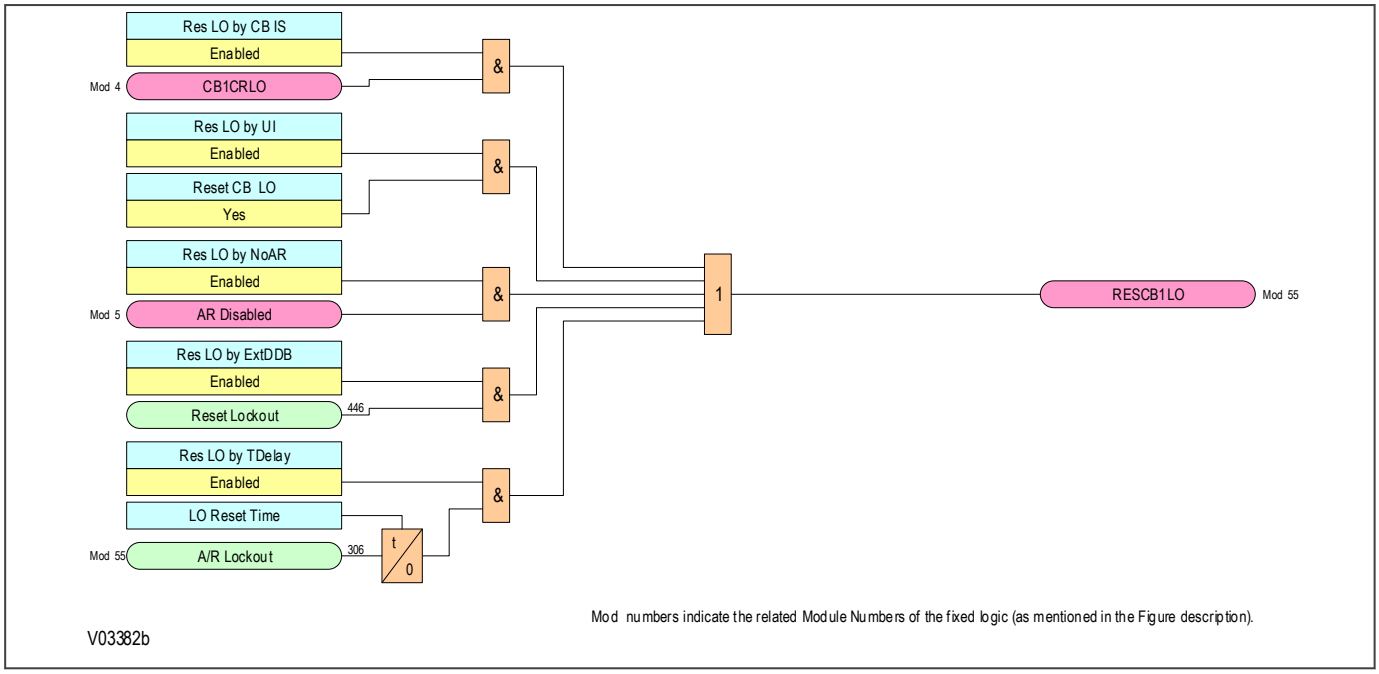


Figure 163: Reset circuit breaker lockout logic (module 57)

13.5.8 APPLICATION NOTES

13.5.8.1 SETTING THE THRESHOLDS FOR THE TOTAL BROKEN CURRENT

Where power lines use oil circuit breakers (OCBs), changing of the oil accounts for a significant proportion of the switchgear maintenance costs. Often, oil changes are performed after a fixed number of CB fault operations. However, this may result in premature maintenance where fault currents tend to be low, because oil degradation may be slower than would normally be expected. The Total Current Accumulator (I^ counter) cumulatively stores the total value of the current broken by the circuit breaker providing a more accurate assessment of the circuit breaker condition.

The dielectric withstand of the oil generally decreases as a function of I^2t, where ‘I’ is the broken fault current and ‘t’ is the arcing time within the interrupter tank. The arcing time cannot be determined accurately, but is generally dependent on the type of circuit breaker being used. Instead, you set a factor (***Broken I^***) with a value between 1 and 2, depending on the circuit breaker.

Most circuit breakers would have this value set to '2', but for some types of circuit breaker, especially those operating on higher voltage systems, a value of 2 may be too high. In such applications ***Broken I^*** may be set lower, typically 1.4 or 1.5.

The setting range for ***Broken I^*** is variable between 1.0 and 2.0 in 0.1 steps.

Note:
Any maintenance program must be fully compliant with the switchgear manufacturer's instructions.

13.5.8.2 SETTING THE THRESHOLDS FOR THE NUMBER OF OPERATIONS

Every circuit breaker operation results in some degree of wear for its components. Therefore routine maintenance, such as oiling of mechanisms, may be based on the number of operations. Suitable setting of the maintenance threshold will allow an alarm to be raised, indicating when preventative maintenance is due. Should maintenance not be carried out, the device can be set to lockout the autoreclose function on reaching a second operations threshold (***No. CB ops Lock***). This prevents further reclosure when the circuit breaker has not been maintained to the standard demanded by the switchgear manufacturer's maintenance instructions.

Some circuit breakers, such as oil circuit breakers (OCBs) can only perform a certain number of fault interruptions before requiring maintenance attention. This is because each fault interruption causes carbonising of the oil, degrading its dielectric properties. The maintenance alarm threshold (setting ***No. CB Ops Maint***) may be set to indicate the requirement for oil dielectric testing, or for more comprehensive maintenance. Again, the lockout threshold ***No. CB Ops Lock*** may be set to disable autoreclosure when repeated further fault interruptions could not be guaranteed. This minimises the risk of oil fires or explosion.

13.5.8.3 SETTING THE THRESHOLDS FOR THE OPERATING TIME

Slow CB operation indicates the need for mechanism maintenance. Alarm and lockout thresholds (***CB Time Maint*** and ***CB Time Lockout***) are provided to enforce this. They can be set in the range of 5 to 500 ms. This time relates to the interrupting time of the circuit breaker.

13.5.8.4 SETTING THE THRESHOLDS FOR EXCESSSIVE FAULT FREQUENCY

Persistent faults will generally cause autoreclose lockout, with subsequent maintenance attention. Intermittent faults such as clashing vegetation may repeat outside of any reclaim time, and the common cause might never be investigated. For this reason it is possible to set a frequent operations counter, which allows the number of operations ***Fault Freq Count*** over a set time period ***Fault Freq Time*** to be monitored. A separate alarm and lockout threshold can be set.

13.6 CB STATE MONITORING

CB State monitoring is used to verify the open or closed state of a circuit breaker. Most circuit breakers have auxiliary contacts through which they transmit their status (open or closed) to control equipment such as IEDs. These auxiliary contacts are known as:

- 52A for contacts that follow the state of the CB
- 52B for contacts that are in opposition to the state of the CB

This device can be set to monitor both of these types of circuit breaker state indication. If the state is unknown for some reason, an alarm can be raised.

Some CBs provide both sets of contacts. If this is the case, these contacts will normally be in opposite states. Should both sets of contacts be open, this would indicate one of the following conditions:

- Auxiliary contacts/wiring defective
- Circuit Breaker (CB) is defective
- CB is in isolated position

Should both sets of contacts be closed, only one of the following two conditions would apply:

- Auxiliary contacts/wiring defective
- Circuit Breaker (CB) is defective

If any of the above conditions exist, an alarm will be issued after a 5 s time delay. An output contact can be assigned to this function via the programmable scheme logic (PSL). The time delay is set to avoid unwanted operation during normal switching duties.

In the CB CONTROL column there is a setting called ***CB Status Input***. This cell can be set at one of the following four options:

- None
- 52A
- 52B
- Both 52A and 52B

Where *None* is selected no CB status is available. Where only 52A is used on its own then the device will assume a 52B signal opposite to the 52A signal. Circuit breaker status information will be available in this case but no discrepancy alarm will be available. The above is also true where only a 52B is used. If both 52A and 52B are used then status information will be available and in addition a discrepancy alarm will be possible, according to the following table:

Auxiliary Contact Position		CB State Detected	Action
52A	52B		
Open	Closed	Breaker open	Circuit breaker healthy
Closed	Open	Breaker closed	Circuit breaker healthy
Closed	Closed	CB failure	Alarm raised if the condition persists for greater than 5 s
Open	Open	State unknown	Alarm raised if the condition persists for greater than 5 s

13.6.1 CB STATE MONITOR LOGIC DIAGRAM

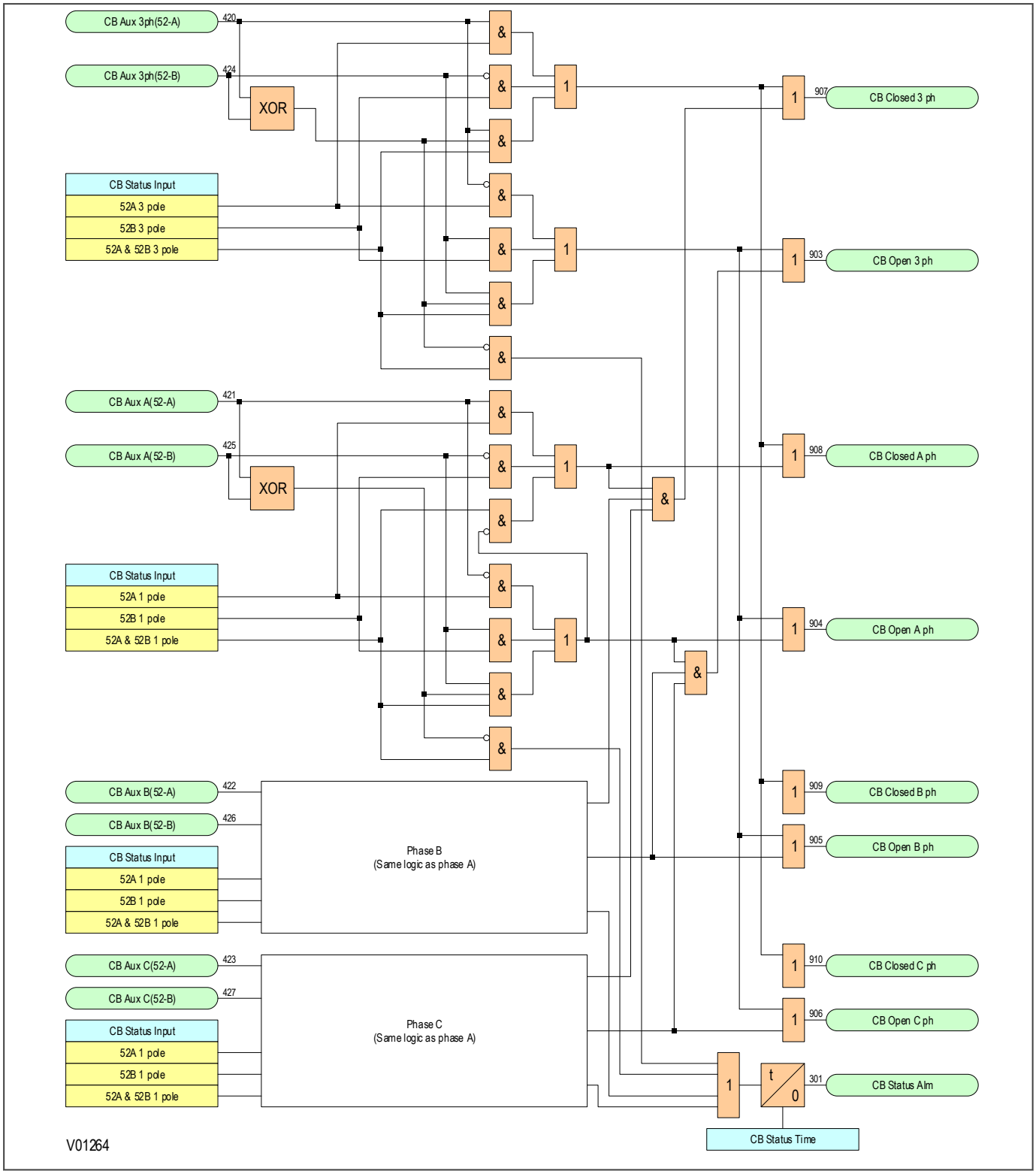


Figure 164: CB state monitor logic (module 1)

13.7 CIRCUIT BREAKER CONTROL

Although some circuit breakers do not provide auxiliary contacts, most provide auxiliary contacts to reflect the state of the circuit breaker. These are:

- CBs with 52A contacts (where the auxiliary contact follows the state of the CB)
- CBs with 52B contacts (where the auxiliary contact is in the opposite state from the state of the CB)
- CBs with both 52A and 52B contacts

Circuit Breaker control is only possible if the circuit breaker in question provides auxiliary contacts. The ***CB Status Input*** cell in the *CB CONTROL* column must be set to the type of circuit breaker. If no CB auxiliary contacts are available then this cell should be set to `None`, and no CB control will be possible.

For local control, the ***CB control by*** cell should be set accordingly.

The output contact can be set to operate following a time delay defined by the setting ***Man Close Delay***. One reason for this delay is to give personnel time to safely move away from the circuit breaker following a CB close command.

The control close cycle can be cancelled at any time before the output contact operates by any appropriate trip signal, or by activating the ***Reset Close Dly*** DDB signal.

The length of the trip and close control pulses can be set via the ***Trip Pulse Time*** and **Close Pulse Time** settings respectively. These should be set long enough to ensure the breaker has completed its open or close cycle before the pulse has elapsed.

If an attempt to close the breaker is being made, and a protection trip signal is generated, the protection trip command overrides the close command.

The ***Reset Lockout by*** setting is used to enable or disable the resetting of lockout automatically from a manual close after the time set by ***Man Close RstDly***.

If the CB fails to respond to the control command (indicated by no change in the state of CB Status inputs) an alarm is generated after the relevant trip or close pulses have expired. These alarms can be viewed on the LCD display, remotely, or can be assigned to output contacts using the programmable scheme logic (PSL).

Note:
*The **CB Healthy Time** and **Sys Check time** set under this menu section are applicable to manual circuit breaker operations only. These settings are duplicated in the AUTORECLOSE menu for autoreclose applications.*

The ***Lockout Reset*** and ***Reset Lockout by*** settings are applicable to CB Lockouts associated with manual circuit breaker closure, CB Condition monitoring (Number of circuit breaker operations, for example) and autoreclose lockouts.

The device includes the following options for control of a single circuit breaker:

- The IED menu (local control)
- The Hotkeys (local control)
- The function keys (local control)
- The opto-inputs (local control)
- SCADA communication (remote control)

13.7.1 CB CONTROL USING THE IED MENU

You can control manual trips and closes with the ***CB Trip/Close*** command in the *SYSTEM DATA* column. This can be set to `No Operation`, `Trip`, or `Close` accordingly.

For this to work you have to set the ***CB control by*** cell to option 1 `Local`, option 3 `Local + Remote`, option 5 `Opto+Local`, or option 7 `Opto+Local+Remote` in the *CB CONTROL* column.

13.7.2 CB CONTROL USING THE HOTKEYS

The hotkeys allow you to manually trip and close the CB without the need to enter the *SYSTEM DATA* column. For this to work you have to set the ***CB control by*** cell to option 1 `Local`, option 3 `Local+Remote`, option 5 `Opto +Local`, or option 7 `Opto+Local+Remote` in the *CB CONTROL* column.

CB control using the hotkey is achieved by pressing the right-hand button directly below LCD screen. This button is only enabled if:

- The ***CB Control by*** setting is set to one of the options where local control is possible (option 1,3,5, or 7)
- The ***CB Status Input*** is set to '52A', '52B', or 'Both 52A and 52B'

If the CB is currently closed, the command text on the bottom right of the LCD screen will read `Trip`. Conversely, if the CB is currently open, the command text will read `Close`.

If you execute a `Trip`, a screen with the CB status will be displayed once the command has been completed. If you execute a `Close`, a screen with a timing bar will appear while the command is being executed. This screen also gives you the option to cancel or restart the close procedure. The time delay is determined by the ***Man Close Delay*** setting in the *CB CONTROL* menu. When the command has been executed, a screen confirming the present status of the circuit breaker is displayed. You are then prompted to select the next appropriate command or exit.

If no keys are pressed for a period of 5 seconds while waiting for the command confirmation, the device will revert to showing the CB Status. If no key presses are made for a period of 25 seconds while displaying the CB status screen, the device will revert to the default screen.

To avoid accidental operation of the trip and close functionality, the hotkey CB control commands are disabled for 10 seconds after exiting the hotkey menu.

The hotkey functionality is summarised graphically below:

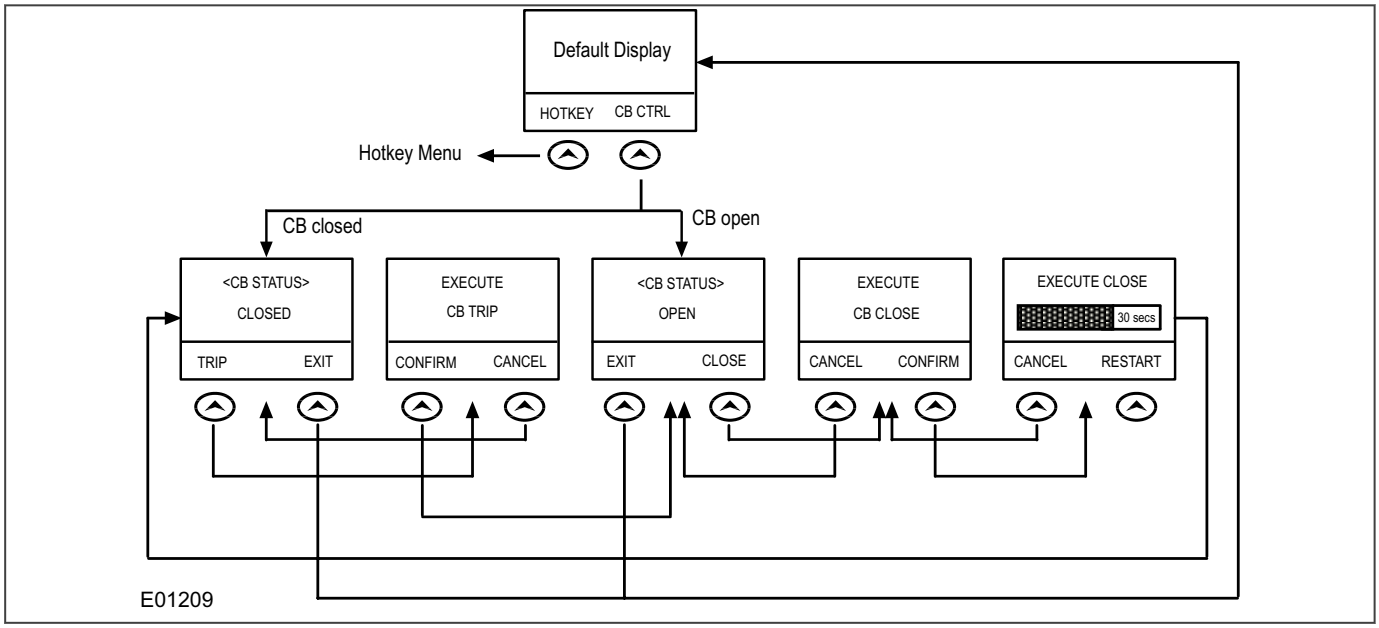


Figure 165: Hotkey menu navigation

13.7.3 CB CONTROL USING THE FUNCTION KEYS

For most models, you can also use the function keys to allow direct control of the circuit breaker. This has the advantage over hotkeys, that the LEDs associated with the function keys can indicate the status of the CB. The

default PSL is set up such that Function key 2 initiates a trip and Function key 3 initiates a close. For this to work you have to set the CB control by cell to option 5 *Opto+Local*, or option 7 *Opto+Local+Remote* in the *CB CONTROL* column.

As shown below, function keys 2 and 3 have already been assigned to CB control in the default PSL.

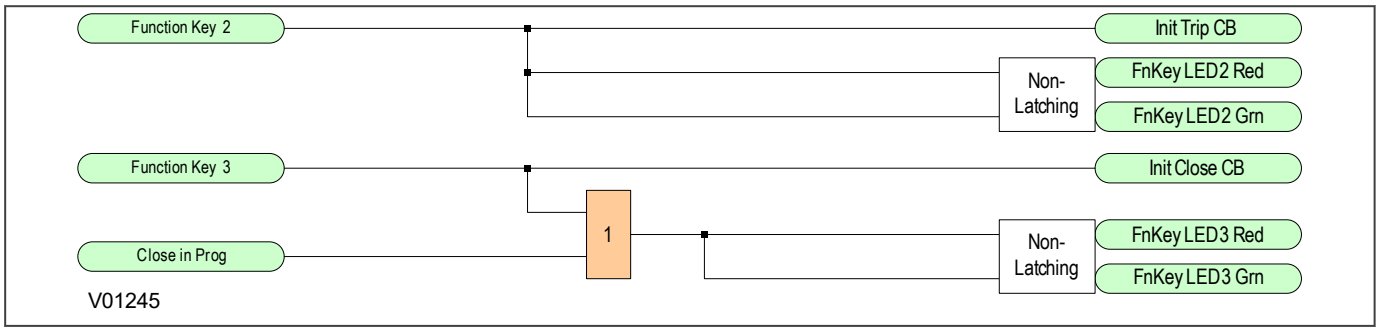


Figure 166: Default function key PSL

The programmable function key LEDs have been mapped such that they will indicate yellow whilst the keys are activated.

Note:
Not all models provide function keys.

13.7.4 CB CONTROL USING THE OPTO-INPUTS

Certain applications may require the use of push buttons or other external signals to control the various CB control operations. It is possible to connect such push buttons and signals to opto-inputs and map these to the relevant DDB signals.

For this to work, you have to set the ***CB control by*** cell to option 4 *opto*, option 5 *Opto+Local*, option 6 *Opto +Remote*, or option 7 *Opto+Local+Remote* in the *CB CONTROL* column.

13.7.5 REMOTE CB CONTROL

Remote CB control can be achieved by setting the ***CB Trip/Close*** cell in the *SYSTEM DATA* column to trip or close by using a command over a communication link.

For this to work, you have to set the ***CB control by*** cell to option 2 *Remote*, option 3 *Local+Remote*, option 6 *Opto+remote*, or option 7 *Opto+Local+Remote* in the *CB CONTROL* column.

We recommend that you allocate separate relay output contacts for remote CB control and protection tripping. This allows you to select the control outputs using a simple local/remote selector switch as shown below. Where this feature is not required the same output contact(s) can be used for both protection and remote tripping.

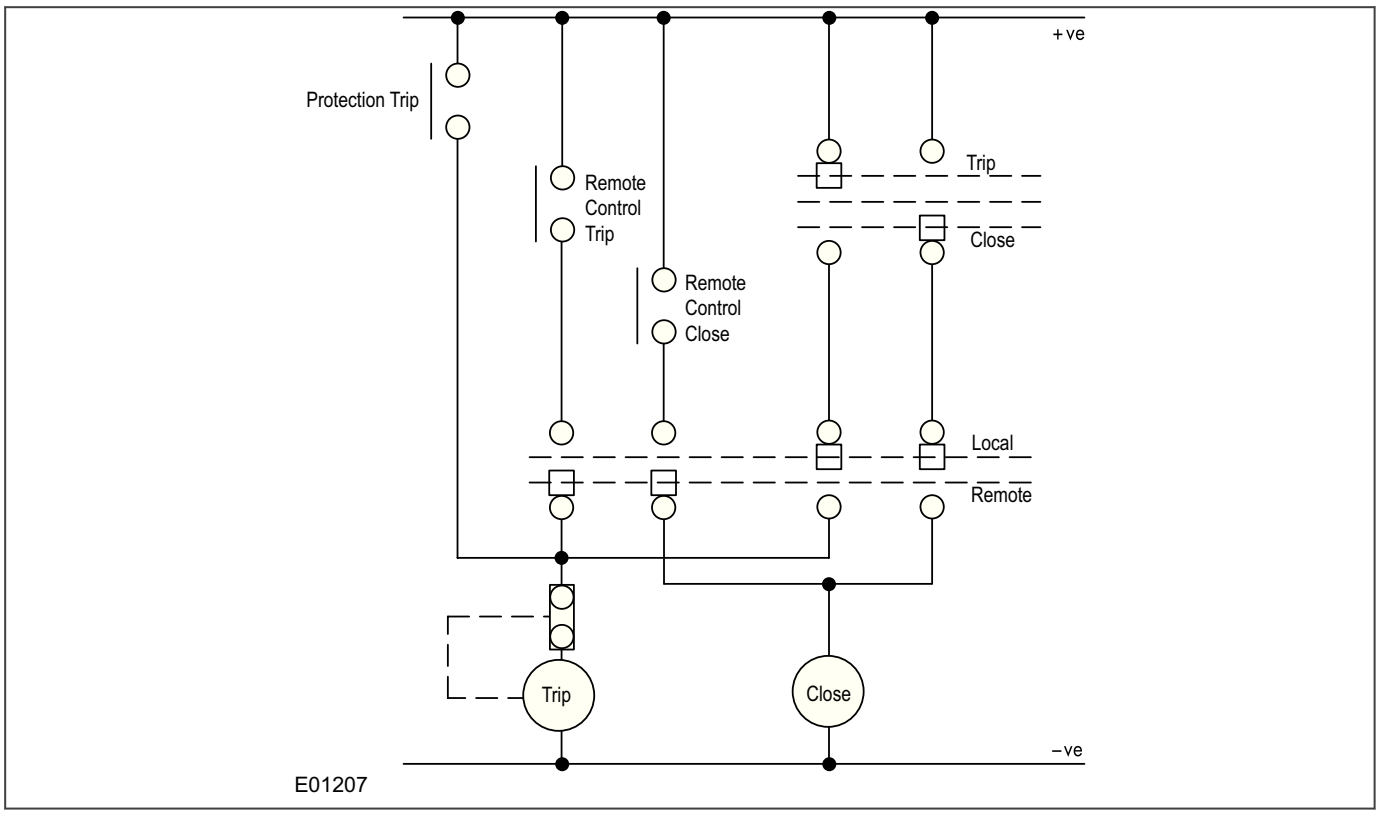


Figure 167: Remote control of circuit breaker

13.7.6 CB HEALTHY CHECK

A CB Healthy check is available if required. This facility accepts an input to one of the opto-inputs to indicate that the breaker is capable of closing (e.g. that it is fully charged). A time delay can be set with the setting ***CB Healthy Time***. If the CB does not indicate a healthy condition within the time period following a Close command, the device will lockout and alarm.

13.7.7 SYNCHRONISATION CHECK

Where the check synchronism function is set, this can be enabled to supervise manual circuit breaker Close commands. A circuit breaker Close command will only be issued if the Check Synchronisation criteria are satisfied. A time delay can be set with the setting ***Sys Check time.*** If the Check Synchronisation criteria are not satisfied within the time period following a Close command the device will lockout and alarm.

13.7.8 CB CONTROL AR IMPLICATIONS

An ***Auto Close CB*** signal from the Auto-close logic bypasses the ***Man Close Delay*** time, and the ***CB Close*** output operates immediately to close the circuit breaker.

If Autoreclose is used it may be desirable to block its operation when performing a manual close. In general, the majority of faults following a manual closure are permanent faults and it is undesirable to allow automatic reclosure.

To ensure that Autoreclose is not initiated for a manual circuit breaker closure on to a pre-existing fault, the ***CB IS Time*** (circuit breaker in service time) setting in the *AUTORECLOSE* menu should be set for the desired time window. This setting ensures that Autoreclose initiation is inhibited for a period equal to setting ***CB IS Time*** following a manual circuit breaker closure. If a protection operation occurs during the inhibit period, Autoreclose is not initiated.

Following manual circuit breaker closure, if either a single phase or a three phase fault occur, the circuit breaker is tripped three phase, but Autoreclose is not locked out for this condition.

13.7.9 CB CONTROL LOGIC DIAGRAM

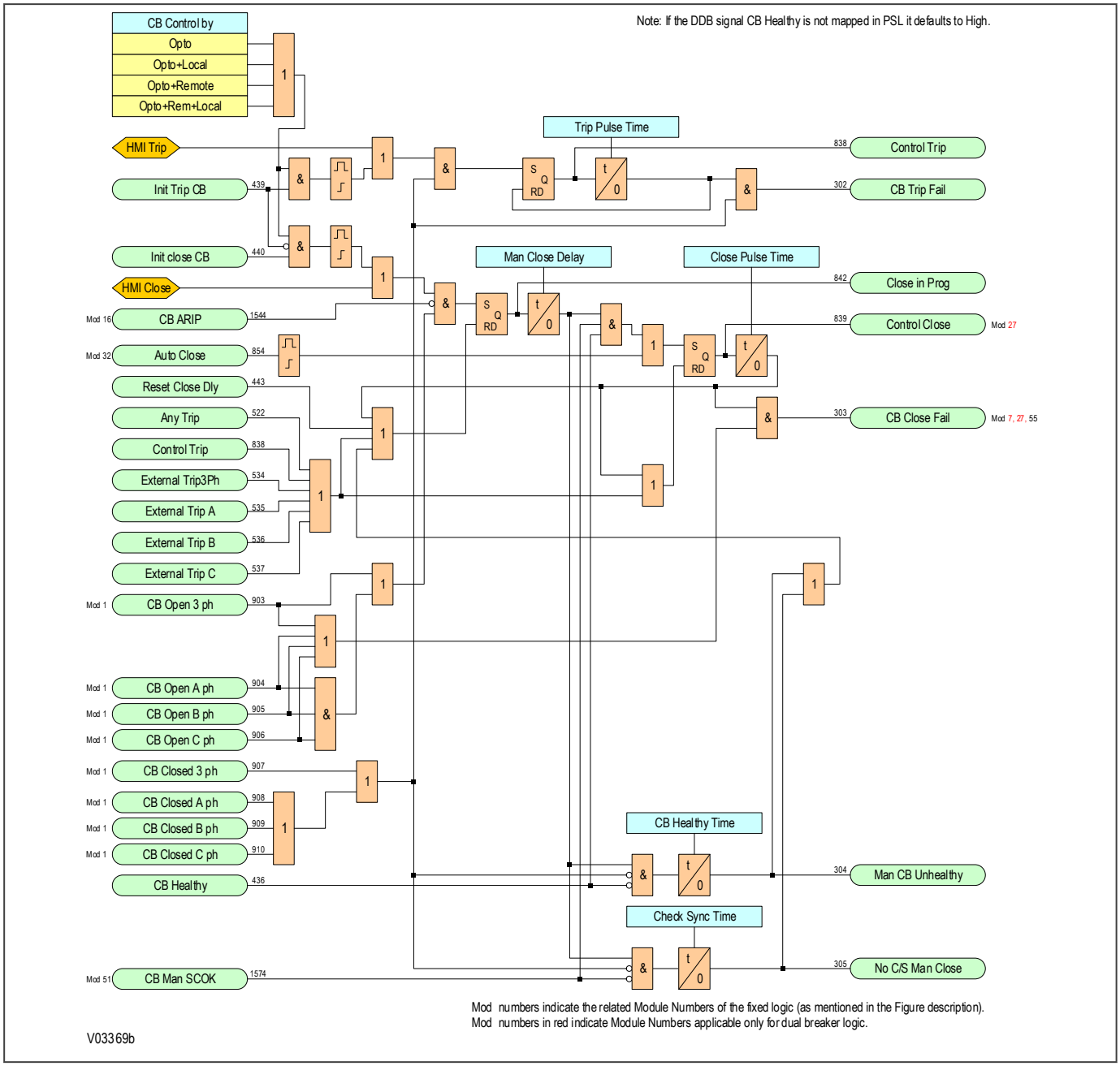


Figure 168: CB control logic (module 43)

13.8 POLE DEAD FUNCTION

The Pole Dead Logic is used to determine and indicate that one or more phases of the line are not energised. A Pole Dead condition is determined either by measuring:

- the line currents and/or voltages*, or
- by monitoring the status of the circuit breaker auxiliary contacts, as shown by dedicated DDB signals.

It can also be used to block operation of underfrequency and undervoltage elements where applicable.

Note:
**P54B, P54C and P54E models only.*

13.8.1 POLE DEAD LOGIC

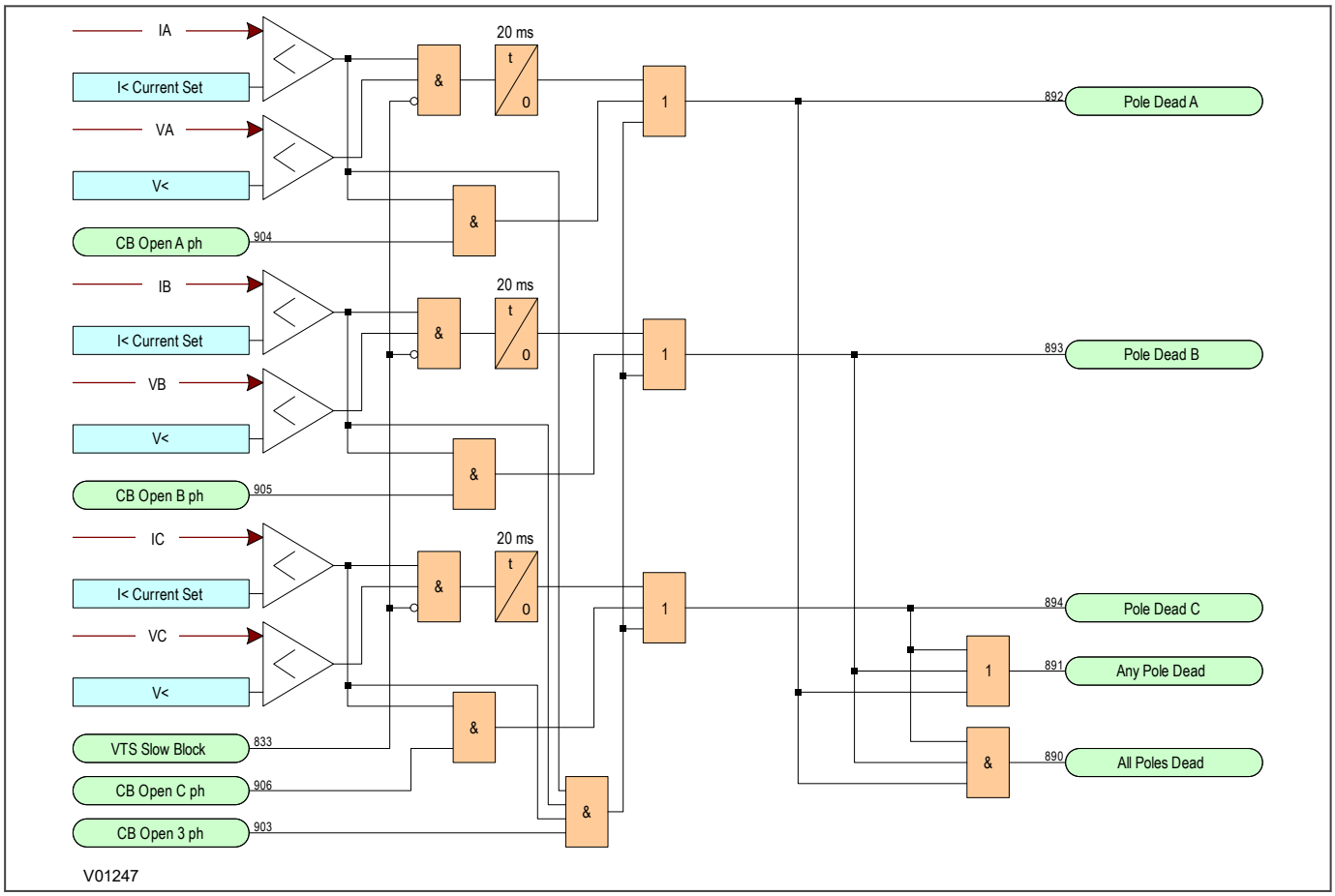


Figure 169: Pole dead logic

If both the line current and voltage values fall below a certain threshold, or a CB Open condition is asserted from the state control logic, the device initiates a Pole Dead condition. The current and voltage thresholds can be set with the ***I< Current Set*** and the ***V< settings*** respectively, in the *CBFAIL&P.DEAD* column.

If one or more poles are dead, the device indicates which phase is dead and asserts the ***Any Pole Dead*** DDB signal. If all phases are dead the ***Any Pole Dead*** signal is accompanied by the ***All Poles Dead*** signal.

If the VT fails, a ***VTS Slow Block*** signal is taken from the VTS logic to block the Pole Dead indications that would be generated by the undervoltage and undercurrent thresholds.

Note:
If the VT is connected at the busbar side, auxiliary contacts (52a or 52b) must be connected to the IED for a correct pole dead indication.

13.9 CB CONDITION MONITORING

The device records various statistics related to each circuit breaker trip operation, allowing an accurate assessment of the circuit breaker condition to be determined. These statistics are available in the *CB CONDITION* column. The menu cells are register values only and cannot be set directly. They may be reset, however, during maintenance. The statistics monitored are:

- Total Current Broken: A register stores the total amount of current that the CB has broken is stored in an accumulator, giving at any time a measure of the total amount of current that the CB has broken since the value was last reset.
- Number of CB operations: A counter registers the number of CB trips that have been performed for each phase, giving at any time the total number of trips that the CB has performed since the value was last reset.
- CB Operate Time: A register stores the total amount of time the CB has transitioned from closed to open is stored in an accumulator, giving at any time a measure of the total time that the CB has spent tripping since the values was last reset.
- Excessive Fault Frequency: A counter registers the number of CB trips that have been performed for all phases, giving at any time the total number of trips performed since the value was last reset.

These statistics are available in the *CB CONDITION* column. The menu cells are register values only and cannot be set directly. They may be reset, however, during maintenance.

> *Note:*
> *When in Commissioning test mode the CB condition monitoring registers are not updated.*

Circuit breaker lockout, can be caused by the following circuit breaker condition monitoring functions:

- Maintenance lockout
- Excessive fault frequency lockout
- Broken current lockout

If the circuit breaker is locked out, the logic generates a lockout alarm

13.10 SYSTEM CHECKS

In some situations it is possible for both "bus" and "line" sides of a circuit breaker to be live when a circuit breaker is open - for example at the ends of a feeder that has a power source at each end. Therefore, it is normally necessary to check that the network conditions on both sides are suitable, before closing the circuit breaker. This applies to both manual circuit breaker closing and autoreclosing. If a circuit breaker is closed when the line and bus voltages are both live, with a large phase angle, frequency or magnitude difference between them, the system could be subjected to an unacceptable shock, resulting in loss of stability, and possible damage to connected machines.

The System Checks functionality involves monitoring the voltages on both sides of a circuit breaker, and if both sides are live, performing a synchronisation check to determine whether any differences in voltage magnitude, phase angle or frequency are within permitted limits.

The pre-closing system conditions for a given circuit breaker depend on the system configuration, and for autoreclosing, on the selected autoreclose program. For example, on a feeder with delayed autoreclosing, the circuit breakers at the two line ends are normally arranged to close at different times. The first line end to close usually has a live bus and a dead line immediately before reclosing. The second line end circuit breaker now sees a live bus and a live line.

If there is a parallel connection between the ends of the tripped feeder the frequencies will be the same, but any increased impedance could cause the phase angle between the two voltages to increase. Therefore just before closing the second circuit breaker, it may be necessary to perform a synchronisation check, to ensure that the phase angle between the two voltages has not increased to a level that would cause unacceptable shock to the system when the circuit breaker closes.

If there are no parallel interconnections between the ends of the tripped feeder, the two systems could lose synchronism altogether and the frequency at one end could "slip" relative to the other end. In this situation, the second line end would require a synchronism check comprising both phase angle and slip frequency checks.

If the second line-end busbar has no power source other than the feeder that has tripped; the circuit breaker will see a live line and dead bus assuming the first circuit breaker has re-closed. When the second line end circuit breaker closes the bus will charge from the live line (dead bus charge).

13.10.1 SYSTEM CHECKS IMPLEMENTATION

The System Checks function provides *Live/Dead Voltage Monitoring*, two stages of *Check Synchronisation* and *System Split* indication.

The System Checks function is enabled or disabled by the ***System Checks*** setting in the *CONFIGURATION* column. If ***System Checks*** is disabled, the *SYSTEM CHECKS* menu becomes invisible, and a ***SysChks Inactive*** DDB signal is set.

The System Checks functionality can also be enabled or disabled by the ***System Checks*** setting in the *SYSTEM CHECKS* column. For the Systems Checks functionality to be enabled, both the ***System Checks*** setting in the *CONFIGURATION* column AND the ***System Checks*** setting in the *SYSTEM CHECKS* column must be enabled. For the System Checks functionality to be disabled, either the ***System Checks*** setting in the *CONFIGURATION* column OR the ***System Checks*** setting in the *SYSTEM CHECKS* column must be enabled. In the latter case, the ***SysChks Inactive*** DDB signal is set.

13.10.1.1 VT CONNECTIONS

The device provides inputs for a three-phase "Main VT" and at least one single-phase VT for check synchronisation. Depending on the primary system arrangement, the Main VT may be located on either the line-side of the busbar-side of the circuit breaker, with the Check Sync VT on the other. Normally, the Main VT is located on the line-side (as per the default setting), but this is not always the case. For this reason, a setting is provided where you can define this. This is the ***Main VT Location*** setting, which is found in the *CT AND VT RATIOS* column.

The Check Sync VT may be connected to one of the phase-to-phase voltages or phase-to-neutral voltages. This needs to be defined using the ***CS Input*** setting in the *CT AND VT RATIOS* column. Options are, A-B, B-C, C-A, A-N, B-N, or C-N.

13.10.1.2 VOLTAGE MONITORING

The settings in the *VOLTAGE MONITORS* sub-heading in the *SYSTEM CHECKS* column allow you to define the threshold at which a voltage is considered live, and a threshold at which the voltage is considered dead. These thresholds apply to both line and bus sides. If the measured voltage falls below the ***Dead Voltage*** setting, a DDB signal is generated (***Dead Bus***, or ***Dead Line***, depending on which side is being measured). If the measured voltage exceeds the ***Live Voltage*** setting, a DDB signal is generated (***Live Bus***, or ***Live Line***, depending on which side is being measured).

13.10.1.3 CHECK SYNCHRONISATION

The device provides two stages of Check Synchronisation. The first stage (CS1) is intended for use in synchronous systems. This means, where the frequencies and phase angles of both sides are compared and if the difference is within set limits, the circuit breaker is allowed to close. The second stage (CS2) is similar to stage, but has an additional adaptive setting. The second stage CS2 is intended for use in asynchronous systems, i.e. where the two sides are out of synchronism and one frequency is slipping continuously with respect to another. If the closing time of the circuit breaker is known, the CB Close command can be issued at a definite point in the cycle such that the CB closes at the point when both sides are in phase.

In situations where it is possible for the voltages on either side of a circuit breaker to be either synchronous or asynchronous, both CS1 and CS2 can be enabled to provide a CB Close signal if either set of permitted closing conditions is satisfied.

Each stage can also be set to inhibit circuit breaker closing if selected blocking conditions such as overvoltage, undervoltage or excessive voltage magnitude difference are detected. CS2 requires the phase angle difference to be decreasing in magnitude before permitting the circuit breaker to close. CS2 has an optional “Adaptive” closing feature, which issues the permissive close signal when the predicted phase angle difference immediately prior to the instant of circuit breaker main contacts closing (i.e. after CB Close time) is as close as practicable to zero.

Slip frequency is the rate of change of phase between each side of the circuit breaker, which is measured by the difference between the voltage signals on either side of the circuit breaker.

Having two system synchronism check stages available allows the circuit breaker closing to be enabled under different system conditions (for example, low slip / moderate phase angle, or moderate slip / small phase angle).

The settings specific to Check Synchronisation are found under the sub-heading *CHECK SYNC* in the *SYSTEM CHECKS* column. The only difference between the CS1 settings and the CS2 settings is that CS2 has a ***CS2 Adaptive*** setting for predictive closure of CB.

13.10.1.4 CHECK SYNCRONISATION VECTOR DIAGRAM

The following vector diagram represents the conditions for the System Check functionality. The Dead Volts setting is represented as a circle around the origin whose radius is equal to the maximum voltage magnitude, whereby the voltage can be considered dead. The nominal line voltage magnitude is represented by a circle around the origin whose radius is equal to the nominal line voltage magnitude. The minimum voltage magnitude at which the system can be considered as Live, is the magnitude difference between the bus and line voltages.

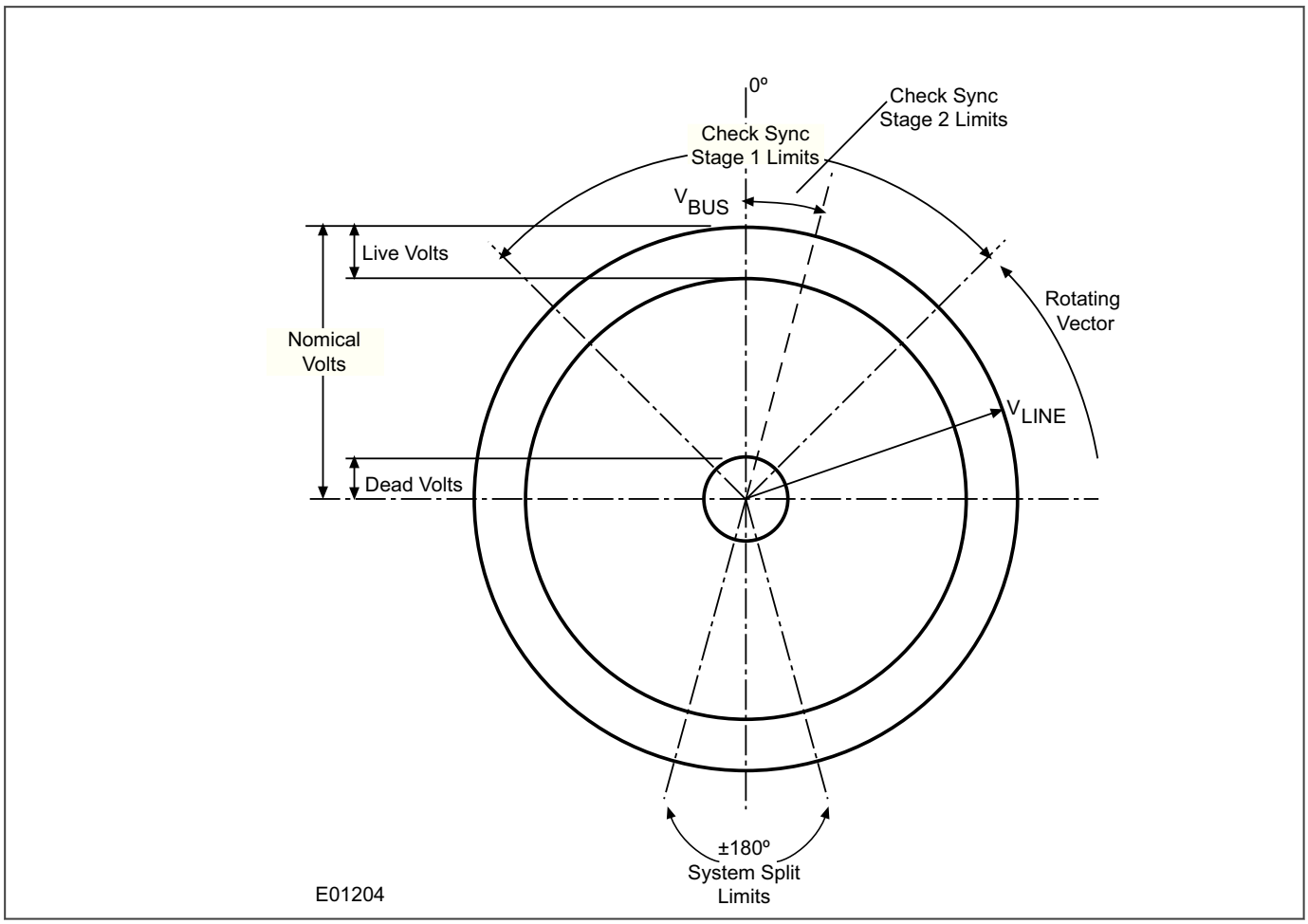


Figure 170: Check synchronisation vector

13.10.2 VOLTAGE MONITOR FOR CB CLOSURE

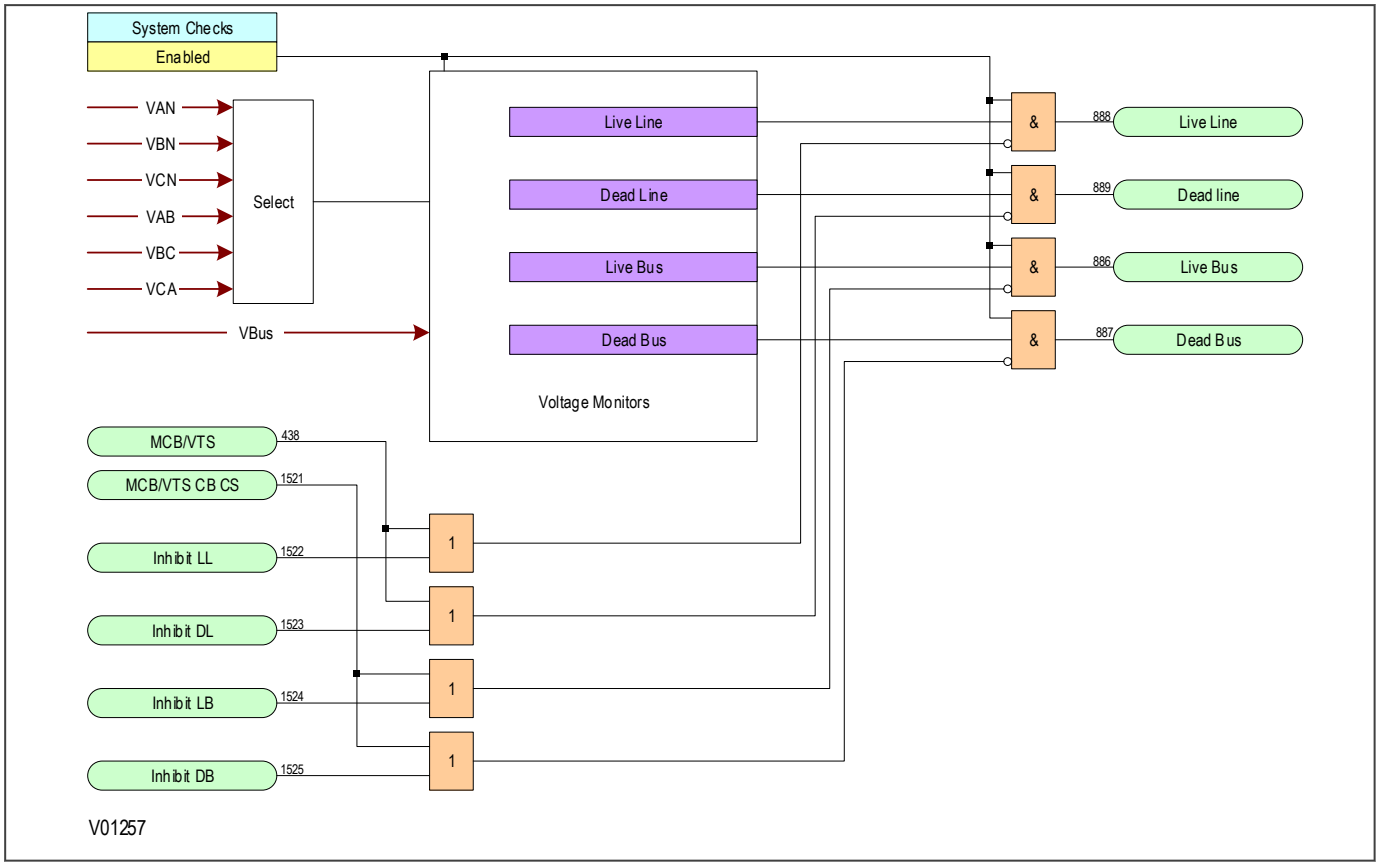


Figure 171: Voltage monitor for CB closure (module 59)

13.10.3 CHECK SYNCHRONISATION MONITOR FOR CB CLOSURE

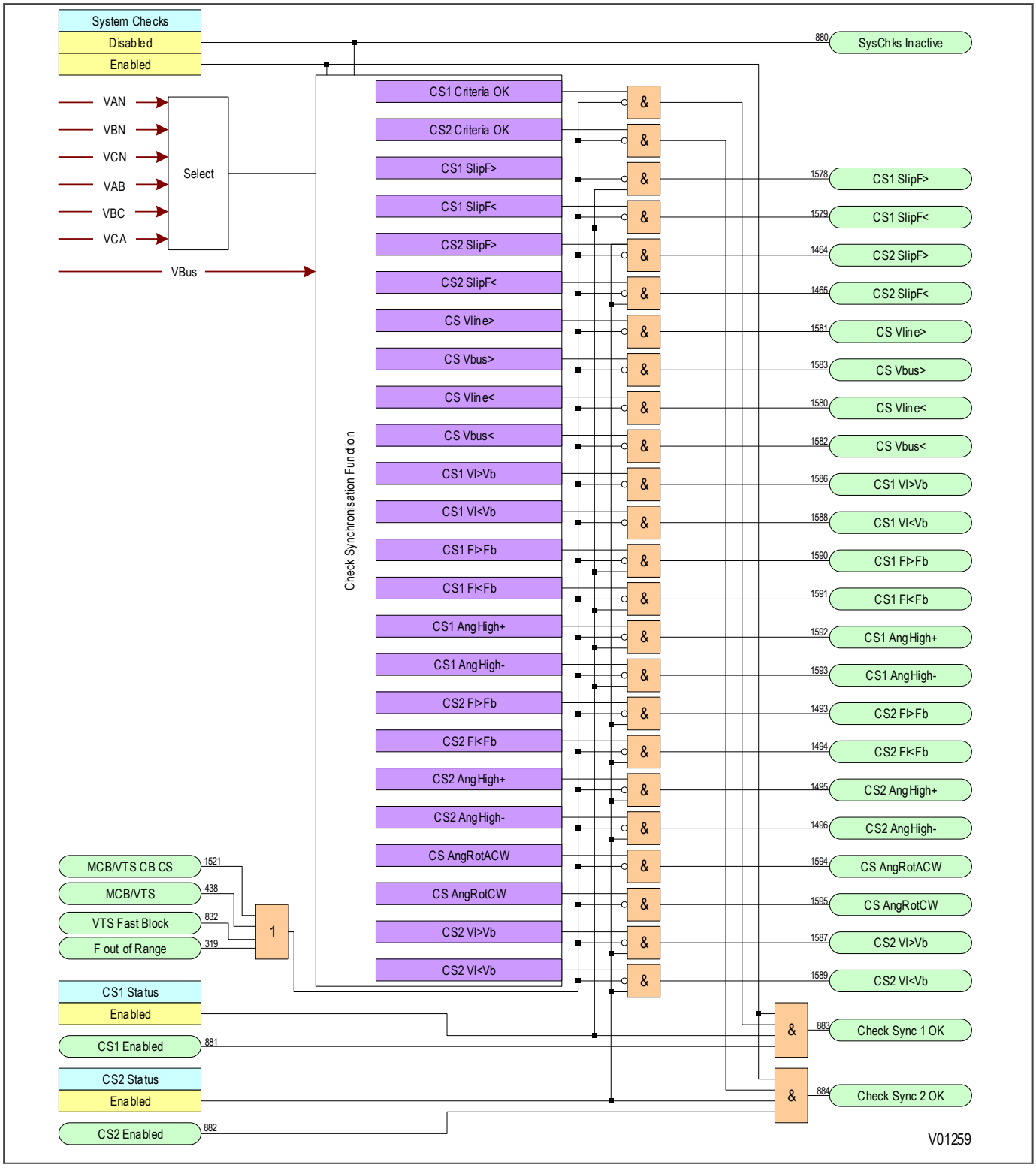


Figure 172: Check synchronisation monitor for CB closure (module 60)

13.10.4 SYSTEM CHECK PSL

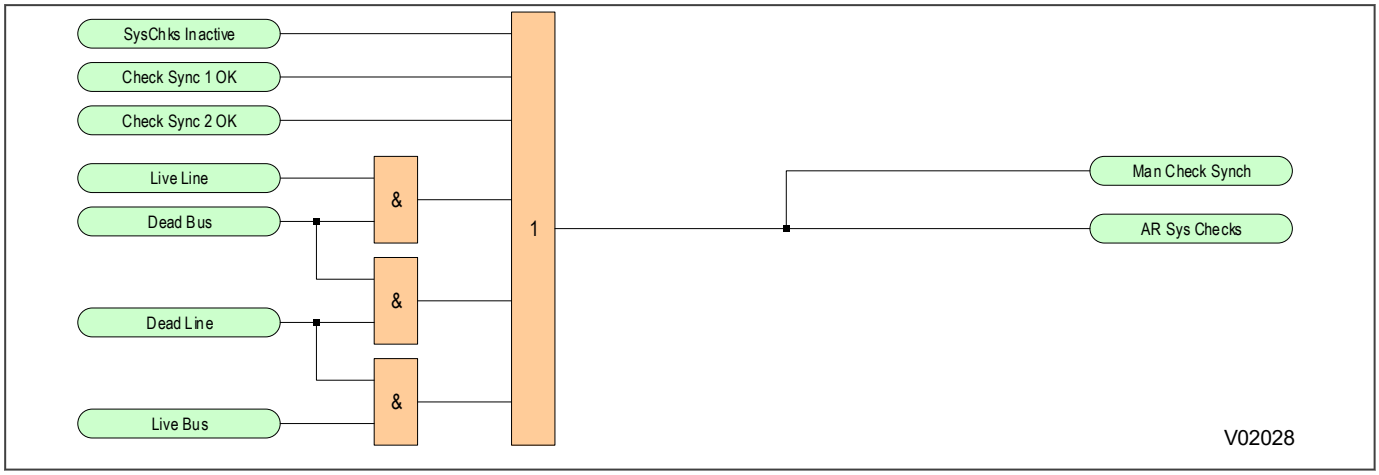


Figure 173: System check PSL

13.10.5 APPLICATION NOTES

13.10.5.1 PREDICTIVE CLOSURE OF CIRCUIT BREAKER

The ***CS2 Adaptive*** setting compensates for the time taken to close the CB. When set to provide CB Close Time compensation, a predictive approach is used to close the circuit breaker ensuring that closing occurs at close to 0º therefore minimising the impact to the power system. The actual closing angle is subject to the constraints of the existing product architecture, i.e. the protection task runs twice per power system cycle, based on frequency tracking over the frequency range of 40 Hz to 65 Hz.

13.10.5.2 VOLTAGE AND PHASE ANGLE CORRECTION

For the Check Synchronisation function, the device needs to convert measured secondary voltages into primary voltages. In some applications, VTs either side of the circuit breaker may have different VT Ratios. In such cases, a magnitude correction factor is required.

There are some applications where the main VT is on the HV side of a transformer and the Check Sync VT is on the LV side, or vice-versa. If the vector group of the transformer is not "0", the voltages are not in phase, so phase correction is also necessary.

The correction factors are as follows and are located in the *CT AND VT RATIOS* column:

- C/S V kSM, where kSM is the voltage correction factor.
- C/S Phase kSA, where kSA is the angle correction factor.

Assuming C/S input setting is A-N, then:

The line and bus voltage magnitudes are matched if $V_{a\ sec} = V_{cs\ sec}$ x C/S V kSA

The line and bus voltage angles are matched if $\angle V_{a\ sec} = \angle V_{cs\ sec}$ + C/S Phase kSA

The following application scenarios show where the voltage and angular correction factors are applied to match different VT ratios:

Scenario	Physical Ratios (ph-N Values)				Setting Ratios				CS Correction Factors	
	Main VT Ratio		CS VT Ratio		Main VT Ratio (ph-ph) Always		CS VT Ratio		kSM	kSA
	Pri (kV)	Sec (V)	Pri (kV)	Sec (V)	Pri (kV)	Sec (V)	Pri (kV)	Sec (V)		
1	220/√3	110/√3	132/√3	100/√3	220	110	132	100	1.1	30º
2	220/√3	110/√3	220/√3	110	220	110	127	110	0.577	0º

Scenario	Physical Ratios (ph-N Values)				Setting Ratios				CS Correction Factors	
	Main VT Ratio		CS VT Ratio		Main VT Ratio (ph-ph) Always		CS VT Ratio		kSM	kSA
	Pri (kV)	Sec (V)	Pri (kV)	Sec (V)	Pri (kV)	Sec (V)	Pri (kV)	Sec (V)		
3	220/√3	110/√3	220/√3	110/3	220	110	381	110	1.732	0°

CHAPTER 14

SUPERVISION

14.1 CHAPTER OVERVIEW

This chapter describes the supervison functions.

This chapter contains the following sections:

Chapter Overview 298
Voltage Transformer Supervision 299
Current Transformer Supervision 303
Trip Circuit Supervision 307

14.2 VOLTAGE TRANSFORMER SUPERVISION

The Voltage Transformer Supervision (VTS) function is used to detect failure of the AC voltage inputs to the protection. This may be caused by voltage transformer faults, overloading, or faults on the wiring, which usually results in one or more of the voltage transformer fuses blowing.

If there is a failure of the AC voltage input, the IED could misinterpret this as a failure of the actual phase voltages on the power system, which could result in unnecessary tripping of a circuit breaker.

The VTS logic is designed to prevent such a situation by detecting voltage input failures, which are NOT caused by power system phase voltage failure, and automatically blocking associated voltage dependent protection elements. A time-delayed alarm output is available to warn of a VTS condition.

The following scenarios are possible with respect to the failure of the VT inputs.

- Loss of one or two-phase voltages
- Loss of all three-phase voltages under load conditions
- Absence of three-phase voltages upon line energisation

14.2.1 LOSS OF ONE OR TWO PHASE VOLTAGES

If the power system voltages are healthy, no Negative Phase Sequence (NPS) current will be present. If however, one or two of the AC voltage inputs are missing, there will be Negative Phase Sequence voltage present, even if the actual power system phase voltages are healthy. VTS works by detecting Negative Phase Sequence (NPS) voltage without the presence of Negative Phase Sequence current. So if there is NPS voltage present, but no NPS current, it is certain that there is a problem with the voltage transformers and a VTS block should be applied to voltage dependent protection functions to prevent maloperation. The use of negative sequence quantities ensures correct operation even where three-limb or V-connected VTs are used.

Note:
Voltage transformer supervision functionality is available in P54B, P54C and P54E models only.

The Negative Sequence VTS Element is blocked by the ***Any Pole Dead*** DDB signal during ***SP AR Dead Time***. The resetting of the blocking signal is delayed by 240 ms after an ***Any Pole Dead*** condition disappears.

14.2.2 LOSS OF ALL THREE PHASE VOLTAGES

If all three voltage inputs are lost, there will be no Negative Phase Sequence quantities present, but the device will see that there is no voltage input. If this is caused by a power system failure, there will be a step change in the phase currents. However, if this is not caused by a power system failure, there will be no change in any of the phase currents. So if there is no measured voltage on any of the three phases and there is no change in any of the phase currents, this indicates that there is a problem with the voltage transformers and a VTS block should be applied to voltage dependent protection functions to prevent maloperation.

To avoid blocking VTS due to changing load condition, the superimposed current signal can only prevent operation of the VTS during the time window of 40 ms following the voltage collapse.

14.2.3 ABSENCE OF ALL THREE PHASE VOLTAGES ON LINE ENERGISATION

On line energisation there should be a change in the phase currents as a result of loading or line charging current. Under this condition we need an alternative method of detecting three-phase VT failure.

If there is no measured voltage on all three phases during line energisation, two conditions might apply:

- A three-phase VT failure
- A three-phase fault.

The first condition would require VTS to block the voltage-dependent functions.

In the second condition, voltage dependent functions should not be blocked, as tripping is required.

To differentiate between these two conditions an overcurrent level detector is used (***VTS I> Inhibit***). This prevents a VTS block from being issued in case of a genuine fault. This overcurrent level detector is only enabled for 240 ms following line energisation (based on an ***All Poles Dead*** signal drop off). It must still be set below any three-phase fault along the line.

If the line is closed where a three-phase VT failure is present, the overcurrent detector will not operate and a VTS block will be applied. Closing onto a three-phase fault will result in operation of the overcurrent detector and prevent a VTS block being applied.

14.2.4 VTS IMPLEMENTATION

VTS is implemented in the *SUPERVISION* column of the relevant settings group.

The following settings are relevant for VT Supervision:

- ***VTS Mode***: determines the mode of operation (Measured + MCB, Measured Only, MCB Only)
- ***VTS Status***: determines whether the VTS Operate output will be a blocking output or an alarm indication only
- ***VTS Reset Mode***: determines whether the Reset is to be manual or automatic
- ***VTS Time Delay***: determines the operating time delay
- ***VTS I> Inhibit***: inhibits VTS operation in the case of a phase overcurrent fault
- ***VTS I2> Inhibit***: inhibits VTS operation in the case of a negative sequence overcurrent fault

For faults with I2 less than the setting ***VTS I2 Inhibit***, VTS will be active and block the associated functions if sufficient V2 is measured. VTS is only enabled during a live line condition (as indicated by the pole dead logic) to prevent operation under dead system conditions.

Thresholds

The negative sequence thresholds used by the element are:

- V2 = 10 V (fixed)
- I2 = 0.05 to 0.5 In settable (default 0.05 In).

The phase voltage level detectors are:

- Drop off = 10 V (fixed)
- Pickup = 30 V (fixed)

The sensitivity of the superimposed current elements is fixed at 0.1 In.

Fuse fail

The device includes a setting (***VT Connected***) in the *CT AND VT RATIOS* column, which determines whether there are voltage transformers connected to it. If set to `No`, this setting has no effect.

If set to `No` it causes the VTS logic to set the ***VTS Slow Block*** and ***VTS Fast Block*** DDBs, but not raise any alarms. It also disables the VTS function. This prevents the pole dead logic working incorrectly if there is no voltage or current. It also blocks the distance, under voltage and other voltage-dependant functions. However, it does not affect the CB open part of the logic.

A VTS condition can be raised by a mini circuit breaker (MCB) status input, by internal logic using IED measurement, or both. The setting ***VTS Mode*** is used to select the method of indicating VT failure.

14.2.5 VTS LOGIC

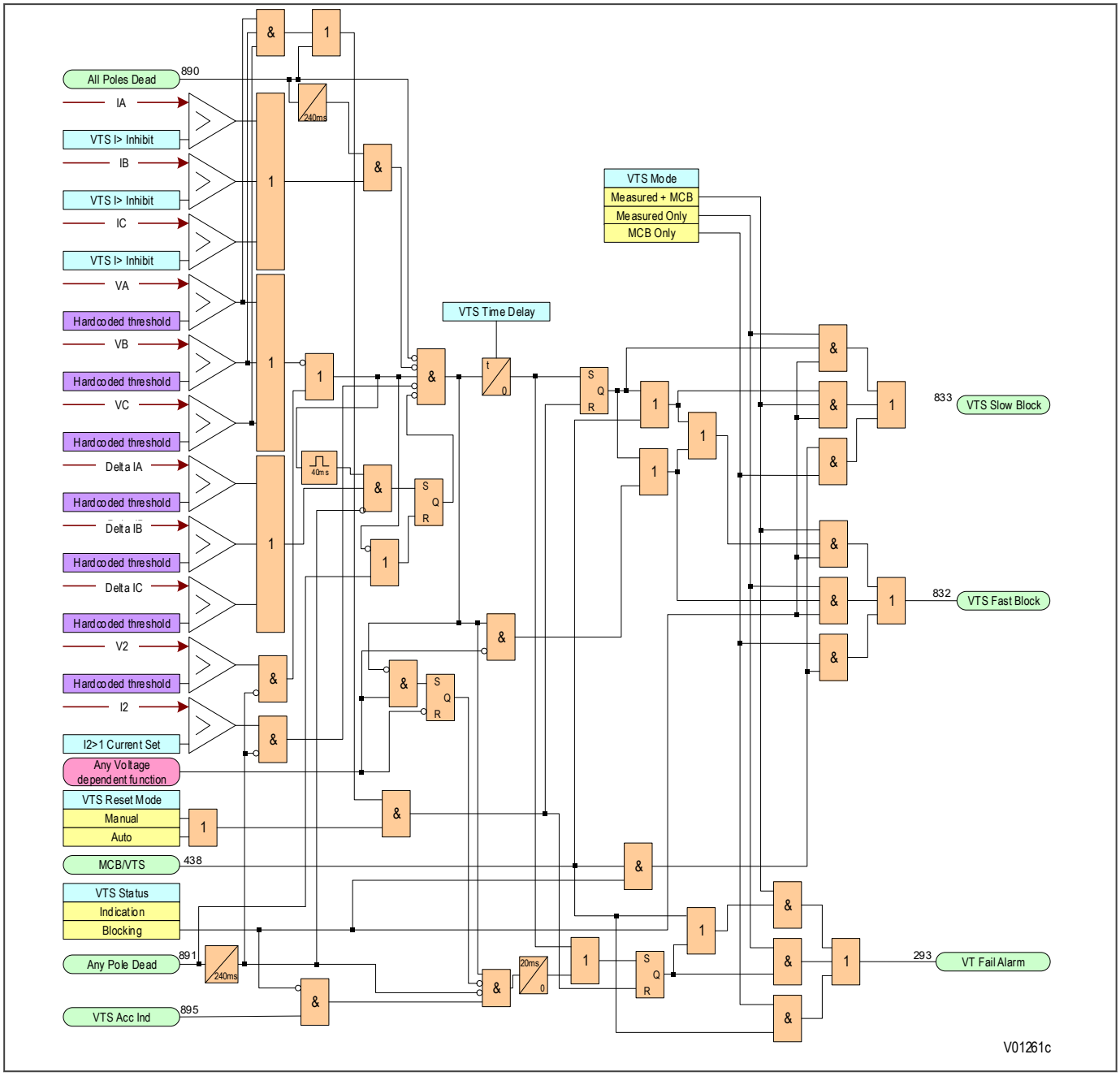


Figure 174: VTS logic

The IED may respond as follows, on operation of any VTS element:

- VTS set to provide alarm indication only
- Optional blocking of voltage-dependent protection elements
- Optional conversion of directional overcurrent elements to non-directional protection (by setting the relevant current protection status cells to `Enabled VTS`. In this case, the directional setting cells are automatically set to `non-directional`.)

The ***VTS I> Inhibit*** or ***VTS I2> Inhibit*** elements are used to override a VTS block if a fault occurs that could trigger the VTS logic. However, once the VTS block is set, subsequent system faults must not override the block. Therefore the VTS block is latched after a settable time delay (***VTS Time Delay***). Once the signal has latched, there are two

methods of resetting. The first is manually using the front panel HMI, or remote communications (if the VTS condition has been removed). The second is in Auto mode, by restoring the 3 phase voltages above the phase level detector settings mentioned previously.

VTS Status can be set to `Disabled`, `Blocking` or `Indication`. If ***VTS Status*** is set to `Blocking`, a VTS condition will block operation of the relevant protection elements. In this case, a VTS indication is given after the ***VTS Time Delay*** has expired. If it is set to `Indication`, their is a risk of maloperation because protection elements are not blocked. In this case the VTS indication is given before the ***VTS Time Delay*** expires, if a trip signal is given (in this case a signal from the VTS acceleration logic is used as an input).

This scheme also operates correctly under very low load or even no load conditions. To achieve this, it uses a combination of time delayed signals derived from the DDB signals ***VTS Fast Block*** and ***All Poles Dead***, to generate the distance blocking DDB signal called ***VTS Blk Distance.***

Note:
*All non-distance voltage-dependent elements are blocked by the **VTS Fast Block** DDB.*

If a miniature circuit breaker (MCB) is used to protect the voltage transformer output circuits, MCB auxiliary contacts can be used to indicate a three-phase output disconnection. It is possible for the VTS logic to operate correctly without this input, but this facility has been provided to maintain compatibility with some practises. Energising an opto-isolated input assigned to the ***MCB/VTS*** provides the necessary block.

The VTS function is inhibited if:

- An ***All Poles Dead*** DDB signal is present
- Any phase overcurrent condition exists
- A Negative Phase Sequence current exists
- If the phase current changes over the period of 1 cycle

14.3 CURRENT TRANSFORMER SUPERVISION

The Current Transformer Supervision function (CTS) is used to detect failure of the AC current inputs to the protection. This may be caused by internal current transformer faults, overloading, or faults on the wiring. If there is a failure of the AC current input, the protection could misinterpret this as a failure of the actual phase currents on the power system, which could result in maloperation. Also, an open circuit in the AC current circuits can cause dangerous CT secondary voltages to be generated.

The IED has two methods of providing Current Transformer Supervision (CTS); differential and standard. The differential method uses the ratio between positive and negative sequence currents to determine CT failure. This method is not voltage dependant and relies on channel communications to declare a CTS condition.

The standard method relies on local measurements of zero sequence currents and voltages. You select the method according to the application. Both methods can be applied individually or in parallel.

The ***CTS Mode*** setting in the *SUPERVISION* column is used to set the method. The options are:

- Disabled
- Standard
- Idiff
- Idiff + Std

The ***CTS Reset Mode*** setting determines whether the CTS will reset automatically or will need manual intervention.

Note:
The P54A model has Disabled and Idiff settings only.

14.3.1 DIFFERENTIAL CTS

Differential CTS does not need any local voltage measurements to determine a CTS condition. It is based on measurement of the ratio of negative sequence current to positive sequence current (I2/I1) at all line ends. When this ratio is small (theoretically zero), one of four possible conditions apply:

- The system is unloaded (both I2 and I1 are zero)
- The system is loaded but balanced (I2 is zero)
- The system has a three phase fault present (I2 is zero)
- There is a genuine 3 phase CT problem (unlikely, but if this is the case it would probably develop from a single or two phase condition)

If the ratio is non-zero, we can assume one of two conditions are present:

- The system has an unbalanced fault (both I2 and I1 are non-zero)
- There is a 1 or 2 phase CT problem (both I2 and I1 are non-zero)

Measurement at a single end cannot provide any more information than this. However, if the ratio is calculated at all ends and compared, the device can make a decision based on the following criteria:

- If the ratio is non-zero at more than two ends, it is almost certainly a genuine fault condition and so the CT supervision is prevented from operating.
- If the ratio is non-zero at one end, there is a chance of either a CT problem or a single-end fed fault condition.

A second criterion looks to see whether the differential system is loaded or not. For this purpose the device looks at the positive sequence current I1. If load current is detected at one-end only, the device assumes that this is an internal fault condition and prevents CTS operation. However, if load current is detected at two or more ends, this indicates CT failure, so CTS operation is allowed.

There are two modes of operation, `Indication` and `Restrain`. You determine the mode of operation with the ***CTS Status*** setting. In `Indication` mode, a CTS alarm is raised but there is no effect on tripping. In `Restrain`

mode, the differential protection is blocked for 20 ms after CT failure detection, then the Current Differential threshold setting is raised above the load current.

For correct operation of the scheme, Differential CTS must be enabled at each end of the protected zone.

14.3.2 DIFFERENTIAL CTS LOGIC

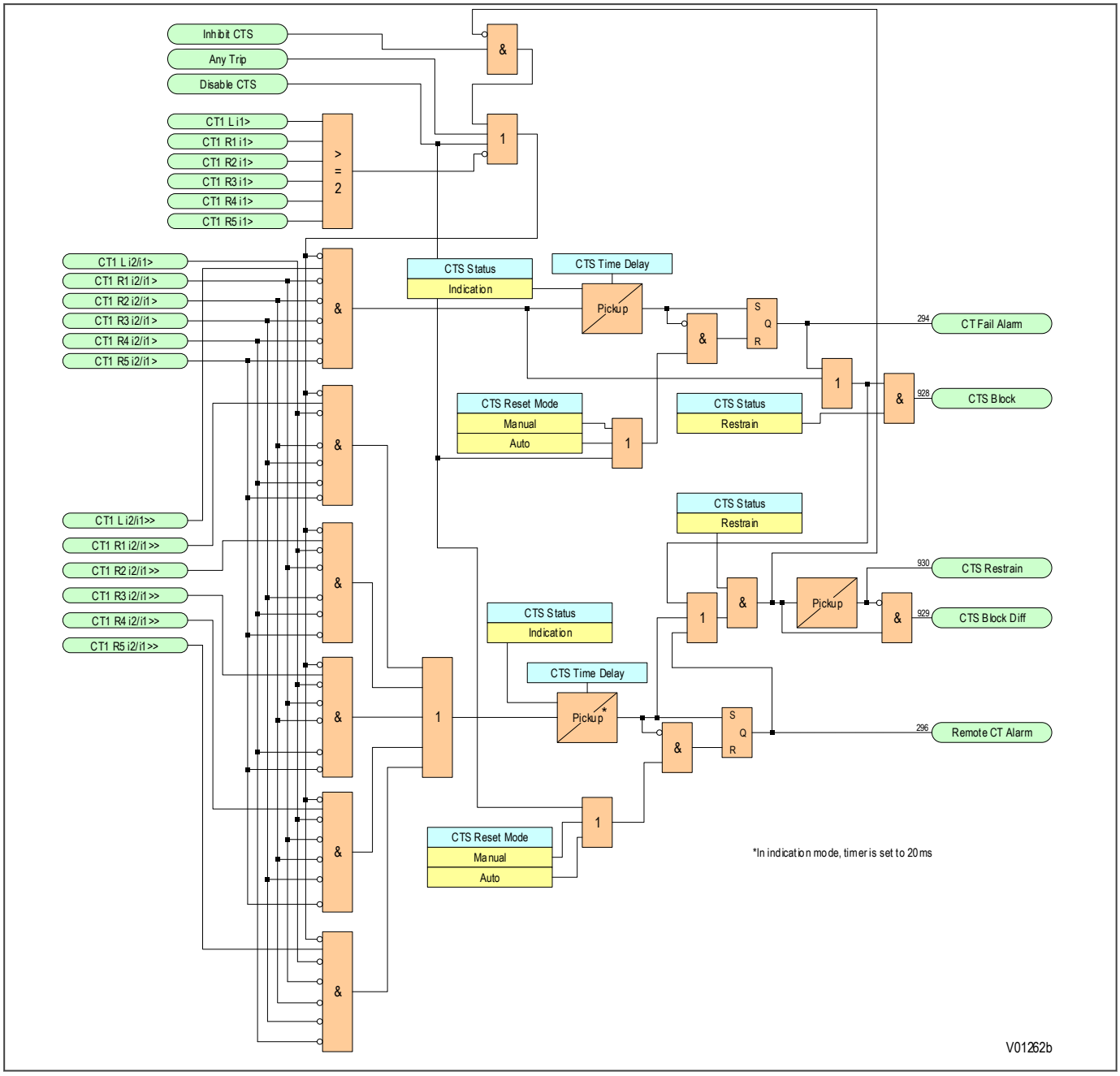


Figure 175: 'Differential' CT supervision logic

14.3.3 STANDARD CTS IMPLEMENTATION

If the power system currents are healthy, no zero sequence voltage are derived. However, if one or more of the AC current inputs are missing, a zero sequence current would be derived, even if the actual power system phase currents are healthy. Standard CTS works by detecting a derived zero sequence current where there is no corresponding derived zero sequence voltage.

The voltage transformer connection used must be able to refer zero sequence voltages from the primary to the secondary side. Therefore, this element should only be enabled where the VT is of a five-limb construction, or comprises three single-phase units with the primary star point earthed.

The CTS function is implemented in the *SUPERVISION* column of the relevant settings group, under the sub-heading *CT SUPERVISION*.

The following settings are relevant for CT Supervision:

- ***CTS Status***: to disable or enable CTS
- ***CTS VN< Inhibit***: inhibits CTS if the zero sequence voltage exceeds this setting
- ***CTS IN> Set***: determines the level of zero sequence current
- ***CTS Time Delay***: determines the operating time delay

14.3.4 STANDARD CTS LOGIC

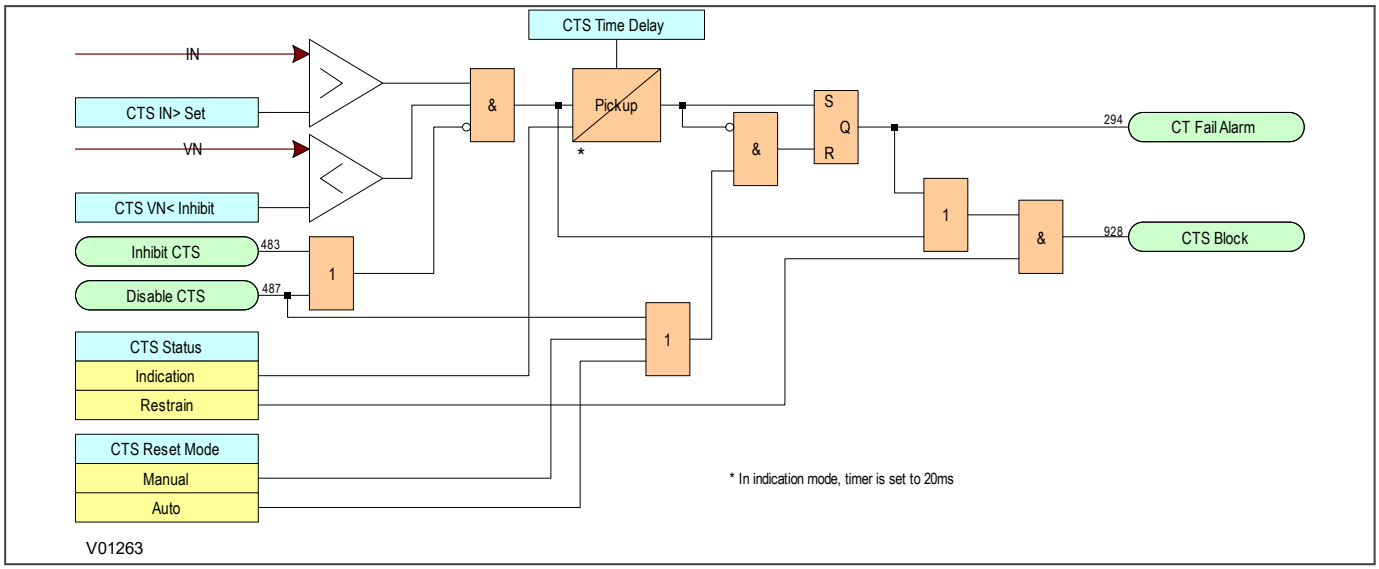


Figure 176: 'Standard' CT supervision logic

Note:
Available in P54b, P54C and P54E models only.

14.3.5 CTS BLOCKING

Both the standard and differential CTS methods block protection elements operating from derived quantities, such as Broken conductor, derived earth fault and negative sequence overcurrent. Measured quantities such as DEF can be selectively blocked by designing an appropriate PSL scheme.

Differential CTS can be used to restrain the differential protection if required.

14.3.6 APPLICATION NOTES

14.3.6.1 SETTING GUIDELINES

The residual voltage setting, ***CTS VN< Inhibit*** and the residual current setting, ***CTS IN> Set***, should be set to avoid unwanted operation during healthy system conditions. For example:

- ***CTS VN< Inhibit*** should be set to 120% of the maximum steady state residual voltage.
- ***CTS IN> Set*** will typically be set below minimum load current.
- ***CTS Time Delay*** is generally set to 5 seconds.

Where the magnitude of residual voltage during an earth fault is unpredictable, the element can be disabled to prevent protection elements being blocked during fault conditions.

14.3.6.2 DIFFERENTIAL CTS SETTING GUIDELINES

The ***Phase Is1 CTS*** setting must be set above the phase current of the maximum load transfer expected, normally at 1.2 In. This setting defines the minimum pick-up level of the current differential protection once the current transformer supervision CTS is detected.

The ***CTS i1>*** setting, once exceeded, indicates that the circuit is loaded. A default setting of 0.1 In is considered suitable for most applications, but could be lowered in case of oversized CTs.

The ***CTS i2/i1>*** setting should be in excess of the worst unbalanced load expected in the circuit under normal operation. It is recommended to read out the values of i2 and i1 in the *MEASUREMENTS 1* column and set the ratio above 5% of the actual ratio.

The ***CTS i2/i1>>*** setting should be kept at the default setting (40% In). If the ratio i2/i1 exceeds the value of this setting at only one end, the CT failure is declared.

> *Note:*
> *The minimum generated i2/i1 ratio will be 50% (case of one CT secondary phase lead being lost), and therefore a setting of 40% is considered appropriate to guarantee sufficient operating speed.*

14.4 TRIP CIRCUIT SUPERVISION

In most protection schemes, the trip circuit extends beyond the IED enclosure and passes through components such as links, relay contacts, auxiliary switches and other terminal boards. Such complex arrangements may require dedicated schemes for their supervision.

There are two distinctly separate parts to the trip circuit; the trip path, and the trip coil. The trip path is the path between the IED enclosure and the CB cubicle. This path contains ancillary components such as cables, fuses and connectors. A break in this path is possible, so it is desirable to supervise this trip path and to raise an alarm if a break should appear in this path.

The trip coil itself is also part of the overall trip circuit, and it is also possible for the trip coil to develop an open-circuit fault.

This product supports a number of trip circuit supervision (TCS) schemes.

14.4.1 TRIP CIRCUIT SUPERVISION SCHEME 1

This scheme provides supervision of the trip coil with the CB open or closed, however, it does not provide supervision of the trip path whilst the breaker is open. The CB status can be monitored when a self-reset trip contact is used. However, this scheme is incompatible with latched trip contacts, as a latched contact will short out the opto-input for a time exceeding the recommended Delayed Drop-off (DDO) timer setting of 400 ms, and therefore does not support CB status monitoring. If you require CB status monitoring, further opto-inputs must be used.

Note:
A 52a CB auxiliary contact follows the CB position. A 52b auxiliary contact is the opposite.

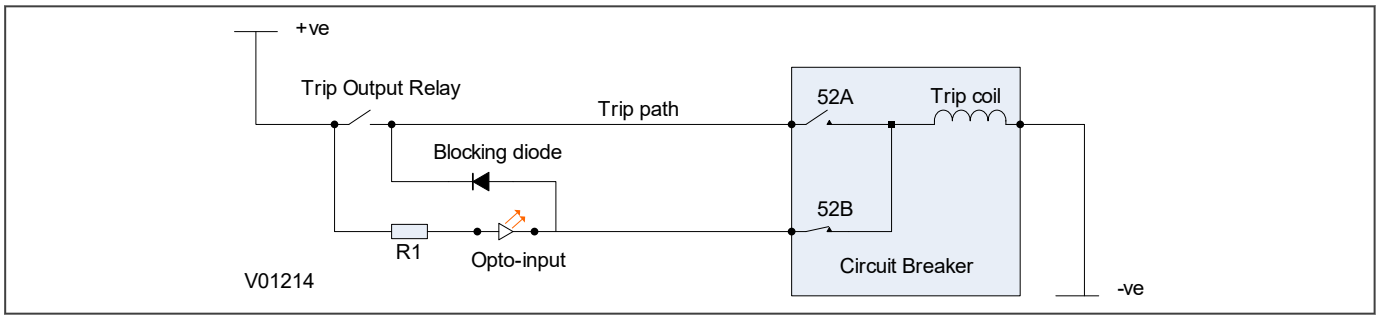


Figure 177: TCS scheme 1

When the CB is closed, supervision current passes through the opto-input, blocking diode and trip coil. When the CB is open, supervision current flows through the opto-input and into the trip coil via the 52b auxiliary contact. This means that *Trip Coil* supervision is provided when the CB is either closed or open, however *Trip Path* supervision is only provided when the CB is closed. No supervision of the trip path is provided whilst the CB is open (pre-closing supervision). Any fault in the trip path will only be detected on CB closing, after a 400 ms delay.

14.4.1.1 RESISTOR VALUES

The supervision current is a lot less than the current required by the trip coil to trip a CB. The opto-input limits this supervision current to less than 10 mA. If the opto-input were to be short-circuited however, it could be possible for the supervision current to reach a level that could trip the CB. For this reason, a resistor R1 is often used to limit the current in the event of a short-circuited opto-input. This limits the current to less than 60mA. The table below shows the appropriate resistor value and voltage setting for this scheme.

Trip Circuit Voltage	Opto Voltage Setting with R1 Fitted	Resistor R1 (ohms)
48/54	24/27	1.2k
110/125	48/54	2.7k
220/250	110/125	5.2k

Warning:
This Scheme is not compatible with Trip Circuit voltages of less than 48 V.

14.4.1.2 PSL FOR TCS SCHEME 1

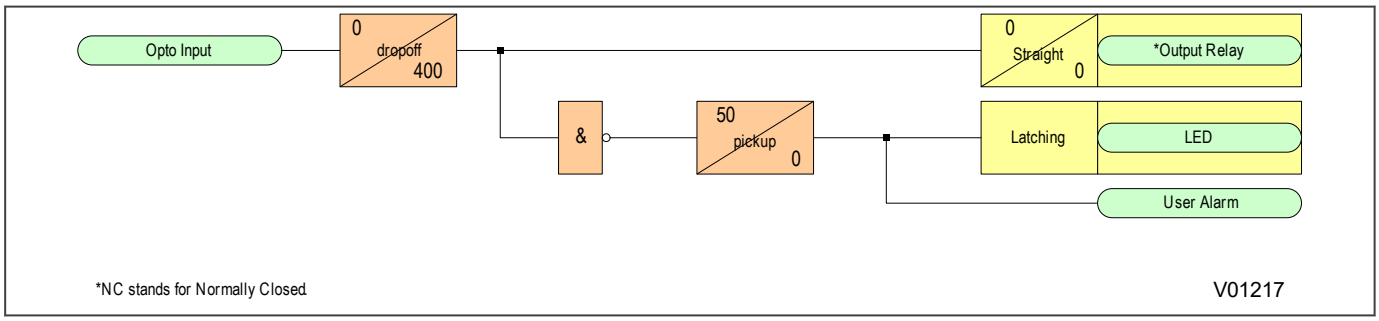


Figure 178: PSL for TCS scheme 1

The opto-input can be used to drive a Normally Closed Output Relay, which in turn can be used to drive alarm equipment. The signal can also be inverted to drive a latching programmable LED and a user alarm DDB signal.

The DDO timer operates as soon as the opto-input is energised, but will take 400 ms to drop off/reset in the event of a trip circuit failure. The 400 ms delay prevents a false alarm due to voltage dips caused by faults in other circuits or during normal tripping operation when the opto-input is shorted by a self-reset trip contact. When the timer is operated the NC (normally closed) output relay opens and the LED and user alarms are reset.

The 50 ms delay on pick-up timer prevents false LED and user alarm indications during the power up time, following a voltage supply interruption.

14.4.2 TRIP CIRCUIT SUPERVISION SCHEME 2

This scheme provides supervision of the trip coil with the breaker open or closed but does not provide pre-closing supervision of the trip path. However, using two opto-inputs allows the IED to correctly monitor the circuit breaker status since they are connected in series with the CB auxiliary contacts. This is achieved by assigning one opto-input to the 52a contact and another opto-input to the 52b contact. Provided the ***CB Status*** setting in the *CB CONTROL* column is set to `Both 52A and 52B`, the IED will correctly monitor the status of the breaker. This scheme is also fully compatible with latched contacts as the supervision current will be maintained through the 52b contact when the trip contact is closed.

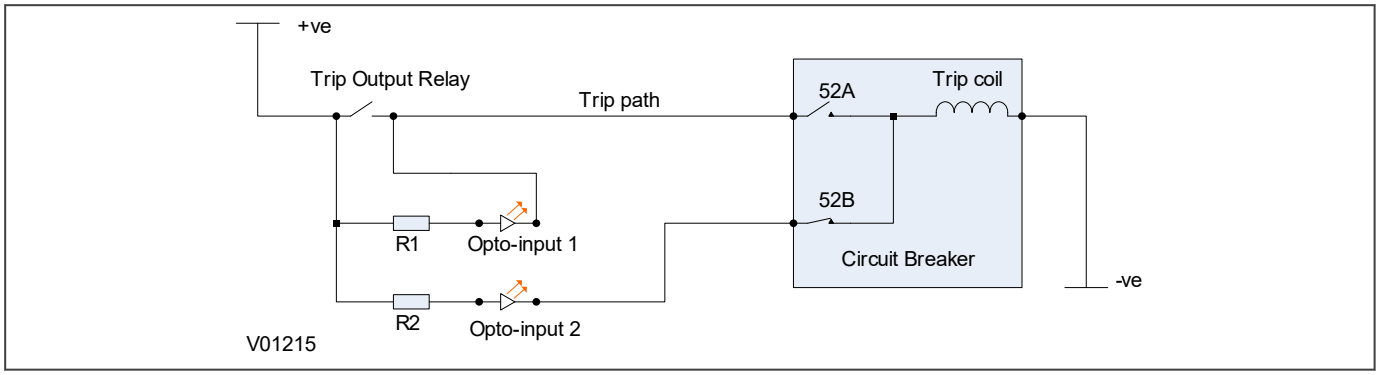


Figure 179: TCS scheme 2

When the breaker is closed, supervision current passes through opto input 1 and the trip coil. When the breaker is open current flows through opto input 2 and the trip coil. No supervision of the trip path is provided whilst the breaker is open. Any fault in the trip path will only be detected on CB closing, after a 400 ms delay.

14.4.2.1 RESISTOR VALUES

Optional resistors R1 and R2 can be added to prevent tripping of the CB if either opto-input is shorted. The table below shows the appropriate resistor value and voltage setting for this scheme.

Trip Circuit Voltage	Opto Voltage Setting with R1 Fitted	Resistor R1 and R2 (ohms)
48/54	24/27	1.2k
110/125	48/54	2.7k
220/250	110/125	5.2k

Warning:
This Scheme is not compatible with Trip Circuit voltages of less than 48 V.

14.4.2.2 PSL FOR TCS SCHEME 2

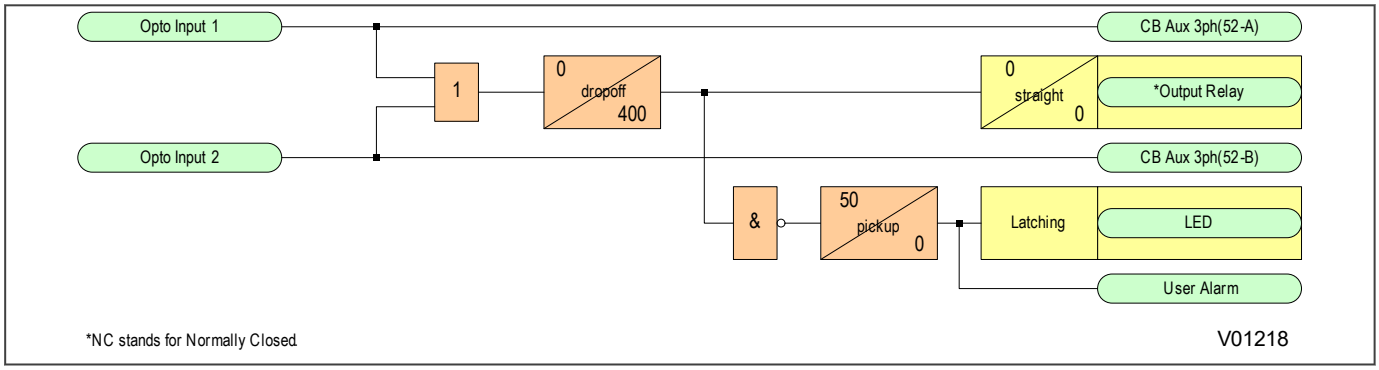


Figure 180: PSL for TCS scheme 2

In TCS scheme 2, both opto-inputs must be low before a trip circuit fail alarm is given.

14.4.3 TRIP CIRCUIT SUPERVISION SCHEME 3

TCS Scheme 3 is designed to provide supervision of the trip coil with the breaker open or closed. It provides pre-closing supervision of the trip path. Since only one opto-input is used, this scheme is not compatible with latched trip contacts. If you require CB status monitoring, further opto-inputs must be used.

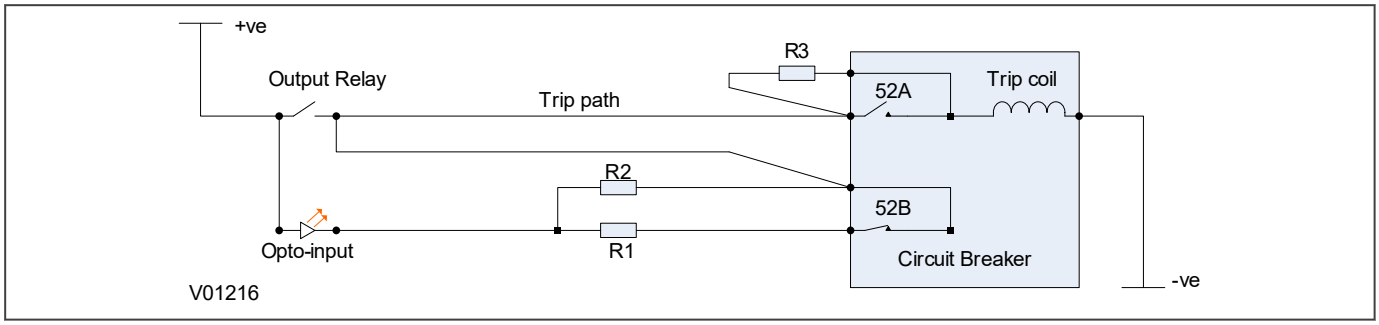


Figure 181: TCS scheme 3

When the CB is closed, supervision current passes through the opto-input, resistor R2 and the trip coil. When the CB is open, current flows through the opto-input, resistors R1 and R2 (in parallel), resistor R3 and the trip coil. The supervision current is maintained through the trip path with the breaker in either state, therefore providing pre-closing supervision.

14.4.3.1 RESISTOR VALUES

Resistors R1 and R2 are used to prevent false tripping, if the opto-input is accidentally shorted. However, unlike the other two schemes. This scheme is dependent upon the position and value of these resistors. Removing them would result in incomplete trip circuit monitoring. The table below shows the resistor values and voltage settings required for satisfactory operation.

Trip Circuit Voltage	Opto Voltage Setting with R1 Fitted	Resistor R1 & R2 (ohms)	Resistor R3 (ohms)
48/54	24/27	1.2k	600
110/250	48/54	2.7k	1.2k
220/250	110/125	5.0k	2.5k

Warning:
This Scheme is not compatible with Trip Circuit voltages of less than 48 V.

14.4.3.2 PSL FOR TCS SCHEME 3

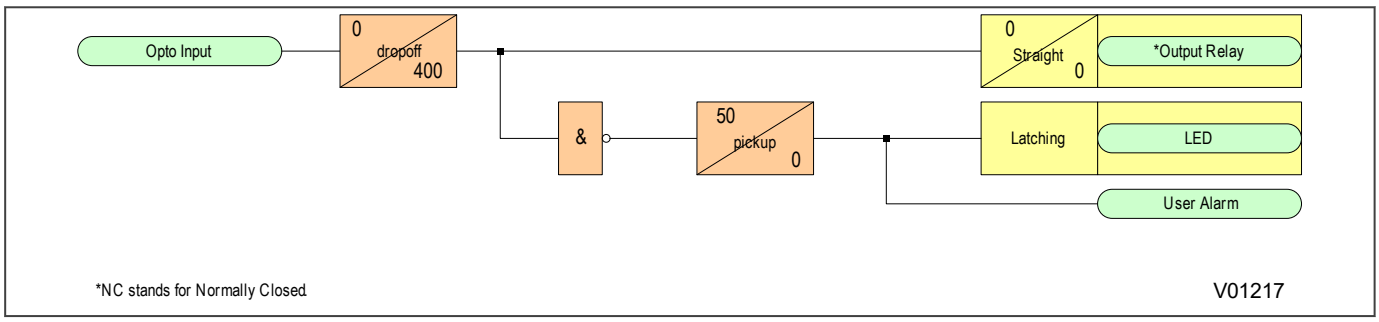


Figure 182: PSL for TCS scheme 3

CHAPTER 15

DIGITAL I/O AND PSL CONFIGURATION

15.1 CHAPTER OVERVIEW

This chapter introduces the PSL (Programmable Scheme Logic) Editor, and describes the configuration of the digital inputs and outputs. It provides an outline of scheme logic concepts and the PSL Editor. This is followed by details about allocation of the digital inputs and outputs, which require the use of the PSL Editor. A separate "Settings Application Software" document is available that gives a comprehensive description of the PSL, but enough information is provided in this chapter to allow you to allocate the principal digital inputs and outputs.

This chapter contains the following sections:

Chapter Overview 312
Configuring Digital Inputs and Outputs 313
Scheme Logic 314
Configuring the Opto-Inputs 316
Assigning the Output Relays 317
Fixed Function LEDs 318
Configuring Programmable LEDs 319
Function Keys 321
Control Inputs 322

15.2 CONFIGURING DIGITAL INPUTS AND OUTPUTS

Configuration of the digital inputs and outputs in this product is very flexible. You can use a combination of settings and programmable logic to customise them to your application. You can access some of the settings using the keypad on the front panel, but you will need a computer running the settings application software to fully interrogate and configure the properties of the digital inputs and outputs.

The settings application software includes an application called the PSL Editor (Programmable Scheme Logic Editor). The PSL Editor lets you allocate inputs and outputs according to your specific application. It also allows you to apply attributes to some of the signals such as a drop-off delay for an output contact.

In this product, digital inputs and outputs that are configurable are:

- Optically isolated digital inputs (opto-inputs). These can be used to monitor the status of associated plant.
- Output relays. These can be used for purposes such as initiating the tripping of circuit breakers, providing alarm signals, etc..
- Programmable LEDs. The number and colour of the programmable LEDs varies according to the particular product being applied.
- Function keys and associated LED indications. These are not provided on all products, but where they are, each function key has an associated tri-colour LED.
- IEC 61850 GOOSE inputs and outputs. These are only provided on products that have been specified for connection to an IEC61850 system, and the details of the GOOSE are presented in the documentation on IEC61850.
- InterMiCOM inputs and outputs. These are not used by all products. If your product is equipped with an InterMiCOM feature, you will find details of allocation and configuration in the chapter dedicated to the InterMiCOM function.

15.3 SCHEME LOGIC

The product is supplied with pre-loaded Fixed Scheme Logic (FSL) and Programmable Scheme Logic (PSL).

The Scheme Logic is a functional module within the IED, through which all mapping of inputs to outputs is handled. The scheme logic can be split into two parts; the Fixed Scheme Logic (FSL) and the Programmable Scheme Logic (PSL). It is built around a concept called the digital data bus (DDB). The DDB encompasses all of the digital signals (DDBs) which are used in the FSL and PSL. The DDBs included digital inputs, outputs, and internal signals.

The FSL is logic that has been hard-coded in the product. It is fundamental to correct interaction between various protection and/or control elements. It is fixed and cannot be changed.

The PSL gives you a facility to develop custom schemes to suit your application if the factory-programmed default PSL schemes do not meet your needs. Default PSL schemes are programmed before the product leaves the factory. These default PSL schemes have been designed to suit typical applications and if these schemes suit your requirements, you do not need to take any action. However, if you want to change the input-output mappings, or to implement custom scheme logic, you can change these, or create new PSL schemes using the PSL editor.

The PSL consists of components such as logic gates and timers, which combine and condition DDB signals.

The logic gates can be programmed to perform a range of different logic functions. The number of inputs to a logic gate are not limited. The timers can be used either to create a programmable delay or to condition the logic outputs. Output contacts and programmable LEDs have dedicated conditioners.

The PSL logic is event driven. Only the part of the PSL logic that is affected by the particular input change that has occurred is processed. This minimises the amount of processing time used by the PSL ensuring industry leading performance.

The following diagram shows how the scheme logic interacts with the rest of the IED.

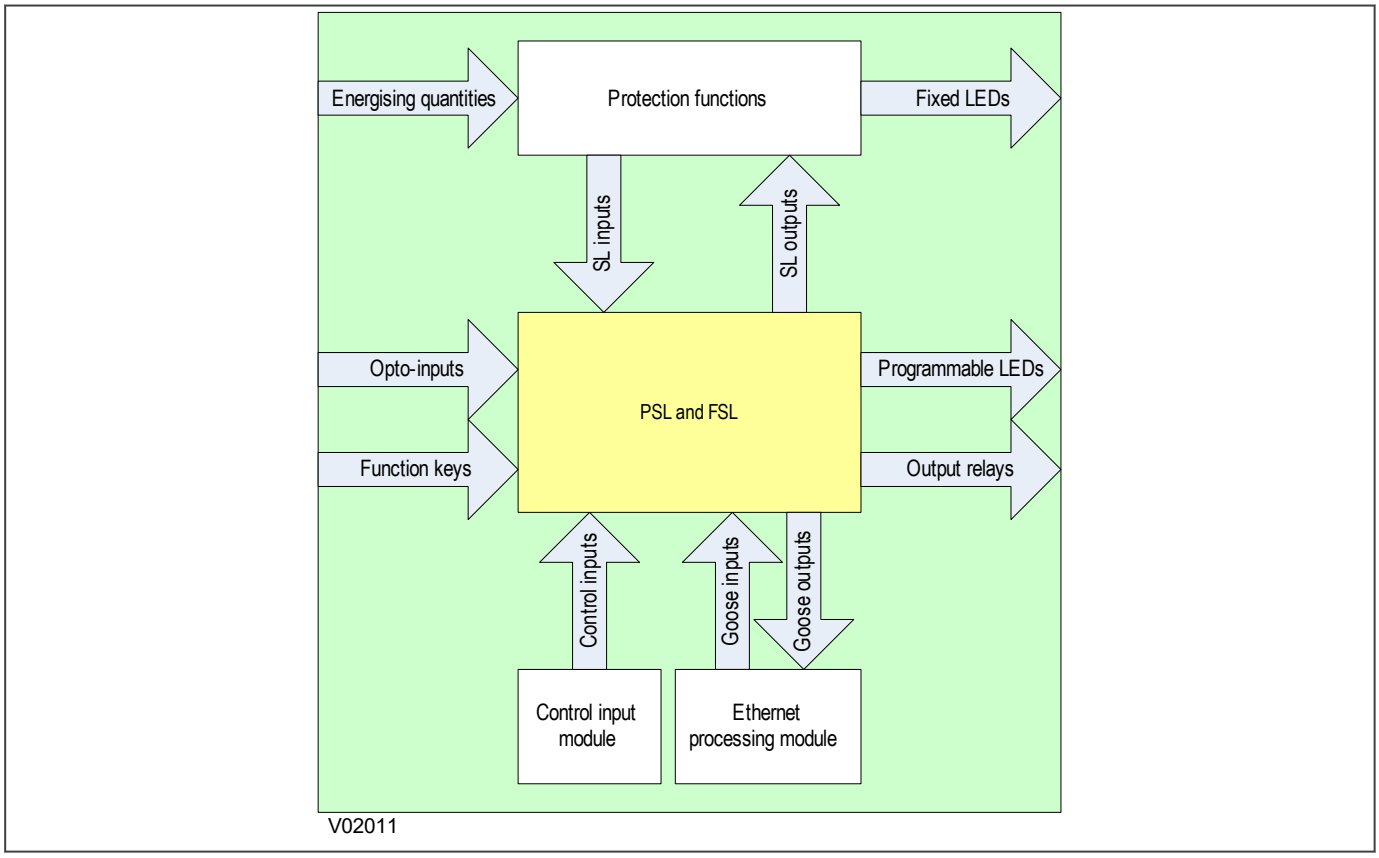


Figure 183: Scheme logic interfaces

15.3.1 PSL EDITOR

The Programmable Scheme Logic (PSL) is a module of programmable logic gates and timers in the IED, which can be used to create customised logic to qualify how the product manages its response to system conditions. The IED's digital inputs are combined with internally generated digital signals using logic gates, timers, and conditioners. The resultant signals are then mapped to digital outputs signals including output relays and LEDs.

The PSL Editor is a tool in the settings application software that allows you to create and edit scheme logic diagrams. You can use the default scheme logic which has been designed to suit most applications, but if it does not suit your application you can change it. If you create a different scheme logic with the software, you need to upload it to the device to apply it.

15.3.2 PSL SCHEMES

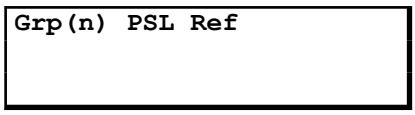
Your product is shipped with default scheme files. These can be used without modification for most applications, or you can choose to use them as a starting point to design your own scheme. You can also create a new scheme from scratch. To create a new scheme, or to modify an existing scheme, you will need to launch the settings application software. You then need to open an existing PSL file, or create a new one, for the particular product that you are using, and then open a PSL file. If you want to create a new PSL file, you should select **File** then **New** then **Blank scheme...** This action opens a default file appropriate for the device in question, but deletes the diagram components from the default file to leave an empty diagram with configuration information loaded. To open an existing file, or a default file, simply double-click on it.

15.3.3 PSL SCHEME VERSION CONTROL

To help you keep track of the PSL loaded into products, a version control feature is included. The user interface contains a *PSL DATA* column, which can be used to track PSL modifications. A total of 12 cells are contained in the *PSL DATA* column; 3 for each setting group.

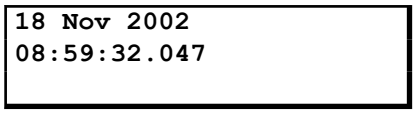
Grp(n) PSL Ref: When downloading a PSL scheme to an IED, you will be prompted to enter the relevant group number and a reference identifier. The first 32 characters of the reference identifier are displayed in this cell. The horizontal cursor keys can scroll through the 32 characters as the LCD display only displays 16 characters.

Example:



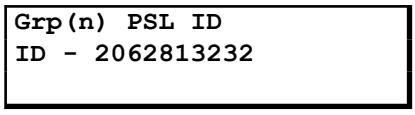
Date/time: This cell displays the date and time when the PSL scheme was downloaded to the IED.

Example:



Grp(n) PSL ID: This cell displays a unique ID number for the downloaded PSL scheme.

Example:



15.4 CONFIGURING THE OPTO-INPUTS

The number of optically isolated status inputs (opto-inputs) depends on the specific model supplied. The use of the inputs will depend on the application, and their allocation is defined in the programmable scheme logic (PSL). In addition to the PSL assignment, you also need to specify the expected input voltage. Generally, all opto-inputs will share the same input voltage range, but if different voltage ranges are being used, this device can accommodate them.

In the *OPTO CONFIG* column there is a global nominal voltage setting. If all opto-inputs are going to be energised from the same voltage range, you select the appropriate value in the setting. If you select `Custom` in the setting, then the cells ***Opto Input 1***, ***Opto Input 2***, etc. become visible. You use these cells to set the voltage ranges for each individual opto-input.

Within the *OPTO CONFIG* column there are also settings to control the filtering applied to the inputs, as well as the pick-up/drop-off characteristic.

The filter control setting provides a bit string with a bit associated with all opto-inputs. Setting the bit to '1' means that a half-cycle filter is applied to the inputs. This helps to prevent incorrect operation in the event of power system frequency interference on the wiring. Setting the field to '0' removes the filter and provides for faster operation.

The ***Characteristic*** setting is a single setting that applies to all the opto-inputs. It is used to set the pick-up/drop-off ratios of the input signals. As standard it is set to 80% pick-up and 60% drop-off, but you can change it to other available thresholds if that suits your operational requirements.

15.5 ASSIGNING THE OUTPUT RELAYS

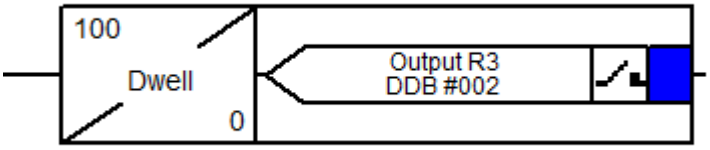
Relay contact action is controlled using the PSL. DDB signals are mapped in the PSL and drive the output relays. The driving of an output relay is controlled by means of a relay output conditioner. Several choices are available for how output relay contacts are conditioned. For example, you can choose whether operation of an output relay contact is latched, has delay on pick-up, or has a delay on drop-off. You make this choice in the **Contact Properties** window associated with the output relay conditioner.

To map an output relay in the PSL you should use the Contact Conditioner button in the toolbar to import it. You then condition it according to your needs. The output of the conditioner respects the attributes you have assigned.

The toolbar button for a Contact Conditioner looks like this:



The PSL contribution that it delivers looks like this:



Note:
Contact Conditioners are only available if they have not all been used. In some default PSL schemes, all Contact Conditioners might have been used. If that is the case, and you want to use them for something else, you will need to re-assign them.

On the toolbar there is another button associated with the relay outputs. The button looks like this:



This is the "Contact Signal" button. It allows you to put replica instances of a conditioned output relay into the PSL, preventing you having to make cross-page connections which might detract from the clarity of the scheme.

15.6 FIXED FUNCTION LEDS

Four fixed-function LEDs on the left-hand side of the front panel indicate the following conditions.

- Trip (Red) switches ON when the IED issues a trip signal. It is reset when the associated fault record is cleared from the front display. Also the trip LED can be configured as self-resetting.
- Alarm (Yellow) flashes when the IED registers an alarm. This may be triggered by a fault, event or maintenance record. The LED flashes until the alarms have been accepted (read), then changes to constantly ON. When the alarms are cleared, the LED switches OFF.
- Out of service (Yellow) is ON when the IED's functions are unavailable.
- Healthy (Green) is ON when the IED is in correct working order, and should be ON at all times. It goes OFF if the unit's self-tests show there is an error in the hardware or software. The state of the healthy LED is reflected by the watchdog contacts at the back of the unit.

15.6.1 TRIP LED LOGIC

When a trip occurs, the trip LED is illuminated. It is possible to reset this with a number of ways:

- Directly with a reset command (by pressing the Clear Key)
- With a reset logic input
- With self-resetting logic

You enable the automatic self-resetting with the ***Sys Fn Links*** cell in the *SYSTEM DATA* column. A '0' disables self resetting and a '1' enables self resetting.

The reset occurs when the circuit is reclosed and the ***Any Pole Dead*** signal has been reset for three seconds providing the ***Any Start*** signal is inactive. The reset is prevented if the ***Any Start*** signal is active after the breaker closes.

The Trip LED logic is as follows:

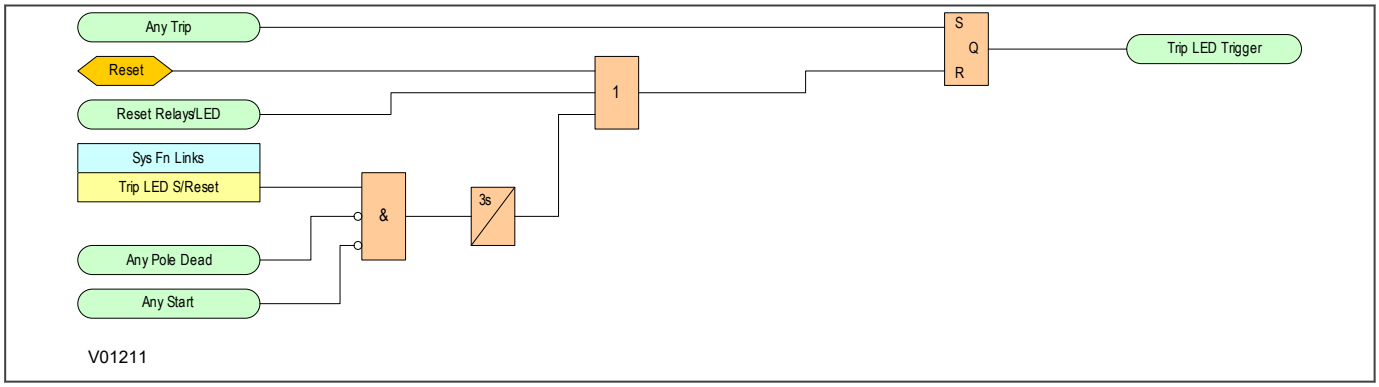


Figure 184: Trip LED logic

15.7 CONFIGURING PROGRAMMABLE LEDS

There are three types of programmable LED signals which vary according to the model being used. These are:

- Single-colour programmable LED. These are red when illuminated.
- Tri-colour programmable LED. These can be illuminated red, green, or amber.
- Tri-colour programmable LED associated with a Function Key. These can be illuminated red, green, or amber.

DDB signals are mapped in the PSL and used to illuminate the LEDs. For single-coloured programmable LEDs there is one DDB signal per LED. For tri-coloured LEDs there are two DDB signals associated with the LED. Asserting ***LED # Grn*** will illuminate the LED green. Asserting ***LED # Red*** will illuminate the LED red. Asserting both DDB signals will illuminate the LED amber.

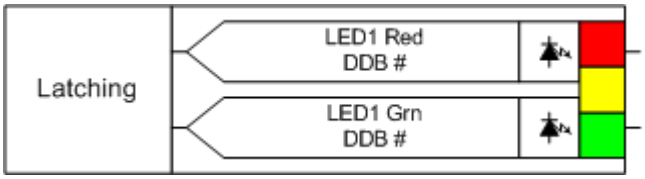
The illumination of an LED is controlled by means of a conditioner. Using the conditioner, you can decide whether the LEDs reflect the real-time state of the DDB signals, or whether illumination is latched pending user intervention.

To map an LED in the PSL you should use the LED Conditioner button in the toolbar to import it. You then condition it according to your needs. The output(s) of the conditioner respect the attribute you have assigned.

The toolbar button for a tri-colour LED looks like this:



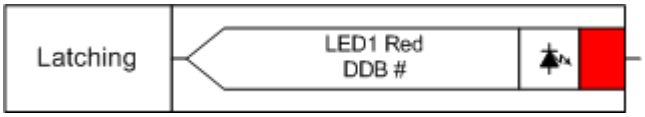
The PSL contribution that it delivers looks like this:



The toolbar button for a single-colour LED looks like this:



The PSL contribution that it delivers looks like this.



Note:
LED Conditioners are only available if they have not all been used up, and in some default PSL schemes they might be. If that is the case and you want to use them for something else, you will need to re-assign them.

On the toolbar there is another button associated with the LEDs. For a tri-coloured LED the button looks like this:



For a single-colour LED it looks like this: 

It is the "LED Signal" button. It allows you to put replica instances of a conditioned LED into the PSL, preventing you having to make cross-page connections which might detract from the clarity of the scheme.

Note:
All LED DDB signals are always shown in the PSL Editor. However, the actual number of LEDs depends on the device hardware. For example, if a small 20TE device has only 4 programmable LEDs, LEDs 5-8 will not take effect even if they are mapped in the PSL.

15.8 FUNCTION KEYS

For most models, a number of programmable function keys are available. This allows you to assign function keys to control functionality via the programmable scheme logic (PSL). Each function key is associated with a programmable tri-colour LED, which you can program to give the desired indication on activation of the function key.

These function keys can be used to trigger any function that they are connected to as part of the PSL. The function key commands are found in the *FUNCTION KEYS* column.

Each function key is associated with a DDB signal as shown in the DDB table. You can map these DDB signals to any function available in the PSL.

The ***Fn Key Status*** cell displays the status (energised or de-energised) of the function keys by means of a binary string, where each bit represents a function key starting with bit 0 for function key 1.

Each function key has three settings associated with it, as shown:

- ***Fn Key (n)***, which enables or disables the function key
- ***Fn Key (n) Mode***, which allows you to configure the key as toggled or normal
- ***Fn Key (n) label***, which allows you to define the function key text that is displayed

The ***Fn Key (n)*** cell is used to enable (unlock) or disable (unlock) the function key signals in PSL. The Lock setting has been provided to prevent further activation on subsequent key presses. This allows function keys that are set to `Toggled` mode and their DDB signal active 'high', to be locked in their active state therefore preventing any further key presses from deactivating the associated function. Locking a function key that is set to the "Normal" mode causes the associated DDB signals to be permanently off. This safety feature prevents any inadvertent function key presses from activating or deactivating critical functions.

When the ***Fn Key (n) Mode*** cell is set to `Toggle`, the function key DDB signal output will remain in the set state until a reset command is given. In the `Normal` mode, the function key DDB signal will remain energised for as long as the function key is pressed and will then reset automatically. In this mode, a minimum pulse duration can be programmed by adding a minimum pulse timer to the function key DDB output signal.

The ***Fn Key Label*** cell makes it possible to change the text associated with each individual function key. This text will be displayed when a function key is accessed in the function key menu, or it can be displayed in the PSL.

The status of all function keys are recorded in non-volatile memory. In case of auxiliary supply interruption their status will be maintained.

Note:
All function key DDB signals are always shown in the PSL Editor. However, the actual number of function keys depends on the device hardware. For example, if a small 20TE device has no function keys, the function key DDBs mapped in the PSL will not take effect.

15.9 CONTROL INPUTS

The control inputs are software switches, which can be set or reset locally or remotely. These inputs can be used to trigger any PSL function to which they are connected. There are three setting columns associated with the control inputs: *CONTROL INPUTS*, *CTRL I/P CONFIG* and *CTRL I/P LABELS*. These are listed in the Settings and Records appendix at the end of this manual.

CHAPTER 16

FIBRE TELEPROTECTION

16.1 CHAPTER OVERVIEW

This chapter provides information about the fibre-optic communication mechanism,which is used to provide unit schemes and general-purpose teleprotection signalling for protection of transmission lines and distribution feeders. The feature is called Fibre Teleprotection.

This chapter contains the following sections:

Chapter Overview 324

Fibre Teleprotection Implementation 325

Communications Supervision 326

IM64 Logic 327

Application Notes 329

16.2 FIBRE TELEPROTECTION IMPLEMENTATION

The Fibre Teleprotection interface is an integral part of the Current Differential protection implementation for this product. It provides the communications necessary for the Current Differential protection schemes. Correct setup of the interface is critical to the operation of the current differential protection provided by this product. Accordingly, the implementation is fully described in the appropriate Current Differential chapter, and you should refer to that chapter to understand and configure the interface.

In addition to enabling the current differential protection, the Teleprotection interface can also be used to communicate general binary command signals such as intertripping signals. These signals can be be freely allocated using the PSL to realise protection schemes such as Permissive and Blocking schemes. If you want to use this product as a general purpose intertripping equipment without using the current differential protection, you should still refer to the Current Differential chapter and follow the guidance provided to set up the scheme.

16.2.1 ERROR HANDLING FOR PROTECTION COMMUNICATIONS

An overview of protection communications error handling is as follows:

2 ended

- If only one comms channel – no redundancy
- If using 2 comms channels – Redundancy

3 to 6 ended

- If a single comms channel fails, or if a terminal is reconfigured out of service, comms can be re-routed the other way around the ring
- If 2 channels fails - No protection

16.3 COMMUNICATIONS SUPERVISION

Since electrical power systems are generally required to operate continuously, it follows that the applied protection must do the same. If the protection uses communications, it must supervise these communications to take appropriate action should they become degraded or lost.

IM64 provides the necessary communications supervision.

There are seven settings associated with the IM64 protection signalling communications supervision which are listed below and described in the settings table:

- Comm Fail Timer
- Comm Fail Mode
- Channel Timeout
- IM Msg Alarm Lvl
- Prop Delay Stats
- MaxCh 1 PropDelay
- MaxCh 2 PropDelay

A communication alarm is raised if the message error rate exceeds the ***IM Msg Alarm Lvl*** setting and persists for the period defined by the ***Comm Fail Timer*** setting. Using the default settings will raise an alarm for a persistent Bit Error Rate (BER) of 1.5 x 10 –3.

The alarm will be apparent at the receiving device, which will reflect the alarm back to the transmitting device.

Note:
*The **Comm Fail Mode** setting applies only to devices configured for dual redundant or three-terminal configuration. It defines what combination of failures on the two communications channels is used to indicate an alarm.*

Note:
*The **MaxCh1 PropDelay** and **MaxCh2 PropDelay** settings for Channel 1 (and Channel 2 if fitted) are only visible if the **Prop Delay Stats** setting is* `Enabled`.

16.4 IM64 LOGIC

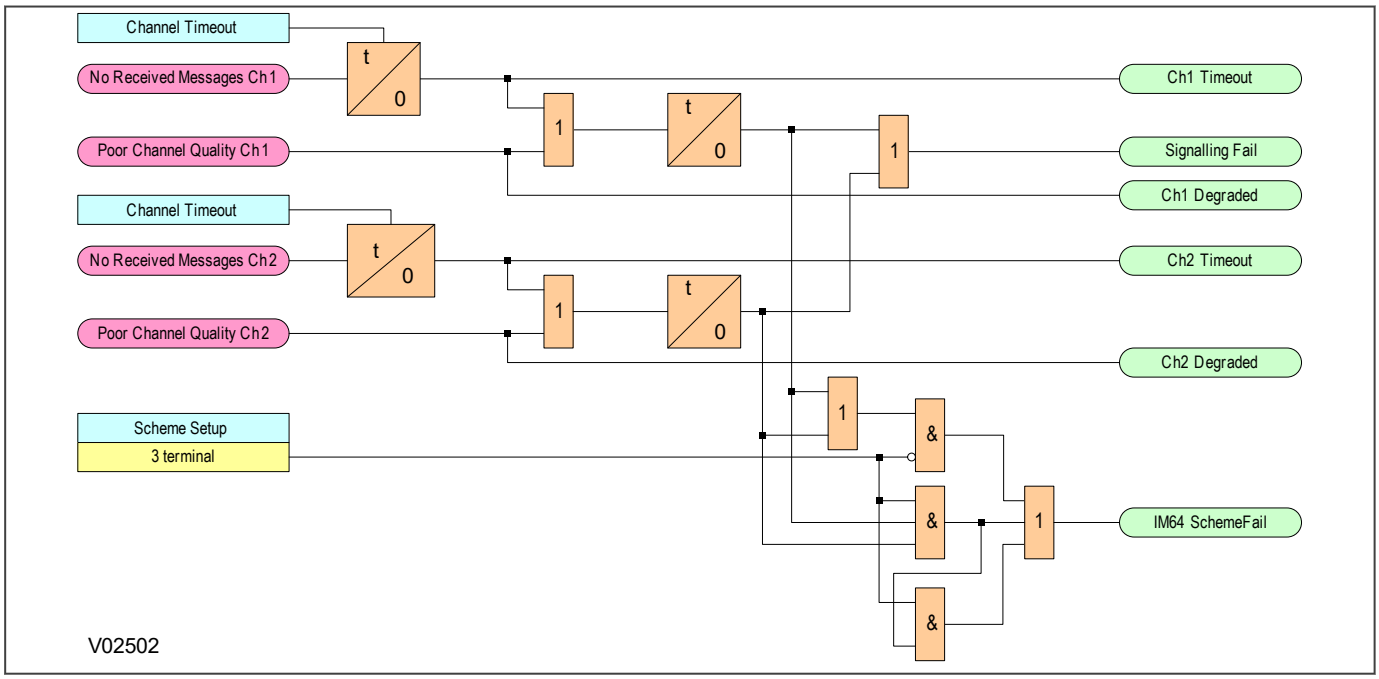


Figure 185: IM64 channel fail and scheme fail logic

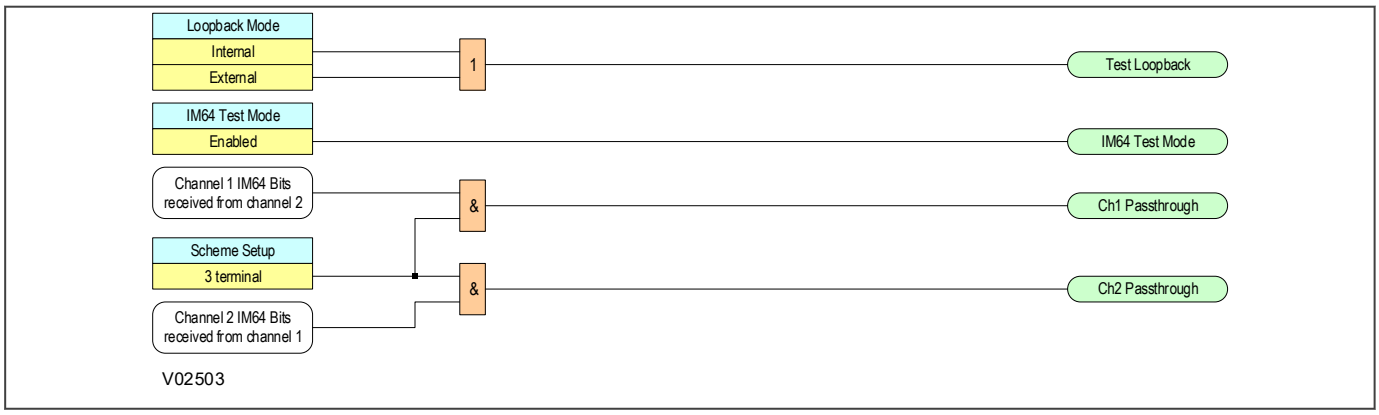


Figure 186: IM64 general alarm signals logic

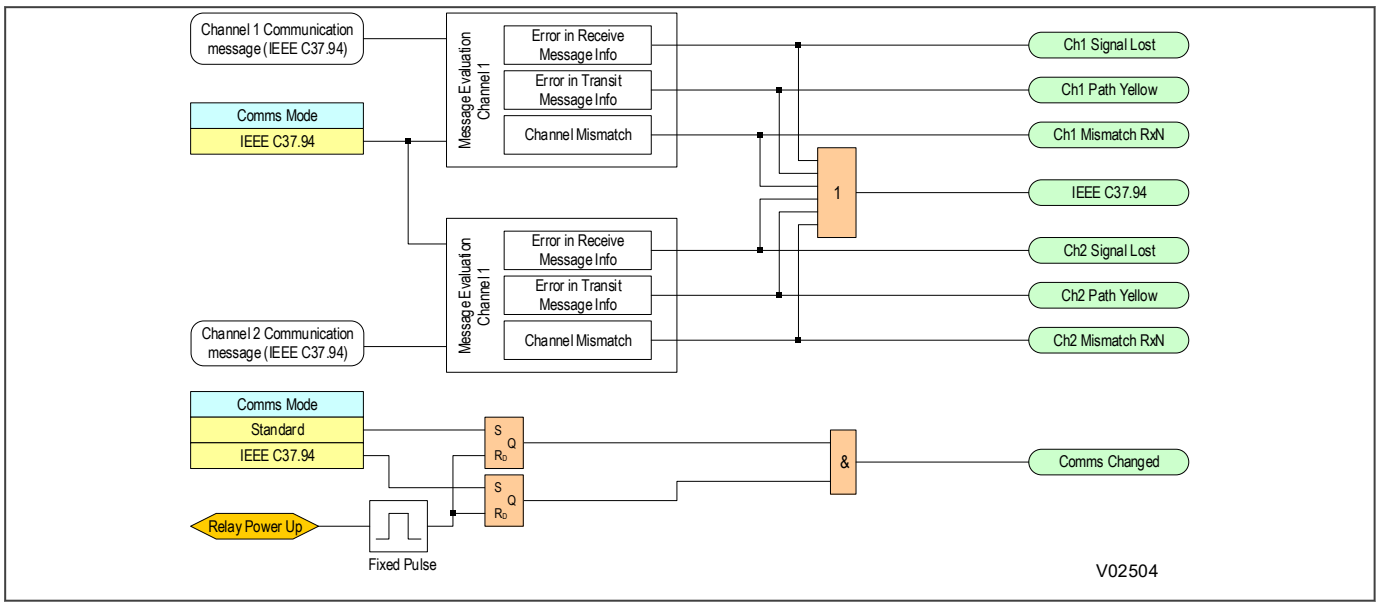


Figure 187: IM64 communications mode and IEEE C37.94 alarm signals

16.5 APPLICATION NOTES

Effective communications are essential for the performance of teleprotection schemes. Disturbances on the communications links need to be detected and reported so that appropriate actions can be taken to ensure that the power system does not go unprotected.

16.5.1 SCHEME RECONFIGURATION

Each relay of the Multi-Ended Line Differential scheme has a reconfiguration feature. This feature allows a relay to be put 'Out of Service' for maintenance or testing purposes. This can be achieved by toggling the Re-Configuration option under *PROT COMMS/IM64* from `Disabled` to `Terminal N`, where *N* is the end to be taken out of service (A-F).

```
PROT COMMS/ IM64
Re-Configuration
Disabled
```

```
PROT COMMS/ IM64
Re-Configuration
Terminal B
```

This affects the overall scheme in the following way:

- The communication channels of the 'reconfigured' relay remain in service. This means there is no interruption to the ring communication or loss of redundancy
- The current (load) values of the reconfigured terminal relay are not included in the idiff and ibias calculations by other relays in the scheme

The following should be taken into consideration during reconfiguration:

- Only one relay end can be reconfigured in a scheme at a given time
- A minimum of 3 terminals need to remain in service after reconfiguration
- The ***Reconfiguration Interlock*** DDB must be asserted before the relay is reconfigured

Any terminal of the scheme can be used to send a reconfiguration command to another terminal that is required to be taken out of service. The relay will get 'reconfiguration confirmation' from all ends. Testing can then be carried out on the relay that is out of service.

Note:
Reconfiguration feature not available in P54A.

16.5.2 ALARM MANAGEMENT

Due to the criticality of IM64 communications for correct scheme performance, there is an extensive regime to monitor signal quality and integrity, generate and report alarms. For most applications, the alarm management provided as standard will satisfy the needs of the scheme.

For some applications, it may be necessary customise the alarm management. You can do this with the programmable scheme logic. This section provides a detailed explanation the communications alarm signals integrated in this product.

16.5.3 ALARM LOGIC

The figures in the logic diagram section show the main alarm DDB signals associated with IM64. Some of the signals are setting or hardware dependent. For example, Channel 2 alarms are not available on a simple two-terminal single communications link application. This section explains the logic, allowing you to understand how you might customise the alarm logic for your application.

The messages received on each channel are individually assessed for quality to ensure the IM64 signalling scheme is available for use. If no messages are received for a period equal to the ***Channel Timeout*** setting or the signal quality falls below a defined value, DDB signals are activated as shown in the IM64 channel fail and scheme fail logic diagram.

Poor quality is indicated if the percentage of incomplete messages exceeds the ***IM Msg Alarm Lvl*** setting in a 100 ms period (rolling window), or if the communications propagation time of the IM64 message exceeds the ***Max Ch PropDelay*** (assuming the ***Prop Delay Stats*** setting is `Enabled`), or if (in IEEE C37.94 configuration only, and not shown on the diagram) the ***Ch Mux Clk*** flag has been raised to indicate an incorrect baud rate.

If either the ***Ch Timeout*** or the ***Ch Degraded*** signal persists in the alarmed state for more than the duration of the ***Comm Fail Timer*** setting, according to the conditions set in the Comm Fail Mode setting, the ***Signalling Fail*** signal is raised.

For two-ended schemes (including dual redundant schemes), the ***IM64 SchemeFail*** signal is generated at the same time as the ***Signalling Fail*** signal. However, for three-terminal applications, the ***IM64 SchemeFail*** signal indicates that the full set of signalling bits cannot be processed by the scheme. Due to the self-healing nature of the three-terminal application, this occurs when both channels at any one terminal are not receiving valid signals. This condition generates a flag in the IM64 message structure which is passed to both remote ends, as well as generating the local ***IM64 SchemeFail*** signal. Using this method, in three-terminal applications the scheme fail indication is raised at all three ends.

The scheme fail signalling is generated by the inability of a device to receive messages through communication failure. The transmitting device only knows that communication to a remote device has failed if it receives notification from the remote device. If a device in the scheme is put into test mode, the communication failure information is not passed on to the remote ends. If the communications failure is bidirectional, there will be no indication at the remote device. If this causes operational issues, it may be necessary to include other signals to enable more precise indication of scheme failure.

In addition to the main IM64 channel fail and scheme fail conceptual logic, there are number of additional alarm DDB signals associated with test modes, reconfiguration for 3-terminal schemes, and the communication mode (‘Standard’ or ‘IEEE C37.94’) shown in the logic diagrams.

The majority of signals are associated with the ‘IEEE C37.94’ communications mode and are not activated if the `Standard` communication mode is selected. The ***Comms Changed*** DDB logic is to show that switching between the different communication modes requires a power cycle to be performed before the change is activated.

16.5.4 TWO-ENDED SCHEME EXTENDED SUPERVISION

For two-terminal applications, the ***Signalling Fail*** and ***IM64 SchemeFail*** signals operate together. As such, the basic indications available on each device should be considered as local-terminal indications only. If remote indication is needed to assure scheme functionality, it is necessary to use additional signals to communicate the status to the remote end. One method of performing this is shown below:

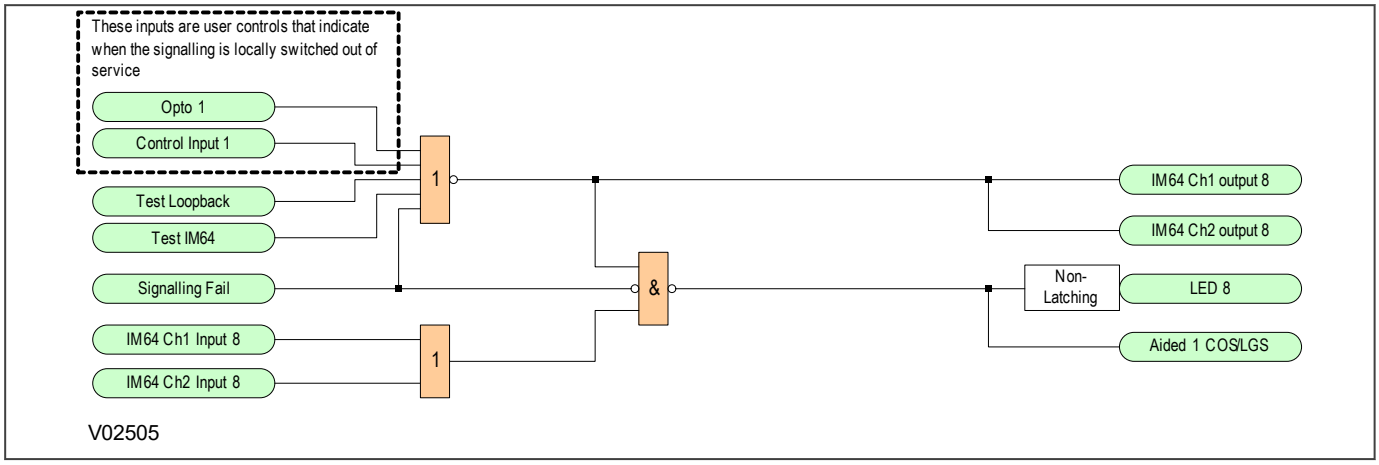


Figure 188: IM64 two-terminal scheme extended supervision

In this example scheme, several signals are used to permanently pass an IM64 signal to the remote terminal. These signals take account of the local ability to receive IM64 messages, local test/loopback modes and any other external methods of switching the signalling scheme out of service. If any of these driving signals are energised, the IM64 message is reset (a “0” sent on IM64 bit 8). This causes both ends to raise an alarm (LED 8 in the example) or switch the aided scheme out of service due to loss of channel.

This is intended only as an example. You may need to customise it for your application requirements.

16.5.5 MULTI-TERMINAL SCHEME EXTENDED SUPERVISION

The example for an IM64 two-terminal scheme above can be used for multi-terminal applications. However for multi-terminal applications, the ***IM64 SchemeFail*** signal that is automatically communicated to all ends of the scheme is used rather than the ***Signalling Fail*** signal.

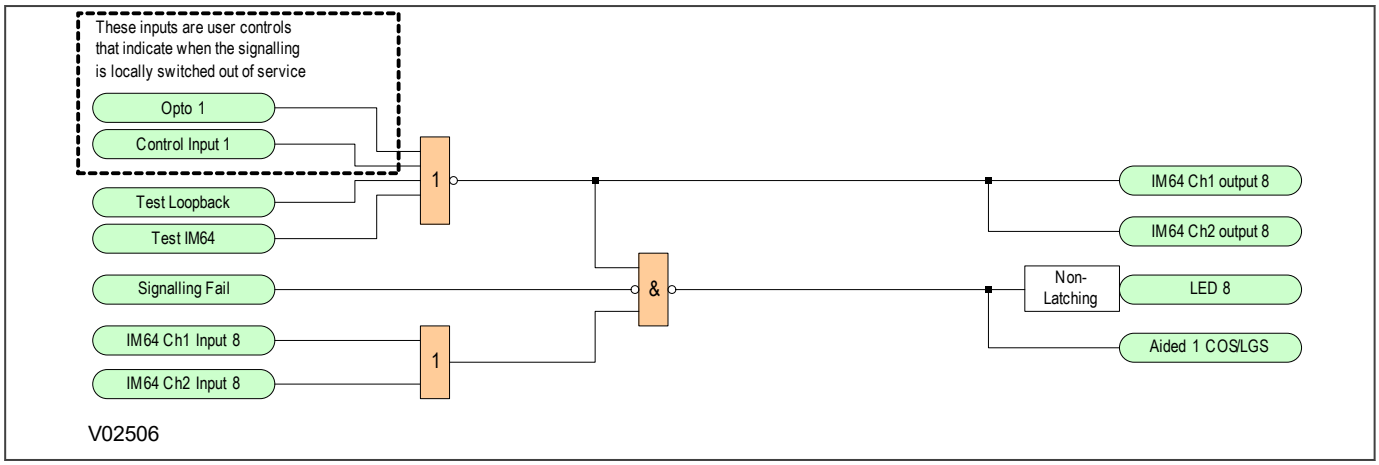


Figure 189: IM64 multi-terminal scheme extended supervision

In this example if both channels at any one terminal fail to receive information, this is communicated to the other terminals. An alarm is raised and the aided scheme is switched out of service. The example given above, also takes into account the test modes and local switching, so the scheme is signalled out of service at all terminals if one terminal is locally disabled.

The logic presented above is intended only as an example. You may need to customise it for your application requirements.

CHAPTER 17

ELECTRICAL TELEPROTECTION

17.1 CHAPTER OVERVIEW

This chapter contains the following sections:

Chapter Overview 333
Introduction 334
Teleprotection Scheme Principles 335
Implementation 336
Configuration 337
Connecting to Electrical InterMiCOM 339
Application Notes 340

17.2 INTRODUCTION

Electrical Teleprotection is an optional feature that uses communications links to create protection schemes. It can be used to replace hard wiring between dedicated relay output contacts and digital input circuits. Two products equipped with electrical teleprotection can connect and exchange commands using a communication link. It is typically used to implement teleprotection schemes.

Using full duplex communications, eight binary command signals can be sent in each direction between connected products. The communication connection complies with the EIA(RS)232 standard. Ports may be connected directly, or using modems. Alternatively EIA(RS)232 converters can be used for connecting to other media such as optical fibres.

Communications statistics and diagnostics enable you to monitor the integrity of the communications link, and a loopback feature is available to help with testing.

17.3 TELEPROTECTION SCHEME PRINCIPLES

Teleprotection schemes use signalling to convey a trip command to remote circuit breakers to isolate circuits. Three types of teleprotection commands are commonly encountered:

- Direct Tripping
- Permissive Tripping
- Blocking Scheme

17.3.1 DIRECT TRIPPING

In direct tripping applications (often described by the generic term: “intertripping”), teleprotection signals are sent directly to a master trip device. Receipt of a command causes circuit breaker operation without any further qualification. Communication must be reliable and secure because any signal detected at the receiving end causes a trip of the circuit at that end. The communications system must be designed so that interference on the communication circuit does not cause spurious trips. If a spurious trip occurs, the primary system might be unnecessarily isolated.

17.3.2 PERMISSIVE TRIPPING

Permissive trip commands are monitored by a protection device. The circuit breaker is tripped when receipt of the command coincides with a ‘start’ condition being detected by the protection at the receiving. Requirements for the communications channel are less onerous than for direct tripping schemes, since receipt of an incorrect signal must coincide with a ‘start’ of the receiving end protection for a trip operation to take place. Permissive tripping is used to speed up tripping for faults occurring within a protected zone.

17.4 IMPLEMENTATION

Electrical InterMiCOM is configured using a combination of settings in the *INTERMICOM COMMS* column, settings in the *INTERMICOM CONF* column, and the programmable scheme logic (PSL).

The eight command signals are mapped to DDB signals within the product using the PSL.

Signals being sent to a remote terminal are referenced in the PSL as ***IM Output 1*** - ***IM Output 8***. Signals received from the remote terminal are referenced as ***IM Input 1*** - ***IM Input 8***.

Note:
As well as the optional Modem InterMiCOM, some products are available with a feature called InterMiCOM64 (IM64). The functionality and assignment of commands in InterMiCOM and InterMiCOM64 are similar, but they act independently and are configured independently.

17.5 CONFIGURATION

Electrical Teleprotection is compliant with IEC 60834-1:1999. For your application, you can customise individual command signals to the differing requirements of security, speed, and dependability as defined in this standard.

You customise the command signals using the ***IM# Cmd Type*** cell in the *INTERMICOM CONF* column.

Any command signal can be configured for:

- Direct intertripping by selecting 'Direct'. (this is the most secure signalling but incurs a time delay to deliver the security).
- Blocking applications by selecting 'Blocking'. (this is the fastest signalling)
- Permissive intertripping applications by selecting 'Permissive. (this is dependable signalling that balances speed and security)

You can also select to 'Disable' the command.

> *Note:*
> *When used in the context of a setting, '#' specifies which command signal (1-8) bit is being configured.*

To ensure that command signals are processed only by their intended recipient, the command signals are packaged into a message (sometimes referred to as a telegram) which contains an address field. A sending device sets a pattern in this field. A receiving device must be set to match this pattern in the address field before the commands will be acted upon. 10 patterns have been carefully chosen for maximum security. You need to choose which ones to use, and set them using the ***Source Address*** and ***Receive Address*** cells in the *INTERMICOM COMMS* column.

The value set in the ***Source Address*** of the transmitting device should match that set in the ***Receive Address*** of the receiving device. For example set ***Source Address*** to `1` at a local terminal and set ***Receive Address*** to `1` at the remote terminal.

The Source Address and Receive Address settings in the device should be set to different values to avoid false operation under inadvertent loopback conditions.

Where more than one pair of devices is likely to share a communication link, you should set each pair to use a different pair of address values.

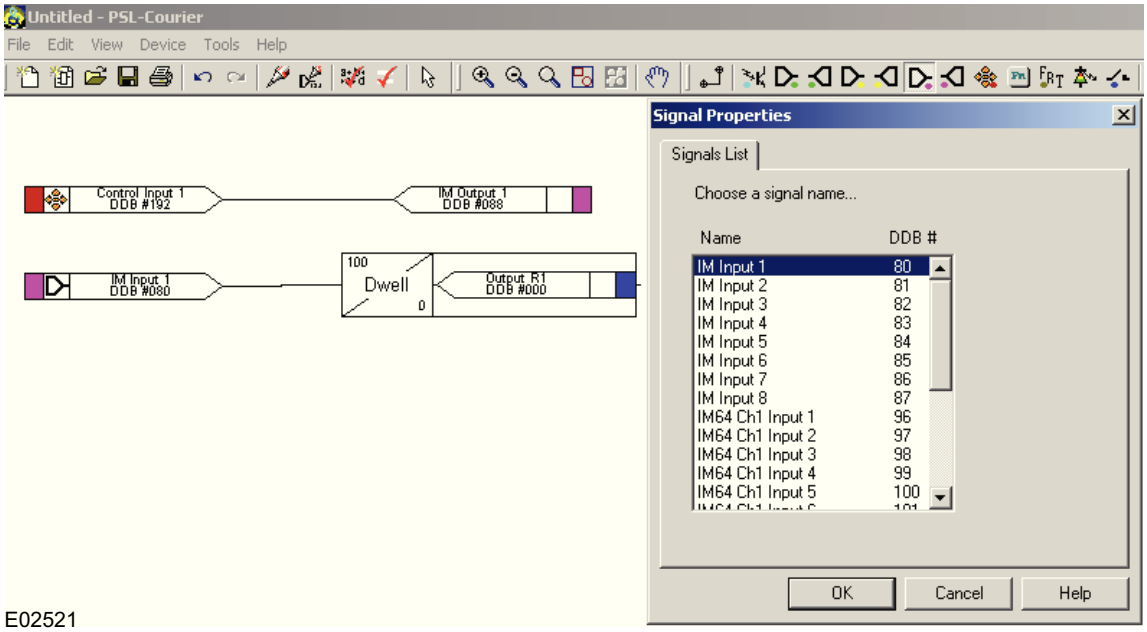
Electrical InterMiCOM has been designed to be resilient to noise on communications links, but during severe noise conditions, the communication may fail. If this is the case, an alarm is raised and you can choose how the input signals are managed using the ***IM# FallBackMode*** cell in the *INTERMICOM CONF* column:

• If you choose `Latched`, the last valid command to be received can be maintained until a new valid message is received.

• If you choose `Default`, the signal will revert to a default value after the period defined in the ***IM# FrameSyncTim*** setting has expired. You choose the default value using the ***IM# DefaultValue*** setting.

Subsequent receipt of a full valid message will reset the alarm, and the new command signals will be used.

As well as the settings described above, you will need to assign input and output signals in the Programmable Scheme Logic (PSL). Use the 'Integral Tripping' buttons to create the logic you want to apply. A typical example is shown below.



E02521

Figure 190: Example assignment of InterMiCOM signals within the PSL

Note:
When an Electrical InterMiCOM signal is sent from a local terminal, only the remote terminal will react to the command. The local terminal will only react to commands initiated at the remote terminal.

17.6 CONNECTING TO ELECTRICAL INTERMICOM

Electrical InterMiCOM uses EIA(RS)232 communication presented on a 9-pin 'D' type connector. The connector is labelled SK5 and is located at the bottom of the 2nd Rear communication board. The port is configured as standard DTE (Data Terminating Equipment).

17.6.1 SHORT DISTANCE

EIA(RS)232 is suitable for short distance connections only - less than 15m. Where this limitation is not a problem, direct connection between devices is possible. For this case, inter-device connections should be made as shown below the figure below.

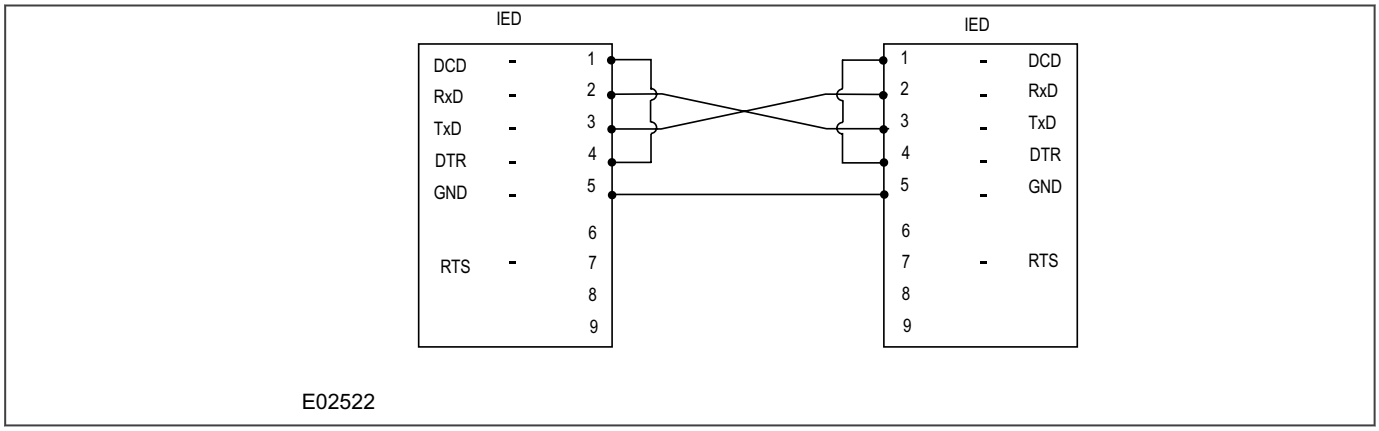


Figure 191: Direct connection

For direct connection, the maximum baud rate can generally be used.

17.6.2 LONG DISTANCE

EIA(RS)232 is suitable for short distance connections only - less than 15m. Where this limitation is a problem, direct connection between devices is not possible. For this case, inter-device connections should be made as shown below the figure below.

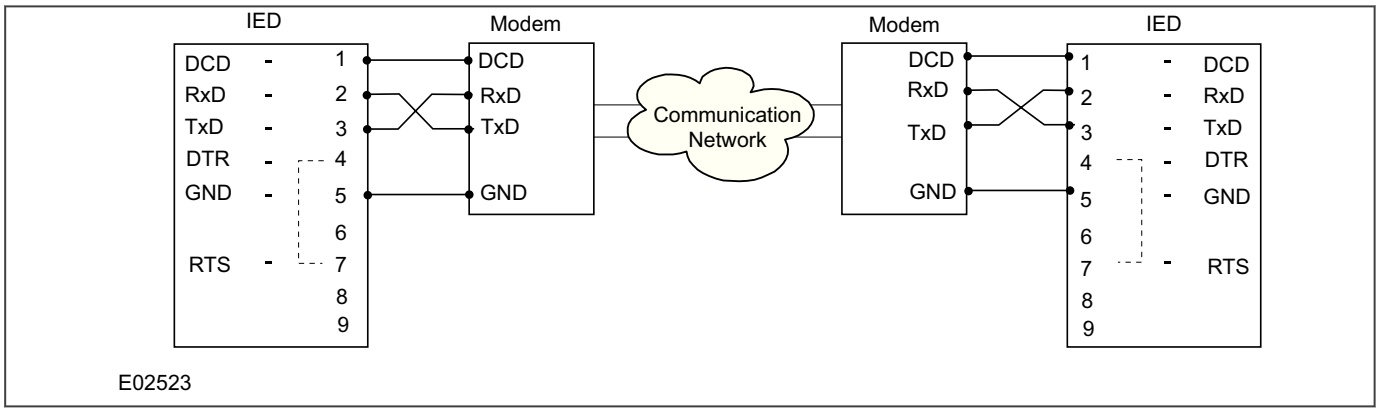


Figure 192: Indirect connection using modems

This type of connection should be used when connecting to devices that have the ability to control the DCD line. The baud rate should be chosen to be suitable for the communications network. If the Modem does not support the DCD function, the DCD terminal on the IED should be connected to the DTR terminal.

17.7 APPLICATION NOTES

Electrical InterMiCOM settings are contained within two columns; *INTERMICOM COMMS* and *INTERMICOM CONF*. The *INTERMICOM COMMS* column contains all the settings needed to configure the communications, as well as the channel statistics and diagnostic facilities. The *INTERMICOM CONF* column sets the mode of each command signal and defines how they operate in case of signalling failure.

Short metallic direct connections and connections using fire-optic converters will generally be set to have the highest signalling speed of 19200b/s. Due to this high signalling rate, the difference in operating time between the direct, permissive, and blocking type signals is small. This means you can select the most secure signalling command type ('Direct' intertrip) for all commands. You do this with the ***IM# Cmd Type*** settings. For these applications you should set the ***IM# Fallback Mode*** to `Default`. You should also set a minimal intentional delay by setting ***IM# FrameSyncTim*** to 10 msecs. This ensures that whenever two consecutive corrupt messages are received, the command will immediately revert to the default value until a new valid message is received.

For applications that use Modem and/or multiplexed connections, the trade-off between speed, security, and dependability is more critical. Choosing the fastest baud rate (data rate) to achieve maximum speed may appear attractive, but this is likely to increase the cost of the telecommunications equipment. Also, telecommunication services operating at high data rates are more prone to interference and suffer from longer re-synchronisation times following periods of disruption. Taking into account these factors we recommend a maximum baud rate setting of 9600 bps. As baud rates decrease, communications become more robust with fewer interruptions, but overall signalling times increase.

At slower baud rates, the choice of signalling mode becomes significant. You should also consider what happens during periods of noise when message structure and content can be lost.

- In 'Blocking' mode, the likelihood of receiving a command in a noisy environment is high. In this case, we recommend you set ***IM# Fallback Mode*** to `Default`, with a reasonably long ***IM# FrameSyncTim*** setting. Set ***IM# DefaultValue*** to '1'. This provides a substitute for a received blocking signal, applying a failsafe for blocking schemes.
- In 'Direct' mode, the likelihood of receiving commands in a noisy environment is small. In this case, we recommend you set ***IM# Fallback Mode*** to `Default` with a short ***IM# FrameSyncTim*** setting. Set ***IM# DefaultValue*** to '0'. This means that if a corrupt message is received, InterMiCOM will use the default value. This provides a substitute for the intertrip signal not being received, applying a failsafe for direct intertripping schemes.
- In 'Permissive' mode, the likelihood of receiving a valid command under noisy communications conditions is somwhere between that of the 'Blocking' mode and the 'Direct' intertrip mode. In this case, we recommended you set ***IM# Fallback Mode*** to `Latched`.

The table below presents recommended ***IM# FrameSyncTim*** settings for the different signalling modes and baud rates:

	Minimum Recommended "IM# FrameSyncTim" Setting			
Baud Rate	Direct Intertrip Mode	Blocking Mode	Minimum Setting (ms)	Maximum Setting (ms)
600	100	250	100	1500
1200	50	130	50	1500
2400	30	70	30	1500
4800	20	40	20	1500
9600	10	20	10	1500
19200	10	10	10	1500

Note:
As we have recommended Latched operation, the table does not contain recommendations for 'Permissive' mode. However, if you do select 'Default' mode, you should set ***IM# FrameSyncTim*** *greater than those listed above. If you set* ***IM# FrameSyncTim*** *lower than the minimum setting listed above, the device could interpret a valid change in a message as a corrupted message.*

We recommend a setting of 25% for the communications failure alarm.

CHAPTER 18

COMMUNICATIONS

18.1 CHAPTER OVERVIEW

This product supports Substation Automation System (SAS), and Supervisory Control and Data Acquisition (SCADA) communication. It embraces the evolution of communications technologies, since microprocessor technologies were introduced into protection, control, and monitoring devices - now known as Intelligent Electronic Devices for the substation (IEDs).

All products support rugged serial communications for SCADA and SAS applications. Optionally, any product can support Ethernet communications for more advanced SCADA and SAS applications.

This chapter contains the following sections:

Chapter Overview 343
Communication Interfaces 344
Serial Communication 345
Ethernet Communication 348
Board Variants 349
Configuring IP Addresses 350
Redundant Ethernet Configurator 354
Redundancy Protocols 360
General Functions for Redundant Ethernet Boards 365
Simple Network Management Protocol (SNMP) 366
Data Protocols 373
Time Synchronisation 405

18.2 COMMUNICATION INTERFACES

The products have a number of standard and optional communication interfaces. The standard and optional hardware and protocols are summarised below:

Port	Availability	Physical Layer	Use	Data Protocols
Front	Standard	USB Type B	Local settings	Courier
Rear Port 1 (RP1 copper)	Standard	RS232/RS485/K-Bus	SCADA Remote settings	Courier, MODBUS, IEC60870-5-103, DNP3.0 (order option)
Rear Port 1 (RP1 fibre)	Optional	Fibre	SCADA Remote settings	Courier, MODBUS, IEC60870-5-103, DNP3.0 (order option)
Rear Port 2 (RP2)	Optional	RS232/RS485/K-Bus	SCADA Remote settings	SK4: Courier only SK5: InterMicom only
Ethernet	Optional	Ethernet	IEC 61850 Remote settings	IEC 61850, Courier (tunnelled)

Note:
Optional communications boards are always fitted into slot A.

Note:
It is only possible to fit one optional communications board, therefore RP2 and Ethernet communications are mutually exclusive.

18.3 SERIAL COMMUNICATION

The physical layer standards that are used for serial communications for SCADA purposes are:

- EIA(RS)485 (often abbreviated to RS485)
- K-Bus (a proprietary customisation of RS485)

USB is used for local communication with the IED (for transferring settings and downloading firmware updates).

RS485 is similar to RS232 but for longer distances and it allows daisy-chaining and multi-dropping of IEDs.

K-Bus is a proprietary protocol quite similar to RS485, but it cannot be mixed on the same link as RS485. Unlike RS485, K-Bus signals applied across two terminals are not polarised.

It is important to note that these are not data protocols. They only describe the physical characteristics required for two devices to communicate with each other.

For a description of the K-Bus standard see K-Bus and GE Vernova's K-Bus interface guide reference R6509.

A full description of the RS485 is available in the published standard.

18.3.1 USB FRONT PORT

The USB interface uses the proprietary Courier protocol for local communication with the MiCOM S1 Agile settings application software.

This is intended for temporary local connection and is not suitable for permanent connection. This interface uses a fixed baud rate of 19200 bps, 11-bit frame (8 data bits, 1 start bit, 1 stop bit, even parity bit), and a fixed device address of '1'.

The USB interface is a Type B connector. Normally a Type A to Type B USB cable will be required to communicate between MiCOM S1 Agile and the IED.

18.3.2 EIA(RS)485 BUS

The RS485 two-wire connection provides a half-duplex, fully isolated serial connection to the IED. The connection is polarised but there is no agreed definition of which terminal is which. If the master is unable to communicate with the product, and the communication parameters match, then it is possible that the two-wire connection is reversed.

The RS485 bus must be terminated at each end with 120 Ω 0.5 W terminating resistors between the signal wires.

The RS485 standard requires that each device be directly connected to the actual bus. Stubs and tees are forbidden. Loop bus and Star topologies are not part of the RS485 standard and are also forbidden.

Two-core screened twisted pair cable should be used. The final cable specification is dependent on the application, although a multi-strand 0.5 mm^2 per core is normally adequate. The total cable length must not exceed 1000 m. It is important to avoid circulating currents, which can cause noise and interference, especially when the cable runs between buildings. For this reason, the screen should be continuous and connected to ground at one end only, normally at the master connection point.

The RS485 signal is a differential signal and there is no signal ground connection. If a signal ground connection is present in the bus cable, then it must be ignored. At no stage should this be connected to the cable's screen or to the product’s chassis. This is for both safety and noise reasons.

It may be necessary to bias the signal wires to prevent jabber. Jabber occurs when the signal level has an indeterminate state because the bus is not being actively driven. This can occur when all the slaves are in receive mode and the master is slow to turn from receive mode to transmit mode. This may be because the master is waiting in receive mode, in a high impedance state, until it has something to transmit. Jabber causes the receiving device(s) to miss the first bits of the first character in the packet, which results in the slave rejecting the message and consequently not responding. Symptoms of this are poor response times (due to retries), increasing message error counts, erratic communications, and in the worst case, complete failure to communicate.

18.3.2.1 EIA(RS)485 BIASING REQUIREMENTS

Biasing requires that the signal lines be weakly pulled to a defined voltage level of about 1 V. There should only be one bias point on the bus, which is best situated at the master connection point. The DC source used for the bias must be clean to prevent noise being injected.

Note:
Some devices may be able to provide the bus bias, in which case external components would not be required.

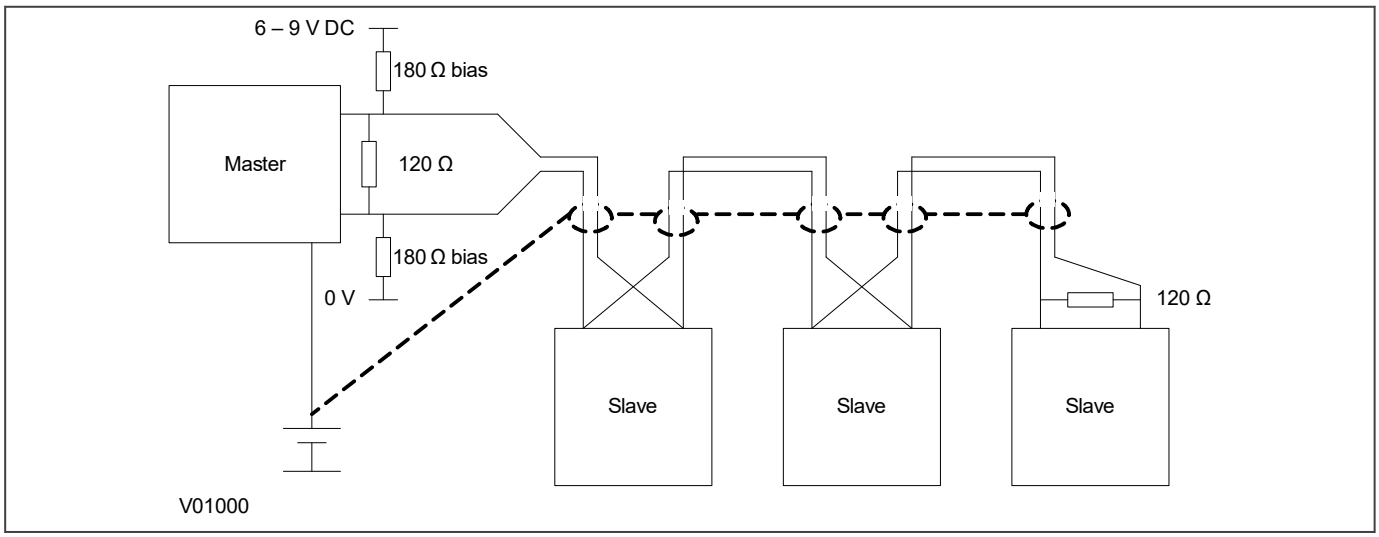


Figure 193: RS485 biasing circuit

Warning:
It is extremely important that the 120 Ω termination resistors are fitted. Otherwise the bias voltage may be excessive and may damage the devices connected to the bus.

18.3.3 K-BUS

K-Bus is a robust signalling method based on RS485 voltage levels. K-Bus incorporates message framing, based on a 64 kbps synchronous HDLC protocol with FM0 modulation to increase speed and security.

The rear interface is used to provide a permanent connection for K-Bus, which allows multi-drop connection.

A K-Bus spur consists of up to 32 IEDs connected together in a multi-drop arrangement using twisted pair wiring. The K-Bus twisted pair connection is non-polarised.

It is not possible to use a standard EIA(RS)232 to EIA(RS)485 converter to convert IEC 60870-5 FT1.2 frames to K-Bus. A protocol converter, namely the KITZ101 or KITZ102, must be used for this purpose. Please consult GE Vernova for information regarding the specification and supply of KITZ devices. The following figure demonstrates a typical K-Bus connection.

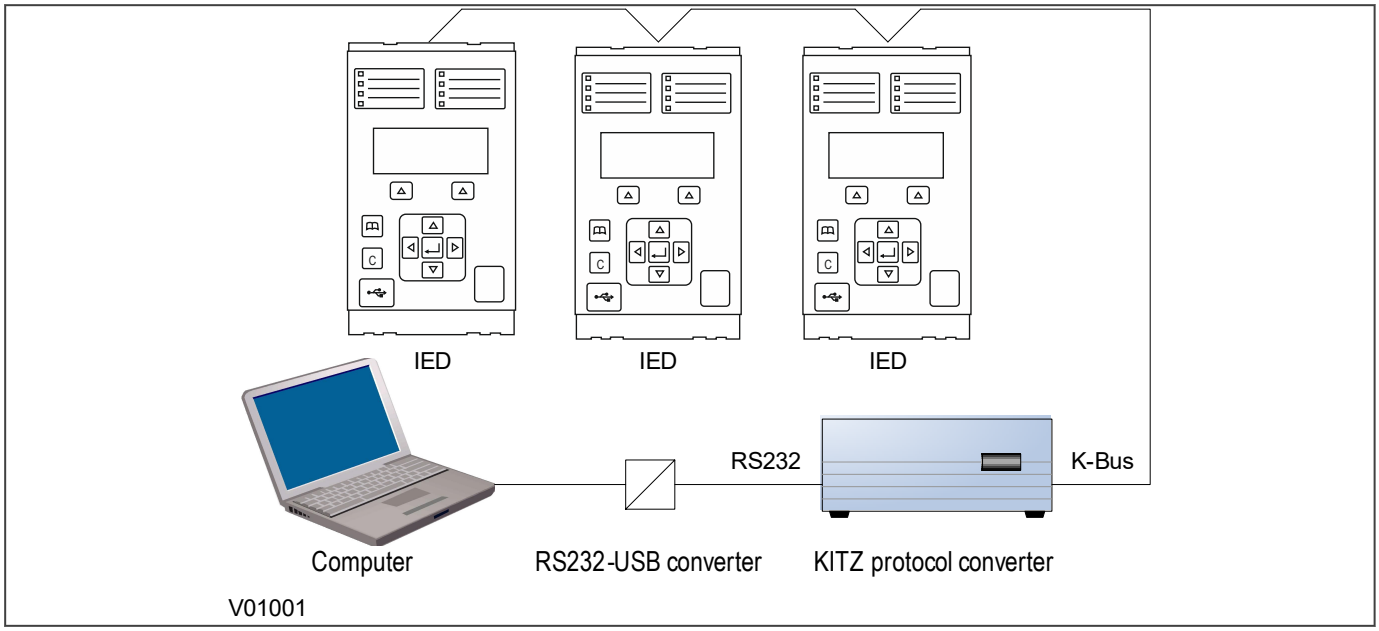


Figure 194: Remote communication using K-Bus

Note:
An RS232-USB converter is only needed if the local computer does not provide an RS232 port.

Further information about K-Bus is available in the publication R6509: K-Bus Interface Guide, which is available on request.

18.4 ETHERNET COMMUNICATION

The type of Ethernet board depends on the chosen model. The available boards and their features are described in the Hardware Design chapter of this manual.

The Ethernet interface is required for IEC 61850, and the Ethernet interface also offers communication with the S1 Agile settings application software for remote configuration and record extraction.

Fibre optic connection is recommended for use in permanent connections in a substation environment, as it offers advantages in terms of noise rejection. The fibre optic ports provide 100 Mbps communication and use either ST or LC connectors, depending on the board chosen. Fibres should be suitable for 1300 nm transmission and be multimode 50/125 µm or 62.5/125 µm.

Some Ethernet boards provide "copper" 100Base-TX ports using an RJ45 connector.

18.5 BOARD VARIANTS

Each board combines Ethernet communications, with IRIG-B timing functionality. There is a choice of embedded protocols for the Ethernet communications, and two types of IRIG-B.

Board variants

Board	Part No.	Compatible with
Redundant Ethernet SHP, 2 multi-mode fibre ports + modulated IRIG-B	ZN0071 001	Proprietary Self-Healing Protocol C264-SWR212 and MiCOM H35x multi-mode switches
Redundant Ethernet SHP, 2 multi-mode fibre ports + demodulated IRIG-B	ZN0071 002	Proprietary Self-Healing Protocol C264-SWR212 and MiCOM H35x multi-mode switches
Redundant Ethernet RSTP, 2 multi-mode fibre ports + modulated IRIG-B	ZN0071 005	Any RSTP device
Redundant Ethernet RSTP, 2 multi-mode fibre ports + demodulated IRIG-B	ZN0071 006	Any RSTP device
Redundant Ethernet DHP, 2 multi-mode fibre ports + modulated IRIG-B	ZN0071 007	Proprietary Dual-Homing Protocol C264-SWD212 and MiCOM H36x multi-mode switches
Redundant Ethernet DHP, 2 multi-mode fibre ports + demodulated IRIG-B	ZN0071 008	Proprietary Dual-Homing Protocol C264-SWD212 and MiCOM H36x multi-mode switches
Redundant Ethernet PRP, 2 multi-mode fibre ports + modulated IRIG-B	ZN0071 009	Any PRP device
Redundant Ethernet PRP, 2 multi-mode fibre ports + demodulated IRIG-B	ZN0071 010	Any PRP device
Redundant Ethernet PRP/HSR, 2 multi-mode fibre ports + modulated IRIG-B	ZN0071 109	Any PRP or HSR device
Redundant Ethernet PRP/HSR, 2 multi-mode fibre ports + demodulated IRIG-B	ZN0071 110	Any PRP or HSR device
Redundant Ethernet PRP/HSR/RSTP/Failover, 2 multi-mode fibre ports + Modulated/Un-Modulated IRIG-B	ZN0087 001	Any PRP, HSR, RSTP or standard Ethernet network.
Redundant Ethernet PRP/HSR/RSTP/Failover, 2 copper ports RJ45 + Modulated/Un-Modulated IRIG-B	ZN0087 002	Any PRP, HSR, RSTP or standard Ethernet network.
Redundant Ethernet PRP/HSR/RSTP/Failover, 1 copper port RJ45 + 1 multi-mode fibre port + Modulated/Un-Modulated IRIG-B	ZN0087 003	Any PRP, HSR, RSTP or standard Ethernet network.

When using any of the redundant Ethernet boards on an IED the final product will have two MAC addresses and will require two IP addresses, one for the managed embedded switch that handles the redundancy and one for the IED that handles the communications at protocol level and to S1 Agile. The MAC address of the embedded switch is printed on the board. The MAC address of the IED is printed on the rear panel of the IED. The redundant Ethernet board is fitted into Slot A of the IED, which is the optional communications slot.

All Ethernet connections are made with 1300 nm multi mode 100BaseFx fiber optic Ethernet ports (ST® connector). The boards can support both IEC 61850 and DNP3.0 over Ethernet.

Note:
SHP and DHP are proprietary protocols providing extremely fast recovery time. These boards offer compatibility with C264-SWR212/SWD212 and MiCOM H35x/H36x multi-mode switches.

18.6 CONFIGURING IP ADDRESSES

An IP address is a logical address assigned to devices in a computer network that uses the Internet Protocol (IP) for communication between nodes. IP addresses are stored as binary numbers but they are represented using Decimal Dot Notation, where four sets of decimal numbers are separated by dots as follows:

XXX.XXX.XXX.XXX

For example:

10.86.254.85

An IP address in a network is usually associated with a subnet mask. The subnet mask defines which network the device belongs to. A subnet mask has the same form as an IP address.

For example:

255.255.255.0

For IEDs fitted with R/S/T Ethernet boards, both the IED and the REB each have their own IP address. The following diagram shows the IED as IP1 and the REB as IP2.

Note:
IP1 and IP2 are different but use the same subnet mask.

The REB IP address (IP2) must be configured through the Ethernet network.

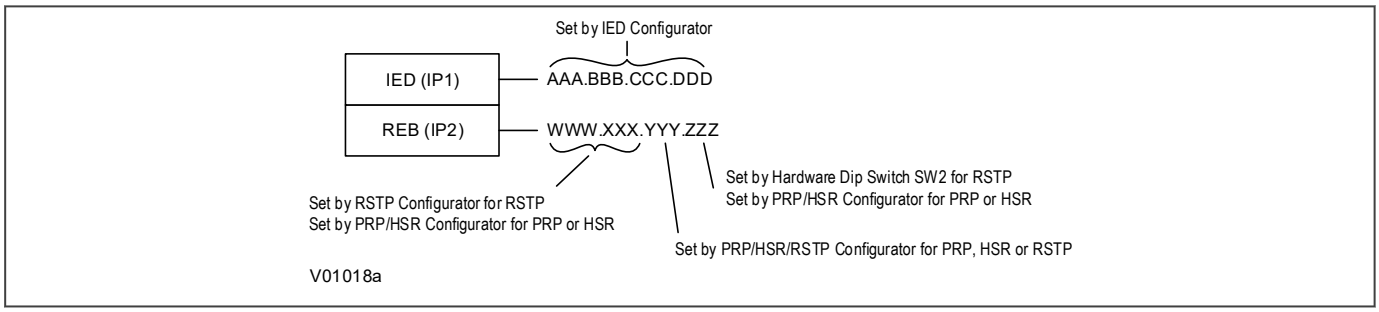


Figure 195: IED and REB IP address configuration

18.6.1 CONFIGURING THE IED IP ADDRESS

If the relay supports IEC 61850, set the IED IP1 address using the IEC 61850 Configurator software. In the IEC 61850 Configurator, set **Media** to **Single Copper or Redundant Fibre** for all Redundant Ethernet Board variants.

If the relay supports DNP3 over Ethernet, set the IED IP1 address by editing the DNP3 file, using the DNP3 Configurator software. In the DNP3 Configurator, set **Ethernet Media** to **Copper**, even though the redundant Ethernet network uses fibre optic cables.

18.6.2 CONFIGURING THE REB IP ADDRESS (R/S/T) ONLY

The board IP address must be configured before connecting the IED to the network to avoid an IP address conflict. The way you configure the IP address depends on the redundancy protocol you have chosen.

PRP/HSR/RSTP/Failover

Starting from S1 Agile 2.0.1. Any card that supports any of PRP/HSR/RSTP/Failover protocols in any of the combinations is configured using the Redundant Ethernet Configurator software tool and if using a ZN008700X card only this tool supports it. If using S1 Agile 1.4.2 or older you will need to use the PRP/HSR Configurator for PRP and/or HSR, and the RSTP Configurator for RSTP cards.

SHP or DHP

If using SHP or DHP the first two octets are set by the Switch Manager software or an SNMP MIB browser. The third octet is fixed at 254 (FE hex, 11111110 binary), and the fourth octet is set by the on-board dip switch.

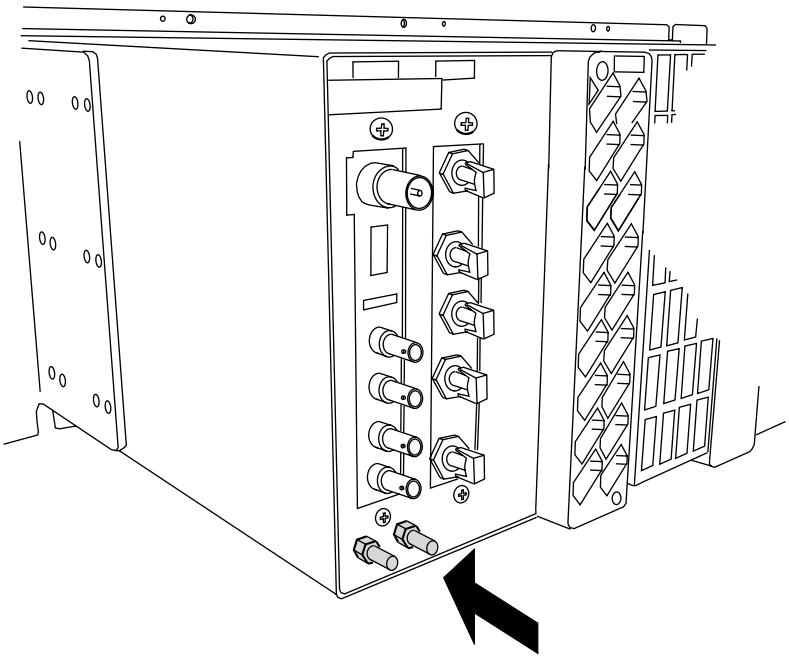
Note:
An H35 (SHP) or H36 (DHP) network device is needed in the network to configure the REB IP address.

18.6.2.1 CONFIGURING THE LAST OCTET (SHP, DHP, RSTP)

If using SHP or DHP, the last octet is configured using board address switch SW2 on the board. Remove the IED front cover to gain access to the board address switch.

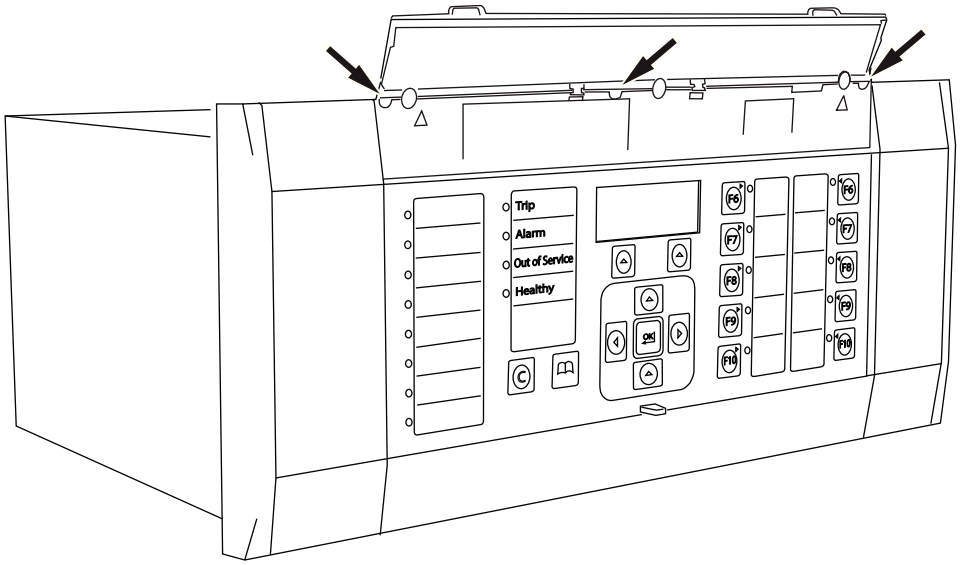
Warning:
Configure the hardware settings before the device is installed.

1. Refer to the safety section of the IED.
2. Switch off the IED. Disconnect the power and all connections.
3. Before removing the front cover, take precautions to prevent electrostatic discharge damage according to the ANSI/ESD-20.20 -2007 standard.
4. Wear a 1 MΩ earth strap and connect it to the earth (ground) point on the back of the IED.



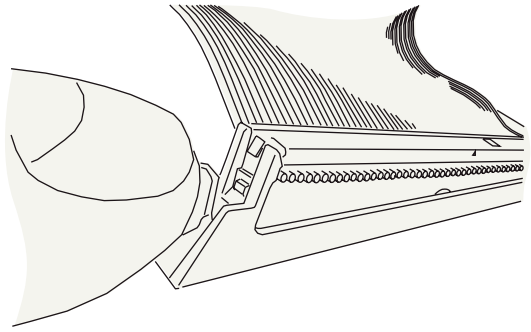
E01019

- Lift the upper and lower flaps. Remove the six screws securing the front panel and pull the front panel outwards.



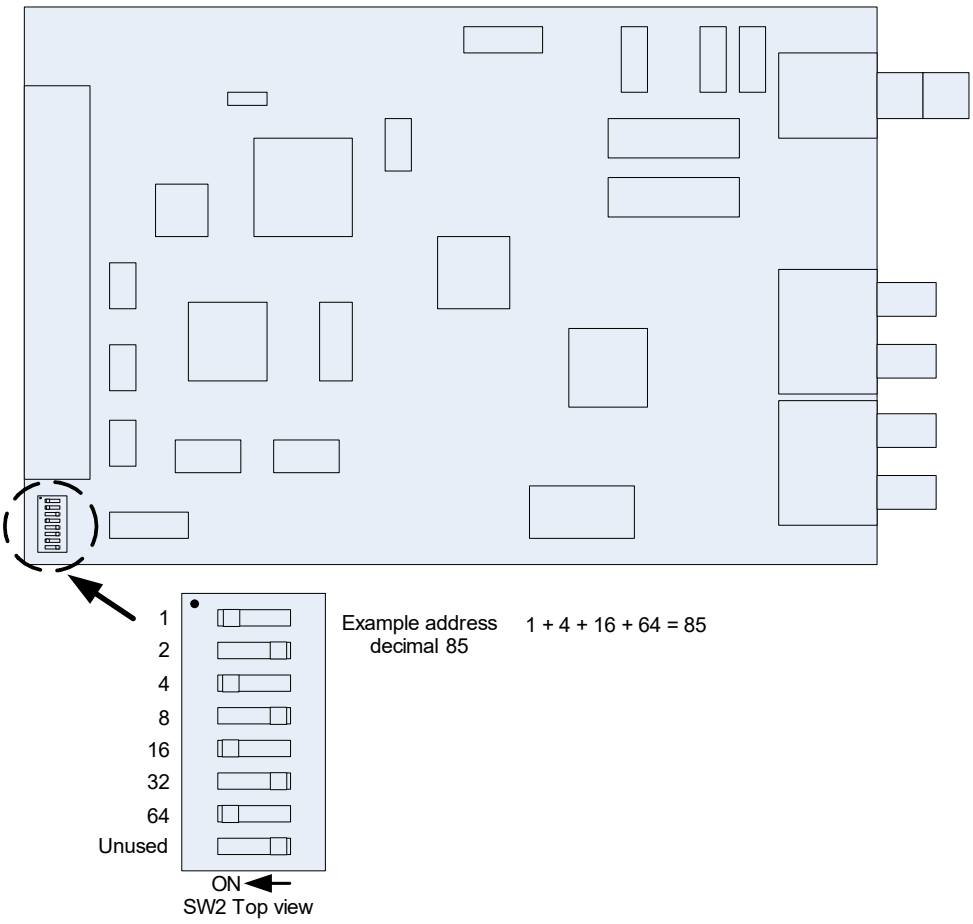
E01020

- Press the levers either side of the connector to disconnect the ribbon cable from the front panel.



E01021

- Remove the redundant Ethernet board. Set the last octet of IP address using the DIP switches. The available range is 1 to 127.



- Once you have set the IP address, reassemble the IED, following these instructions in the reverse order.

Warning:
Take care not to damage the pins of the ribbon cable connector on the front panel when reinserting the ribbon cable.

18.7 REDUNDANT ETHERNET CONFIGURATOR

The Redundant Ethernet Configurator tool is intended for MiCOM Px4x IEDs with redundant Ethernet using PRP (Parallel Redundancy Protocol), HSR (High-availability Seamless Redundancy), RSTP (Rapid Spanning Tree Protocol) or Failover. This tool is used to identify IEDs, switch between PRP, HSR, RSTP and Failover, configure their parameters, configure the redundancy IP address, or configure the SNTP IP address.

18.7.1 CONNECTING THE IED TO A PC

Connect the IED to the PC on which the Configurator tool is used. This connection is done through an Ethernet switch or through a media converter.

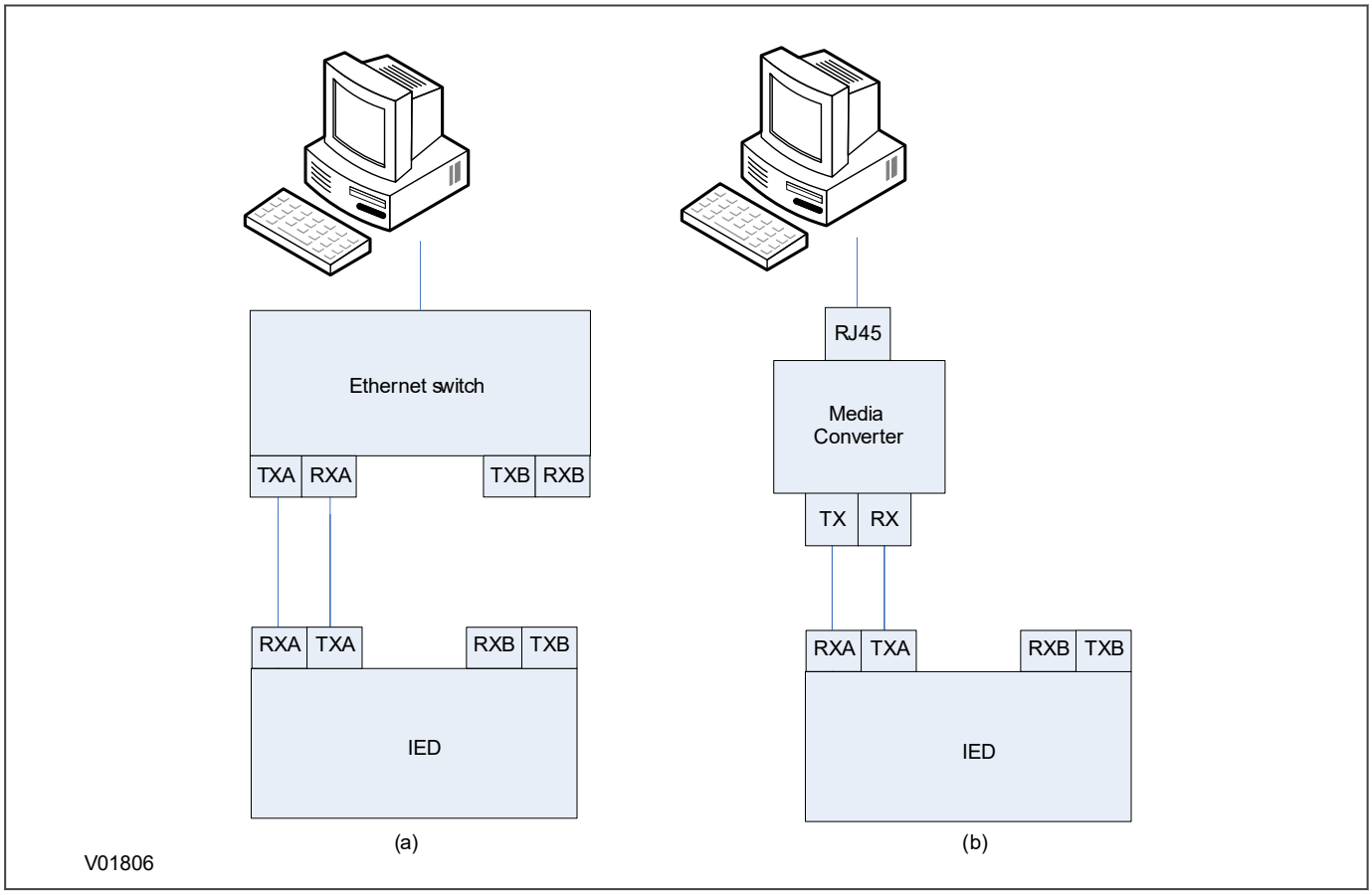


Figure 196: Connection using (a) an Ethernet switch and (b) a media converter

18.7.2 INSTALLING THE CONFIGURATOR

The Redundant Ethernet Configurator is installed as part of S1 Agile 2.0.1 onwards.

18.7.3 STARTING THE CONFIGURATOR

To start the configurator:

1. Go to S1 Agile and select the **Ethernet Configuration** tile, then select the **Redundant Ethernet Configurator** tile.
2. The Login screen appears. For user mode login, enter the **Login name** as **User** and click **OK** with no password. This level allows for IP address changes only. For Admin mode login, enter the **Login name** as **Admin** and password **Admin** and click **OK**. This level allows for network protocol configurations.
3. If the login screen does not appear, check all network connections.
4. From the **Network Board** drop-down list select the Network Board, IP Address and MAC Address of the PC in which the Configurator is running.

18.7.4 DEVICE IDENTIFICATION

To configure the redundant Ethernet board, go to the main window and click the **Identify Device** button. A list of devices are shown with the following details:

- Device address
- MAC address
- Version number of the firmware
- SNTP IP address
- Date & time of the real-time clock, from the board.

Select the device you wish to configure. The MAC address of the selected device is highlighted.

18.7.5 SELECTING THE DEVICE MODE

You must now select the device mode that you wish to use. This will be either PRP, HSR, RSTP or Failover. To do this, select the appropriate radio button then click the **Update** button. You will be asked to confirm a device reboot. Click **OK** to confirm.

18.7.6 FILTER BY BOARD TYPE

Once the list has been populated you can use the filter option to show only Process Bus cards or Station Bus cards by selecting the appropriate checkbox.

18.7.7 PASSWORD CONFIGURATION

To assign a password the current password needs to be input first, then a new password can be given. The default password is AAAA.

If the password does not follow NERC rules a message will be shown. Click on the **NERC Rules** button to review the rules.

If the password is not known, the password can be recovered by using the **Recover Password** button and following the instructions.

18.7.8 IP ADDRESS CONFIGURATION

To change the network address component of the IP address:

1. From the main window click the **IP Config** button. The **Device setup** screen appears.
2. Enter the required board IP address and click **OK**. This is the network address for the redundancy card, not the IED IP address, which is set in the IED Configurator or DNP3.0 over Ethernet section.
3. The board network address is updated and displayed in the main window.

18.7.9 SNTP IP ADDRESS CONFIGURATION

If using SNMP to poll information from the REB, an SNTP server can be used to synchronise the time of the reported messages. To configure the SNTP server IP address:

1. From the main window click the **SNTP Config** button. The **Device setup** screen appears.
2. Enter the required **MAC SNTP address** and server **IP SNTP Address**. Click **OK**.
3. The updated MAC and IP SNTP addresses appear in the main screen.

18.7.10 CHECK MAC TABLE FOR CONNECTED EQUIPMENT

To check what devices are connected to the device being monitored:

1. From the main window, select the device.
2. Click the **MAC Table** button.
3. At the bottom of the main window, a box shows the ports where devices are connected and their MAC addresses.

18.7.11 PRP CONFIGURATION

To view or configure the PRP Parameters:

1. Ensure that you have set the device mode to **PRP**.
2. Click the **PRP/HSR Configuration** button. The **PRP Configuration Parameters** screen appears.
3. To view the available parameters, click the **Get PRP Parameters** button.
4. To change the parameters, click the **Set Parameters** button and modify their values.

If you need to restore the default values of the parameters, click the **Restore Defaults** button.

The configurable parameters are as follows:

- **Multicast Address**: Use this field to configure the multicast destination address. All DANPs in the network must be configured to operate with the same multicast address for the purpose of network supervision.
- **Node Forget Time**: This is the time after which a node entry is cleared in the nodes table.
- **Life Check Interval**: This defines how often a node sends a PRP_Supervision frame. All DANPs shall be configured with the same Life Check Interval.

18.7.12 HSR CONFIGURATION

To view or configure the HSR Parameters:

1. Click the **PRP/HSR Configuration** button. The **HSR Configuration Parameters** screen appears.
2. To view the available parameters in the board that is connected, click the **Get HSR Parameters** button.
3. To change the parameters, click the **Set HSR Parameters** button and modify their values.

If you need to restore the default values of the parameters, click the **Restore Defaults** button.

The configurable parameters are as follows:

- **Multicast Address**: Use this field to configure the multicast destination address. All DANPs in the network must be configured to operate with the same multicast address for the purpose of network supervision.
- **Node Forget Time**: This is the time after which a node entry is cleared in the nodes table.
- **Life Check Interval**: This defines how often a node sends a PRP Supervision frame. All DANPs must be configured with the same Life Check Interval.

- **Proxy Node Table Forget Time**: This is the time after which a node entry is cleared in the ProxyTable.
- **Proxy Node Table Max Entries**: This is the maximum number of entries in the ProxyTable.
- **Entry Forget Time**: This is the time after which an entry is removed from the duplicates.
- **Node Reboot Interval**: This is the minimum time during which a node that reboots remains silent.

18.7.13 RSTP CONFIGURATION

1. To view or configure the RSTP Bridge Parameters, from the main window, click the device address to select the device. The selected device MAC address appears highlighted.
2. Click the **RSTP Configuration** button. The **RSTP Configuration** screen appears.
3. To view the available parameters in the board that is connected, click the **Get RSTP Parameters** button.
4. To set the configurable parameters such as Bridge Max Age, Bridge Hello Time, Bridge Forward Delay, and Bridge Priority, modify the parameter values according to the following table and click **Set RSTP Parameters**.

S.No	Parameter	Default Value (second)	Minimum Value (second)	Maximum Value (second)
1	Bridge Max Age	20	6	40
2	Bridge Hello Time	2	1	10
3	Bridge Forward Delay	15	4	30
4	Bridge Priority	32768	0	61440

18.7.14 BRIDGE PARAMETERS

To read the RSTP bridge parameters from the board,

1. From the main window click the device address to select the device. The **RSTP Configuration** window appears, and the default tab is **Bridge Parameters**.
2. Click the **Get RSTP Parameters** button. This displays all the RSTP bridge parameters from the Ethernet board.
3. To modify the RSTP parameters, enter the values and click **Set RSTP Parameters**.
4. To restore the default values, click **Restore Default** and click **Set RSTP Parameters**.

The greyed parameters are read-only and cannot be modified.

Note:
When assigning the bridge priority, make sure the root of the network is the Ethernet switch, not the IEDs. This reduces the number of hops to reach all devices in the network. Ensure the priority values for all IEDs are higher than that of the switch.

18.7.15 PORT PARAMETERS

This function is useful if you need to view the parameters of each port.

1. From the main window, click the device address to select the device. The **RSTP Configuration** window appears.
2. Select the **Port Parameters** tab, then click **Get Parameters** to read the port parameters. Alternatively, select the port numbers to read the parameters.

18.7.16 PORT STATES

This is used to see which ports of the board are enabled or disabled.

1. From the main window, click the device address to select the device. The **RSTP Configuration** window appears.
2. Select the **Port States** tab then click the **Get Port States** button. This lists the ports of the Ethernet board. A tick shows they are enabled.

18.7.17 FAILOVER CONFIGURATION

To view or configure the Failover Parameters:

Click the **Failover Configuration** button. The **Failover Configuration** screen appears.

1. To view the available parameters in the board that is connected, click the **Get Failover Parameters** button.
2. To change the parameters, click the **Set Failover Parameters** button and modify their values.

If you need to restore the default values of the parameters, click the **Restore Defaults** button. The configurable parameters are as follows:

- Port A and Port B select your main port for the Failover (Port A is the port at the top of your REB).
- The Failover time defines how long it takes for the redundancy switch over to trigger. The minimum value is 2s.

18.7.18 FILTERING DATABASE

The Filtering Database is used to determine how frames are forwarded or filtered across the Redundant Ethernet Board (REB). Filtering information specifies the set of ports to which frames received from a specific port are forwarded. The REB examines each received frame to see if the frame's destination address matches a source address listed in the Filtering Database. If there is a match, the device uses the filtering/forwarding information for that source address to determine how to forward or filter the frame. Otherwise, the frame is forwarded to all the ports in the REB.

General Tab

The Filtering Database contains two types of entry: static and dynamic. The Static Entries are the source addresses entered by an administrator. The Dynamic Entries are the source addresses learnt by the switch process. The Dynamic Entries are removed from the Filtering Database after the Ageing Time. The Database holds a maximum of 1024 entries.

1. To access the forwarding database functions, if required, click the Filtering Database button in the main window
2. To view the Forwarding Database Size, Number of Static Entries and Number of Dynamic Entries, click **Read Database Info**
3. To set the Ageing Time, enter the number of seconds in the text box and click the **Set** button

Filtering Entries Tab

The **Filtering Entries** section allows to set the Static MAC addresses and read dynamic ones. This will likely not be used in any application.

GOOSE Filtering Tab

The Filtering entries section allows to set the Static MAC addresses and read dynamic ones. This will likely not be used in any application. The GOOSE Filtering allows to filter GOOSE from being received based on Multicast MAC addresses. This can be done either by clicking on the checkboxes or by typing the desired range.

18.7.19 END OF SESSION

To finish the session:

1. In the main window, click the **Quit** button, a new screen appears.
2. If a database backup is required, click **Yes**, a new screen appears.
3. Click the **...** button to browse the path. Enter the name in the text box.

18.8 REDUNDANCY PROTOCOLS

REB variants for each of the following protocols are available:

- PRP (Parallel Redundancy Protocol)
- HSR (High-availability Seamless Redundancy)
- RSTP (Rapid Spanning Tree Protocol)
- Failover

PRP and HSR are open standard, so their implementation is compatible with any standard PRP or HSR device respectively. PRP and HSR provide "bumpless" redundancy. RSTP is also an open standard, so its implementation is compatible with any standard RSTP devices. RSTP provides redundancy, however, it is not "bumpless", the standard instead utilises a loop free topology that is recalculated when a device fails and does not forward messages during recalculation.

18.8.1 PARALLEL REDUNDANCY PROTOCOL (PRP)

Power system companies have traditionally used proprietary protocols for redundant communications. This is because standardised protocols could not meet the requirements for real-time systems. Even a short loss of connectivity may result in loss of functionality.

However, Parallel Redundancy Protocol (PRP) uses the IEC 62439 standard in Dual Star Topology networks, designed for IEDs from different manufacturers to operate with each other in a substation redundant-Ethernet network. PRP provides bumpless redundancy for real-time systems and is the standard for double Star-topology networks in substations.

18.8.1.1 PRP NETWORKS

Redundant networks usually rely on the network’s ability to reconfigure if there is a failure. However, PRP uses two independent networks in parallel.

PRP implements the redundancy functions in the end nodes rather than in network elements. This is one major difference to RSTP. An end node is attached to two similar LANs of any topology which operate in parallel.

The sending node replicates each frame and transmits them over both networks. The receiving node processes the frame that arrives first and discards the duplicate. Therefore, there is no distinction between the working and backup path. The receiving node checks that all frames arrive in sequence and that frames are correctly received on both ports.

The PRP layer manages this replicate and discard function and hides the two networks from the upper layers. This scheme works without reconfiguration and switchover, so it stays available ensuring no data loss.

There should be no common point of failure between the two LANs. Therefore, they are not powered by the same source and cannot be connected directly together. They are identical in protocol at the MAC level but may differ in performance and topology. Both LANs must be on the same subnet so all IP addresses must be unique.

18.8.1.2 NETWORK ELEMENTS

A PRP compatible device has two ports that operate in parallel. Each port is connected to a separate LAN. In the IEC 62439 standard, these devices are called DANP (Doubly Attached Node running PRP). A DAN has two ports, one MAC address and one IP address.

A Single Attached Node (SAN) is a non-critical node attached to only one LAN. SANs that need to communicate with each other must be on the same LAN.

The following diagram shows an example of a PRP network. The Doubly Attached Nodes DANP 1 and DANP 2 have full node redundancy. The Singly Attached Nodes SAN 1 and SAN 4 do not have any redundancy. Singly attached nodes can be connected to both LANs using a Redundancy Box (RedBox). The RedBox converts a singly attached node into a doubly attached node. Devices such as PCs with one network board, printers, and IEDs with

one network board are singly attached nodes. A SAN behind a RedBox appears like a DAN so is called a Virtual DAN (VDAN).

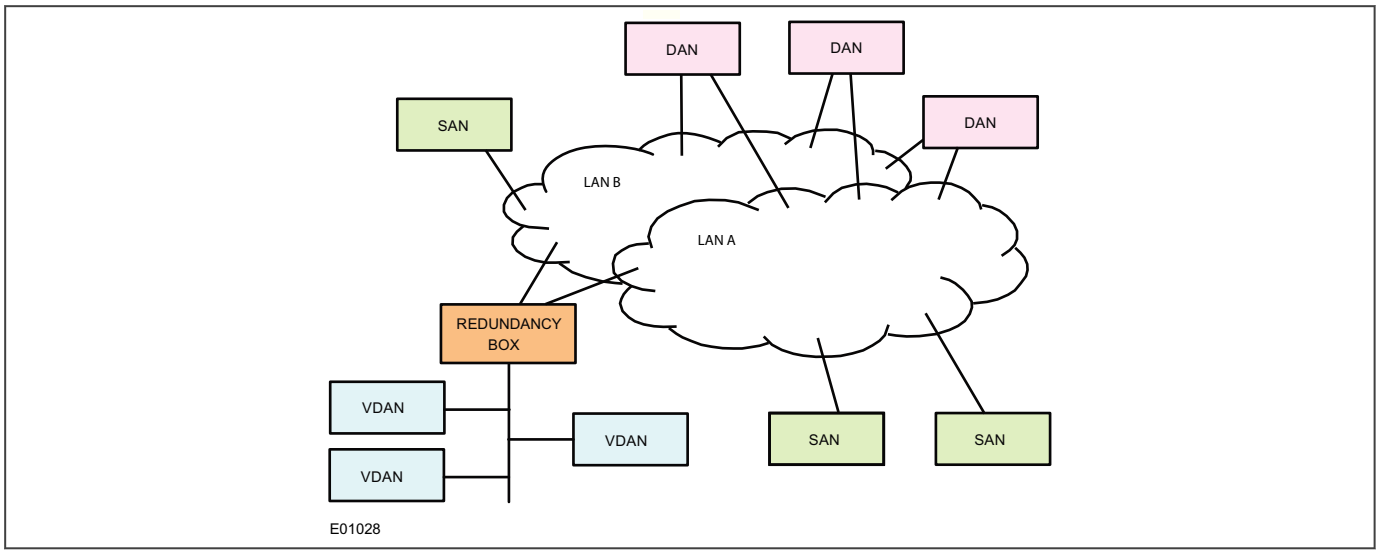


Figure 197: Example PRP redundant network

In a DAN, both ports share the same MAC address, so it does not affect the way devices talk to each other in an Ethernet network (Address Resolution Protocol at layer 2). Every data frame is seen by both ports.

When a DAN sends a frame of data, the frame is duplicated on both ports and therefore on both LAN segments. This provides a redundant path for the data frame if one of the segments fails. Under normal conditions, both LAN segments are working, and each port receives identical frames. There are two ways of handling this: Duplicate Accept and Duplicate Discard.

The GE Vernova RedBox is the H49 switch. This is compatible with any other vendor's PRP device.

18.8.2 HIGH-AVAILABILITY SEAMLESS REDUNDANCY (HSR)

HSR is standardised in IEC 62439-3 (clause 5) for use in ring topology networks. Similar to PRP, HSR provides bumpless redundancy and meets the most demanding needs of substation automation. HSR has become the reference standard for ring-topology networks in the substation environment. The HSR implementation of the redundancy Ethernet board (REB) is compatible with any standard HSR device.

HSR works on the premise that each device connected in the ring is a doubly attached node running HSR (referred to as DANH). Similar to PRP, singly attached nodes such as printers are connected via Ethernet Redundancy Boxes (RedBox).

18.8.2.1 HSR MULTICAST TOPOLOGY

When a DANH is sending a multicast frame, the frame (C frame) is duplicated (A frame and B frame), and each duplicate frame A/B is tagged with the destination MAC address and the sequence number. The frames A and B differ only in their sequence number, which is used to identify one frame from the other. Each frame is sent to the network via a separate port. The destination DANH receives two identical frames, removes the HSR tag of the first frame received and passes this (frame D) on for processing. The other duplicate frame is discarded. The nodes forward frames from one port to the other unless it was the node that injected it into the ring.

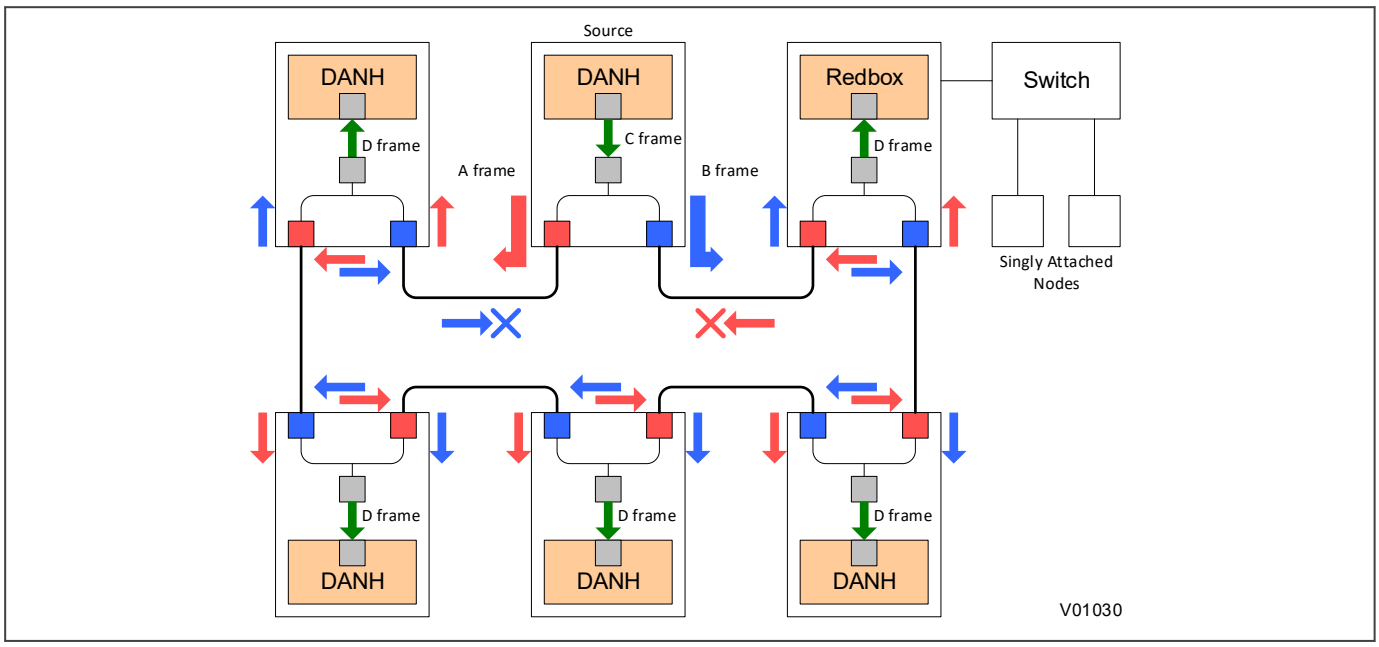


Figure 198: HSR multicast topology

Only about half of the network bandwidth is available in HSR for multicast or broadcast frames because both duplicate frames A & B circulate the full ring.

18.8.2.2 HSR UNICAST TOPOLOGY

With unicast frames, there is just one destination, and the frames are sent to that destination alone. All non-recipient devices simply pass the frames on. They do not process them in any way. In other words, D frames are produced only for the receiving DANH. This is illustrated below.

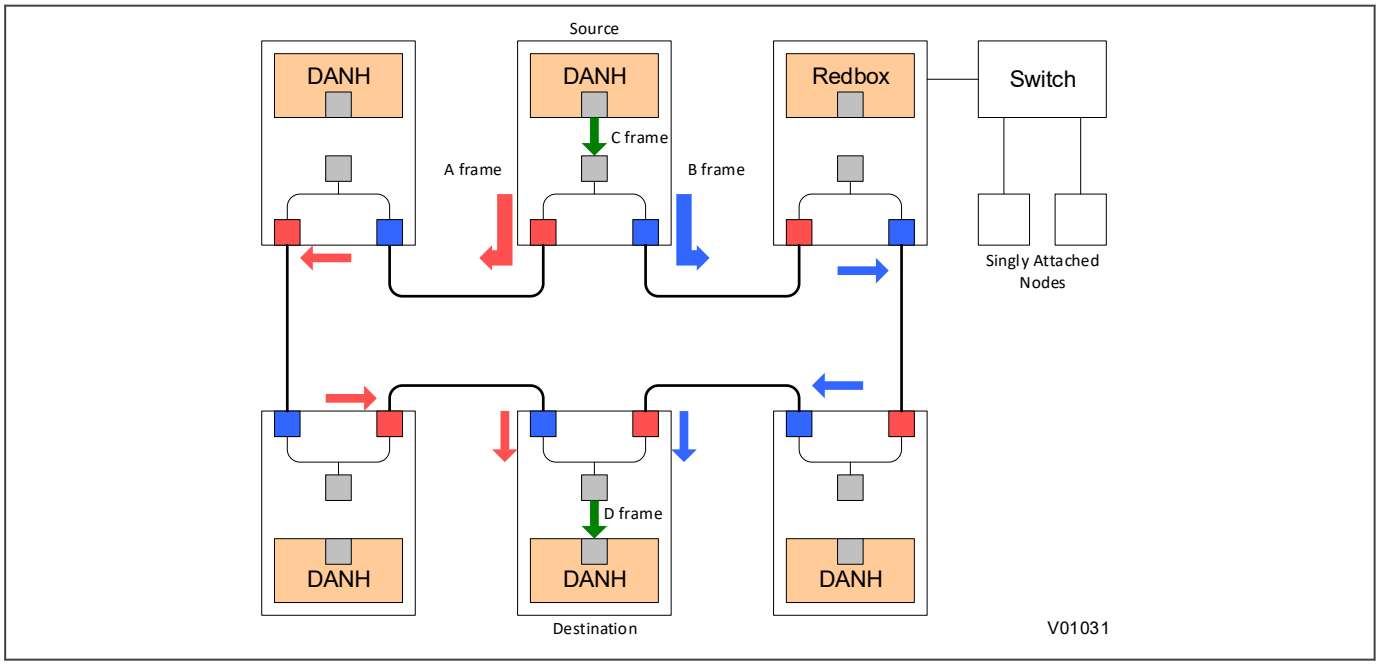


Figure 199: HSR unicast topology

For unicast frames, the whole bandwidth is available as both frames A & B stop at the destination node.

18.8.2.3 HSR APPLICATION IN THE SUBSTATION

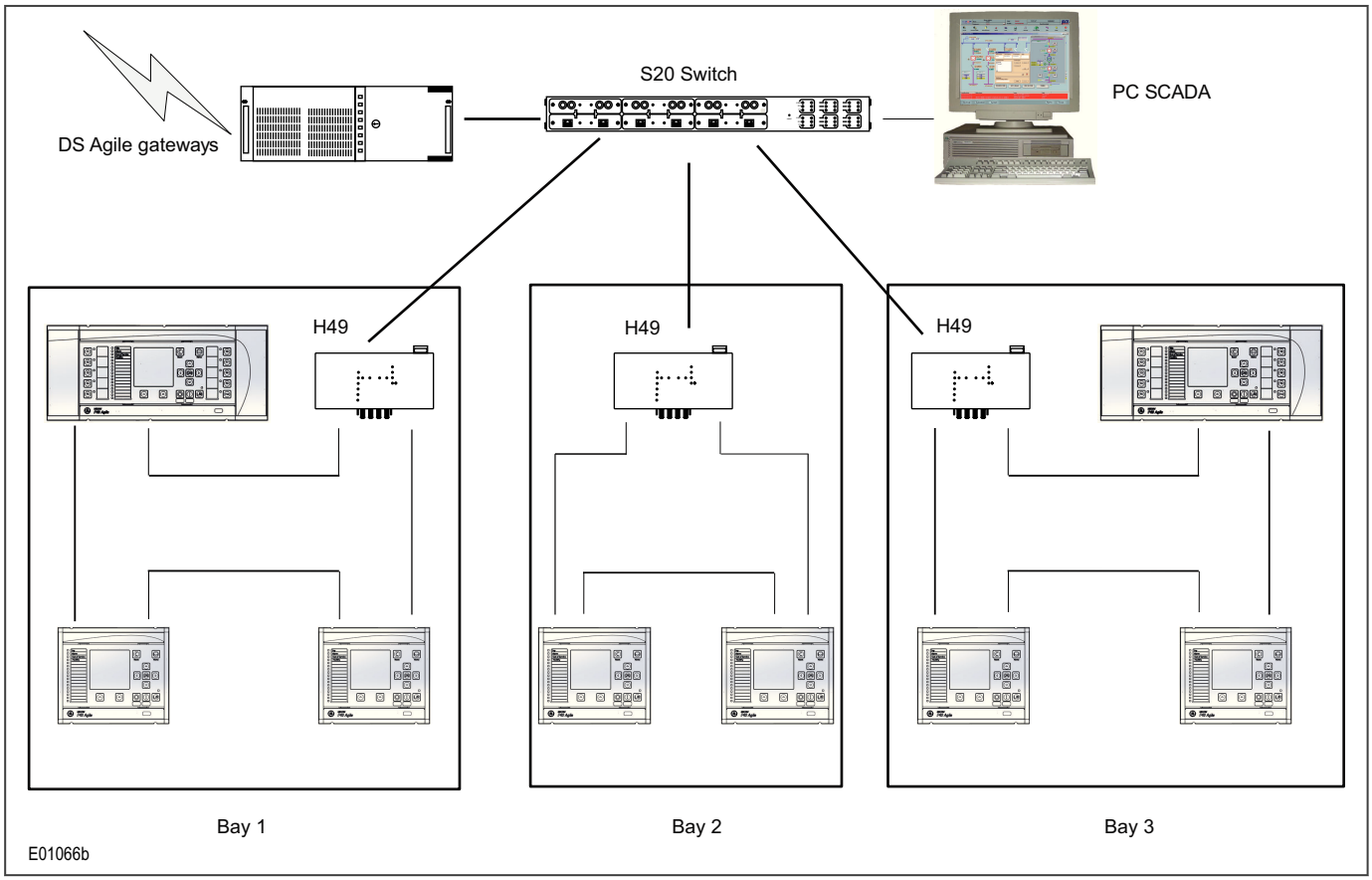


Figure 200: HSR application in the substation

18.8.3 RAPID SPANNING TREE PROTOCOL (RSTP)

RSTP is a standard used to quickly reconnect a network fault by finding an alternative path, allowing loop-free network topology. Although RSTP can recover network faults quickly, the fault recovery time depends on the number of devices and the topology. The recovery time also depends on the time taken by the devices to determine the root bridge and compute the port roles (discarding, learning, forwarding). The devices do this by exchanging Bridge Protocol Data Units (BPDUs) containing information about bridge IDs and root path costs. See the IEEE 802.1D 2004 standard for further information.

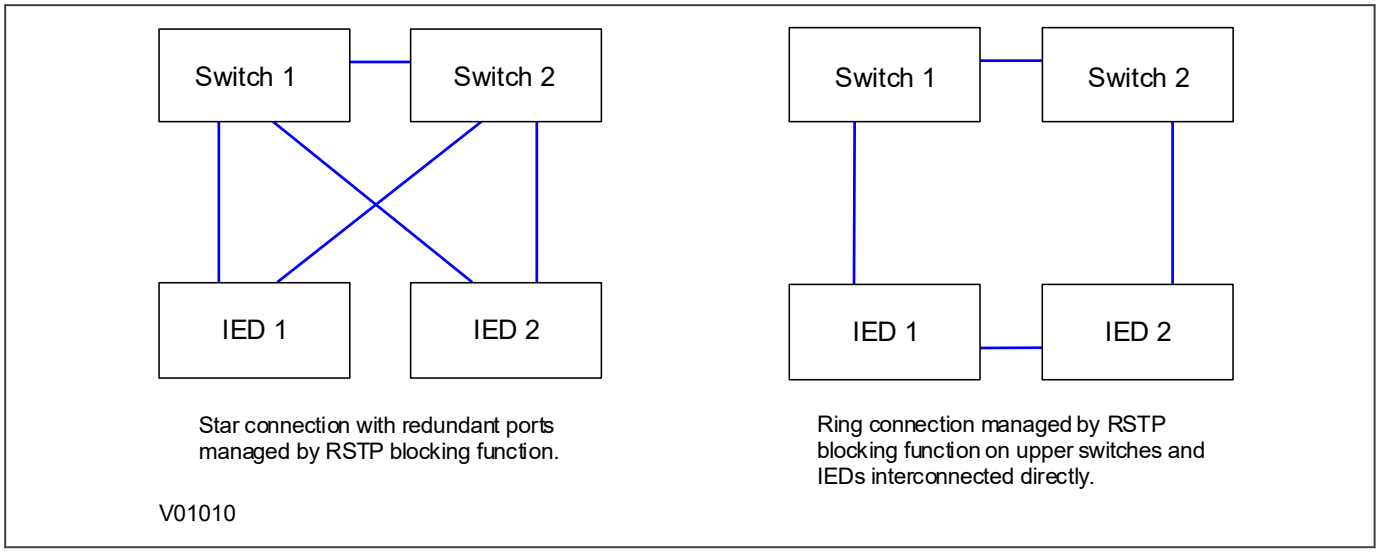


Figure 201: IED attached to redundant Ethernet star or ring circuit

The RSTP solution is based on open standards. It is therefore compatible with other Manufacturers' IEDs that use the RSTP protocol. The RSTP recovery time is typically 300 ms but it increases with network size, therefore cannot achieve the desired bumpless redundancy.

To ensure optimal performance of the protocol, make sure that one of the Ethernet switches is always the root of the RSTP topology.

18.8.4 FAILOVER

Failover is a simple redundancy mechanism that is not tied to any protocol. It works by selecting a main port and a switching time that can be as low as 2 seconds. When the main port link fails, the redundant port becomes physically active. At no point are both ports physically active, which means it can be used on any redundant or non-redundant network.

18.9 GENERAL FUNCTIONS FOR REDUNDANT ETHERNET BOARDS

The following functions apply to all redundant Ethernet protocols.

18.9.1 FORWARDING

The MiCOM Ethernet switch products support store and forward mode. The switch forwards messages with known addresses to the appropriate port. The messages with unknown addresses, the broadcast messages and the multicast messages are forwarded out to all ports except the source port. MiCOM switches do not forward error packets, 802.3x pause frames, or local packets. 802.1p priority tagging is enabled on all ports.

18.10 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Simple Network Management Protocol (SNMP) is a network protocol designed to manage devices in an IP network. The MiCOM P40 Modular products can provide up to two SNMP interfaces on Ethernet models; one to the IED's Main Processor for device level status information, and another directly to the redundant Ethernet board (where applicable) for specific Ethernet network level information.

Two versions of SNMP are supported: Version 2c, and a secure implementation of version 3 that includes cyber-security. Only the Main Processor SNMP interface supports Version 3.

18.10.1 SNMP MANAGEMENT INFORMATION BASES

SNMP uses a Management Information Base (MIB), which contains information about parameters to supervise. The MIB format is a tree structure, with each node in the tree identified by a numerical Object Identifier (OID). Each OID identifies a variable that can be read using SNMP with the appropriate software. The information in the MIB is standardised.

Each device in a network (workstation, server, router, bridge, etc.) maintains a MIB that reflects the status of the managed resources on that system, such as the version of the software running on the device, the IP address assigned to a port or interface, the amount of free hard drive space, or the number of open files. The MIB does not contain static data, but is instead an object-oriented, dynamic database that provides a logical collection of managed object definitions. The MIB defines the data type of each managed object and describes the object.

18.10.2 MAIN PROCESSOR MIBS STRUCTURE

The Main Processor MIB uses a private OID with a specific number assigned by the IANA. Some items in this MIB also support SNMP traps (where indicated). These are items that can automatically notify a host without being read.

Address											Name	Trigger Trap?
0											ROOT NODE	
	1										ISO	
		3									Org	
			6								DOD	
				1							Internet	
					4						Private	
						1					Enterprise	
							43534				(IANA No)	
								1			Px4x	
									1		System Data	
										1	Description	YES
										2	Plant Reference	YES
										3	Model Number	NO
										4	Serial Number	NO
										5	Frequency	NO
										6	Plant Status	YES
										7	Active Group	YES
										8	Software Ref.1	NO
										9	Software Ref.2	NO
										10	Access Level (UI)	YES
									2		Date and Time	

Address											Name	Trigger Trap?
										1	Date Time	NO
										2	IRIG-B Status	YES
										3	Battery Status	YES
										4	Active Sync source	YES
										5	SNTP Server 1	NO
										6	SNTP Server 2	NO
										7	SNTP Status	YES
										8	PTP Status	YES
									3		System Alarms	
										1	Invalid Message Format	YES
										2	Main Protection Fail	YES
										3	Comms Changed	YES
										4	Max Prop. Alarm	YES
										5	9-2 Sample Alarm	YES
										6	9-2LE Cfg Alarm	YES
										7	Battery Fail	YES
										8	Rear Communication Fail	YES
										9	GOOSE IED Missing	YES
										10	Intermicom loopback	YES
										11	Intermicom message fail	YES
										12	Intermicom data CD fail	YES
										13	Intermicom Channel fail	YES
										14	Backup setting fail	YES
										15	User Curve commit to flash failure	YES
										16	SNTP time Sync fail	YES
										17	PTP failure alarm	YES
									4		Device Mode	
										1	IED Mod/Beh	YES
										2	Simulation Mode of Subscription	YES

18.10.3 REDUNDANT ETHERNET BOARD MIB STRUCTURE

The Redundant Ethernet board MIB uses three types of OID:

- sysDescr
- sysUpTime
- sysName

MIB structure for RSTP

Address												Name
0												CCITT
	1											ISO
		3										Org
			6									DOD
				1								Internet

Address												Name
					2							mgmt
						1						Mib-2
							1					sys
								1				sysDescr
								3				sysUpTime
								4				sysName
Remote Monitoring												
							16					RMON
								1				statistics
									1			etherstat
										1		etherStatsEntry
											9	etherStatsUndersizePkts
											10	etherStatsOversizePkts
											12	etherStatsJabbers
											13	etherStatsCollisions
											14	etherStatsPkts64Octets
											15	etherStatsPkts65to127Octets
											16	etherStatsPkts128to255Octets
											17	etherStatsPkts256to511Octets
											18	etherStatsPkts512to1023Octets

MIB structure for PRP/HSR

Address												Name
0												ITU
	1											ISO
		0										Standard
			62439									IECHighavailibility
				3								PRP
					1							linkRedundancyEntityObjects
						0						lreConfiguration
							0					lreConfigurationGeneralGroup
								1				lreManufacturerName
								2				lreInterfaceCount
							1					lreConfigurationInterfaceGroup
								0				lreConfigurationInterfaces
									1			lreInterfaceConfigTable
										1		lreInterfaceConfigEntry
											1	lreInterfaceConfigIndex
											2	lreRowStatus
											3	lreNodeType
											4	lreNodeName
											5	lreVersionName
											6	lreMacAddressA

Address												Name
											7	IreMacAddressB
											8	IreAdapterAdminStateA
											9	IreAdapterAdminStateB
											10	IreLinkStatusA
											11	IreLinkStatusB
											12	IreDuplicateDiscard
											13	IreTransparentReception
											14	IreHsrLREMode
											15	IreSwitchingEndNode
											16	IreRedBoxIdentity
											17	IreSanA
											18	IreSanB
											19	IreEvaluateSupervision
											20	IreNodesTableClear
											21	IreProxyNodeTableClear
						1						IreStatistics
							1					IreStatisticsInterfaceGroup
								0				IreStatisticsInterfaces
									1			IreInterfaceStatsTable
											1	IreInterfaceStatsIndex
											2	IreCntTotalSentA
											3	IreCntTotalSentB
											4	IreCntErrWrongLANA
											5	IreCntErrWrongLANB
											6	IreCntReceivedA
											7	IreCntReceivedB
											8	IreCntErrorsA
											9	IreCntErrorsB
											10	IreCntNodes
											11	IreOwnRxCntA
											12	IreOwnRxCntB
									3			IreProxyNodeTable
										1		IreProxyNodeEntry
											1	reProxyNodeIndex
											2	reProxyNodeMacAddress
		3										Org
			6									Dod
				1								Internet
					2							mgmt
						1						mib-2
							1					System
								1				sysDescr
								3				sysUpTime

Address												Name
								5				sysName
								7				sysServices
							2					interfaces
								2				ifTable
									1			ifEntry
										1		ifIndex
										2		ifDescr
										3		ifType
										4		ifMtu
										5		ifSpeed
										6		ifPhysAddress
										7		ifAdminStatus
										8		ifOpenStatus
										9		ifLastChange
										10		ifInOctets
										11		ifInUcastPkts
										12		ifInNUcastPkts
										13		ifInDiscards
										14		ifInErrors
										15		ifInUnknownProtos
										16		ifOutOctets
										17		ifOutUcastPkts
										18		ifOutNUcastPkts
										19		ifOutDiscards
										20		ifOutErrors
										21		ifOutQLen
										22		ifSpecific
							16					rmon
								1				statistics
									1			etherStatsTable
										1		etherStatsEntry
											1	etherStatsIndex
											2	etherStatsDataSource
											3	etherStatsDropEvents
											4	etherStatsOctets
											5	etherStatsPkts
											6	etherStatsBroadcastPkts
											7	etherStatsMulticastPkts
											8	etherStatsCRCAlignErrors
											9	etherStatsUndersizePkts
											10	etherStatsOversizePkts
											11	etherStatsFragments
											12	etherStatsJabbers

Address												Name
											13	etherStatsCollisions
											14	etherStatsPkts64Octets
											15	etherStatsPkts65to127Octets
											16	etherStatsPkts128to255Octets
											17	etherStatsPkts256to511Octets
											18	etherStatsPkts512to1023Octets
											19	etherStatsPkts1024to1518Octets
											20	etherStatsOwner
											21	etherStatsStatus

18.10.4 ACCESSING THE MIB

Various SNMP client software tools can be used. We recommend using an SNMP MIB browser, which can perform the basic SNMP operations such as GET, GETNEXT and RESPONSE.

Note:
There are two IP addresses visible when communicating with the Redundant Ethernet Card via the fibre optic ports: Use the one for the IED itself to the Main Processor SNMP interface, and use the one for the on-board Ethernet switch to access the Redundant Ethernet Board SNMP interface. See the configuration chapter for more information.

18.10.5 MAIN PROCESSOR SNMP CONFIGURATION

You configure the main processor SNMP interface using the HMI panel. Two different versions are available; SNMPv2c and SNMPv3:

To enable the main processor SNMP interface:

1. Select the COMMUNICATIONS column and scroll to the SNMP PARAMETERS heading
2. You can select either v2C, V3 or both. Selecting None will disable the main processor SNMP interface.

SNMP Trap Configuration

SNMP traps allow for unsolicited reporting between the IED and up to two SNMP managers with unique IP addresses. The device MIB details what information can be reported using Traps. To configure the SNMP Traps:

1. Move down to the cell ***Trap Dest. IP 1*** and enter the IP address of the first destination SNMP manager. Setting this cell to `0.0.0.0` disables the first Trap interface.
2. Move down to the cell ***Trap Dest. IP 2*** and enter the IP address of the second destination SNMP manager. Setting this cell to `0.0.0.0` disables the Second Trap interface.

SNMP V3 Security Configuration

SNMPv3 provides a higher level of security via authentication and privacy protocols. The IED adopts a secure SNMPv3 implementation with a user-based security model (USM).

Authentication is used to check the identity of users, privacy allows for encryption of SNMP messages. Both are optional; however, you must enable authentication to enable privacy. To configure these security options:

1. If SNMPv3 has been enabled, set the ***Security Level*** setting. There are three levels: without authentication and without privacy (*noAuthNoPriv*), with authentication but without privacy (*authNoPriv*), and with authentication and with privacy (*authPriv*).
2. If Authentication is enabled, use the ***Auth Protocol*** setting to select the authentication type. There are two options: *HMAC-MD5-96* or *HMAC-SHA-96*.
3. Using the ***Auth Password*** setting, enter the 8-character password to be used by the IED for authentication.
4. If privacy is enabled, use the ***Encrypt Protocol*** setting to set the 8-character password that will be used by the IED for encryption.

Note:
When setting the SNMP browser for RBAC compatible relays, the Context Name should be 'px4x'.

SNMP V2C Security Configuration

SNMPv2c implements authentication between the master and agent using a parameter called ***Community Name***. This is effectively the password but it is not encrypted during transmission (this makes it inappropriate for some scenarios in which case version 3 should be used instead). To configure the SNMP 2c security:

1. If SNMPv2c has been enabled, use the ***Community Name*** setting to set the password that will be used by the IED and SNMP manager for authentication. This may be between one and 8 characters.

18.11 DATA PROTOCOLS

The products supports a wide range of protocols to make them applicable to many industries and applications. The exact data protocols supported by a particular product depend on its chosen application, but the following table gives a list of the data protocols that are typically available.

DATA PROTOCOLS

Data Protocol	Layer 1 Protocol	Description
Courier	USB, K-Bus, RS232, RS485, Ethernet	Standard for SCADA communications developed by GE Vernova
MODBUS	RS485	Standard for SCADA communications developed by Modicon
IEC 60870-5-103	RS485	IEC standard for SCADA communications
DNP 3.0	RS485	Standard for SCADA communications
IEC 61850	Ethernet	IEC standard for substation automation. Facilitates interoperability.

The relationship of these protocols to the lower level physical layer protocols are as follows:

Data Protocols	IEC 60870-5-103				
	MODBUS				
	DNP3.0	IEC 61850			
	Courier	Courier	Courier	Courier	Courier
Data Link Layer	EIA(RS)485	Ethernet	EIA(RS)232	K-Bus	USB
Physical Layer	Copper or Optical Fibre				USB Type B

18.11.1 COURIER

This section should provide sufficient detail to enable understanding of the Courier protocol at a level required by most users. For situations where the level of information contained in this manual is insufficient, further publications (R6511 and R6512) containing in-depth details about the protocol and its use, are available on request.

Courier is a GE Vernova proprietary communication protocol. Courier uses a standard set of commands to access a database of settings and data in the IED. This allows a master to communicate with a number of slave devices. The application-specific elements are contained in the database rather than in the commands used to interrogate it, meaning that the master station does not need to be preconfigured. Courier also provides a sequence of event (SOE) and disturbance record extraction mechanism.

18.11.1.1 PHYSICAL CONNECTION AND LINK LAYER

Courier can be used with four physical layer protocols: USB, K-Bus, EIA(RS)232 or EIA(RS)485.

Several connection options are available for Courier:

- The front USB port (for connection to Settings application software on, for example, a laptop).
- Rear Port 1 (RP1) - for permanent SCADA connection via serial RS485 or K-Bus
- Optional fibre port (RP1 in slot A) - for permanent SCADA connection via serial optical fibre
- Optional Rear Port 2 (RP2) - for permanent SCADA connection via serial RS485, K-Bus, or RS232

Optional Ethernet board (NIC) - for remote communication with the S1 Agile settings application software across an Ethernet network.

For either of the serial rear ports, both the IED address, and baud rate can be selected using the front panel menu or by the settings application software.

Note:
*Changing the **RP2 Port Config** setting (K-Bus, EIA(RS)232) requires the IED to be rebooted, for the change to become effective.*

18.11.1.2 COURIER DATABASE

The Courier database is two-dimensional and resembles a table. Each cell in the database is referenced by a row and column address. Both the column and the row can take a range from 0 to 255 (0000 to FFFF Hexadecimal. Addresses in the database are specified as hexadecimal values, for example, 0A02 is column 0A row 02. Associated settings or data are part of the same column. Row zero of the column has a text string to identify the contents of the column and to act as a column heading.

The product-specific menu databases contain the complete database definition.

18.11.1.3 SETTINGS CATEGORIES

There are two main categories of settings in protection IEDs:

- Control and support settings
- Protection settings

With the exception of the Disturbance Recorder settings, changes made to the control and support settings are implemented immediately and stored in non-volatile memory. Changes made to the Protection settings and the Disturbance Recorder settings are stored in 'scratchpad' memory and are not immediately implemented. These need to be committed by writing to the ***Save Changes*** cell in the *CONFIGURATION* column.

18.11.1.4 SETTING CHANGES

Courier provides two mechanisms for making setting changes. Either method can be used for editing any of the settings in the database.

Method 1

This uses a combination of three commands to perform a settings change:

First, enter Setting mode: This checks that the cell is settable and returns the limits.

1. Preload Setting: This places a new value into the cell. This value is echoed to ensure that setting corruption has not taken place. The validity of the setting is not checked by this action.
2. Execute Setting: This confirms the setting change. If the change is valid, a positive response is returned. If the setting change fails, an error response is returned.
3. Abort Setting: This command can be used to abandon the setting change.

This is the most secure method. It is ideally suited to on-line editors because the setting limits are extracted before the setting change is made. However, this method can be slow if many settings are being changed because three commands are required for each change.

Method 2

The Set Value command can be used to change a setting directly. The response to this command is either a positive confirm or an error code to indicate the nature of a failure. This command can be used to implement a setting more rapidly than the previous method; however, the limits are not extracted. This method is therefore most suitable for off-line setting editors such as MiCOM S1 Agile, or for issuing preconfigured control commands.

18.11.1.5 EVENT EXTRACTION

You can extract events either automatically (rear serial port only) or manually (either serial port). For automatic extraction, all events are extracted in sequential order using the Courier event mechanism. This includes fault and

maintenance data if appropriate. The manual approach allows you to select events, faults, or maintenance data as desired.

18.11.1.5.1 AUTOMATIC EVENT RECORD EXTRACTION

This method is intended for continuous extraction of event and fault information as it is produced. It is only supported through the rear Courier port.

When new event information is created, the ***Event*** bit is set in the ***Status*** byte. This indicates to the Master device that event information is available. The oldest, non-extracted event can be extracted from the IED using the ***Send Event*** command. The IED responds with the event data.

Once an event has been extracted, the ***Accept Event*** command can be used to confirm that the event has been successfully extracted. When all events have been extracted, the ***Event*** bit is reset. If there are more events still to be extracted, the next event can be accessed using the ***Send Event*** command as before.

18.11.1.5.2 MANUAL EVENT RECORD EXTRACTION

The *VIEW RECORDS* column (location 01) is used for manual viewing of event, fault, and maintenance records. The contents of this column depend on the nature of the record selected. You can select events by event number and directly select a fault or maintenance record by number.

Event Record Selection ('Select Event' cell: 0101)

This cell can be set the number of stored events. For simple event records (Type 0), cells 0102 to 0105 contain the event details. A single cell is used to represent each of the event fields. If the event selected is a fault or maintenance record (Type 3), the remainder of the column contains the additional information.

Fault Record Selection ('Select Fault' cell: 0105)

This cell can be used to select a fault record directly, using a value between 0 and 4 to select one of up to five stored fault records. (0 is the most recent fault and 4 is the oldest). The column then contains the details of the fault record selected.

Maintenance Record Selection ('Select Maint' cell: 01F0)

This cell can be used to select a maintenance record using a value between 0 and 4. This cell operates in a similar way to the fault record selection.

If this column is used to extract event information, the number associated with a particular record changes when a new event or fault occurs.

Event Types

The IED generates events under certain circumstances such as:

- Change of state of output contact
- Change of state of opto-input
- Protection element operation
- Alarm condition
- Setting change
- Password entered/timed-out

Event Record Format

The IED returns the following fields when the Send Event command is invoked:

- Cell reference
- Time stamp
- Cell text
- Cell value

The Menu Database contains tables of possible events, and shows how the contents of the above fields are interpreted. Fault and Maintenance records return a Courier Type 3 event, which contains the above fields plus two additional fields:

- Event extraction column
- Event number

These events contain additional information, which is extracted from the IED using column B4. Row 01 contains a ***Select Record*** setting that allows the fault or maintenance record to be selected. This setting should be set to the event number value returned in the record. The extended data can be extracted from the IED by uploading the text and data from the column.

18.11.1.6 DISTURBANCE RECORD EXTRACTION

The stored disturbance records are accessible through the Courier interface. The records are extracted using column (B4).

The ***Select Record*** cell can be used to select the record to be extracted. Record 0 is the oldest non-extracted record. Older records which have already been extracted are assigned positive values, while younger records are assigned negative values. To help automatic extraction through the rear port, the IED sets the ***Disturbance*** bit of the ***Status*** byte, whenever there are non-extracted disturbance records.

Once a record has been selected, using the above cell, the time and date of the record can be read from the ***Trigger Time*** cell (B402). The disturbance record can be extracted using the block transfer mechanism from cell B40B and saved in the COMTRADE format. The settings application software software automatically does this.

18.11.1.7 PROGRAMMABLE SCHEME LOGIC SETTINGS

The programmable scheme logic (PSL) settings can be uploaded from and downloaded to the IED using the block transfer mechanism.

The following cells are used to perform the extraction:

- ***Domain*** cell (B204): Used to select either PSL settings (upload or download) or PSL configuration data (upload only)
- ***Sub-Domain*** cell (B208): Used to select the Protection Setting Group to be uploaded or downloaded.
- ***Version*** cell (B20C): Used on a download to check the compatibility of the file to be downloaded.
- ***Transfer Mode*** cell (B21C): Used to set up the transfer process.
- ***Data Transfer*** cell (B120): Used to perform upload or download.

The PSL settings can be uploaded and downloaded to and from the IED using this mechanism. The settings application software must be used to edit the settings. It also performs checks on the validity of the settings before they are transferred to the IED.

The language of a recovered PSL file depends on the language of a settings file sent on the same interface used to recover the PSL file. All interfaces are set by default to English, which means by default, the relay will recover the PSL file in English on all interfaces.

As an example, if the PSL file needs to be recovered in French through the front port, the user is required to send the settings file to the relay in French through the front port prior to recovering the PSL file. While the PSL file will be

recovered in French through the front port, it will still be recovered in English through Ethernet and the rear RS485 port if available, unless and until the settings file is sent in French on those interfaces as well.

18.11.1.8 TIME SYNCHRONISATION

The time and date can be set using the time synchronisation feature of the Courier protocol. The device will correct for the transmission delay. The time synchronisation message may be sent as either a global command or to any individual IED address. If the time synchronisation message is sent to an individual address, then the device will respond with a confirm message. If sent as a global command, the (same) command must be sent twice. A time synchronisation Courier event will be generated/produced whether the time-synchronisation message is sent as a global command or to any individual IED address.

If the clock is being synchronised using the IRIG-B input then it will not be possible to set the device time using the Courier interface. An attempt to set the time using the interface will cause the device to create an event with the current date and time taken from the IRIG-B synchronised internal clock.

18.11.1.9 COURIER CONFIGURATION

To configure the device:

1. Select the *CONFIGURATION* column and check that the ***Comms settings*** cell is set to `Visible`.
2. Select the *COMMUNICATIONS* column.
3. Move to the first cell down (***RP1 protocol***). This is a non-settable cell, which shows the chosen communication protocol – in this case `Courier`.

```
COMMUNICATIONS
RP1 Protocol
Courier
```

4. Move down to the next cell (***RP1 Address***). This cell controls the address of the RP1 port on the device. Up to 32 IEDs can be connected to one spur. It is therefore necessary for each IED to have a unique address so that messages from the master control station are accepted by one IED only. Courier uses an integer number between 1 and 254 for the Relay Address. It is set to 255 by default, which has to be changed. It is important that no two IEDs share the same address.

```
COMMUNICATIONS
RP1 Address
100
```

5. Move down to the next cell (***RP1 InactivTimer***). This cell controls the inactivity timer. The inactivity timer controls how long the IED waits without receiving any messages on the rear port before revoking any password access that was enabled and discarding any changes. For the rear port this can be set between 1 and 30 minutes.

```
COMMUNICATIONS
RP1 Inactivtimer
10.00 mins.
```

6. If the optional fibre optic connectors are fitted, the ***RP1 PhysicalLink*** cell is visible. This cell controls the physical media used for the communication (Copper or Fibre optic).

```
COMMUNICATIONS
RP1 PhysicalLink
Copper
```

7. Move down to the next cell (***RP1 Card Status***). This cell is not settable. It displays the status of the chosen physical layer protocol for RP1.

```
COMMUNICATIONS
RP1 Card Status
K-Bus OK
```

8. Move down to the next cell (***RP1 Port Config***). This cell controls the type of serial connection. Select between K-Bus or RS485.

```
COMMUNICATIONS
RP1 Port Config
K-Bus
```

9. If using EIA(RS)485, the next cell (***RP1 Comms Mode***) selects the communication mode. The choice is either IEC 60870 FT1.2 for normal operation with 11-bit modems, or 10-bit no parity. If using K-Bus this cell will not appear.

```
COMMUNICATIONS
RP1 Comms Mode
IEC 60870 FT1.2
```

10. If using EIA(RS)485, the next cell down controls the baud rate. Three baud rates are supported; 9600, 19200 and 38400. If using K-Bus this cell will not appear as the baud rate is fixed at 64 kbps.

```
COMMUNICATIONS
RP1 Baud rate
19200
```

18.11.2 IEC 60870-5-103

The specification IEC 60870-5-103 (Telecontrol Equipment and Systems Part 5 Section 103: Transmission Protocols), defines the use of standards IEC 60870-5-1 to IEC 60870-5-5, which were designed for communication with protection equipment.

This section describes how the IEC 60870-5-103 standard is applied to the Px40 platform. It is not a description of the standard itself. The level at which this section is written assumes that the reader is already familiar with the IEC 60870-5-103 standard.

This section should provide sufficient detail to enable understanding of the standard at a level required by most users.

The IEC 60870-5-103 interface is a master/slave interface with the device as the slave device. The device conforms to compatibility level 2, as defined in the IEC 60870-5-103.standard.

The following IEC 60870-5-103 facilities are supported by this interface:

- Initialisation (reset)
- Time synchronisation
- Event record extraction
- General interrogation
- Cyclic measurements
- General commands
- Disturbance record extraction
- Private codes

18.11.2.1 PHYSICAL CONNECTION AND LINK LAYER

Two connection options are available for IEC 60870-5-103:

- Rear Port 1 (RP1) - for permanent SCADA connection via RS485
- Optional fibre port (RP1 in slot A) - for permanent SCADA connection via optical fibre

If the optional fibre optic port is fitted, a menu item appears in which the active port can be selected. However, the selection is only effective following the next power up.

The IED address and baud rate can be selected using the front panel menu or by the settings application software.

18.11.2.2 INITIALISATION

Whenever the device has been powered up, or if the communication parameters have been changed a reset command is required to initialize the communications. The device will respond to either of the two reset commands; Reset CU or Reset FCB (Communication Unit or Frame Count Bit). The difference between the two commands is that the Reset CU command will clear any unsent messages in the transmit buffer, whereas the Reset FCB command does not delete any messages.

The device will respond to the reset command with an identification message ASDU 5. The Cause of Transmission (COT) of this response will be either Reset CU or Reset FCB depending on the nature of the reset command. The content of ASDU 5 is described in the IEC 60870-5-103 section of the Menu Database, available from GE Vernova separately if required.

In addition to the above identification message, it will also produce a power up event.

18.11.2.3 TIME SYNCHRONISATION

The time and date can be set using the time synchronisation feature of the IEC 60870-5-103 protocol. The device will correct for the transmission delay as specified in IEC 60870-5-103. If the time synchronisation message is sent as a send/confirm message, then the device will respond with a confirm message. A time synchronisation Class 1 event will be generated/produced whether the time-synchronisation message is sent as a send confirm or a broadcast (send/no reply) message.

If the clock is being synchronised using the IRIG-B input, then it will not be possible to set the device time using the IEC 60870-5-103 interface. An attempt to set the time via the interface will cause the device to create an event with the current date and time taken from the IRIG-B synchronised internal clock.

18.11.2.4 CONFIGURABLE IEC 60870-5-103 SIGNAL LIST

From Software Version 91 onwards, there is a setting cell which allows the IEC 60870-5-103 private range signals to be selected and de-selected from IEC 60870-5-103 communication.

The IEC 60870-5-103 standard (compatible range) signals, that are provided according to the relay type and implementation, are always enabled. These signals cannot be disabled.

This setting cell is ***Config Mode*** in the *PROTOCOL CFG* column.

There are two settings associated with this cell. These are:

Setting	Description
Fixed	In this mode, the IED behaviour for IEC 60870-5-103 protocol is identical to pre-Software Version 91 IEDs. All the implemented signals (IEC 60870-5-103 compatible range and private range signals) are enabled for IEC 60870-5-103 communication. The COT behaviour will be according to the device IEC 60870-5-103 profile. This mode is provided for backward compatibility. This is the default setting.
Std+UserConfig	In this mode, the user can select which IEC 60870-5-103 private range signals are enabled for IEC 60870-5-103 communication. The selection is done using DDB mask setting cells in the *PROTOCOL CFG* column. The DDB mask value controls only the signal selection (enabled or disabled) for IEC 60870-5-103 communication. It does not modify the COT behaviour of the signals. The COT behaviour of the private range signals will be according to the device IEC 60870-5-103 profile. By default, only IEC 60870-5-103 standard signals are enabled. All private range signals are disabled.

When the ***Config Mode*** cell is set to `Std+UserConfig`, the DDB masks become visible in the *PROTOCOL CFG* column. These masks function in a similar way to the DDB masks in the *RECORD CONTROL* column. Editing these masks controls the DDB signals that are enabled for communication of the equivalent IEC 60870-5-103 private range signal, as listed in the IEC 60870-5-103 profile in the Menu Database.

Within these masks, only individual DDBs that are equivalent to IEC 60870-5-103 private range signals are editable. By default, all of the individual DDBs that are equivalent to IEC 60870-5-103 private range signals are set to 0 (zero), that is disabled for communication. Setting any individual DDB to 1 (one), enables the equivalent IEC 60870-5-103 private range signal for communication.

Within these masks, individual DDBs that are either equivalent to IEC 60870-5-103 standard range signals, or do not have any equivalent IEC 60870-5-103 private range signal, are not editable.

18.11.2.5 SPONTANEOUS EVENTS

Events are categorised using the following information:

- Function type
- Information Number

The IEC 60870-5-103 profile in the Menu Database contains a complete listing of all events produced by the device.

From Software Version 91 onwards, the IEC 60870-5-103 private range signals can be individually selected for spontaneous communication, by setting the ***Config Mode*** cell to `Std+UserConfig` and configuring the DDB masks as required.

18.11.2.6 GENERAL INTERROGATION (GI)

The GI request can be used to read the status of the device, the function numbers, and information numbers that will be returned during the GI cycle. These are shown in the IEC 60870-5-103 profile in the Menu Database.

From Software Version 91 onwards, the IEC 60870-5-103 private range signals can be individually selected for GI reporting, by setting the ***Config Mode*** cell to `Std+UserConfig` and configuring the DDB masks as required.

18.11.2.7 CYCLIC MEASUREMENTS

The device will produce measured values using ASDU 9 on a cyclical basis, this can be read from the device using a Class 2 poll (note ADSU 3 is not used). The rate at which the device produces new measured values can be controlled using the measurement period setting. This setting can be edited from the front panel menu or using MiCOM S1 Agile. It is active immediately following a change.

The device transmits its measurands with maximum value of 2.4 times the rated value of the measurement.

18.11.2.8 COMMANDS

A list of the supported commands is contained in the Menu Database. The device will respond to other commands with an ASDU 1, with a cause of transmission (COT) indicating ‘negative acknowledgement’.

18.11.2.9 TEST MODE

It is possible to disable the device output contacts to allow secondary injection testing to be performed using either the front panel menu or the front serial port. The IEC 60870-5-103 standard interprets this as ‘test mode’. An event will be produced to indicate both entry to and exit from test mode. Spontaneous events and cyclic measured data transmitted whilst the device is in test mode will have a COT of ‘test mode’.

18.11.2.10 DISTURBANCE RECORDS

The disturbance records are stored in uncompressed format and can be extracted using the standard mechanisms described in IEC 60870-5-103.

Note:
IEC 60870-5-103 only supports up to 8 records.

18.11.2.11 COMMAND/MONITOR BLOCKING

The device supports a facility to block messages in the monitor direction (data from the device) and also in the command direction (data to the device). Messages can be blocked in the monitor and command directions using one of the two following methods

- The menu command ***RP1 CS103Blcking*** in the *COMMUNICATIONS* column
- The DDB signals Monitor Blocked and Command Blocked

18.11.2.12 IEC 60870-5-103 CONFIGURATION

To configure the device:

1. Select the *CONFIGURATION* column and check that the ***Comms settings*** cell is set to `Visible`.
2. Select the *COMMUNICATIONS* column.
3. Move to the first cell down (***RP1 Protocol***). Set this to the table cell, which shows the chosen communication protocol – in this case `IEC 60870-5-103`.

```
COMMUNICATIONS
RP1 Protocol
IEC 60870-5-103
```

4. Move down to the next cell (***RP1 Address***). This cell controls the IEC 60870-5-103 address of the IED. Up to 32 IEDs can be connected to one spur. It is therefore necessary for each IED to have a unique address so that messages from the master control station are accepted by one IED only. IEC 60870-5-103 uses an integer number between 0 and 254 for the address. It is important that no two IEDs have the same IEC 60870 5 103 address. The IEC 60870-5-103 address is then used by the master station to communicate with the IED.

```
COMMUNICATIONS
RP1 address
162
```

5. Move down to the next cell (***RP1 Baud Rate***). This cell controls the baud rate to be used. Two baud rates are supported by the IED, `9600 bits/s` and `19200 bits/s`. Make sure that the baud rate selected on the IED is the same as that set on the master station.

```
COMMUNICATIONS
RP1 Baud rate
9600 bits/s
```

6. Move down to the next cell (***RP1 Meas Period***). The next cell down controls the period between IEC 60870-5-103 measurements. The IEC 60870-5-103 protocol allows the IED to supply measurements at regular intervals. The interval between measurements is controlled by this cell, and can be set between 1 and 60 seconds.

```
COMMUNICATIONS
RP1 Meas Period
30.00 s
```

7. If the optional fibre optic connectors are fitted, the ***RP1 PhysicalLink*** cell is visible. This cell controls the physical media used for the communication (Copper or Fibre optic).

```
COMMUNICATIONS
RP1 PhysicalLink
Copper
```

8. The next cell down (***RP1 CS103Blcking***) can be used for monitor or command blocking.

```
COMMUNICATIONS
RP1 CS103Blcking
Disabled
```

9. There are three settings associated with this cell; these are:

Setting:	Description:
Disabled	No blocking selected.
Monitor Blocking	When the monitor blocking DDB Signal is active high, either by energising an opto input or control input, reading of the status information and disturbance records is not permitted. When in this mode the device returns a "Termination of general interrogation" message to the master station.
Command Blocking	When the command blocking DDB signal is active high, either by energising an opto input or control input, all remote commands will be ignored (i.e. CB Trip/Close, change setting group etc.). When in this mode the device returns a "negative acknowledgement of command" message to the master station.

18.11.3 DNP 3.0

This section describes how the DNP 3.0 standard is applied in the product. It is not a description of the standard itself. The level at which this section is written assumes that the reader is already familiar with the DNP 3.0 standard.

The descriptions given here are intended to accompany the device profile document that is included in the Menu Database document. The DNP 3.0 protocol is not described here, please refer to the documentation available from the user group. The device profile document specifies the full details of the DNP 3.0 implementation. This is the standard format DNP 3.0 document that specifies which objects; variations and qualifiers are supported. The device profile document also specifies what data is available from the device using DNP 3.0. The IED operates as a DNP 3.0 slave and supports subset level 2, as described in the DNP 3.0 standard, plus some of the features from level 3.

The DNP 3.0 protocol is defined and administered by the DNP Users Group. For further information on DNP 3.0 and the protocol specifications, please see the DNP website (www.dnp.org).

18.11.3.1 PHYSICAL CONNECTION AND LINK LAYER

DNP 3.0 can be used with EIA(RS)485.

Several connection options are available for DNP 3.0

- Rear Port 1 (RP1) - for permanent SCADA connection via RS485
- Optional fibre port (RP1 in slot A) - for permanent SCADA connection via optical fibre

The baud rate can be selected using the front panel menu or by the settings application software.

When using a serial interface, the data format is: 1 start bit, 8 data bits, 1 stop bit and optional configurable parity bit.

18.11.3.2 OBJECT 1 BINARY INPUTS

Object 1, binary inputs, contains information describing the state of signals in the IED, which mostly form part of the digital data bus (DDB). In general, these include the state of the output contacts and opto-inputs, alarm signals, and protection start and trip signals. The ‘DDB number’ column in the device profile document provides the DDB numbers for the DNP 3.0 point data. These can be used to cross-reference to the DDB definition list. See the

relevant Menu Database document. The binary input points can also be read as change events using Object 2 and Object 60 for class 1-3 event data.

Note:
For the DNP Events to be transmitted it is mandatory to have the corresponding DDBs of the Configured Point Index to be included in the Courier Event Record. The RECORD CONTROL Menu lists all the DDBs, and the mask settings control their inclusion/exclusion as a Courier Event.

18.11.3.3 OBJECT 10 BINARY OUTPUTS

Object 10, binary outputs, contains commands that can be operated using DNP 3.0. Therefore, the points accept commands of type pulse on (null, trip, close) and latch on/off as detailed in the device profile in the relevant Menu Database document, and execute the command once for either command. The other fields are ignored (queue, clear, trip/close, in time and off time).

There is an additional image of the Control Inputs. Described as Alias Control Inputs, they reflect the state of the Control Input, but with a dynamic nature.

- If the Control Input DDB signal is already SET and a new DNP SET command is sent to the Control Input, the Control Input DDB signal goes momentarily to RESET and then back to SET.
- If the Control Input DDB signal is already RESET and a new DNP RESET command is sent to the Control Input, the Control Input DDB signal goes momentarily to SET and then back to RESET.

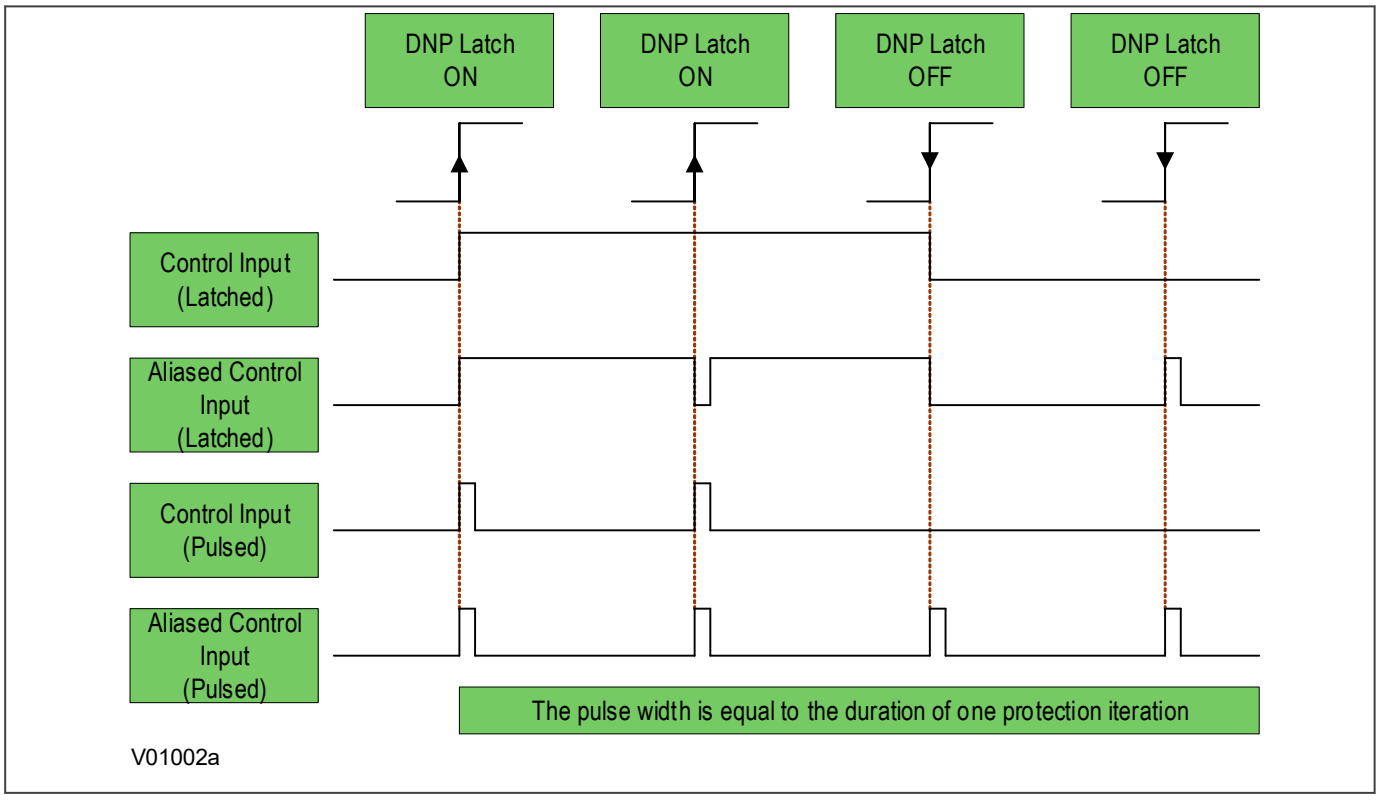


Figure 202: Control input behaviour

Many of the IEDs functions are configurable so some of the Object 10 commands described in the following sections may not be available. A read from Object 10 reports the point as off-line and an operate command to Object 12 generates an error response.

Examples of Object 10 points that may be reported as off-line are:

- Activate setting groups: Ensure setting groups are enabled
- CB trip/close: Ensure remote CB control is enabled
- Reset NPS thermal: Ensure NPS thermal protection is enabled
- Reset thermal O/L: Ensure thermal overload protection is enabled
- Reset RTD flags: Ensure RTD Inputs is enabled
- Control inputs: Ensure control inputs are enabled

18.11.3.4 OBJECT 20 BINARY COUNTERS

Object 20, binary counters, contains cumulative counters and measurements. The binary counters can be read as their present 'running' value from Object 20, or as a 'frozen' value from Object 21. The running counters of object 20 accept the read, freeze and clear functions. The freeze function takes the current value of the object 20 running counter and stores it in the corresponding Object 21 frozen counter. The freeze and clear function resets the Object 20 running counter to zero after freezing its value.

Binary counter and frozen counter change event values are available for reporting from Object 22 and Object 23 respectively. Counter change events (Object 22) only report the most recent change, so the maximum number of events supported is the same as the total number of counters. Frozen counter change events (Object 23) are generated whenever a freeze operation is performed, and a change has occurred since the previous freeze command. The frozen counter event queues store the points for up to two freeze operations.

18.11.3.5 OBJECT 30 ANALOGUE INPUT

Object 30, analogue inputs, contains information from the IED's measurements columns in the menu. All Object 30 points can be reported as 16 or 32-bit integer values with flag, 16 or 32-bit integer values without flag, as well as short floating point values.

Analogue values can be reported to the master station as primary, secondary or normalised values (which takes into account the IED's CT and VT ratios), and this is settable in the *COMMUNICATIONS* column in the IED. Corresponding deadband settings can be displayed in terms of a primary, secondary or normalised value. Deadband point values can be reported and written using Object 34 variations.

The deadband is the setting used to determine whether a change event should be generated for each point. The change events can be read using Object 32 or Object 60. These events are generated for any point which has a value changed by more than the deadband setting since the last time the data value was reported.

Any analogue measurement that is unavailable when it is read is reported as offline. For example, the frequency would be offline if the current and voltage frequency is outside the tracking range of the IED. All Object 30 points are reported as secondary values in DNP 3.0 (with respect to CT and VT ratios).

18.11.3.6 OBJECT 40 ANALOGUE OUTPUT

The conversion to fixed-point format requires the use of a scaling factor, which is configurable for the various types of data within the IED such as current, voltage, and phase angle. All Object 40 points report the integer scaling values and Object 41 is available to configure integer scaling quantities.

18.11.3.7 OBJECT 50 TIME SYNCHRONISATION

Function codes 1 (read) and 2 (write) are supported for Object 50 (time and date) variation 1. The DNP Need Time function (the duration of time waited before requesting another time sync from the master) is supported and is configurable in the range 1 - 30 minutes.

If the clock is being synchronised using the IRIG-B input, then it will not be possible to set the device time using the Courier interface. An attempt to set the time using the interface will cause the device to create an event with the current date and time taken from the IRIG-B synchronised internal clock.

18.11.3.8 DNP3 DEVICE PROFILE

This section describes the specific implementation of DNP version 3.0 within GE Vernova MiCOM P40 Agile IEDs for both compact and modular ranges.

The devices use the DNP 3.0 Slave Source Code Library version 3 from Triangle MicroWorks Inc.

This document, in conjunction with the DNP 3.0 Basic 4 Document Set, and the DNP Subset Definitions Document, provides complete information on how to communicate with the devices using the DNP 3.0 protocol.

This implementation of DNP 3.0 is fully compliant with DNP 3.0 Subset Definition Level 2. It also contains many Subset Level 3 and above features.

18.11.3.8.1 DNP3 DEVICE PROFILE TABLE

The following table provides the device profile in a similar format to that defined in the DNP 3.0 Subset Definitions Document. While it is referred to in the DNP 3.0 Subset Definitions as a “Document”, it is just one component of a total interoperability guide. This table, in combination with the subsequent Implementation and Points List tables should provide a complete interoperability/configuration guide for the device.

The following table provides the device profile in a similar format to that defined in the DNP 3.0 Subset Definitions Document. While it is referred to in the DNP 3.0 Subset Definitions as a "Document", it is just one component of a total interoperability guide. This table, in combination with the subsequent Implementation and Points List tables should provide a complete interoperability/configuration guide for the device.

DNP 3.0 Device Profile Document	
Vendor Name:	GE Vernova
Device Name:	MiCOM P40Agile Protection Relays - compact and modular range
Models Covered:	All models
Highest DNP Level Supported*: * This is the highest DNP level FULLY supported. Parts of level 3 are also supported	For Requests: Level 2 For Responses: Level 2
Device Function:	Slave
Notable objects, functions, and/or qualifiers supported in addition to the highest DNP levels supported (the complete list is described in the DNP 3.0 Implementation Table): For static (non-change event) object requests, request qualifier codes 00 and 01 (start-stop), 07 and 08 (limited quantity), and 17 and 28 (index) are supported in addition to the request qualifier code 06 (no range (all points)) Static object requests sent with qualifiers 00, 01, 06, 07, or 08 will be responded with qualifiers 00 or 01 Static object requests sent with qualifiers 17 or 28 will be responded with qualifiers 17 or 28 For change-event object requests, qualifiers 17 or 28 are always responded 16-bit and 32-bit analogue change events with time may be requested The read function code for Object 50 (time and date) variation 1 is supported Analogue Input Deadbands, Object 34, variations 1 through 3, are supported Floating Point Analogue Output Status and Output Block Objects 40 and 41 are supported Sequential file transfer, Object 70, variations 2 through 7, are supported Device Attribute Object 0 is supported	
Maximum Data Link Frame Size (octets):	Transmitted: 292 Received: 292
Maximum Application Fragment Size (octets)	Transmitted: Configurable (100 to 2048). Default 2048 Received: 249
Maximum Data Link Retries:	Fixed at 2
Maximum Application Layer Retries:	None
Requires Data Link Layer Confirmation:	Configurable to Never or Always
Requires Application Layer Confirmation:	When reporting event data (Slave devices only) When sending multi-fragment responses (Slave devices only)

DNP 3.0 Device Profile Document	
Timeouts while waiting for:	
Data Link Confirm:	Configurable
Complete Application Fragment:	None
Application Confirm:	Configurable
Complete Application Response:	None
Others:	
Data Link Confirm Timeout:	Configurable from 0 (Disabled) to 120s, default 10s.
Application Confirm Timeout:	Configurable from 1 to 120s, default 2s.
Select/Operate Arm Timeout:	Configurable from 1 to 10s, default 10s.
Need Time Interval (Set IIN1-4):	Configurable from 1 to 30, default 10min.
Application File Timeout	60 s
Analog Change Event Scan Period:	Fixed at 0.5s
Counter Change Event Scan Period	Fixed at 0.5s
Frozen Counter Change Event Scan Period	Fixed at 1s
Maximum Delay Measurement Error:	2.5 ms
Time Base Drift Over a 10-minute Interval:	7 ms
Sends/Executes Control Operations:	
Write Binary Outputs:	Never
Select/Operate:	Always
Direct Operate:	Always
Direct Operate - No Ack:	Always
Count > 1	Never
Pulse On	Always
Pulse Off	Sometimes
Latch On	Always
Latch Off	Always
Queue	Never
Clear Queue	Never
Note: Paired Control points will accept Pulse On/Trip and Pulse On/Close, but only single point will accept the Pulse Off control command.	
Reports Binary Input Change Events when no specific variation requested:	Configurable to send one or the other
Reports time-tagged Binary Input Change Events when no specific variation requested:	Binary input change with time
Sends Unsolicited Responses:	Never
Sends Static Data in Unsolicited Responses:	Never No other options are permitted
Default Counter Object/Variation:	Configurable, Point-by-point list attached Default object: 20 Default variation: 1

DNP 3.0 Device Profile Document	
Counters Roll Over at:	32 bits
Sends multi-fragment responses:	Yes
Sequential File Transfer Support:	
Append File Mode	No
Custom Status Code Strings	No
Permissions Field	Yes
File Events Assigned to Class	No
File Events Send Immediately	Yes
Multiple Blocks in a Fragment	No
Max Number of Files Open	1

18.11.3.8.2 DNP3 IMPLEMENTATION TABLE

The implementation table provides a list of objects, variations and control codes supported by the device:

Object			Request (Library Will Parse)				Response (Library Will Respond With)			
Object Number	Variation Number	Description	Function Codes (dec)		Qualifier Codes (hex)		Function Codes (dec)		Qualifier Codes (hex)	
1	0	Binary Input (Variation 0 is used to request default variation)	1 22	(read) (assign class)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)				
1	1 (default - see note 1)	Binary Input	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
1	2	Binary Input with Flag	1	(read)	00, 01 06 07, 08 17, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
2	0	Binary Input Change - Any Variation	1	(read)	06 07, 08	(no range, or all) (limited qty)				
2	1	Binary Input Change without Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
2	2	Binary Input Change with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
10	0	Binary Output Status - Any Variation	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)				
10	2 (default - see note 1)	Binary Output Status	1	(read)	00, 01 06 07, 08 17, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
12	1	Control Relay Output Block	3 4 5 6	(select) (operate) (direct op) (dir. op, noack)	17, 28	(index)	129	response		echo of request
20	0	Binary Counter - Any Variation	1 22	(read) (assign class)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)				
			7 8 9 10	(freeze) (freeze noack) (freeze clear) (frz. cl. Noack)	00, 01 06 07, 08	(start-stop) (no range, or all) (limited qty)				

Object			Request (Library Will Parse)				Response (Library Will Respond With)			
Object Number	Variation Number	Description	Function Codes (dec)		Qualifier Codes (hex)		Function Codes (dec)		Qualifier Codes (hex)	
20	1	32-Bit Binary Counter with Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
20	2	16-Bit Binary Counter with Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
20	5 (default - see note 1)	32-Bit Binary Counter without Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
20	6	16-Bit Binary Counter without Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
21	0	Frozen Counter - Any Variation	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)				
21	1	32-Bit Frozen Counter with Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
21	2	16-Bit Frozen Counter with Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
21	5	32-Bit Frozen Counter with Time of Freeze	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 1)
21	6	16-Bit Frozen Counter with Time of Freeze	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) 17, 28 (index - see note 1)
21	9 (default - see note 1)	32-Bit Frozen Counter without Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
21	10	16-Bit Frozen Counter without Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
`22	0	Counter Change Event - Any Variation	1	(read)	06 07, 08	(no range, or all) (limited qty)				
22	1 (default - see note 1)	32-Bit Counter Change Event without Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
22	2	16-Bit Counter Change Event without Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
22	5	32-Bit Counter Change Event with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
22	6	16-Bit Counter Change Event with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
23	0	Frozen Counter Event (Variation 0 is used to request default variation)	1	(read)	06 07, 08	(no range, or all) (limited qty)				
23	1 (default - see note 1)	32-Bit Frozen Counter Event	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
23	2	16-Bit Frozen Counter Event	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
23	5	32-Bit Frozen Counter Event with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
23	6	16-Bit Frozen Counter Event with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)

Object			Request (Library Will Parse)				Response (Library Will Respond With)			
Object Number	Variation Number	Description	Function Codes (dec)		Qualifier Codes (hex)		Function Codes (dec)		Qualifier Codes (hex)	
30	0	Analog Input - Any Variation	1 22	(read) (assign class)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)				
30	1	32-Bit Analog Input	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
30	2	16-Bit Analog Input	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
30	3 (default - see note 1)	32-Bit Analog Input without Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
30	4	16-Bit Analog Input without Flag	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
30	5	Short floating point	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
32	0	Analog Change Event - Any Variation	1	(read)	06 07, 08	(no range, or all) (limited qty)				
32	1 (default - see note 1)	32-Bit Analog Change Event without Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
32	2	16-Bit Analog Change Event without Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
32	3	32-Bit Analog Change Event with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
32	4	16-Bit Analog Change Event with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
32	5	Short floating point Analog Change Event without Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
32	7	Short floating point Analog Change Event with Time	1	(read)	06 07, 08	(no range, or all) (limited qty)	129	response	17, 28	(index)
34	0	Analog Input Deadband (Variation 0 is used to request default variation)	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)				
34	1	16 Bit Analog Input Deadband	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
			2	(write)	00, 01 07, 08 17, 27, 28	(start-stop) (limited qty) (index)				
34	2 (default - see note 1)	32 Bit Analog Input Deadband	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
			2	(write)	00, 01 07, 08 17, 27, 28	(start-stop) (limited qty) (index)				
34	3	Short Floating Point Analog Input Deadband	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
			2	(write)	00, 01 07, 08 17, 27, 28	(start-stop) (limited qty) (index)				

Object			Request (Library Will Parse)				Response (Library Will Respond With)			
Object Number	Variation Number	Description	Function Codes (dec)		Qualifier Codes (hex)		Function Codes (dec)		Qualifier Codes (hex)	
40	0	Analog Output Status (Variation 0 is used to request default variation)	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)				
40	1 (default - see note 1)	32-Bit Analog Output Status	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
40	2	16-Bit Analog Output Status	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
40	3	Short Floating Point Analog Output Status	1	(read)	00, 01 06 07, 08 17, 27, 28	(start-stop) (no range, or all) (limited qty) (index)	129	response	00, 01 17, 28	(start-stop) (index - see note 2)
41	1	32-Bit Analog Output Block	3 4 5 6	(select) (operate) (direct op) (dir. op, noack)	17, 28 27	(index) (index)	129	response		echo of request
41	2	16-Bit Analog Output Block	3 4 5 6	(select) (operate) (direct op) (dir. op, noack)	17, 28 27	(index) (index)	129	response		echo of request
41	3	Short Floating Point Analog Output Block	3 4 5 6	(select) (operate) (direct op) (dir. op, noack)	17, 27, 28	(index)	129	response		echo of request
50	1 (default - see note 1)	Time and Date	1	(read)	07	(limited qty = 1)	129	response	07	(limited qty = 1)
			2	(write)	07	(limited qty = 1)				
60	0	Not defined								
60	1	Class 0 Data	1	(read)	06	(no range, or all)				
60	2	Class 1 Data	1	(read)	06 07, 08	(no range, or all) (limited qty)				
			22	(assign class)	06	(no range, or all)				
60	3	Class 2 Data	1	(read)	06 07, 08	(no range, or all) (limited qty)				
			22	(assign class)	06	(no range, or all)				
60	4	Class 3 Data	1	(read)	06 07, 08	(no range, or all) (limited qty)				
			22	(assign class)	06	(no range, or all)				
70	0	File Event - Any Variation	1	(read)	06 07, 08	(no range, or all) (limited qty)				
			22	(assign class)	06	(no range, or all)				
70	2	File Authentication	29	(authenticate)	5b	(free-format)	129	response		5B (free-format)
70	3	File Command	25 27	(open) (delete)	5b	(free-format)				
70	4	File Command Status	26 30	(close) (abort)	5b	(free-format)	129	response		5B (free-format)
70	5	File Transfer	1	(read)	5b	(free-format)	129	response		5B (free-format)
70	6	File Transfer Status					129	response		5B (free-format)
70	7	File Descriptor	28	(get file info)	5b	(free-format)	129	response		5B (free-format)
80	1	Internal Indications	1	(read)	00, 01	(start-stop)	129	response	00, 01	(start-stop)
		No Object (function code only)	13	(cold restart)						
		No Object (function code only)	14	(warm restart)						
		No Object (function code only)	23	(delay meas.)						

Note:
A Default variation refers to the variation responded to when variation 0 is requested and/or in class 0, 1, 2, or 3 scans.

Note:
For static (non-change-event) objects, qualifiers 17 or 28 are only responded to when a request is sent with qualifiers 17 or 28, respectively. Otherwise, static object requests sent with qualifiers 00, 01, 06, 07, or 08, will be responded to with qualifiers 00 or 01. For change-event objects, qualifiers 17 or 28 are always responded to.

18.11.3.8.3 DNP3 INTERNAL INDICATIONS

The following table lists the DNP3.0 Internal Indications (IIN) and identifies those that are supported by the device.

The IIN form an information element used to convey the internal states and diagnostic results of a device. This information can be used by a receiving station to perform error recovery or other suitable functions. The IIN is a two-octet field that follows the function code in all responses from the device. When a request cannot be processed due to formatting errors or the requested data is not available, the IIN is always returned with the appropriate bits set.

Bit	Indication	Description	Supported
Octet 1			
0	All stations message received	Set when a request is received with the destination address of the all stations address (6553510). It is cleared after the next response (even if a response to a global request is required). This IIN is used to let the master station know that a "broadcast" message was received by the relay.	Yes
1	Class 1 data available	Set when data that has been configured as Class 1 data is ready to be sent to the master. The master station should request this class data from the relay when this bit is set in a response.	Yes
2	Class 2 data available	Set when data that has been configured as Class 2 data is ready to be sent to the master. The master station should request this class data from the relay when this bit is set in a response.	Yes
3	Class 3 data available	Set when data that has been configured as Class 3 data is ready to be sent to the master. The master station should request this class data from the relay when this bit is set in a response.	Yes
4	Time-synchronisation required	The relay requires time synchronisation from the master station (using the Time and Date object). This IIN is cleared once the time has been synchronised. It can also be cleared by explicitly writing a 0 into this bit of the Internal Indication object.	Yes
5	Local	Set when some or all of the relays digital output points (Object 10/12) are in the Local state. That is, the relays control outputs are NOT accessible through the DNP protocol. This IIN is clear when the relay is in the Remote state. That is, the relays control outputs are fully accessible through the DNP protocol.	No
6	Device in trouble	Set when an abnormal condition exists in the relay. This IIN is only used when the state cannot be described by a combination of one or more of the other IIN bits.	No
7	Device restart	Set when the device software application restarts. This IIN is cleared when the master station explicitly writes a 0 into this bit of the Internal Indications object.	Yes
Octet 2			
0	Function code not implemented	The received function code is not implemented within the relay.	Yes
1	Requested object(s) unknown	The relay does not have the specified objects or there are no objects assigned to the requested class. This IIN should be used for debugging purposes and usually indicates a mismatch in device profiles or configuration problems.	Yes
2	Out of range	Parameters in the qualifier, range or data fields are not valid or out of range. This is a 'catch-all' for application request formatting errors. It should only be used for debugging purposes. This IIN usually indicates configuration problems.	Yes
3	Buffer overflow	Event buffer(s), or other application buffers, have overflowed. The master station should attempt to recover as much data as possible and indicate to the user that there may be lost data. The appropriate error recovery procedures should be initiated by the user.	Yes
4	Already executing	The received request was understood but the requested operation is already executing.	
5	Bad configuration	Set to indicate that the current configuration in the relay is corrupt. The master station may download another configuration to the relay.	Yes
6	Reserved	Always returned as zero.	
7	Reserved	Always returned as zero.	

18.11.3.8.4 DNP3 RESPONSE STATUS CODES

When the device processes Control Relay Output Block (Object 12) requests, it returns a set of status codes; one for each point contained within the original request. The complete list of codes appears in the following table:

Code Number	Identifier Name	Description
0	Success	The received request has been accepted, initiated, or queued.
1	Timeout	The request has not been accepted because the 'operate' message was received after the arm timer (Select Before Operate) timed out. The arm timer was started when the select operation for the same point was received.
2	No select	The request has not been accepted because no previous matching 'select' request exists. (An 'operate' message was sent to activate an output that was not previously armed with a matching 'select' message).
3	Format error	The request has not been accepted because there were formatting errors in the control request ('select', 'operate', or 'direct operate').
4	Not supported	The request has not been accepted because a control operation is not supported for this point.
5	Already active	The request has not been accepted because the control queue is full or the point is already active.
6	Hardware error	The request has not been accepted because of control hardware problems.
7	Local	The request has not been accepted because local access is in progress.
8	Too many operations	The request has not been accepted because too many operations have been requested.
9	Not authorised	The request has not been accepted because of insufficient authorisation.
127	Undefined	The request not been accepted because of some other undefined reason.

Note:
Code numbers 10 through to 126 are reserved for future use.

18.11.3.9 DNP3 CONFIGURATION

o configure the device:

1. Select the *CONFIGURATION* column and check that the ***Comms settings*** cell is set to `Visible`.
2. Select the *COMMUNICATIONS* column.
3. Move to the first cell down (***RP1 protocol***). This is a non-settable cell, which shows the chosen communication protocol – in this case `DNP3.0`.
4. Move down to the next cell (***RP1 Address***). This cell controls the DNP3.0 address of the IED. Up to 32 IEDs can be connected to one spur, therefore it is necessary for each IED to have a unique address so that messages from the master control station are accepted by only one IED. DNP3.0 uses a decimal number between 1 and 65519 for the Relay Address. It is important that no two IEDs have the same address.
5. Move down to the next cell (***RP1 Baud Rate***). This cell controls the baud rate to be used. Six baud rates are supported by the IED 1200 bps, 2400 bps, 4800 bps, 9600 bps, 19200 bps and 38400 bps. Make sure that the baud rate selected on the IED is the same as that set on the master station.
6. Move down to the next cell (***RP1 Parity***). This cell controls the parity format used in the data frames. The parity can be set to be one of `None`, `Odd` or `Even`. Make sure that the parity format selected on the IED is the same as that set on the master station.
7. If the optional fibre optic connectors are fitted, the ***RP1 PhysicalLink*** cell is visible. This cell controls the physical media used for the communication (Copper or Fibre optic).
8. Move down to the next cell (***RP1 Time Sync***). This cell affects the time synchronisation request from the master by the IED. It can be set to `enabled` or `disabled`. If enabled, it allows the DNP3.0 master to synchronise the time on the IED.

18.11.3.9.1 DNP3 CONFIGURATOR

A PC support package for DNP3.0 is available as part of the supplied settings application software (MiCOM S1 Agile) to allow configuration of the device's DNP3.0 response. The configuration data is uploaded from the device to the PC in a block of compressed format data and downloaded in a similar manner after modification. The new DNP3.0 configuration takes effect after the download is complete. To restore the default configuration at any time, from the *CONFIGURATION* column, select the ***Restore Defaults*** cell then select `All Settings`.

In MiCOM S1 Agile, the DNP3.0 data is shown in three main folders, one folder each for the point configuration, integer scaling and default variation (data format). The point configuration also includes screens for binary inputs, binary outputs, counters and analogue input configuration.

If the device supports DNP Over Ethernet, the configuration related settings are done in the folder **DNP Over Ethernet**.

18.11.4 IEC 61850

This section describes how the IEC 61850 standard is applied to GE Vernova products. It is not a description of the standard itself. The level at which this section is written assumes that the reader is already familiar with the IEC 61850 standard.

IEC 61850 is the international standard for Ethernet-based communication in substations. It enables integration of all protection, control, measurement and monitoring functions within a substation, and additionally provides the means for interlocking and inter-tripping. It combines the convenience of Ethernet with the security that is essential in substations today.

There are two editions of most parts of the IEC 61850 standard: Edition 1 and Edition 2. The edition which this product supports depends on the Software Version.

From Software Version 90 onwards, it supports Edition 2.

An additional section detailing the enhancements in Edition 2 models is documented later in this chapter, if applicable.

18.11.4.1 BENEFITS OF IEC 61850

The standard provides:

- Standardised models for IEDs and other equipment within the substation
- Standardised communication services (the methods used to access and exchange data)
- Standardised formats for configuration files
- Peer-to-peer communication

The standard adheres to the requirements laid out by the ISO OSI model and therefore provides complete vendor interoperability and flexibility on the transmission types and protocols used. This includes mapping of data onto Ethernet, which is becoming more and more widely used in substations, in favour of RS485. Using Ethernet in the substation offers many advantages, most significantly including:

- Ethernet allows high-speed data rates (currently 100 Mbps, rather than tens of kbps or less used by most serial protocols)
- Ethernet provides the possibility to have multiple clients
- Ethernet is an open standard in everyday use
- There is a wide range of Ethernet-compatible products that may be used to supplement the LAN installation (hubs, bridges, switches)

18.11.4.2 IEC 61850 INTEROPERABILITY

A major benefit of IEC 61850 is interoperability. IEC 61850 standardises the data model of substation IEDs, which allows interoperability between products from multiple vendors.

An IEC 61850-compliant device may be interoperable, but this does not mean it is interchangeable. You cannot simply replace a product from one vendor with that of another without reconfiguration. However, the terminology is pre-defined and anyone with prior knowledge of IEC 61850 should be able to integrate a new device very quickly without having to map all the new data. IEC 61850 brings improved substation communications and interoperability to the end user, at a lower cost.

18.11.4.3 THE IEC 61850 DATA MODEL

The data model of any IEC 61850 IED can be viewed as a hierarchy of information, whose nomenclature and categorisation are defined and standardised in the IEC 61850 specification.

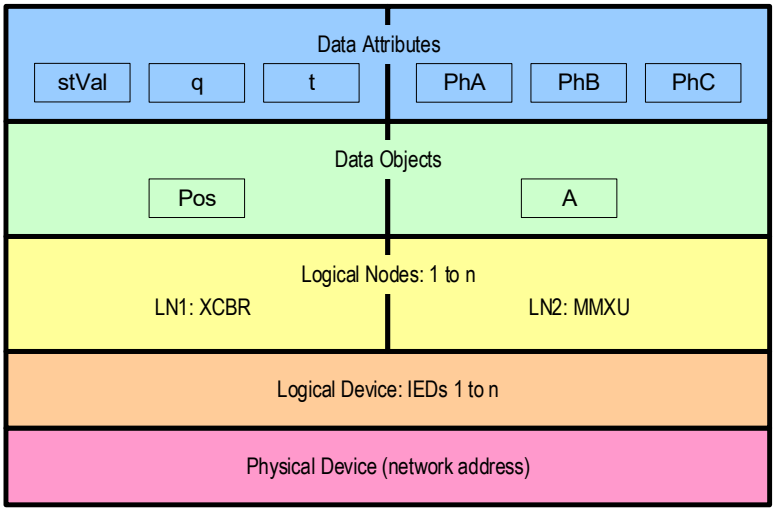


Figure 203: Data model layers in IEC 61850

The levels of this hierarchy can be described as follows:

Data Frame format

Layer	Description
Physical Device	Identifies the actual IED within a system. Typically, the device's name or IP address can be used (for example Feeder_1 or 10.0.0.2.
Logical Device	Identifies groups of related Logical Nodes within the Physical Device. For the MiCOM IEDs, 5 Logical Devices exist: Control, Measurements, Protection, Records, System.
Wrapper/Logical Node Instance	Identifies the major functional areas within the IEC 61850 data model. Either 3 or 6 characters are used as a prefix to define the functional group (wrapper) while the actual functionality is identified by a 4 character Logical Node name suffixed by an instance number. For example, XCBR1 (circuit breaker), MMXU1 (measurements), FrqPTOF2 (overfrequency protection, stage 2).
Data Object	This next layer is used to identify the type of data you will be presented with. For example, Pos (position) of Logical Node type XCBR.
Data Attribute	This is the actual data (measurement value, status, description, etc.). For example, stVal (status value) indicates the actual position of circuit breaker for Data Object type Pos of Logical Node type XCBR.

18.11.4.4 IEC 61850 IN MICOM IEDS

IEC 61850 is implemented by using a separate Ethernet card. This Ethernet card manages the majority of the IEC 61850 implementation and data transfer to avoid any impact on the performance of the protection functions.

To communicate with an IEC 61850 IED on Ethernet, it is necessary only to know its IP address. This can then be configured into either:

- An IEC 61850 client (or master), for example a bay computer (MiCOM C264)
- An HMI
- An MMS browser, with which the full data model can be retrieved from the IED, without any prior knowledge of the IED

The IEC 61850 compatible interface standard provides capability for the following:

- Read access to measurements
- Refresh of all measurements at a standard rate.
- Generation of non-buffered and buffered reports on change of status or measurement
- SNTP time synchronisation over an Ethernet link. This is used to synchronise the IEDs internal real time clock.
- GOOSE peer-to-peer communication
- Disturbance record extraction by IEC 61850 MMS file transfer. The record is extracted as an ASCII format COMTRADE file
- Controls (Direct and Select Before Operate)

Note:
Setting changes are not supported in the current IEC 61850 implementation. Currently these setting changes are carried out using the settings application software.

18.11.4.5 IEC 61850 DATA MODEL IMPLEMENTATION

The data model naming adopted in the IEDs has been standardised for consistency. Therefore, the Logical Nodes are allocated to one of the five Logical Devices, as appropriate.

The data model is described in the Model Implementation Conformance Statement (MICS) document, which is available as a separate document.

18.11.4.6 IEC 61850 COMMUNICATION SERVICES IMPLEMENTATION

The IEC 61850 communication services which are implemented in the IEDs are described in the Protocol Implementation Conformance Statement (PICS) document, which is available as a separate document.

18.11.4.7 IEC 61850 PEER-TO-PEER (GOOSE) COMMUNICATIONS

The implementation of IEC 61850 Generic Object Oriented Substation Event (GOOSE) enables faster communication between IEDs offering the possibility for a fast and reliable system-wide distribution of input and output data values. The GOOSE model uses multicast services to deliver event information. Multicast messaging means that messages are sent to selected devices on the network. The receiving devices can specifically accept frames from certain devices and discard frames from the other devices. It is also known as a publisher-subscriber system. When a device detects a change in one of its monitored status points it publishes a new message. Any device that is interested in the information subscribes to the data it contains.

18.11.4.8 GOOSE MESSAGE VALIDATION

Whenever a new GOOSE message is received its validity is checked before the dataset is decoded and used to update the Programmable Scheme Logic. As part of the validation process a check is made for state and sequence number anomalies. If an anomaly is detected, the 'out-of-order' GOOSE message is discarded. When a message is discarded the last valid message remains active until a new valid GOOSE message is received or its validity period (TAL) expires.

Out-of-order GOOSE message indicators and reporting are provided to the subscriber via the IEC 61850 LGOS logical node.

18.11.4.9 MAPPING GOOSE MESSAGES TO VIRTUAL INPUTS

Each GOOSE signal contained in a subscribed GOOSE message can be mapped to any of the virtual inputs within the PSL. The virtual inputs allow the mapping to internal logic functions for protection control, directly to output contacts or LEDs for monitoring.

An IED can subscribe to all GOOSE messages but only the following data types can be decoded and mapped to a virtual input:

- BOOLEAN
- BSTR2
- INT16
- INT32
- INT8
- UINT16
- UINT32
- UINT8

18.11.4.9.1 IEC 61850 GOOSE CONFIGURATION

All GOOSE configuration is performed using the IEC 61850 Configurator tool available in the MiCOM S1 Agile software application.

All GOOSE publishing configuration can be found under the **GOOSE Publishing** tab in the configuration editor window. All GOOSE subscription configuration parameters are under the **External Binding** tab in the configuration editor window.

Settings to enable GOOSE signalling and to apply Test Mode are available using the HMI.

18.11.4.10 ETHERNET FUNCTIONALITY

IEC 61850 **Associations** are unique and made between the client and server. If Ethernet connectivity is lost for any reason, the associations are lost and will need to be re-established by the client. The IED has a **TCP_KEEPALIVE** function to monitor each association and terminate any which are no longer active.

The IED allows the re-establishment of associations without disruption of its operation, even after its power has been removed. As the IED acts as a server in this process, the client must request the association. Uncommitted settings are cancelled when power is lost, and reports requested by connected clients are reset. The client must re-enable these when it next creates the new association to the IED.

18.11.4.11 IEC 61850 CONFIGURATION

You cannot configure the device for IEC 61850 Edition 1 using the HMI panel on the product. For this you must use the IEC 61850 Configurator, which is part of the settings application software. If the device is compatible with Edition 2, you can configure it with the HMI. To configure IEC 61850 Edition 2 using the HMI, you must first enable the IP from the HMI setting, after which you can set the media (copper or fibre), IP address, subnet mask and gateway address.

IEC 61850 allows IEDs to be directly configured from a configuration file. The IED's system configuration capabilities are determined from an IED Capability Description file (ICD), supplied with the product. By using ICD files from the products to be installed, you can design, configure and test (using simulation tools), a substation's entire protection scheme before the products are installed into the substation.

To help with this process, the settings application software provides an IEC 61850 Configurator tool, which allows the pre-configured IEC 61850 configuration file to be imported and transferred to the IED. As well as this, you can manually create configuration files for all products, based on their original IED capability description (ICD file).

Other features include:

- The extraction of configuration data for viewing and editing
- A sophisticated error checking sequence to validate the configuration data before sending to the IED

Note:
Some configuration data is available in the IEC61850 CONFIG. column, allowing read-only access to basic configuration data.

18.11.4.11.1 IEC 61850 CONFIGURATION BANKS

There are two configuration banks:

- Active Configuration Bank
- Inactive Configuration Bank

Any new configuration sent to the IED as an MCL file is automatically stored in the Inactive Configuration Bank, therefore not immediately affecting the current configuration.

Following this, the IEC 61850 IED Configurator tool can be used to transmit a command, which authorises activation of the new configuration contained in the inactive configuration bank. This is done by switching the active and inactive configuration banks. The capability of switching the configuration banks is also available using the *IEC61850 CONFIG.* column of the HMI.

The SCL Name and Revision attributes of both configuration banks are available in the *IEC61850 CONFIG.* column of the HMI.

18.11.4.11.2 IEC 61850 NETWORK CONNECTIVITY

Configuration of the IP parameters and SNTP (Simple Network Time Protocol) time synchronisation parameters is performed by the IEC 61850 Configurator tool. If these parameters are not available using an SCL (Substation Configuration Language) file, they must be configured manually.

Every IP address on the Local Area Network must be unique. Duplicate IP addresses result in conflict and must be avoided. Most IEDs check for a conflict on every IP configuration change and at power up and they raise an alarm if an IP conflict is detected.

The IED can be configured to accept data from other networks using the ***Gateway*** setting. If multiple networks are used, the IP addresses must be unique across networks.

18.11.4.12 SELECTION OF THE IEC 61850 EDITION

From Software Version 90 onwards, it is possible to select between Edition 1 and Edition 2. Edition 1 and Edition 2 implementations have different IEC 61850 data models and different ICD files. Only one can be active at any time in the product, so the selection is a decision related to system engineering.

Selection of Edition 1 or Edition 2 is done based on the configuration file (MCL) that is sent to the product and activated.

To configure the product for Edition 1, start with the Edition 1 ICD file. This can be done in one of two ways:

1. Using the system engineering process of an IEC 61850 system. In this case, import either the Edition 1 ICD file (for example “P545____91A_ED1.ICD”) or the Edition 2 ICD file (for example “P545____91A_ED2.ICD”), as applicable, into the System Configuration Tool. Perform the system configuration, then export the configured file (.SCD or CID). Import this configured file into MiCOM S1 Agile’s IEC 61850 Configurator.
2. Using the IED Configurator tool to manually configure the product. Launch the IED Configurator tool. Select **File**, **New** and then check only the **Edition 1** or **Edition 2** box, as applicable, and then proceed to select the product model and software version. Configure the parameters manually and save the MCL file.

In either case, the Edition 1 or Edition 2 configuration is activated in the product by sending the configuration file to the product from the IED Configurator and switching it to the Active Bank, after which the Ethernet application will restart with the new configuration.

18.11.4.13 IEC 61850 EDITION 2

Many parts of the IEC 61850 standard have now been released as the second edition. This offers some significant enhancements including:

- Improved interoperability
- Many new logical nodes
- Better defined testing: it is now possible to perform off-line testing and simulation of functions

Edition 2 implementation requires use of version 3.8 of the IEC 61850 configurator, which is installed with version 2.0.1 of MiCOM S1 Agile.

18.11.4.13.1 BACKWARD COMPATIBILITY

IEC 61850 system - backward compatibility

An Edition 1 IED can operate with an Edition 2 IEC 61850 system, provided that the Edition 1 IEDs do not subscribe to GOOSE messages with data objects or data attributes which are only available in Edition 2.

The following figure explains this concept:

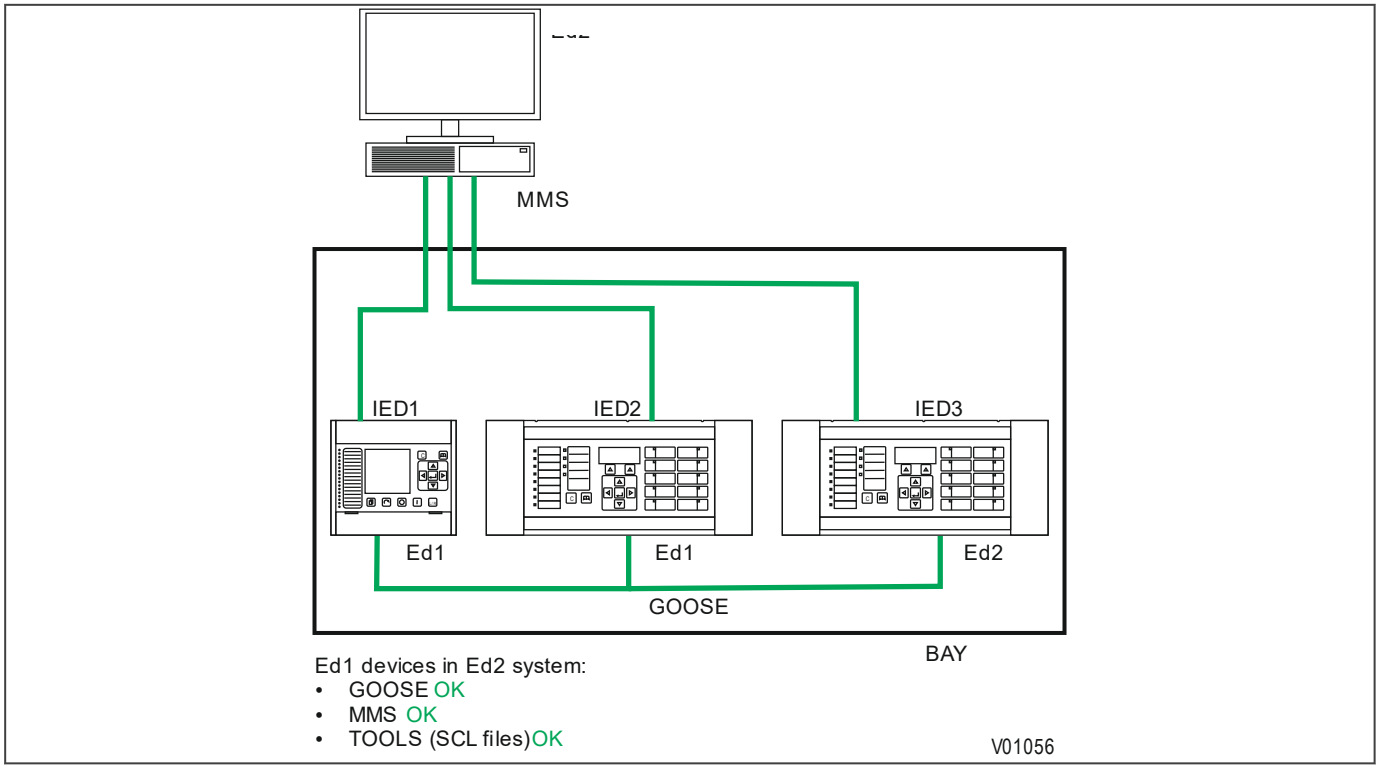


Figure 204: Edition 2 system - backward compatibility

An Edition 2 IED cannot normally operate within an Edition 1 IEC 61850 system. An Edition 2 IED can work for GOOSE messaging in a mixed system, providing the client is compatible with Edition 2.

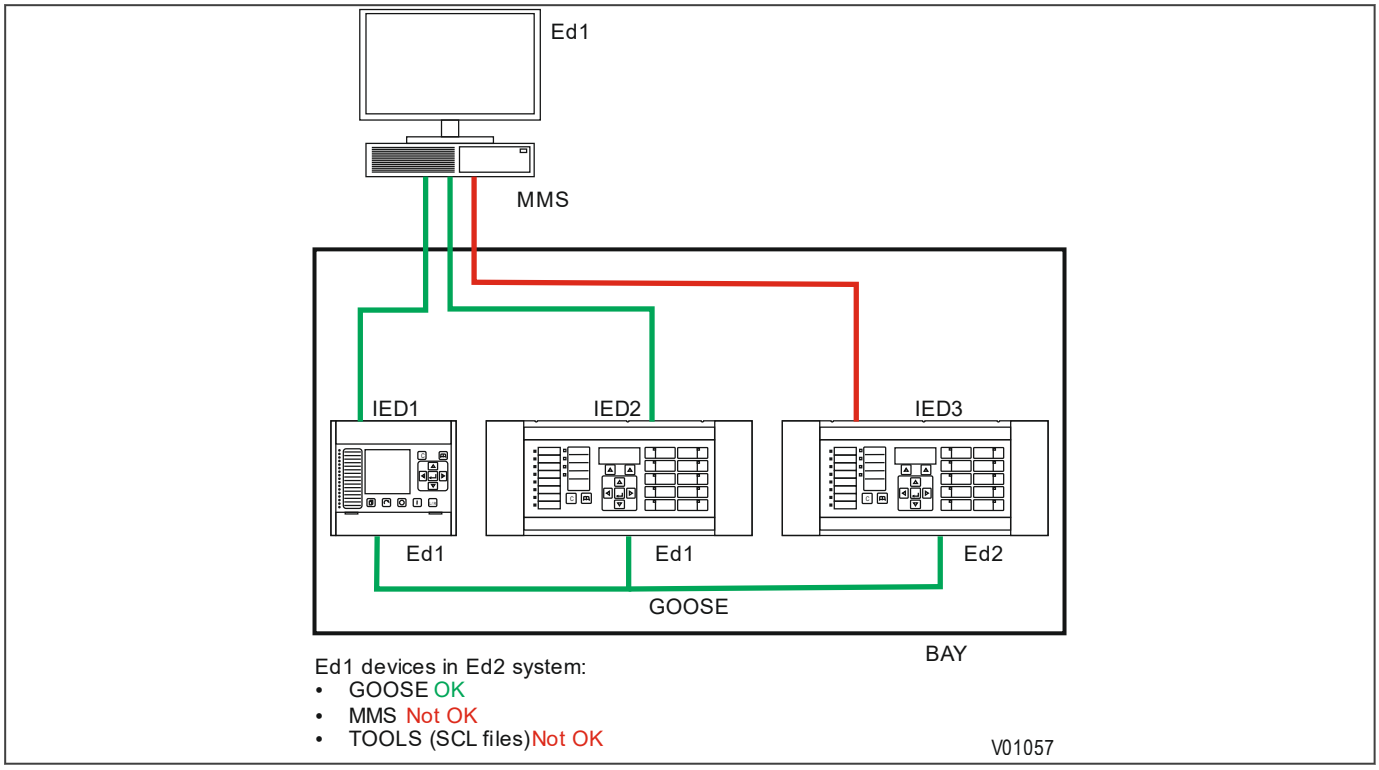


Figure 205: Edition 1 system - forward compatibility issues

18.11.4.13.2 EDITION-2 COMMON DATA CLASSES

The following common data classes (CDCs) are new to Edition 2 and therefore should not be used in GOOSE control blocks in mixed Edition 1 and Edition 2 systems

- Histogram (HST)
- Visible string status (VSS)
- Object reference setting (ORG)
- Controllable enumerated status (ENC)
- Controllable analogue process value (APC)
- Binary controlled analogue process value (BAC)
- Enumerated status setting (ENG)
- Time setting group (TSG)
- Currency setting group (CUG)
- Visible string setting (VSG)
- Curve shape setting (CSG)

Of these, only ENS and ENC types are available from a MiCOM P40 IED when publishing GOOSE messages, so Data Objects using these Common Data Classes should not be published in mixed Edition 1 and Edition 2 systems.

For compatibility between Edition 1 and Edition 2 IEDs, SCL files using SCL schema version 2.1 must be used. For a purely Edition 2 system, use the schema version 3.1.

18.11.4.13.3 STANDBY PROTECTION REDUNDANCY

With digital substation architectures, measurements can be shared freely on the process bus across the substation and between different devices without any additional wiring. This is because there are no longer any electrical connections to instruments transformers that restrict the location of IEDs.

The new IEC 61850 Edition 2 test modes enable the introduction of standby protection IEDs at any location within the substation, which has access to both station and process buses. In the case of failure, these devices can temporarily replace the protection functions inside other IEDs.

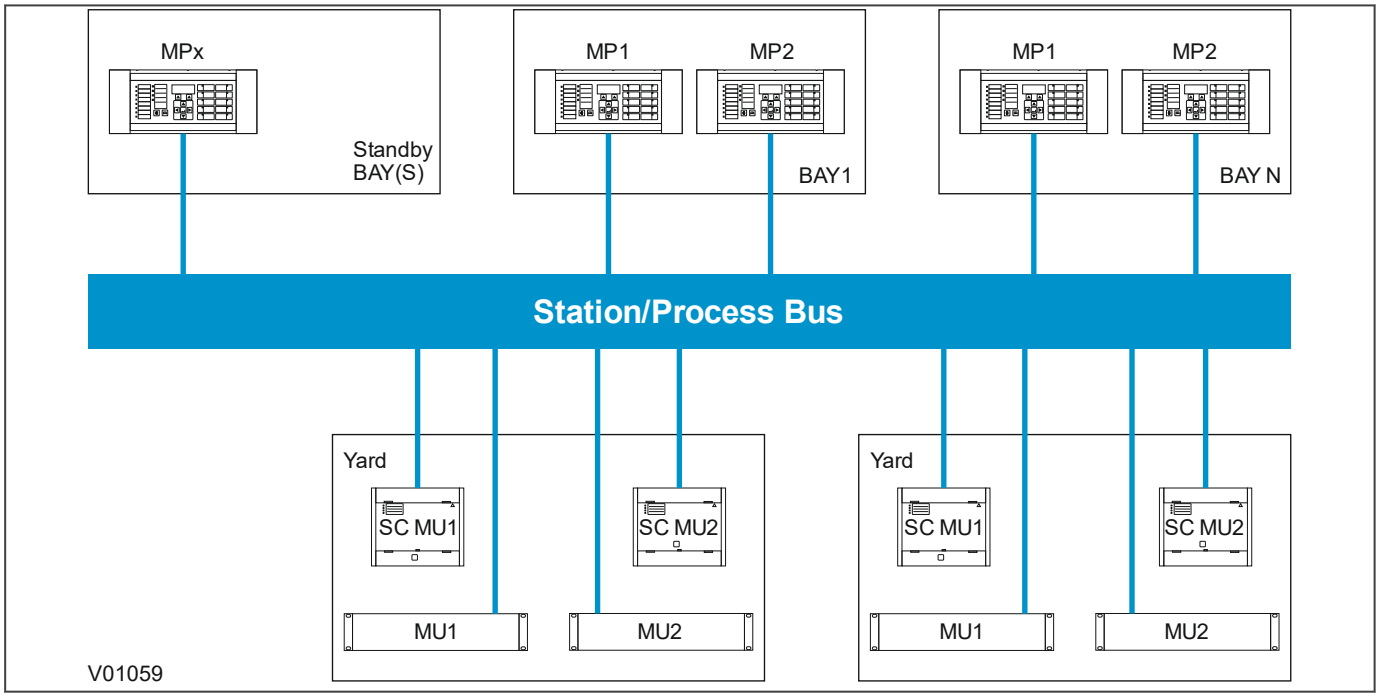


Figure 206: Example of standby IED

See the example below. If a failure occurs in the Bay 1 protection IED (MP2), we could disable this device and activate a standby protection IED to replace its functionality.

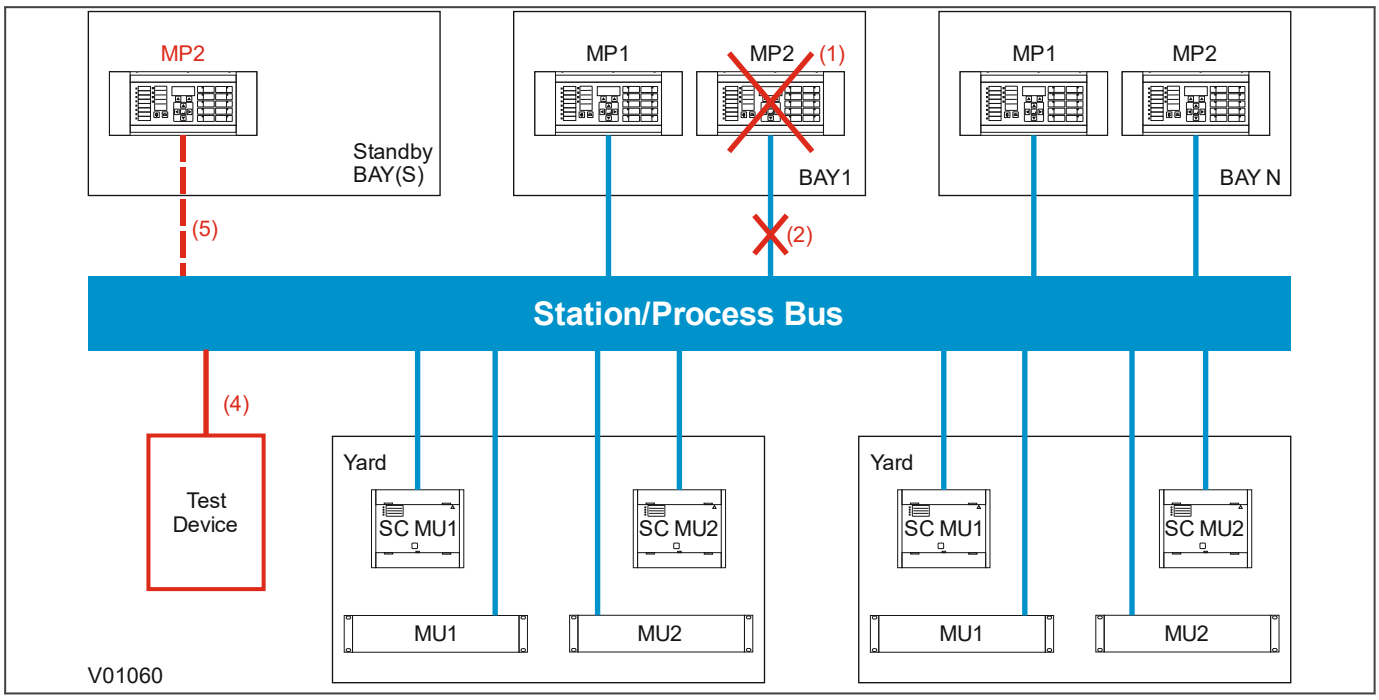


Figure 207: Standby IED activation process

The following sequence would occur under this scenario:

1. During the installation phase, a spare standby IED is installed in the substation. This can remain inactive, until it is needed to replace functions in one of several bays. The device is connected to the process bus but does not have any subscriptions enabled.
2. If a failure occurs (in this example, bay 1), first isolate the faulty device by disabling its process bus and station bus interfaces. You do this by turning off the attached network interfaces.
3. Retrieve the configuration that the faulty device normally uses, and load this into the standby redundant IED.
4. Place the IED into the "Test Blocked" mode, as defined in IEC 61850-7-4 Edition Two. This allows test signals to be injected into the network, which will check that the configuration is correct. GOOSE signals issued by the device will be flagged as "test" so that subscribing switchgear controllers know not to trip during this testing. In this way the protection can be tested all the way up to the switchgear control merging units without having to operate primary circuit breakers, or by carrying out any secondary injection.
5. Take the standby IED out of "Test-Blocked" mode and activate it so that it now replaces the protection functions that were disabled from the initial device failure.

The standby IED reduces downtime in the case of device failure, as protection functions can be restored quickly before the faulted device is replaced.

18.11.5 READ ONLY MODE

With IEC 61850 and Ethernet/Internet communication capabilities, security has become an important issue. For this reason, all relevant GE Vernova IEDs have been adapted to comply with the latest cyber-security standards.

In addition to this, a facility is provided which allows you to enable or disable the communication interfaces. This feature is available for products using Courier, IEC 60870-5-103, or IEC 61850.

18.11.5.1 IEC 60870-5-103 PROTOCOL BLOCKING

If Read-Only Mode is enabled for RP1 or RP2 with IEC 60870-5-103, the following commands are blocked at the interface:

- Write parameters (=change setting) (private ASDUs)
- General Commands (ASDU20), namely:
  - INF16 auto-recloser on/off
  - INF19 LED reset
  - Private INFs (for example: CB open/close, Control Inputs)

The following commands are still allowed:

- Poll Class 1 (Read spontaneous events)
- Poll Class 2 (Read measurands)
- GI sequence (ASDU7 'Start GI', Poll Class 1)
- Transmission of Disturbance Records sequence (ASDU24, ASDU25, Poll Class 1)
- Time Synchronisation (ASDU6)
- General Commands (ASDU20), namely:
  - INF23 activate characteristic 1
  - INF24 activate characteristic 2
  - INF25 activate characteristic 3
  - INF26 activate characteristic 4

Note:
For IEC 60870-5-103, Read Only Mode function is different from the existing Command block feature.

18.11.5.2 COURIER PROTOCOL BLOCKING

If Read-Only Mode is enabled for RP1 or RP2 with Courier, the following commands are blocked at the interface:

- Write settings
- All controls, including:
  - Reset Indication (Trip LED)
  - Operate Control Inputs
  - CB operations
  - Auto-reclose operations
  - Reset demands
  - Clear event/fault/maintenance/disturbance records
  - Test LEDs & contacts

The following commands are still allowed:

- Read settings, statuses, measurands
- Read records (event, fault, disturbance)
- Time synchronisation
- Change active setting group

18.11.5.3 IEC 61850 PROTOCOL BLOCKING

If Read-Only Mode is enabled for the Ethernet interfacing with IEC 61850, the following commands are blocked at the interface:

- All controls, including:
  - Enable/disable protection
  - Operate Control Inputs
  - CB operations (Close/Trip, Lock)
  - Reset LEDs

The following commands are still allowed:

- Read statuses, measurands
- Generate reports
- Extract disturbance records
- Time synchronisation
- Change active setting group

18.11.5.4 READ-ONLY SETTINGS

The following settings are available for enabling or disabling Read Only Mode.

- RP1 Read Only
- RP2 Read Only (only for products that have RP2)
- NIC Read Only (where Ethernet is available)

18.11.5.5 READ-ONLY DDB SIGNALS

The remote read only mode is also available in the PSL using three dedicated DDB signals:

- RP1 Read Only
- RP2 Read Only (only for products that have RP2)
- NIC Read Only (where Ethernet is available)

Using the PSL, these signals can be activated by opto-inputs, Control Inputs and function keys if required.

18.12 TIME SYNCHRONISATION

Effective management of today's energy systems requires precise time recording of events experienced by different devices across the network. This is achieved by synchronising real-time clocks across the devices and can be achieved in different ways. This device supports synchronisation in various ways depending on the chosen options and communication protocols.

- Using the IRIG-B input (if fitted)
- Using the SNTP time protocol (for Ethernet IEC 61850 versions)
- Using IEEE 1588 Precision Time Protocol (PTP)
- By using the time synchronisation functionality inherent in the data protocols
- Using a dedicated opto-input mapped via the PSL

The time synchronisation sources can be configured in a priority order using the Primary Source and Secondary Source cells in the DATE AND TIME column. If the Primary source becomes unavailable, the Secondary source will be used, if available.

All the protection functionality implemented in this device operates entirely independently of the real time clock. It does not matter to the protection if the clock is not set or is incorrectly synchronised. Even though the time stamping of any associated records may be compromised, the protection functionality will not.

18.12.1 IRIG-B

IRIG stands for Inter Range Instrumentation Group, which is a standards body responsible for standardising different time code formats. There are several different formats starting with IRIG-A, followed by IRIG-B and so on. The letter after the "IRIG" specifies the resolution of the time signal in pulses per second (PPS). IRIG-B, the one which we use has a resolution of 100 PPS. IRIG-B is used when accurate time-stamping is required.

The following diagram shows a typical GPS time-synchronised substation application. The satellite RF signal is picked up by a satellite dish and passed on to receiver. The receiver receives the signal and converts it into time signal suitable for the substation network. IEDs in the substation use this signal to govern their internal clocks and event recorders.

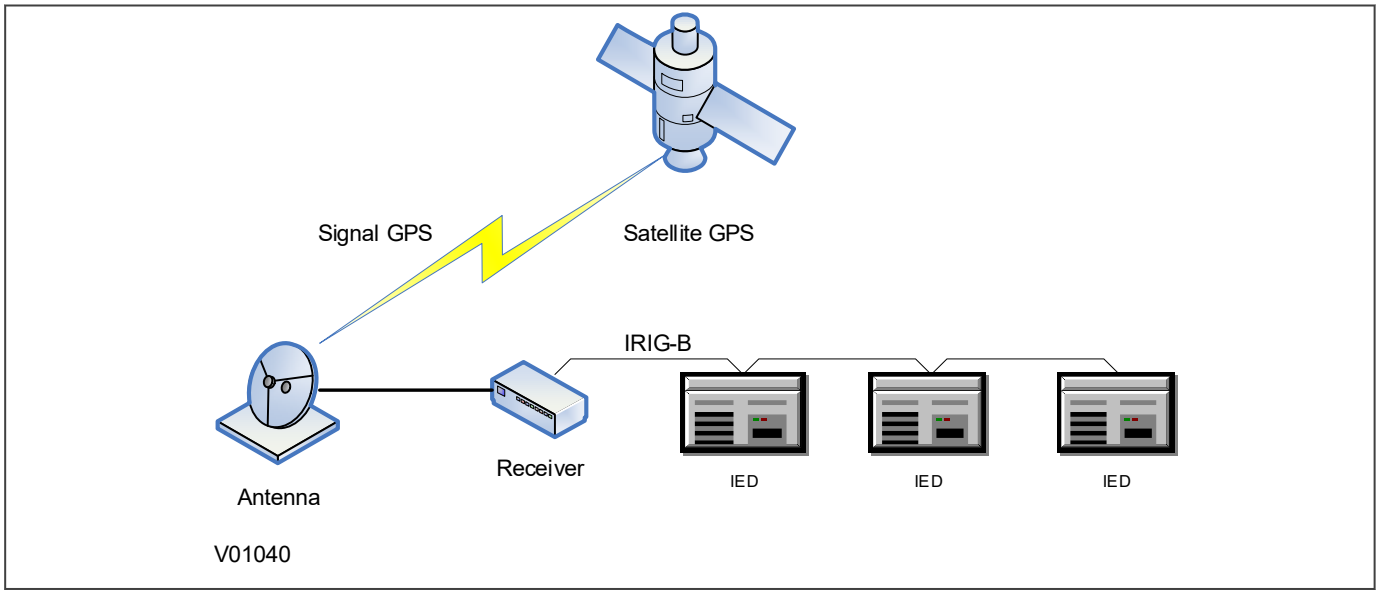


Figure 208: GPS satellite timing signal

The IRIG-B time code signal is a sequence of one second time frames. Each frame is split up into ten 100 mS slots as follows:

- Time-slot 1: Seconds
- Time-slot 2: Minutes
- Time-slot 3: Hours
- Time-slot 4: Days
- Time-slot 5 and 6: Control functions
- Time-slots 7 to 10: Straight binary time of day

The first four time-slots define the time in BCD (Binary Coded Decimal). Time-slots 5 and 6 are used for control functions, which control deletion commands and allow different data groupings within the synchronisation strings. Time-slots 7-10 define the time in SBS (Straight Binary Second of day).

18.12.1.1 IRIG-B IMPLEMENTATION

Depending on the chosen hardware options, the product can be equipped with an IRIG-B input for time synchronisation purposes. The IRIG-B interface is implemented either on a dedicated card, or together with other communication functionality such as Ethernet. The IRIG-B connection is presented by a connector is a BNC connector. IRIG-B signals are usually presented as an RF-modulated signal. There are two types of input to our IRIG-B boards: demodulated or modulated. A board that accepts a demodulated input is used where the IRIG-B signal has already been demodulated by another device before being fed to the IED. A board that accepts a modulated input has an on-board demodulator.

To set the device to use IRIG-B, use the setting ***Primary Source*** cell in the *DATE AND TIME* column.

The IRIG-B status can be viewed in the ***IRIG-B Status*** cell in the *DATE AND TIME* column.

18.12.2 SNTP

SNTP is used to synchronise the clocks of computer systems over packet-switched, variable-latency data networks, such as IP. SNTP can be used as the time synchronisation method for models using IEC 61850 over Ethernet.

The device is synchronised by the main SNTP server. This is achieved by entering the IP address of the SNTP server into the IED using the IEC 61850 Configurator software described in the settings application software manual. A second server is also configured with a different IP address for backup purposes.

This function issues an alarm when there is a loss of time synchronisation on the SNTP server. This could be because there is no response or no valid clock signal.

The HMI menu does not contain any configurable settings relating to SNTP, as the only way to configure it is using the IEC 61850 Configurator. However, it is possible to view some parameters in the *COMMUNICATIONS* column under the sub-heading SNTP parameters. Here you can view the SNTP server addresses and the SNTP poll rate in the cells ***SNTP Server 1***, ***SNTP Server 2*** and ***SNTP Poll rate*** respectively.

The SNTP time synchronisation status is displayed in the ***SNTP Status*** cell in the *DATE AND TIME* column.

18.12.2.1 LOSS OF SNTP SERVER SIGNAL ALARM

This function issues an alarm when there is a loss of time synchronisation on the SNTP server. It is issued when the SNTP sever has not detected a valid time synchronisation response within its 5 second window. This is because there is no response or no valid clock. The alarm is mapped to IEC 61850.

18.12.3 IEEE 1588 PRECISION TIME PROTOCOL

The MiCOM P40 modular products support IEEE 1588 Precision Time Protocol (PTP) as a slave-only clock. MiCOM relays are profile unaware, which means that they will accept synchronisation from any PTP profile. Power Utility Profile (IEC 61850-9-3) is specifically designed to perform well for substation related applications, with PMU applications needing the most stringent requirements.

18.12.3.1 ACCURACY AND DELAY CALCULATION

A time synchronisation accuracy of within 5 ms is possible. Both peer-to-peer or end-to-end mode delay measurement can be used.

In peer-to-peer mode, delays are measured between each link in the network and are compensated for. This provides greater accuracy but requires that every device between the Grand Master and Slaves supports the peer-to-peer delay measurement.

In end-to-end mode, delays are only measured between each Grand Master and Slave. The advantage of this mode is that the requirements for the switches on the network are lower; they do not need to independently calculate delays. The main disadvantage is that more inaccuracy is introduced, because the method assumes that forward and reverse delays are always the same, which may not always be correct.

When using end-to-end mode, the IED can be connected in a ring or line topology using RSTP or Self Healing Protocol without any additional Transparent Clocks. But because the IED is a slave-only device, additional inaccuracy is introduced. The additional error will be less than 1ms for a network of eight devices.

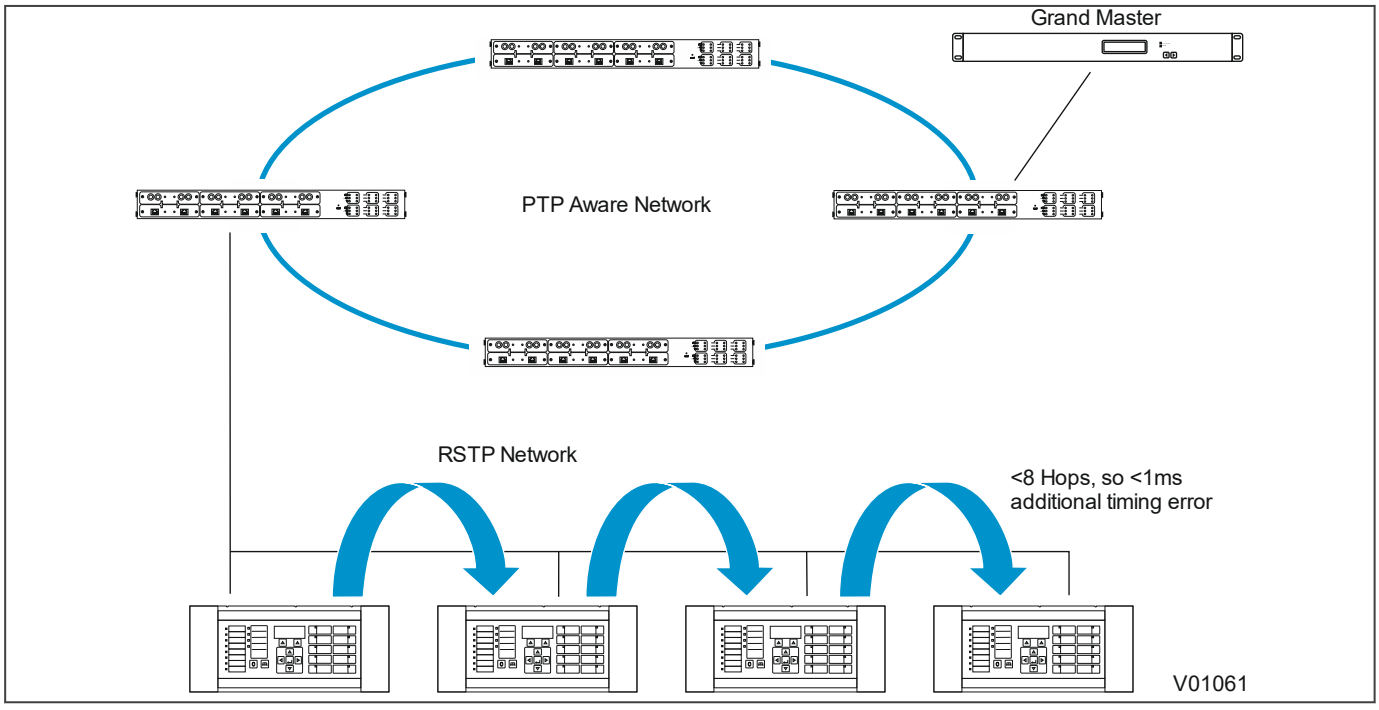


Figure 209: Timing error using ring or line topology

18.12.3.2 PTP DOMAINS

PTP traffic can be segregated into different domains using Boundary Clocks. These allow different PTP clocks to share the same network while maintaining independent synchronisation within each grouped set.

18.12.4 TIME SYNCHRONISATION USING THE COMMUNICATION PROTOCOLS

All communication protocols have in-built time synchronisation mechanisms. If an external time synchronisation mechanism such as IRIG-B, SNTP, or IEEE 1588 PTP is not used to synchronise the devices, the time synchronisation mechanism within the relevant serial protocol is used. The real time is usually defined in the master station and communicated to the relevant IEDs via one of the rear serial ports using the chosen protocol. It is also possible to define the time locally using settings in the *DATE AND TIME* column.

The time synchronisation for each protocol is described in the relevant protocol description section.

18.12.5 REAL TIME CLOCK SYNCHRONISATION VIA OPTO-INPUTS

In modern protective schemes it is often desirable to synchronise the IED's real time clock so that events from different IEDs can be placed in chronological order. This can be done using the IRIG-B input, if fitted, or via the communication interface connected to the substation control system. In addition to these methods P40 IEDs offer the facility to synchronise via an opto-input by routing it in PSL to DDB 400 (***Time Sync.***). Pulsing this input results in the real time clock snapping to the nearest minute. The recommended pulse duration is 20 ms to be repeated no more than once per minute. An example of the time sync. function is shown.

IRIG-B Interface (Demodulated)	
Time of "Sync. Pulse"	**Corrected Time**
19:47:00 to 19:47:29	19:47:00
19:47:30 to 19:47:59	19:48:00

Note:
The above assumes a time format of hh:mm:ss.

To avoid the event buffer from being filled with unnecessary time sync. events, it is possible to ignore any event that is generated by the time sync. opto input. This can be done by applying the following settings:

Menu Text	Value
RECORD CONTROL	
Opto Input Event	Enabled
Protection Event	Enabled
DDB 63 - 32 (Opto Inputs)	Set "Time Sync." associated opto to 0

To improve the recognition time of the time sync. opto input by approximately 10 ms, the opto input filtering could be disabled. This is achieved by setting the appropriate bit to 0 in the ***Opto Filter Cntl.*** cell (*OPTO CONFIG.* column). Disabling the filtering may make the opto input more susceptible to induced noise. Fortunately the effects of induced noise can be minimised by using the methods described in the Software Design chapter.

CHAPTER 19

CYBERSECURITY

19.1 DISCLAIMER

GE Vernova Grid Automation products are digital devices designed to be installed and operated in utility substations & industrial plant environments and connected to secure private networks. GE Vernova IEDs should not be connected to the public internet.

GE Vernova strongly recommends that users protect their digital devices using a defense-in-depth strategy which will protect their products, their network, their systems and interfaces against cyber security threats. This includes, but is not limited to, placing digital devices inside the control system network security perimeter, deploying and maintaining access controls, monitoring and intrusion detection, security awareness training, security policies, network segmentation and firewalls installation, strong and active password management, data encryption, antivirus and other mitigating applicable technologies.

GE Vernova IEDs are available with standard features, and in some products additional optional software options, which provide cyber security mechanisms to help users protect against cyber security intrusion. GE Vernova strongly recommends using all available cyber security options.

For additional details and recommendations on how to protect the GE Vernova IEDs, please see Cyber Security sections of the manuals. GE Vernova Grid Automation may also provide additional instructions and recommendations to users from time to time relating to IED and cyber security threats or vulnerabilities.

It is the users' sole responsibility to make sure that all GE Vernova Grid Automation IEDs are installed and operated considering its cyber security capabilities, security context, and the instructions and recommendations provided to the user relating to GE Vernova. Users assume all risks and liability associated with damages or losses incurred in connection with any and all cyber security incidences.

IT IS THE SOLE RESPONSIBILITY OF THE USER TO SECURE THEIR NETWORK AND ASSOCIATED DEVICES AGAINST CYBER SECURITY INTRUSIONS OR ATTACKS. GE VERNOVA GRID AUTOMATION AND ITS AFFILIATES ARE NOT LIABLE FOR ANY DAMAGES AND/OR LOSSES ARISING FROM OR RELATED TO SUCH SECURITY INTRUSION OR ATTACKS.

19.2 OVERVIEW

In the past, substation networks were traditionally isolated and the protocols and data formats used to transfer information between devices were often proprietary.

For these reasons, the substation environment was very secure against cyber-attacks. The terms used for this inherent type of security are:

- Security by isolation (if the substation network is not connected to the outside world, it cannot be accessed from the outside world).
- Security by obscurity (if the formats and protocols are proprietary, it is very difficult to interpret them).

However, note that these are not recognised defences against attackers.

The increasing sophistication of protection schemes, coupled with the advancement of technology and the desire for vendor interoperability, has resulted in standardisation of networks and data interchange within substations. Today, devices within substations use standardised protocols for communication. Furthermore, substations can be interconnected with open networks, such as the internet or corporate-wide networks, which use standardised protocols for communication. This introduces a major security risk making the grid vulnerable to cyber-attacks, which could in turn lead to major electrical outages.

Clearly, there is now a need to secure communication and equipment within substation environments. This chapter describes the security measures that have been put in place for our range of Intelligent Electronic Devices (IEDs).

Note:
Cyber-security compatible devices do not enforce NERC compliance, they merely facilitate it. It is the responsibility of the user to ensure that compliance is adhered to as and when necessary.

This chapter contains the following sections:

Disclaimer 410
Overview 411
The Need for Cybersecurity 412
Standards 413
Cyber-Security Implementation 417
Roles and Permissions 418
Authentication 421
Security Event Management 433

19.3 THE NEED FOR CYBERSECURITY

Cybersecurity provides protection against unauthorised disclosure, transfer, modification, or destruction of information or information systems, whether accidental or intentional. To achieve this, there are several security requirements:

- Confidentiality (preventing unauthorised access to information)
- Integrity (preventing unauthorised modification)
- Availability/Authentication (preventing the denial of service and assuring authorised access to information)
- Non-repudiation (preventing the denial of an action that took place)
- Traceability/Detection (monitoring and logging of activity to detect intrusion and analyse incidents)

The threats to Cybersecurity may be unintentional (e.g. natural disasters, human error), or intentional (e.g. cyber-attacks by hackers).

Good Cybersecurity can be achieved with a range of measures, such as closing down vulnerability loopholes, implementing adequate security processes and procedures and providing technology to help achieve this.

Examples of vulnerabilities are:

- Indiscretions by personnel (users keep passwords on their computer)
- Bad practice (users do not change default passwords, or everyone uses the same password to access all substation equipment)
- Bypassing of controls (users turn off security measures)
- Inadequate technology (substation is not firewalled)

Examples of availability issues are:

- Equipment overload, resulting in reduced or no performance
- Expiry of a certificate preventing access to equipment

To help tackle these issues, standards organisations have produced various standards. Compliance with these standards significantly reduces the threats associated with lack of Cybersecurity.

19.4 STANDARDS

There are several standards, which apply to substation Cybersecurity. The standards currently applicable to GE Vernova's IEDs are NERC and IEEE1686.

Standard	Country	Description
NERC CIP (North American Electric Reliability Corporation)	USA	Framework for the protection of the grid critical Cyber Assets
BDEW (German Association of Energy and Water Industries)	Germany	Requirements for Secure Control and Telecommunication Systems
ANSI ISA 99	USA	ICS oriented then Relevant for EPU completing existing standard and identifying new topics such as patch management
IEEE 1686	International	International Standard for substation IED Cybersecurity capabilities
IEC 62351	International	Power system data and Comm. protocol
ISO/IEC 27002	International	Framework for the protection of the grid critical Cyber Assets
NIST SP800-53 (National Institute of Standards and Technology)	USA	Complete framework for SCADA SP800-82and ICS Cybersecurity
CPNI Guidelines (Centre for the Protection of National Infrastructure)	UK	Clear and valuable good practices for Process Control and SCADA security

19.4.1 NERC COMPLIANCE

The North American Electric Reliability Corporation (NERC) created a set of standards for the protection of critical infrastructure. These are known as the CIP standards (Critical Infrastructure Protection). These were introduced to ensure the protection of 'Critical Cyber Assets', which control or have an influence on the reliability of North America’s electricity generation and distribution systems.

These standards have been compulsory in the USA for several years now. Compliance auditing started in June 2007, and utilities face extremely heavy fines for non-compliance.

NERC CIP standards

CIP Standard	Description
CIP-002-1 Critical Cyber Assets	Define and document the Critical Assets and the Critical Cyber Assets
CIP-003-1 Security Management Controls	Define and document the Security Management Controls required to protect the Critical Cyber Assets
CIP-004-1 Personnel and Training	Define and Document Personnel handling and training required protecting Critical Cyber Assets
CIP-005-1 Electronic Security	Define and document logical security perimeters where Critical Cyber Assets reside. Define and document measures to control access points and monitor electronic access
CIP-006-1 Physical Security	Define and document Physical Security Perimeters within which Critical Cyber Assets reside
CIP-007-1 Systems Security Management	Define and document system test procedures, account and password management, security patch management, system vulnerability, system logging, change control and configuration required for all Critical Cyber Assets
CIP-008-1 Incident Reporting and Response Planning	Define and document procedures necessary when Cybersecurity Incidents relating to Critical Cyber Assets are identified
CIP-009-1 Recovery Plans	Define and document Recovery plans for Critical Cyber Assets

19.4.1.1 CIP 002

CIP 002 concerns itself with the identification of:

- Critical assets, such as overhead lines and transformers
- Critical cyber assets, such as IEDs that use routable protocols to communicate outside or inside the Electronic Security Perimeter; or are accessible by dial-up

Power Utility Responsibilities	GE Vernova's Contribution
Create the list of the assets	We can help the power utilities to create this asset register automatically. We can provide audits to list the Cyber assets

19.4.1.2 CIP 003

CIP 003 requires the implementation of a Cybersecurity policy, with associated documentation, which demonstrates the management's commitment and ability to secure its Critical Cyber Assets.

The standard also requires change control practices whereby all entity or vendor-related changes to hardware and software components are documented and maintained.

Power Utility Responsibilities	GE Vernova's Contribution
To create a Cybersecurity policy	We can help the power utilities to have access control to its critical assets by providing centralised Access control. We can help the customer with its change control by providing a section in the documentation where it describes changes affecting the hardware and software.

19.4.1.3 CIP 004

CIP 004 requires that personnel with authorised cyber access or authorised physical access to Critical Cyber Assets, (including contractors and service vendors), have an appropriate level of training.

Power Utility Responsibilities	GE Vernova's Contribution
To provide appropriate training of its personnel	We can provide Cybersecurity training

19.4.1.4 CIP 005

CIP 005 requires the establishment of an Electronic Security Perimeter (ESP), which provides:

- The disabling of ports and services that are not required
- Permanent monitoring and access to logs (24x7x365)
- Vulnerability Assessments (yearly at a minimum)
- Documentation of Network Changes

Power Utility Responsibilities	GE Vernova's Contribution
To monitor access to the ESP To perform the vulnerability assessments To document network changes	To disable all ports not used in the IED To monitor and record all access to the IED

19.4.1.5 CIP 006

CIP 006 states that Physical Security controls, providing perimeter monitoring and logging along with robust access controls, must be implemented and documented. All cyber assets used for Physical Security are considered critical and should be treated as such:

Power Utility Responsibilities	GE Vernova's Contribution
Provide physical security controls and perimeter monitoring Ensure that people who have access to critical cyber assets don’t have criminal records	GE Vernova cannot provide additional help with this aspect

19.4.1.6 CIP 007

CIP 007 covers the following points:

- Test procedures
- Ports and services
- Security patch management
- Antivirus
- Account management
- Monitoring
- An annual vulnerability assessment should be performed

Power Utility Responsibilities	GE Vernova's Contribution
To provide an incident response team and have appropriate processes in place	Test procedures, we can provide advice and help on testing Ports and services, our devices can disable unused ports and services Security patch management, we can provide assistance Antivirus, we can provide advise and assistance Account management, we can provide advice and assistance Monitoring, our equipment monitors and logs access

19.4.1.7 CIP 008

CIP 008 requires that an incident response plan be developed, including the definition of an incident response team, their responsibilities and associated procedures.

Power Utility Responsibilities	GE Vernova's Contribution
To provide an incident response team and have appropriate processes in place.	GE Vernova Vernova cannot provide additional help with this aspect.

19.4.1.8 CIP 009

CIP 009 states that a disaster recovery plan should be created and tested with annual drills.

Power Utility Responsibilities	GE Vernova's Contribution
To implement a recovery plan	To provide guidelines on recovery plans and backup/restore documentation

19.4.2 IEEE 1686-2013

IEEE 1686-2013 is an IEEE Standard for substation IEDs' Cybersecurity capabilities. It proposes practical and achievable mechanisms to achieve secure operations.

The following features described in this standard apply:

- Passwords are 8 characters long and can contain upper-case, lower-case, numeric and special characters.
- Passwords are never displayed or transmitted to a user.
- IED functions and features are assigned to different password levels. The assignment is fixed.

- The audit trail is recorded, listing events in the order in which they occur, held in a circular buffer.
- Records contain all defined fields from the standard and record all defined function event types where the function is supported.
- No password defeat mechanism exists. Instead a secure recovery password scheme is implemented.
- Unused ports (physical and logical) may be disabled.

19.5 CYBER-SECURITY IMPLEMENTATION

GE Vernova IEDs have always been and will continue to be equipped with state-of-the-art security measures. Due to the ever-evolving communication technology and new threats to security, this requirement is not static. Hardware and software security measures are continuously being developed and implemented to mitigate the associated threats and risks.

From Software Version 90 onwards, the MiCOM P40 Agile products provide enhanced security through the following features:

- An Authentication, Authorisation, Accounting (AAA) Remote Authentication Dial-In User Service (RADIUS) client that is managed centrally, enables user attribution, provides accounting of all user activities, and uses secure standards based on strong cryptography for authentication and credential protection. In other words, this option uses a RADIUS.
- Server for user authentication. There is provision for both remote (RADIUS) and local (device) authentication.
- A Role-Based Access Control (RBAC) system that provides a permission model that allows access to the device operations and configurations based on specific roles and individual user accounts configured on the AAA server. That is, Administrator, Engineer, Operator, and Viewer roles are used.
- Security event reporting through both proprietary event logs and the Syslog protocol for supporting Security Information Event Management (SIEM) systems for centralised cybersecurity monitoring.
- Encryption of passwords – stored within the IED, in network messages between the MiCOM S1 Agile software and the IED, and in network messages between the RADIUS server and the IED (subject to the RADIUS server configuration).

19.5.1 INITIAL SETUP

The requirements for initial setup of the IED for cyber-security and RBAC will depend on:

1. which interfaces, if any, the cyber-security is required,
2. the intended authentication method, as defined in the setting ***Auth. Method*** in *SECURITY CONFIG* column (see the Authentication methods section).

When the authentication method is configured as *Device Only*, there are four pre-defined usernames, **VIEWER**, **OPERATOR, ENGINEER**, and **ADMINISTRATOR** that align with the **VIEWER**, **OPERATOR**, **ENGINEER** and **ADMINISTRATOR** roles (see the Device Users section).

When the authentication method is configured as ‘Server Only’ or ‘Server + Device’, users must be set up on the Radius server (see the RADIUS users section). These users are separate from the pre-defined Device users. RADIUS server information must be configured in the IED to connect to the RADIUS server(s) for Server authentication (see the RADIUS server settings section). It is recommended that the Radius shared secret be changed from the default (see the RADIUS client-server validation section).

Whatever the authentication method, it is strongly recommended that the password for the Administrator be changed from the default. Changing the passwords for the other roles is optional.

19.6 ROLES AND PERMISSIONS

19.6.1 ROLES

The P40 Agile products provide 4 specific roles to which individual user accounts can be configured:

- VIEWER (Level 0) Read some, Write minimal
- OPERATOR (Level 1) Read All, Write Few
- ENGINEER (Level 2) Read All, Write Some
- ADMINISTRATOR (Level 3) Read All, Write All

Only one role of one type is allowed to be logged in at a time. For example, one Operator can be logged in but not a second Operator at the same time. This prevents subsets of settings from being changed at the same time.

Roles are mapped to Access Level definitions:

VIEWER - No password required - Read access to Security features, Model Number, Serial Number, S/W version, Description, Plant reference, Security code (UI Only), Encryption key (UI Only), User Banner and security related cells. This role will allow maximum concurrent access provided by P40. Viewer is the default role

OPERATOR - Operator password required - Read access to all data and settings. Write access to Primary/ Secondary selector, Operator password setting, Password reset cell and log extraction cells (record selector). This role will not allow concurrent access.

ENGINEER - Engineer password required - Read access to all data and settings. Write access to Reset demands and counters. This role will not allow concurrent access.

ADMINISTRATOR - Administrator password required - Read access to all data and settings. Write access to All settings, PSL, IED Config, Security settings (port disabling etc). This role can enable the bypass mode and forcefully logout any other role. This role will not allow concurrent access.

The IED defines the following roles with reference to the roles defined by IEC 62351-8.

P40 Roles	IEC 62351- 8 Roles	Access Level
VIEWER	VIEWER	Level 0
OPERATOR	OPERATOR	Level 1
ENGINEER	ENGINEER	Level 2
ADMINISTRATOR	SECADM + SECAUD	Level 3

By default, the IED is delivered with default factory roles account and passwords. These default passwords are shown in the below table.

Role	Default Password
ADMINISTRATOR	ChangeMe1#
ENGINEER	ChangeMe1#
OPERATOR	ChangeMe1#
VIEWER	NA

Note:
It is strongly recommended that the password for the Administrator be changed from the default. Changing the passwords for the other roles is optional.

Administrators have the following rights as well:

- Setting the Bypass mode
- Forcefully logging out any other role
- Setting Authentication Method

'Firmware lock' is not supported by the P40 Agile IED. Firmware upgrade is not managed by the main software. The process involves using a dedicated firmware loading software tool. There is no access or control to this process via the main product firmware.

19.6.2 PERMISSIONS

Authentication and authorisation are two different processes. An authenticated user cannot perform any action on the IED unless a privilege has been explicitly granted to them. This is the concept of “least privileges” access.

Privileges must be granted to users through roles. A role is a collection of privileges, and roles are granted to users. Each user is associated to only one role. The privilege/role matrix is stored on the IED. This is known as Role-Based-Access Control (RBAC).

On successful user authentication, the IED will load the user’s role list. If the user’s role changes, the user must logout and log back in to exercise his/her privileges.

Existing User level/permission mapping in P40 are:

Role	Meaning	Read Operation	Write Operation
VIEWER	Read Some Write Minimal	SYSTEM DATA column: Description Plant Reference Model Number Serial Number S/W Ref. Access Level Security Feature SECURITY CONFIG column: User Banner Attempts Remain Blk Time Remain Fallback PW level Security Code (UI only)	Password Entry LCD Contrast (UI only)
OPERATOR	Read All Write Few	All data and settings are readable. Poll Measurements	All items writeable at "Viewer". Select Event, Main and Fault (upload) Extract Events (e.g. via MiCOM S1 Agile)
ENGINEER	Read All Write Some	All data and settings are readable. Poll Measurements	All items writeable at "Operator". Setting Cells that change visibility (Visible/Invisible). Setting Values (Primary/Secondary) selector Commands: Reset Indication Reset Demand Reset Statistics Reset CB Data / counters

Role	Meaning	Read Operation	Write Operation
ADMINISTRATOR	Read All Write All	All data and settings are readable. Poll Measurements	All items writeable at "Engineer". Change all Setting cells Operations: Extract and download Setting file. Extract and download PSL Extract and download MCL (IEC 61850) Extraction of Disturbance Recorder Courier/MODBUS Accept Event (auto event extraction, e.g. via AE2R) Commands: Change Active Group setting Close/Open CB Change Comms device address. Set Date & Time Switch MCL banks/Switch Conf. Bank in UI (IEC 61850) Enable/Disable Device ports (in SECURITY CONFIG column) All password settings Bypass Enable/disable Change Authentication Method

The table below shows the predefined permissions assignment for the predefined Roles according to IEC 62351-8

Role	View	Read	Dataset	Report	File Read	File Write	File Mngt	Control	Config.	Setting Group	Security
VIEWER	x			x							
OPERATOR	x	x		x				x			
ENGINEER	x	x	x	x		x	x		x		
ADMINISTRATOR	x	x	x	x	x	x	x	x	x	x	x

The table below shows the predefined permissions description according to IEC 62351-8

Permission	Description
VIEW	Allows the subject/role to discover what objects are present within a Logical Device by presenting the type ID of those objects.
READ	Allows the subject/role to obtain all or some of the values in addition to the type and ID of objects that are present within a Logical-Device
DATASET	Allows the subject/role to have full management rights for both permanent and non-permanent DataSets
REPORTING	Allows a subject/role to use buffered reporting as well as un-buffered reporting
FILEREAD	Allows the subject/role to have read rights for file objects
FILEWRITE	Allows the subject/role to have write rights for file objects. This right includes the FILEREAD right
FILEMNGT	Allows the role to transfer files to the Logical-Device, as well as delete existing files on the Logical-Device
CONTROL	Allows a subject to perform control operations
CONFIG	Allows a subject to locally or remotely configure certain aspects of the server
SETTINGGROUP	Allows a subject to remotely configure Settings Groups
SECURITY	Allows a subject/role to perform security functions at both a Server/Service Access Point and Logical-Device basis

19.7 AUTHENTICATION

19.7.1 AUTHENTICATION METHODS

The IED supports Bypass (no authentication), Device authentication and Server authentication.

Authentication Method	Description
Bypass Auth.	IED does not provide security, any user (Local/Remote) can login to the IED. IED does not validate user and password. In this case, there is no need to enter user-id and password to login.
Device Only	IED allows role access using local authentication
Server Only	IED uses RADIUS server to validate access
Server + Device	IED uses server authentication to validate user first. And it allows fallback to device authentication if the RADIUS server(s) are unavailable.

If ***Bypass Auth.*** is enabled, the IED ignores the ***Auth. Method*** setting.

The ***Auth. Method*** setting offers the following options for user authentication:

- *Server + Device* (This is the default setting for IEC 61850+Courier; IEC 61850+103; DNP3OE - where applicable)
- *Device Only* (This is the default setting for Courier/IEC 60870-5-103/MODBUS/DNP3)
- *Server Only*

Only an **ADMINISTRATOR** role may change the ***Auth. Method*** setting. If Administrator changes it, the role remains logged in. But only when the user log-out, their access-level is revoked.

If Authentication method is *Server Only* and RADIUS Server IP addresses are configured, no device user has access to the IED (only the RADIUS users will have access). Only the RADIUS Administrator role will be able to switch to "Server and Device auth". When the setting is “Server Only” but RADIUS Server IP are not configured (both Primary & Secondary are 0.0.0.0), the IED will automatically fall back to Device authentication.

When Authentication method is *Server Only*, if the RADIUS server(s) are unavailable, the user should first take actions to recover the RADIUS connection. If both RADIUS servers ultimately failed to recover, the user should follow the password reset procedure to reset the ***Auth. Method*** setting to *Device Only*.

19.7.2 BYPASS

In ***Bypass Auth.*** mode, the IED does not provide security - any user can login. IED does not validate user and password. The bypass security feature provides an easier access, with no authentication and encryption for situations when this is considered safe. Only the Administrator can enable Bypass mode.

There are five modes for authentication bypass:

1. *Disabled* – no interfaces in ***Bypass Auth.*** mode (normal authentication is active)
2. *Local & Remote*
   a. Front Panel;
   b. Front Port
   c. Rear Ports
   d. Ethernet

3. *Local* – will bypass authentication for
   a. Front Panel;
   b. Front Port
4. *Remote* – will bypass authentication for
   a. Ethernet
   b. Rear Ports
5. *HMI-Only* – will bypass authentication only for front panel

Bypass Authentication for Bypass Mode	Front panel	Front Port	Rear Port	Ethernet
Disabled				
Local & Remote	X	X	X	X
Local	X	X		
Remote			X	X
HMI-Only	X			

The DDB signal ***Security Bypass*** is available to indicate that the IED is in ***Bypass Auth.*** mode.

19.7.3 LOGIN

A user can only login through the following methods:

- Front Panel User Interface
- Using MiCOM S1 Agile, connected to either the Front Port, Rear Port 1 or 2, or NIC (Ethernet) interface.

The interfaces/protocols implemented in P40 are listed in the following table.

The product supports both RBAC (with *Server + Device* authentication) and original Access Level. The Courier Interfaces/HMI use the RBAC whilst other protocols such as MODBUS, IEC 60870-5-103, DNP3 use the original Access Level to authenticate.

The following table shows different product variants that supports different protocols on Rear ports and Network port.

Local Access	Front Port	Rear Port (1/2)	NIC (Ethernet) Port	Supported Auth. Mechanism
HMI Courier	Courier	Courier	-	Device
HMI Courier	Courier	Courier	IEC 61850 + SNMP + Courier tunnel	Server and Device
HMI Courier	Courier	MODBUS (no server, device auth only, old access levels)	-	Device Old Access level for MODBUS
HMI Courier	Courier	IEC 60870-5-103 (no server, device auth only, old access levels)	-	Device Old Access level for 103
HMI Courier	Courier	IEC 60870-5-103 (no server, device auth only, old access levels)	IEC 61850 + SNMP + Courier tunnel	Server and Device Old Access level for 103
HMI Courier	Courier	DNP3 (no server, device auth only, old access levels)	-	Device Old Access level for DNP3
HMI Courier	Courier	Courier	DNP3 + SNMP + Courier tunnel	Server and Device Old Access level for DNP3

19.7.3.1 FRONT PANEL LOGIN

Front panel User Interface supports both Device authentication and Server authentication. The P40 gives the user the option to enter a username in HMI panel.

The user can type their password in the password cell.

For Device authentication, the user must enter one of the pre-defined usernames **VIEWER**, **OPERATOR**, **ENGINEER**, **ADMINISTRATOR**. The user can scroll through these names using either of the hotkeys. Users must then enter their password.

For Server authentication, the user can enter any valid pre-defined Radius server username. Using the front panel User Interface, the user can change the displayed character type (digit, uppercase letter, lowercase letter, special character) by either of the hotkeys. For ease of typing, it is preferable to do Server authentication login using MiCOM S1 Agile.

After successful log in, a confirmation message is displayed, showing the logged in username. For example:

```
LOGIN SUCCESS
OPERATOR
```

19.7.3.2 MICOM S1 LOGIN

When the user attempts to login, MiCOM S1 Agile will prompt the user with a login dialog box that contains a username text entry field and a password text entry field. The username field is a combo-dropdown style text field that includes the fixed usernames (**Administrator**, **Engineer**, **Operator**, **Viewer**) for Device authentication - the user can pick one of these if they wish, or type any other pre-defined username for Radius authentication in the textbox.

19.7.3.3 WARNING BANNER

After successful authentication and authorisation to access the IED, MiCOM S1 Agile will display a security warning banner to the user.

If **I Agree** is selected, the integrated authentication and authorisation is completed. Selecting **I Disagree** causes the program to close and the login user to logout.

For S1 Agile authentication, this is a pop-up dialog that the user must click to acknowledge.

19.7.3.4 LOGIN FAILED

When Device authentication fails, a failure message is displayed:

```
LOGIN FAILED
```

For front panel authentication, this is shown for 2 seconds on the LCD.

For S1 Agile authentication, this is a pop-up dialog that the user must click to acknowledge.

19.7.4 USER SESSIONS

Open sessions will be automatically closed by the IED after a configurable session timeout.

The inactivity timer configuration setting defines the period of time that the IED waits in idleness before a logged in user is automatically logged out.

If there is any data change that does not commit to IED, the data change is discarded when user logged out. If there is any access that does not finish, the access will fail when user logged out. Front panel will display the default page when user reaches the defined inactivity time.

If the keypad is inactive for configured UI inactivity timer, user logout message is displayed. And front panel user interface reverts to the Viewer access level.

Currently in the P40, the inactivity timer for both front port and HMI is fixed to 15 minutes. Already, ***RP1 InactivTimer*** and ***RP2 InactivTimer*** settings control the inactivity timer for RP1 and RP2. There are two new settings to support configurable inactivity timer for front port and front panel user interface:

- ***FP InactvTimer***
- ***UI InactivTimer***

Administrator, Operator and Engineer roles will accept only one session to the device at one time. Only Viewer allows 4 concurrent sessions at one time.

Only one user session is allowed from all the access methods mentioned below:

- Front Panel Push buttons
- Front Port (serial) FP1
- Rear Port 1 (RP1)
- Rear Port 2 (RP2)
- Ethernet Port (NIC)

Setting Name	Description	Min	Max	Default	Units	Minimum Permissions
Attempts Limit	Number of failed authentications before the device blocks subsequent authentication attempts for the lockout period. A value of 0 means Lockout is disabled.	0 (lockout disabled)	99	3	-	Administrator
Lockout Period	The period of time in seconds a user is prevented from logging in, after being locked out.	1	5940	5	sec	Administrator
FP InactivTimer	FP Inactivity Timer is the time of idleness on Front Port before a logged in user is automatically logged out and revert the access level to the viewer role	0 (no Inactivity Timeout)	30	10	min	Administrator
UI InactivTimer	UI Inactivity Timer is the time of idleness on Front Panel before a logged in user is automatically logged out and revert the access level to the viewer role	0 (no Inactivity Timeout)	30	10	min	Administrator

The recommended settings for ***Attempts Limit*** is `3` and ***Lockout Period*** is `5 sec` to discourage brute force attacks. If the Lockout period is too large, anybody can lockout Device users.

19.7.5 USER LOCKING POLICY

A local user locking policy is implemented for Device access:

- This user locking policy applies to both Device users.
- The account is unlocked at the first successful login after the ***Lockout Period***
- By default, if the user consecutively fails to login 3 times, the user account will be locked for 3 minutes.

Each user account records how long it has been locked if the account is locked.

Each user account records how many times it has consecutively failed to login. User account failed times include all interfaces login attempts. For example, if the ***Attempts Limit*** setting is `3` and the operator failed to login from front panel 2 times, and they changed to login from the Courier interface, but failed again, then the Operator would be locked out.

When the IED is powered on, these ***Attempts Limit*** counter resets to zero.

When the user account exceeds the ***Attempts Limit*** it is locked for ***Lockout period***, at that time ***Attempt limit*** resets to zero.

The locked user account will be unlocked automatically, after the configured “Lockout Period” is expired.

All user accounts need to wait until the lockout period expires. No user can unlock the locked account.

If the locked account attempts to login the IED from the Front Panel, the following text is displayed (example):

```
OPERATOR
IS LOCKED
```

Usernames are specific to each user account, such as **Engineer**, **Operator** and **Administrator** for Device authentication.

When supporting both RBAC enabled interfaces and non-RBAC interfaces (such as MODBUS), the P40 handles features such as user-locking feature as follows

- If an RBAC user exceeds the invalid password limit, that user gets locked for all the interfaces.
- On a non-RBAC interface, if an Access Level exceeds the invalid password limit, P40 only blocks that.

19.7.6 LOGOUT

Each user should ***Log out*** after reading or configuring the IED.

Both S1 Agile and the Front Panel provide a one step logout.

The user can only log out from the front panel, if they logged in from the front panel. If the user logged in from S1 Agile, they have to logout from S1 Agile.

19.7.6.1 FRONT PANEL LOGOUT

Go up to the top of the menu tree. When you are at the Column Heading level and you press the Up button, you may be prompted to log out with the following display:

```
ENTER TO LOGOUT
CLEAR TO CANCEL
```

If you confirm, the following message is displayed for 2 seconds:

```
LOGGED OUT <ROLE NAME>
LOGGED OUT
ADMINISTRATOR
```

If you decide not to log out (i.e. you cancel), the following message is displayed for 2 seconds.

```
LOGOUT CANCELLED
ADMINISTRATOR
```

19.7.6.2 MICOM S1 LOGOUT

Right-click on the device name in the System Explorer panel in MiCOM S1 Agile and select **Log Off**.

In the Log Off confirmation dialog, click **Yes**.

19.7.7 DEVICE USERS

For device authentication, the user must enter one of the pre-defined usernames **VIEWER**, **OPERATOR**, **ENGINEER**, or **ADMINISTRATOR**. This means that device users and roles are same in the P40, and therefore there can be only one user for each role.

19.7.8 PASSWORD POLICY

Cyber-security requires strong passwords and validation for NERC compliance.

The NERC password complexity policy requires an alpha-numeric password (for all accesses, front panel, and network/local port) that meets the following **mandatory** requirements:

1. Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
2. Passwords must be at least eight characters in length, but not exceed 16 characters in length.
3. Passwords must contain characters from all four categories:
   a. English uppercase characters (A through Z).
   b. English lowercase characters (a through z).
   c. Numeric (digits 0 through 9).
   d. Special non-alphanumeric characters (such as @,!,#,{, but not limited to only those)

For Device authentication, the IED will enforce that configured passwords meet these requirements.

For Server authentication, the password complexity and user locking policy is defined in the external Radius server.

19.7.9 CHANGE PASSWORD

In the Device authentication mode, **VIEWER** does not have a password associated with it.

The password can be changed either from the front panel User Interface, or from MiCOM S1 Agile using the **Change/Set Password** option in the **Supervise Device** dialog box.



Caution:
It is recommended that user passwords are changed periodically.

19.7.10 RADIUS

When the ***Auth. Method*** setting is configured as *Server Only* or *Server + Device*, a user must log in with a username and password that has been predefined on the Radius server.

This log in can be performed from any interface, as described in the Login section. The IED will authenticate the user to the active RADIUS server, over the Ethernet connection.

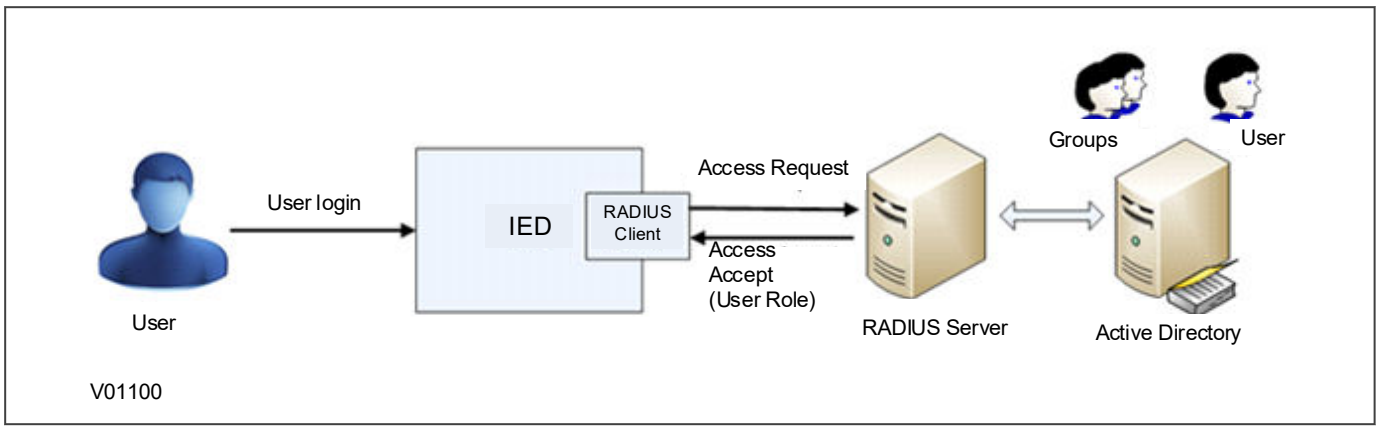


Figure 210: RADIUS server/client communication

19.7.10.1 RADIUS USERS

For Server authentication, RADIUS users and passwords are created in the RADIUS server (in the Active Directory).

The username must consist of uppercase letters (A to Z) and digits (0 to 9) only. No lowercase letters or special characters are allowed.

Each RADIUS user must have a password that meets the password policy of the Active Directory (not the password policy of the P40) and have one of the four roles assigned in the Active Directory.

The number of RADIUS users is not limited by the IED.

RADIUS password changes are done in the Active Directory (after password expiration).

19.7.10.2 RADIUS CLIENT

Two Radius servers are supported by the IED in the configuration for redundancy. The IED will try each in sequence until one responds.

The IED will first try server 1 up to the configured number of retries, leaving a request timeout between each request. If, after this point there is still no valid answer from server 1, the IED will switch to server 2 and repeat for up to the configured number of retries.

If the number of retries for the second server is exceeded, the IED will give up entirely on Server authentication. If Authentication Method is *Server + Device*, the IED will fallback to Device authentication. A **RADIUS Server unavailable** security event is also logged under this condition.

The RADIUS implementation supports the following authentication protocols:

- EAP-TTLS-MSCHAP2
- PAP
- EAP-PEAP-MSCHAP2
- PAP EAP-TTLS-PAP (Default)

The RADIUS implementation queries the Role ID vendor attribute and establish the logged in user security context with that role.

RADIUS Config.	Value
Vendor ID	2910
Vendor Attribute	1
P40 Role Values	
Administrator	3
Engineer	2
Operator	1
Viewer	0

19.7.10.3 RADIUS SERVER SETTINGS

The following RADIUS server information must be configured in the IED to connect to the RADIUS server(s) for Server authentication.

Setting Name	Description	Min	Max	Default	Units	Minimum Permissions
RADIUS Pri IP	IP address of Server 1. Default value indicates no Primary Radius server is configured, and so Radius is disabled.	0.0.0.0	255.255.255.255	0.0.0.0	-	Administrator
RADIUS Sec IP	IP address of Server 2. Default value indicates no Secondary Radius server is configured.	0.0.0.0	255.255.255.255	0.0.0.0	-	Administrator
RADIUS Auth Port	Radius authentication port	1	65535	1812	-	Administrator
RADIUS Security	Authentication protocol to be used by Radius server	EAP-TTLS-MSCHAP2 PAP EAP-PEAP-MSCHAP2 PAP EAP-TTLS-PAP		PAP EAP-TTLS-PAP	-	Administrator
RADIUS Timeout	Timeout in seconds between re-transmission requests	1	900	2	sec	Administrator
RADIUS Retries	Number of retries before giving up	1	99	10	-	Administrator
RADIUS Secret	Shared Secret used in authentication. It is only displayed as asterisks.	1 character	16 characters	ChangeMe1#	-	Administrator

The data cell ***RADIUS Status*** indicates the status of the currently-selected RADIUS server. This will display either *Disabled*, *Server OK*, or *Failed*.

19.7.10.4 RADIUS ACCOUNTING

RADIUS accounting is not supported by the IED. The user can achieve accounting through syslog (see the SYSLOG section).

19.7.10.5 RADIUS CLIENT-SERVER VALIDATION

Client-server validation is achieved using a shared secret. The IED must be configured with the ***RADIUS Secret*** setting to match the shared secret configured in the RADIUS server. It is recommended (but not enforced) that this setting meets the P40 password requirements.

Note:
It is recommended that the shared secret be changed from the default before using Radius authentication.

The IED does not support exchange of CA certificates. The RADIUS server may send a certificate but the IED will not verify it.

19.7.11 RECOVERY

19.7.11.1 RESTORE TO LOCAL FACTORY DEFAULT

The ***Restore Defaults*** setting is available to facilitate NERC CIP compliance requirements for decommissioning critical cyber devices. Only the **Administrator** role can change this setting.

The ***Restore Defaults*** setting under the *CONFIGURATION* column is used to restore a setting group to factory default settings.

0 = *No Operation*

1 = *All Settings*

2 = *Setting Group 1*

3 = *Setting Group 2*

4 = *Setting Group 3*

5 = *Setting Group 4*

To restore the default values to the settings in any setting group, set the ***Restore Defaults*** setting to the relevant Group number. Alternatively, it is possible to set the ***Restore Defaults*** setting to *All Settings* to restore the default values to all the IEDs settings, not only one setting group.

Note:
Restoring defaults to all settings includes the rear communication port settings, which may result in communication via the rear port being disrupted if the new (default) settings do not match those of the master station.

Data (events, DR, fault records, protection counters etc.) is left untouched. When decommissioning critical cyber IEDs, users may want to clear all data and events as well.

19.7.11.2 PASSWORD RESET PROCEDURE

If you mislay a devices password (if Administrator forgets their password), the passwords can be reset to default using a recovery password. To obtain the recovery password you must contact the Contact Centre and supply the Serial Number (TEST ID) and the security code. The Contact Centre will use these details to generate a Recovery Password.

The Serial Number required is a six-digit code followed by one letter, found in the SYSTEM DATA column of the IED. It is the same as the TEST ID shown on the label on top of the IED.

The security code is a 16-character string of uppercase characters. It is a read-only parameter. The device generates its own security code randomly. A new code is generated under the following conditions:

- On power up
- Whenever settings are set back to default
- On expiry of validity timer (see below)
- When the recovery password is entered

This reset procedure can be only accomplished through front panel exclusively and cannot be done over any other interface. As soon as the security code is displayed on the front panel User Interface, a validity timer is started. This validity timer is set to 72 hours and is not configurable. This provides enough time for the Contact Centre to manually generate and send a recovery password. The Service Level Agreement (SLA) for recovery password generation is one working day, so 72 hours is sufficient time, even allowing for closure of the Contact Centre over weekends and bank holidays.

The procedure is:

The security code is displayed on confirmation. The validity timer is then started. The security code can only be read from the front panel.

This reset procedure can be only accomplished through front panel exclusively and cannot be done over the Ethernet/serial port, but only when physically present in front of the IED. In the event of losing all passwords (if the Administrator forgets their password) the user could reset the IED to default passwords, following the procedure below:

1. User navigates to ***Security Code*** cell in *SECURITY CONFIG* column
2. To prevent accidental reading of the IED ***Security Code***, the cell will initially display a warning message:

```
PRESS ENTER TO
READ SEC. CODE
```

3. Press Enter to read the ***Security Code***.
4. User sends an email to the Contact Centre providing the full IED serial number and displayed ***Security Code***, using a recognisable corporate email account
5. Contact Centre emails the user with the Recovery Password. The recovery password is intended for recovery only. It is not a replacement password that can be used continually. It can only be used once - for password recovery.
6. User logs in with the username **ADMINISTRATOR** and the recovery password into the ***Password*** setting in *SYSTEM DATA* column.
7. Then IED will prompt

```
RESET PASSWORD?
ENTER or CLEAR
```

8. Press Enter to continue the reset procedure
9. If the recovery password successfully validates, the default passwords are restored for each access level for Device authentication.
10. Change ***Auth. Method*** setting to `Server + Device` if applicable.

Note:
Restoring passwords to defaults does not affect any other settings and does not provoke reboot of the IED. The protection and control functions of the IED are always maintained.

19.7.11.3 ACCESS LEVEL DDBS

The current level of access for each interface is available for use in the Programmable Scheme Logic (PSL) as these DDB signals:

- ***HMI Access Lvl 1***
- ***HMI Access Lvl 2***
- ***FPort AccessLvl1***
- ***FPort AccessLvl2***

- ***RPrt1 AccessLvl1***
- ***RPrt1 AccessLvl2***
- ***RPrt2 AccessLvl1***
- ***RPrt2 AccessLvl2***

Each pair of DDB signals indicates the access level as follows:

- Level 1 off, Level 2 off = 0
- Level 1 on, Level 2 off = 1
- Level 1 off, Level 2 on = 2
- Level 1 on, Level 2 on = 3

KEY:

HMI = Human Machine Interface

FPort = Front Port

RPrt = Rear Port

Lvl = Level

19.7.12 DISABLING PHYSICAL PORTS

It is possible to disable unused physical ports. A level 3 password is needed to perform this action.

To prevent accidental disabling of a port, a warning message is displayed according to whichever port is required to be disabled. For example, if rear port 1 is to be disabled, the following message appears:

```
REAR PORT 1 TO BE
DISABLED.CONFIRM
```

The following ports can be disabled, depending on the model.

- Front port (***Front Port*** setting)
- Rear port 1 (***Rear Port 1*** setting)
- Rear port 2 (***Rear Port 2*** setting)
- Ethernet port (***Ethernet Port*** setting)

Note:
It is not possible to disable a port from which the disabling port command originates.
We do not generally advise disabling the physical Ethernet port.

19.7.13 DISABLING LOGICAL PORTS

It is possible to disable unused logical ports. A level 3 password is needed to perform this action.

Note:
The port disabling setting cells are not provided in the settings file. It is only possible to do this using the HMI front panel.

The following protocols can be disabled:

- IEC 61850 (***IEC 61850*** setting)
- DNP3 Over Ethernet (***DNP3 OE*** setting)--where available
- Courier Tunnelling (***Courier Tunnel*** setting)

Note:
If any of these protocols are enabled or disabled, the Ethernet card will reboot.

19.8 SECURITY EVENT MANAGEMENT

To implement NERC-compliant cyber-security, a range of security events are logged in the Security Event file.

19.8.1 SECURITY EVENTS: COURIER

Event Value	Display
PASSWORD LEVEL UNLOCKED	USER LOGGED IN ON {int} LEVEL {n}
PASSWORD LEVEL RESET	USER LOGGED OUT ON {int} LEVEL {n}
PASSWORD SET BLANK	P/WORD SET BLANK BY {int} LEVEL {p}
PASSWORD SET NON-COMPLIANT	P/WORD NOT-NERC BY {int} LEVEL {p}
PASSWORD MODIFIED	PASSWORD CHANGED BY {int} LEVEL {p}
PASSWORD ENTRY BLOCKED	PASSWORD BLOCKED ON {int}
PASSWORD ENTRY UNBLOCKED	P/WORD UNBLOCKED ON {int}
INVALID PASSWORD ENTERED	INV P/W ENTERED ON <int}
PASSWORD EXPIRED	P/WORD EXPIRED ON {int}
PASSWORD ENTERED WHILE BLOCKED	P/W ENT WHEN BLK ON {int}
RECOVERY PASSWORD ENTERED	RCVY P/W ENTERED ON {int}
IED SECURITY CODE READ	IED SEC CODE RD ON {int}
IED SECURITY CODE TIMER EXPIRED	IED SEC CODE EXP -
PORT DISABLED	PORT DISABLED BY {int} PORT {prt}
PORT ENABLED	PORT ENABLED BY {int} PORT {prt}
DEF. DISPLAY NOT NERC COMPLIANT	DEF DSP NOT-NERC
PSL SETTINGS DOWNLOADED	PSL STNG D/LOAD BY {int} GROUP {grp}
DNP SETTINGS DOWNLOADED	DNP STNG D/LOAD BY {int}
TRACE DATA DOWNLOADED	TRACE DAT D/LOAD BY {int}
IEC 61850 CONFIG DOWNLOADED	IED CONFG D/LOAD BY {int}
USER CURVES DOWNLOADED	USER CRV D/LOAD BY {int} GROUP {crv}

Event Value	Display
PSL CONFIG DOWNLOADED	PSL CONFG D/LOAD BY {int} GROUP {grp}
SETTINGS DOWNLOADED	SETTINGS D/LOAD BY {int} GROUP {grp}
PSL SETTINGS UPLOADED	PSL STNG UPLOAD BY {int} GROUP {grp}
DNP SETTINGS UPLOADED	DNP STNG UPLOAD BY {int}
TRACE DATA UPLOADED	TRACE DAT UPLOAD BY {int}
IEC 61850 CONFIG UPLOADED	IED CONFG UPLOAD BY {int}
USER CURVES UPLOADED	USER CRV UPLOAD BY {int} GROUP {crv}
PSL CONFIG UPLOADED	PSL CONFG UPLOAD BY {int} GROUP {grp}
SETTINGS UPLOADED	SETTINGS UPLOAD BY {int} GROUP {grp}
EVENTS HAVE BEEN EXTRACTED	EVENTS EXTRACTED BY {int} {nov} EVNTS
ACTIVE GROUP CHANGED	ACTIVE GRP CHNGE BY {int} GROUP {grp}
CS SETTINGS CHANGED	C & S CHANGED BY {int}
DR SETTINGS CHANGED	DR CHANGED BY {int}
SETTING GROUP CHANGED	SETTINGS CHANGED BY {int} GROUP {grp}
POWER ON	POWER ON -
SOFTWARE_DOWNLOADED	S/W DOWNLOADED -

where:

- int is the interface definition (UI, FP, RP1, RP2, TNL, TCP)
- prt is the port ID (FP, RP1, RP2, TNL, DNP3, IEC, ETHR)
- grp is the group number (1, 2, 3, 4)
- crv is the Curve group number (1, 2, 3, 4)
- n is the new access level (0, 1, 2, 3)
- p is the password level (1, 2, 3)
- nov is the number of events (1 - nnn)

Each new event has an incremented unique number, therefore missing events appear as gap in the sequence. The unique identifier forms part of the event record that is read or uploaded from the IED.

Note:
It is no longer possible to clear Event, Fault, Maintenance, and Disturbance Records.

19.8.2 SYSLOG

Security events are also logged to a remote syslog server.

All login and logout attempts from local and central authentication, whether successful or failed, are logged. The contents of each successful or failed, login and logout security event include a specific username.

The security log cannot be cleaned by any of the available roles.

The contents of each login and/or logout security event include the relevant interface. The following interfaces are supported:

Interface	Abbr.
Front Port	FP
Rear Port 1	RP1
Rear Port 2	RP2
Ethernet	NET
Front Panel	UI

The following events are available to be logged to the syslog server:

Event Categorisation	Severity
Login - Authentication successful	Informational (6)
Login - Authentication Failure	Informational (6)
Logout	Informational (6)
RADIUS Server Unavailable	Alert (1)
Session timeout	Informational (6)
Account Locked	Notice (5)
User accessed while locked	Notice (5)
ByPass Activate	Notice (5)
ByPass Deactivate	Notice (5)
Password Change	Notice (5)
Recovery password is entered to reset the passwords	Notice (5)
Settings/Configuration Changed	Notice (5)
Settings/Configuration uploaded (to S1 Agile)	Notice (5)
Event Records uploaded	Notice (5)
Default settings restored	Notice (5)
Active Setting Group Changed	Notice (5)
	Notice (5)
	Notice (5)
	Notice (5)
Default user curves restored	Notice (5)
	Notice (5)
	Notice (5)

19.8.3 SYSLOG CLIENT

The IED supports security event reporting through the Syslog protocol for supporting Security Information Event Management (SIEM) systems for centralised cyber security Monitoring over UDP protocol.

The IED is a Syslog client that supports two Syslog servers. The following settings are available in the *COMMUNICATIONS* column.

Setting Name	Description	Min	Max	Default	Units	Min. Permission
SysLog Pri IP	The IP address of the target Syslog server (Primary)	0.0.0.0	223.255.255.254	0.0.0.0	-	Administrator
SysLog Sec IP	The IP address of the target Syslog server (Secondary)	0.0.0.0	223.255.255.254	0.0.0.0	-	Administrator
SysLog Port	The UDP port number of the target Syslog server	1	65535	514	-	Administrator

19.8.4 SYSLOG FUNCTIONALITY

The P40 supports the RFC 5424 UDP protocol.

The table below shows the format of a Syslog event.

Header	<PRIVAL>1 YYYY-MM-DDTHH:mm:ss.fffZ IEDName userlog - MSGID	
	PRIVAL	32 + [event severity] 32 is derived from the facility number 4 (meaning security/authorization messages) Event severity is derived from the received message.
	YYYY	4 Digit year; i.e. 2018 Derived from the received message timestamp.
	MM	2 Digit month; 01 to 12 (for January to December). Derived from the received message timestamp.
	DD	2 Digit day of month; 01 to 31 (depending upon the month) Derived from the received message timestamp.
	HH	2 Digit hour of day; 00 to 23 Derived from the received message timestamp.
	mm	2 Digit count of minutes elapsed in the current hour; 00 to 59 Derived from the received message timestamp.
	ss	2 Digit count of seconds elapsed in the current minute; 00 to 59 Derived from the received message timestamp.
	fff	3 Digit fraction of seconds (millisecond resolution); 0 to 999 Derived from the received message timestamp.
	IP Addr	IP Address assigned to the Ethernet Board.
	MSGID	Unique message type identity Derived from the received message event type.
Data (common)	[timeQuality tzKnown=X]	
	X	Timezone quality attribute for event timestamp (in header) 0; indicating Local Time offset and DST settings are not enabled (i.e. timestamp is UTC)

Data (Platform event)	[gePlatformEvt channel=IFACE accessLevel=AL evtid=UUID extra=EDATA] DETAIL	
	IFACE	Channel access type Copied from the received message interface name.
	AL	Access Level Copied from the received message access level.
	UUID	Unique event identification Copied from the received message unique id.
	EDATA	Extra event data - meaning of which is specific to the event type (see MSGID in header) Copied from the received message extra info.
	DETAIL	Event details. Derived from the received message event text and value.
Data (Enhanced event)	[geUserInfo channel=IFACE loginId=USER] DETAIL	
	IFACE	Channel access type Copied from the received message interface name.
	USER	Logged in username who generated the event Copied from the received message user id.
	DETAIL	Event details. Copied from the received message event text.
Formatted Examples:	<38>1 2018-02-06T11:46:32.074Z Feeder1 userlog - 5120 [timeQuality tzKnown=0][gePlatformEvt channel=UI accessLevel=3 evtid=4 extra=0] User Logged In on UI Level 3User Logged In on UI Level 3 <38>1 2018-02-06T11:46:32.074Z Feeder1 userlog - 9999 [timeQuality tzKnown=0][geUserInfo channel=UI loginId=user1] Login - Authentication successful	

Sample Syslog messages are shown below:

Event	Access Method	Syslog Message (As from Syslog Server)
Authentication Successful	UI	04-17-2019 14:43:32 Auth.Info 192.168.1.30 1 1994-01-23T21:34:06.102Z 192.168.1.30 userlog - 9999 [timeQuality tzKnown=0][geUserInfo channel=FP loginid=ADMINISTRATOR] Login - Authentication successful
Authentication Failure	Serial	04-19-201913:36:08Auth.Info192.168.1.301 1994-01-25T20:26:42.872Z 192.168.1.30 userlog - 9999 [timeQuality tzKnown=0][geUserInfo channel=RP1 loginid=ENGINEER] Login - Authentication fail
Network Login Success	Courier Tunnel (device authentication)	04-17-201915:29:20Auth.Info192.168.1.301 1994-01-23T22:19:58.168Z 192.168.1.30 userlog - 9999 [timeQuality tzKnown=0][geUserInfo channel=NET loginid=ENGINEER] Login - Authentication successful
Logout	Serial	04-19-201913:52:08Auth.Info192.168.1.301 1994-01-25T20:42:42.782Z 192.168.1.30 userlog - 9999 [timeQuality tzKnown=0][geUserInfo channel=RP1 loginid=ADMINISTRATOR] Logout
RADIUS Unavailable	FP	04-18-201912:40:14Auth.Alert192.168.1.301 1994-01-24T19:30:55.839Z 192.168.1.30 userlog - 5163 [timeQuality tzKnown=0][gePlatformEvt channel=FP accessLevel=0 evtid=3715 extra=0] RADIUS UnAvailbl
Bypass Activated	FP	04-18-201912:39:19Auth.Warning192.168.1.301 1994-01-24T19:30:00.573Z 192.168.1.30 userlog - 9998 [timeQuality tzKnown=0][geUserInfo channel=FP loginid=ADMINISTRATOR] ByPass Activated
Settings modified	Courier Tunnel	04-18-201911:52:35Auth.Notice192.168.1.301 1994-01-24T18:43:16.537Z 192.168.1.30 userlog - 5149 [timeQuality tzKnown=0][gePlatformEvt channel=NET accessLevel=3 evtid=3677 extra=0] Settings Upload By TNL

CHAPTER 20

INSTALLATION

20.1 CHAPTER OVERVIEW

This chapter provides information about installing the product.

This chapter contains the following sections:

Chapter Overview 439
Handling the Goods 440
Mounting the Device 441
Cables and Connectors 443
Case Dimensions 448

20.2 HANDLING THE GOODS

Our products are of robust construction but require careful treatment before installation on site. This section discusses the requirements for receiving and unpacking the goods, as well as associated considerations regarding product care and personal safety.



Caution:
Before lifting or moving the equipment you should be familiar with the Safety Information chapter of this manual.

20.2.1 RECEIPT OF THE GOODS

On receipt, ensure the correct product has been delivered. Unpack the product immediately to ensure there has been no external damage in transit. If the product has been damaged, make a claim to the transport contractor and notify us promptly.

For products not intended for immediate installation, repack them in their original delivery packaging.

20.2.2 UNPACKING THE GOODS

When unpacking and installing the product, take care not to damage any of the parts and make sure that additional components are not accidentally left in the packing or lost. Do not discard any CDROMs or technical documentation (where included). These should accompany the unit to its destination substation and put in a dedicated place.

The site should be well lit to aid inspection, clean, dry and reasonably free from dust and excessive vibration. This particularly applies where installation is being carried out at the same time as construction work.

20.2.3 STORING THE GOODS

If the unit is not installed immediately, store it in a place free from dust and moisture in its original packaging. Keep any dehumidifier bags included in the packing. The dehumidifier crystals lose their efficiency if the bag is exposed to ambient conditions. Restore the crystals before replacing it in the carton. Ideally regeneration should be carried out in a ventilating, circulating oven at about 115°C. Bags should be placed on flat racks and spaced to allow circulation around them. The time taken for regeneration will depend on the size of the bag. If a ventilating, circulating oven is not available, when using an ordinary oven, open the door on a regular basis to let out the steam given off by the regenerating silica gel.

On subsequent unpacking, make sure that any dust on the carton does not fall inside. Avoid storing in locations of high humidity. In locations of high humidity the packaging may become impregnated with moisture and the dehumidifier crystals will lose their efficiency.

The device can be stored between –25º to +70ºC for unlimited periods or between -40°C to + 85°C for up to 96 hours (see technical specifications).

To avoid deterioration of electrolytic capacitors, power up units that are stored in a de-energised state once a year, for one hour continuously.

20.2.4 DISMANTLING THE GOODS

If you need to dismantle the device, always observe standard ESD (Electrostatic Discharge) precautions. The minimum precautions to be followed are as follows:

- Use an antistatic wrist band earthed to a suitable earthing point.
- Avoid touching the electronic components and PCBs.

20.3 MOUNTING THE DEVICE

The products are dispatched either individually or as part of a panel or rack assembly.

Individual products are normally supplied with an outline diagram showing the dimensions for panel cut-outs and hole centres.

The products are designed so the fixing holes in the mounting flanges are only accessible when the access covers are open.

If you use a P991 or MMLG test block with the product, when viewed from the front, position the test block on the right-hand side of the associated product. This minimises the wiring between the product and test block, and allows the correct test block to be easily identified during commissioning and maintenance tests.

20.3.1 FLUSH PANEL MOUNTING

Panel-mounted devices are flush mounted into panels using M4 SEMS Taptite self-tapping screws with captive 3 mm thick washers (also known as a SEMS unit).



Caution:
Do not use conventional self-tapping screws, because they have larger heads and could damage the faceplate.

Alternatively, you can use tapped holes if the panel has a minimum thickness of 2.5 mm.

For applications where the product needs to be semi-projection or projection mounted, a range of collars are available.

If several products are mounted in a single cut-out in the panel, mechanically group them horizontally or vertically into rigid assemblies before mounting in the panel.



Caution:
Do not fasten products with pop rivets because this makes them difficult to remove if repair becomes necessary.

20.3.2 RACK MOUNTING

Panel-mounted variants can also be rack mounted using single-tier rack frames (our part number FX0021 001), as shown in the figure below. These frames are designed with dimensions in accordance with IEC 60297 and are supplied pre-assembled ready to use. On a standard 483 mm (19 inch) rack this enables combinations of case widths up to a total equivalent of size 80TE to be mounted side by side.

The two horizontal rails of the rack frame have holes drilled at approximately 26 mm intervals. Attach the products by their mounting flanges using M4 Taptite self-tapping screws with captive 3 mm thick washers (also known as a SEMS unit).



Caution:
Risk of damage to the front cover molding. Do not use conventional self-tapping screws, including those supplied for mounting MiDOS products because they have slightly larger heads.

Once the tier is complete, the frames are fastened into the racks using mounting angles at each end of the tier.

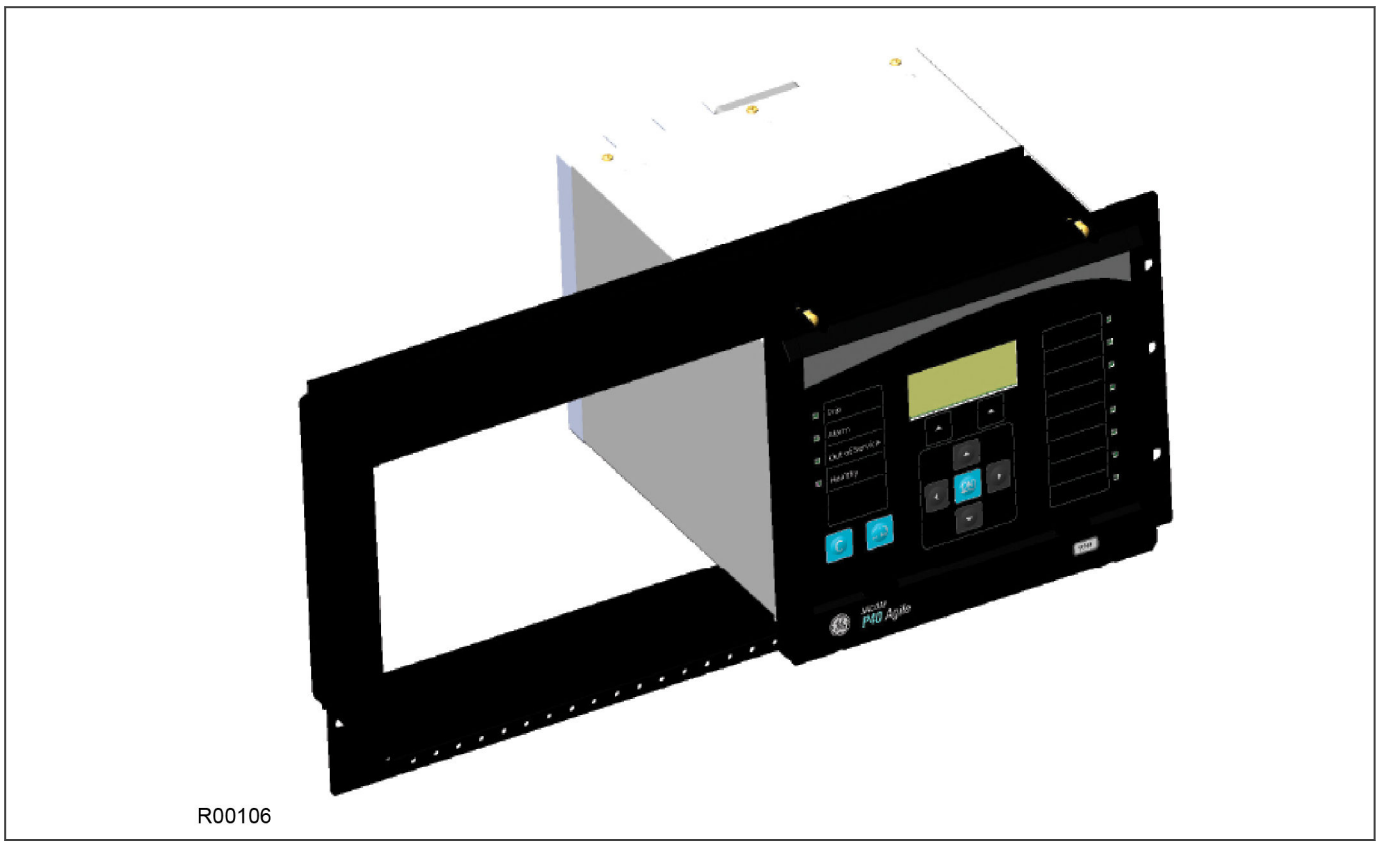


Figure 211: Rack mounting of products

Products can be mechanically grouped into single tier (4U) or multi-tier arrangements using the rack frame. This enables schemes using products from different product ranges to be pre-wired together before mounting.

Use blanking plates to fill any empty spaces. The spaces may be used for installing future products or because the total size is less than 80TE on any tier. Blanking plates can also be used to mount ancillary components. The part numbers are as follows:

Case Size Summation	Blanking Plate Part Number
5TE	GJ2028 001
10TE	GJ2028 002
15TE	GJ2028 003
20TE	GJ2028 004
25TE	GJ2028 005
30TE	GJ2028 006
35TE	GJ2028 007
40TE	GJ2028 008
60TE	GJ2028 012
80TE	GJ2028 016

20.4 CABLES AND CONNECTORS

This section describes the type of wiring and connections that should be used when installing the device. For pin-out details please refer to the Hardware Design chapter or the wiring diagrams.

Caution:
Before carrying out any work on the equipment you should be familiar with the Safety Section and the ratings on the equipment's rating label.

20.4.1 TERMINAL BLOCKS

The device may use one or more of the terminal block types shown in the following diagram. The terminal blocks are fastened to the rear panel with screws.

- Heavy duty (HD) terminal blocks for CT and VT circuits
- Medium duty (MD) terminal blocks for the power supply, relay outputs and rear communications port
- MiDOS terminal blocks for CT and VT circuits
- RTD/CLIO terminal block for connection to analogue transducers

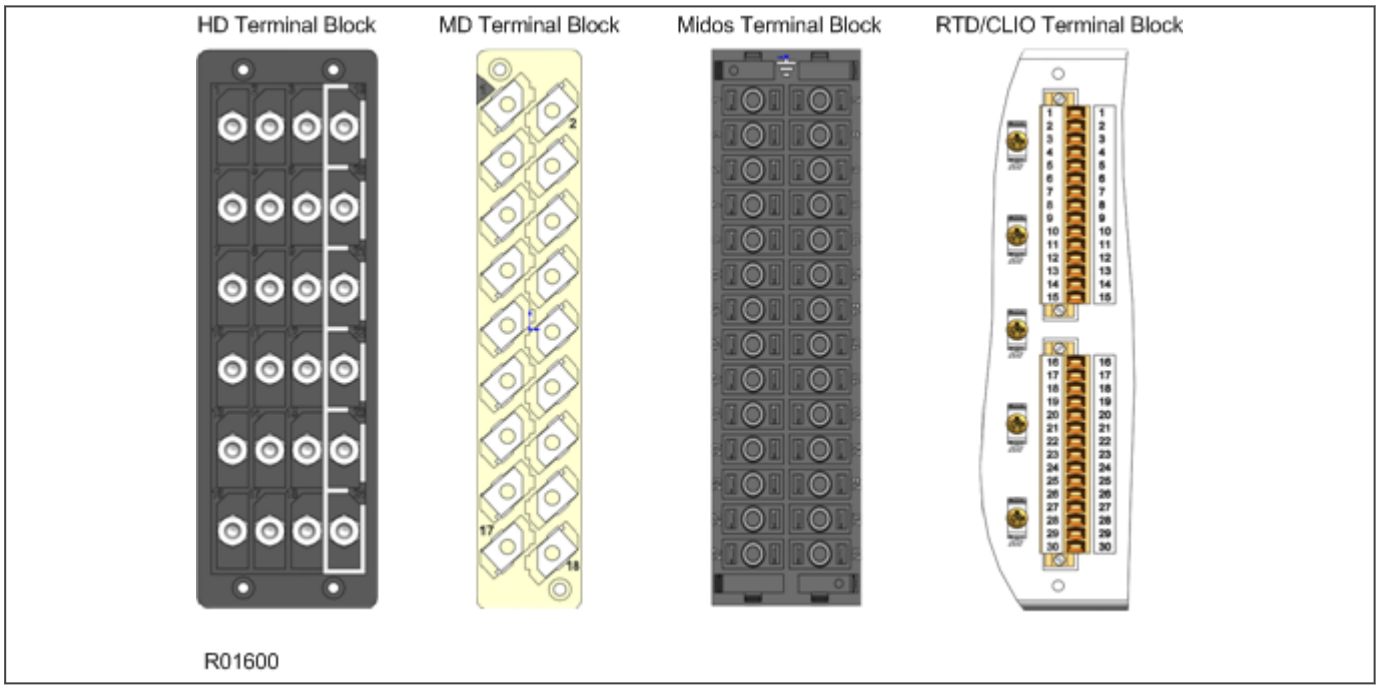


Figure 212: Terminal block types

MiCOM products are supplied with sufficient M4 screws for making connections to the rear mounted terminal blocks using ring terminals, with a recommended maximum of two ring terminals per terminal.

If required, M4 90° crimp ring terminals can be supplied in three different sizes depending on wire size. Each type is available in bags of 100.

Part Number	Wire Size	Insulation Colour
ZB9124 901	0.25 - 1.65 mm^2 (22 - 16 AWG)	Red
ZB9124 900	1.04 - 2.63 mm^2 (16 - 14 AWG)	Blue

Note:
IP2x shields and side cover panels may be fitted to provide IP20 ingress protection for MiCOM terminal blocks. The shields and covers can be attached during installation or retrofitted to upgrade existing installations. The shields are supplied with four language fitting instructions, publication number: IP2x-TM-4L-n (where n is the current issue number). For more information, contact your local sales office or our worldwide Contact Centre.

20.4.2 POWER SUPPLY CONNECTIONS

These should be wired with 1.5 mm PVC insulated multi-stranded copper wire terminated with M4 ring terminals.

The wire should have a minimum voltage rating of 300 V RMS.



Caution:
Protect the auxiliary power supply wiring with a maximum 16 A high rupture capacity (HRC) type NIT or TIA fuse.

20.4.3 EARTH CONNNECTION

Every device must be connected to the cubicle earthing bar using the M4 earth terminal.

Use a wire size of at least 2.5 mm^2 terminated with a ring terminal.

Due to the physical limitations of the ring terminal, the maximum wire size you can use is 6.0 mm^2 using ring terminals that are not pre-insulated. If using pre insulated ring terminals, the maximum wire size is reduced to 2.63 mm^2 per ring terminal. If you need a greater cross-sectional area, use two wires in parallel, each terminated in a separate ring terminal.

The wire should have a minimum voltage rating of 300 V RMS.

Note:
To prevent any possibility of electrolytic action between brass or copper ground conductors and the rear panel of the product, precautions should be taken to isolate them from one another. This could be achieved in several ways, including placing a nickel-plated or insulating washer between the conductor and the product case, or using tinned ring terminals.

20.4.4 CURRENT TRANSFORMERS

Current transformers would generally be wired with 2.5 mm^2 PVC insulated multi-stranded copper wire terminated with M4 ring terminals.

Due to the physical limitations of the ring terminal, the maximum wire size you can use is 6.0 mm^2 using ring terminals that are not pre-insulated. If using pre insulated ring terminals, the maximum wire size is reduced to 2.63 mm^2 per ring terminal. If you need a greater cross-sectional area, use two wires in parallel, each terminated in a separate ring terminal.

The wire should have a minimum voltage rating of 300 V RMS.



Caution:
Current transformer circuits must never be fused.

Note:
If there are CTs present, spring-loaded shorting contacts ensure that the terminals into which the CTs connect are shorted before the CT contacts are broken.

Note:
For 5A CT secondaries, we recommend using 2 x 2.5 mm^2 PVC insulated multi-stranded copper wire.

20.4.5 VOLTAGE TRANSFORMER CONNECTIONS

Voltage transformers should be wired with 2.5 mm^2 PVC insulated multi-stranded copper wire terminated with M4 ring terminals.

The wire should have a minimum voltage rating of 300 V RMS.

20.4.6 WATCHDOG CONNECTIONS

These should be wired with 1 mm PVC insulated multi-stranded copper wire terminated with M4 ring terminals.

The wire should have a minimum voltage rating of 300 V RMS.

20.4.7 EIA(RS)485 AND K-BUS CONNECTIONS

For connecting the EIA(RS485) / K-Bus ports, use 2-core screened cable with a maximum total length of 1000 m or 200 nF total cable capacitance.

To guarantee the performance specifications, you must ensure continuity of the screen, when daisy chaining the connections.

Two-core screened twisted pair cable should be used. It is important to avoid circulating currents, which can cause noise and interference, especially when the cable runs between buildings. For this reason, the screen should be continuous and connected to ground at one end only, normally at the master connection point.

The K-Bus signal is a differential signal and there is no signal ground connection. If a signal ground connection is present in the bus cable then it must be ignored. At no stage should this be connected to the cable's screen or to the product’s chassis. This is for both safety and noise reasons.

A typical cable specification would be:

- Each core: 16/0.2 mm^2 copper conductors, PVC insulated
- Nominal conductor area: 0.5 mm^2 per core
- Screen: Overall braid, PVC sheathed

20.4.8 IRIG-B CONNECTION

The IRIG-B input and BNC connector have a characteristic impedance of 50 ohms. We recommend that connections between the IRIG-B equipment and the product are made using coaxial cable of type RG59LSF with a halogen free, fire retardant sheath.

20.4.9 OPTO-INPUT CONNECTIONS

These should be wired with 1 mm^2 PVC insulated multi-stranded copper wire terminated with M4 ring terminals.

Each opto-input has a selectable preset ½ cycle filter. This makes the input immune to noise induced on the wiring. This can, however slow down the response. If you need to switch off the ½ cycle filter, either use double pole switching on the input, or screened twisted cable on the input circuit.



Caution:
Protect the opto-inputs and their wiring with a maximum 16 A high rupture capacity (HRC) type NIT or TIA fuse.

20.4.10 OUTPUT RELAY CONNECTIONS

These should be wired with 1 mm PVC insulated multi-stranded copper wire terminated with M4 ring terminals.

20.4.11 ETHERNET METALLIC CONNECTIONS

If the device has a metallic Ethernet connection, it can be connected to a 100Base-TX Ethernet hub. Due to noise sensitivity, we recommend this type of connection only for short distance connections, ideally where the products and hubs are in the same cubicle. For increased noise immunity, CAT 6 (category 6) STP (shielded twisted pair) cable and connectors can be used.

The connector for the Ethernet port is a shielded RJ-45. The pin-out is as follows:

Pin	Signal Name	Signal Definition
1	TXP	Transmit (positive)
2	TXN	Transmit (negative)
3	RXP	Receive (positive)
4	-	Not used
5	-	Not used
6	RXN	Receive (negative)
7	-	Not used
8	-	Not used

20.4.12 ETHERNET FIBRE CONNECTIONS

We recommend the use of fibre-optic connections for permanent connections in a substation environment. The 100 Mbps fibre optic port uses type ST or LC connectors depending on the order option (one for Tx and one for Rx), compatible with 50/125 µm or 62.5/125 µm multimode fibres at 1300 nm wavelength.

Note:
For models equipped with redundant Ethernet connections the product must be partially dismantled to set the fourth octet of the second IP address. This ideally, should be done before installation.

20.4.13 USB CONNECTION

The IED has a type B USB socket inside the bottom compartment. A standard USB printer cable (type A one end, type B the other end) can be used to connect a local PC to the IED. This cable is the same as that used for connecting a printer to a PC.

20.4.14 GPS FIBRE CONNECTION

Some products use a GPS 1 PPS timing signal. If applicable, this is connected to a fibre-optic port on the coprocessor board in slot B. The fibre-optic port uses an ST type connector, compatible with fibre multimode 50/125 µm or 62.5/125 µm – 850 nm.

20.4.15 FIBRE COMMUNICATION CONNECTIONS

The fibre optic port consists of one or two channels using ST type connectors (one for Tx and one for Rx). The type of fibre used depends on the option selected.

850 nm and 1300 nm multimode systems use 50/125 µm or 62.5/125 µm multimode fibres. 1300 nm and 1550 nm single mode systems use 9/125 µm single mode fibres.

20.5 CASE DIMENSIONS

Not all products are available in all case sizes.

20.5.1 CASE DIMENSIONS 40TE

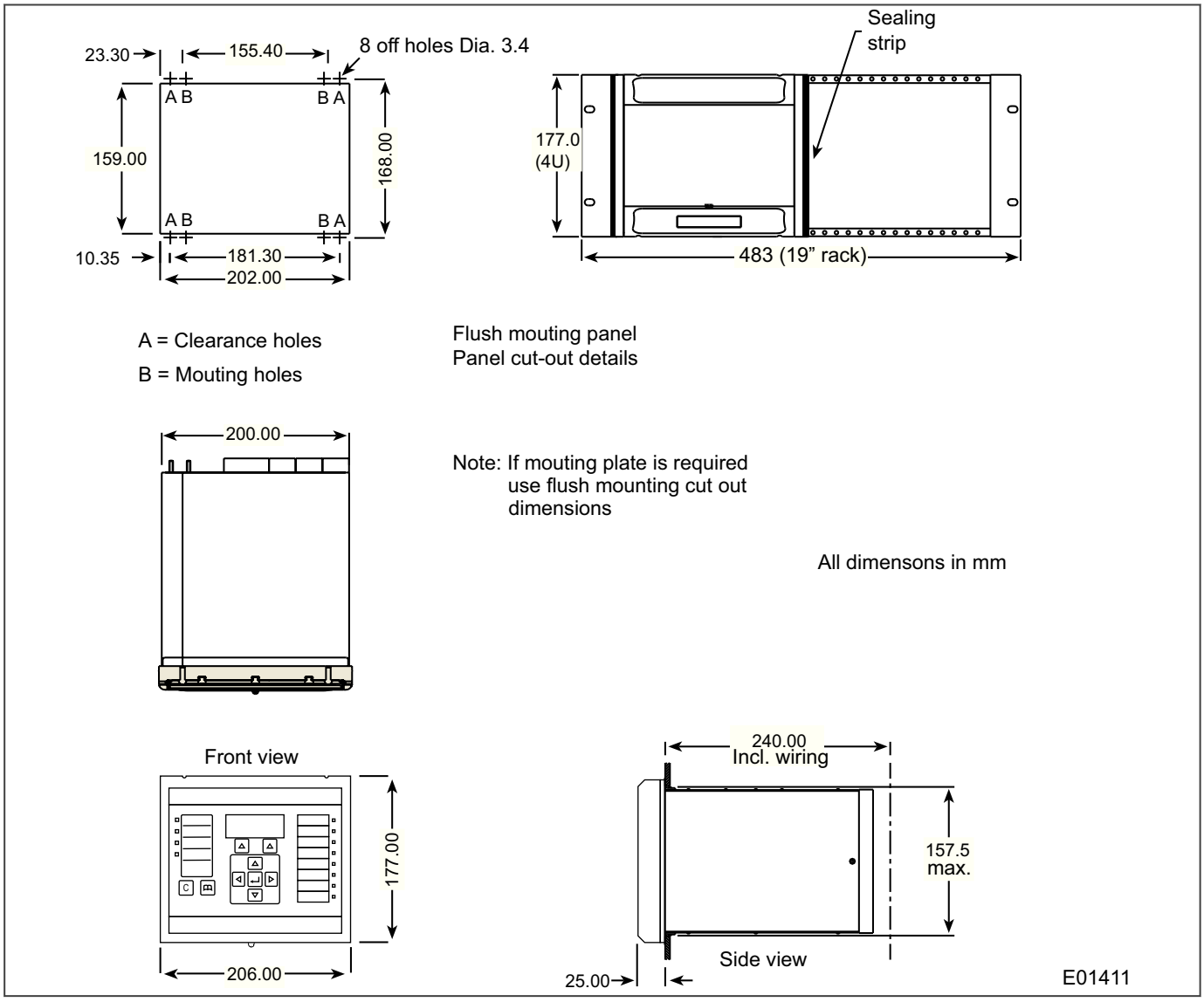


Figure 213: 40TE case dimensions

20.5.2 CASE DIMENSIONS 60TE

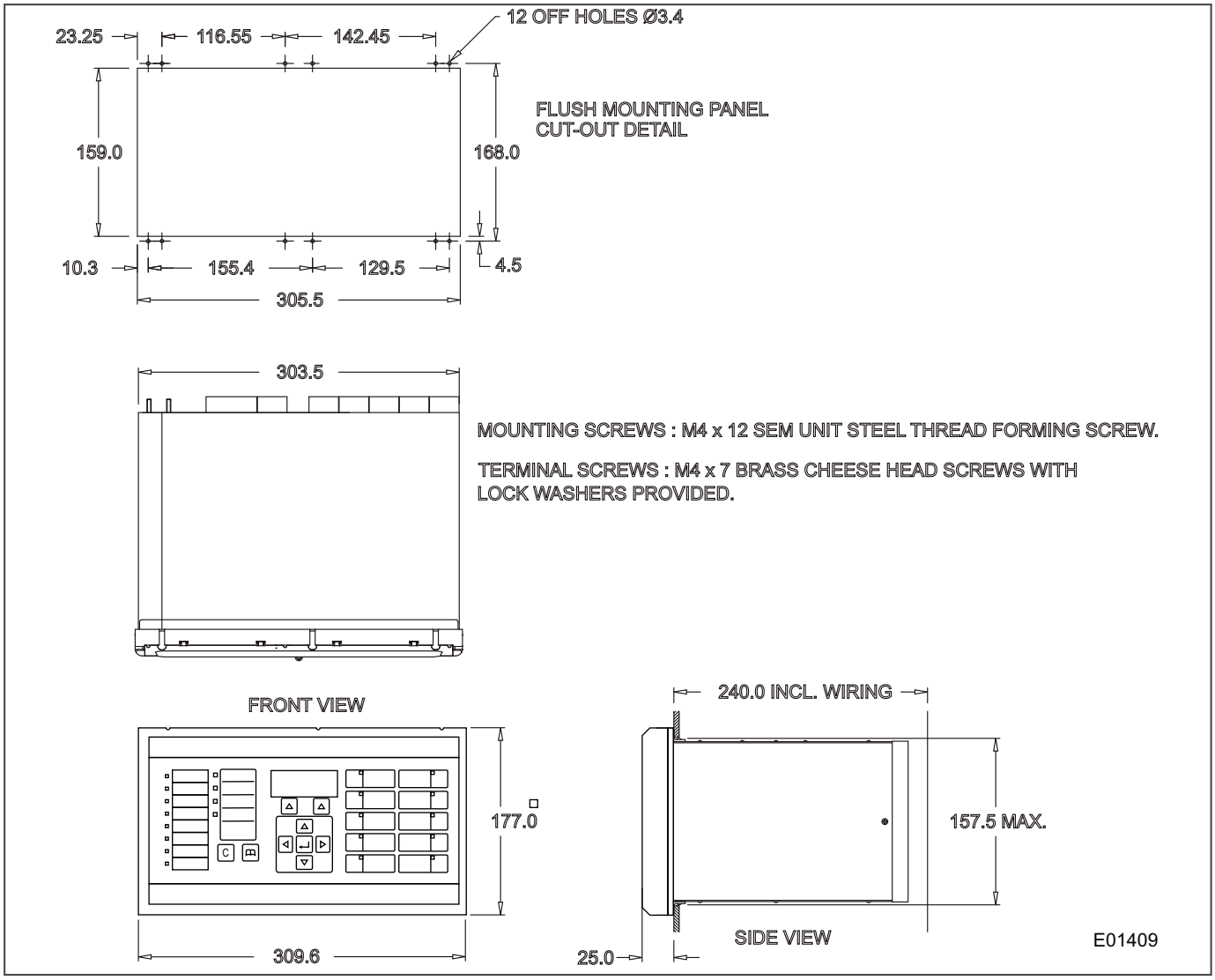


Figure 214: 60TE case dimensions

20.5.3 CASE DIMENSIONS 80TE

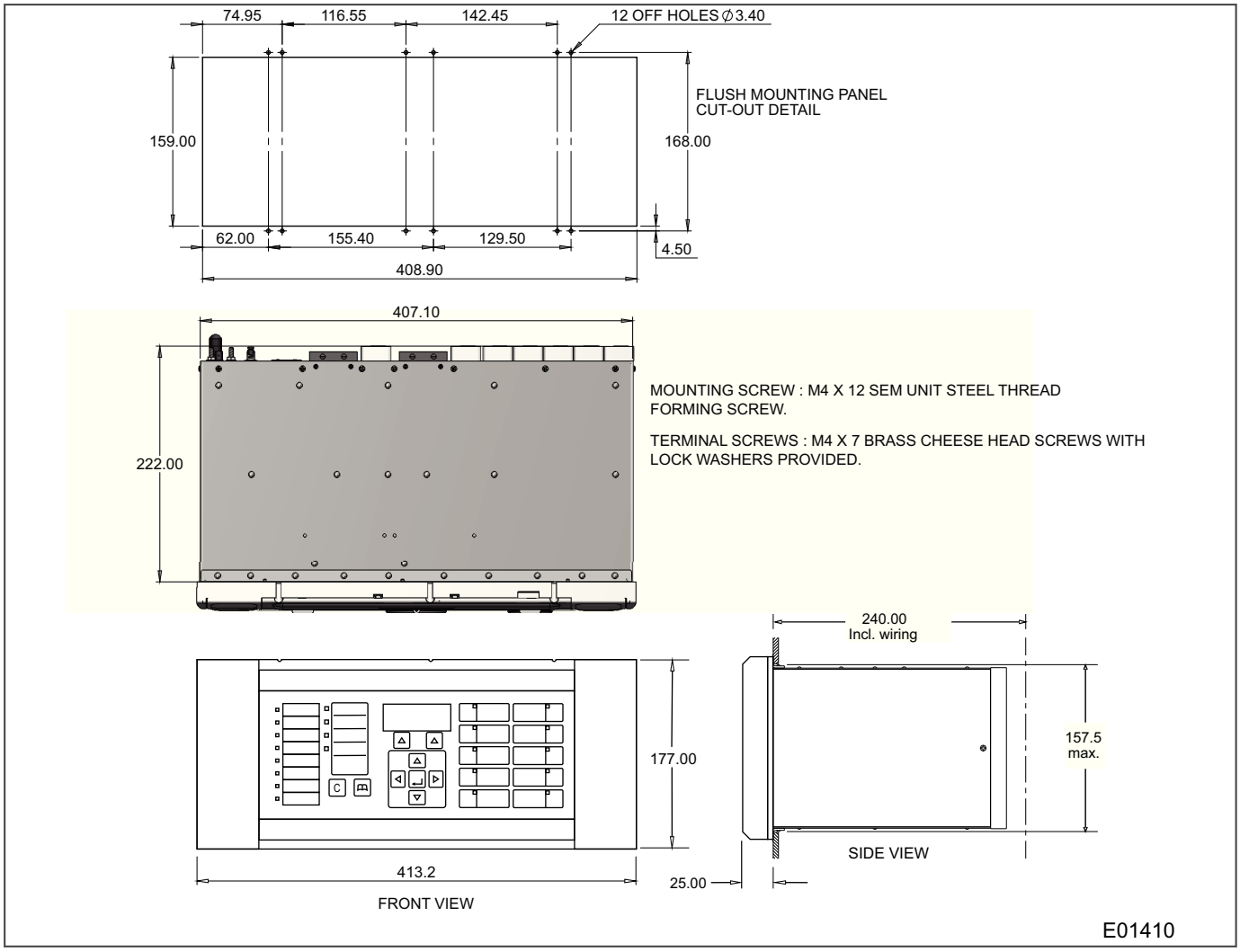


Figure 215: 80TE case dimensions

CHAPTER 21

COMMISSIONING INSTRUCTIONS

21.1 CHAPTER OVERVIEW

This chapter contains the following sections:

Chapter Overview 452
General Guidelines 453
Commissioning Test Menu 454
Commissioning Equipment 457
Product Checks 459
Electrical Intermicom Communication Loopback 468
Intermicom 64 Communication 470
Setting Checks 472
IEC 61850 Edition 2 Testing 474
Current Differential Protection 479
Protection Timing Checks 483
System Check and Check Synchronism 485
Check Trip and Autoreclose Cycle 486
End-to-End Communication Tests 487
Onload Checks 489
Final Checks 491

21.2 GENERAL GUIDELINES

GE Vernova IEDs are self-checking devices and will raise an alarm in the unlikely event of a failure. This is why the commissioning tests are less extensive than those for non-numeric electronic devices or electro-mechanical relays.

To commission the devices, you (the commissioning engineer) do not need to test every function. You need only verify that the hardware is functioning correctly and that the application-specific software settings have been applied. You can check the settings by extracting them using the settings application software, or by means of the front panel interface (HMI panel).

The menu language is user-selectable, so you can change it for commissioning purposes if required.

Note:
Remember to restore the language setting to the customer's preferred language on completion.



Caution:
Before carrying out any work on the equipment you should be familiar with the contents of the Safety Section or Safety Guide SFTY/4LM as well as the ratings on the equipment's rating label.



Warning:
With the exception of the CT shorting contacts check, do not disassemble the device during commissioning.

21.3 COMMISSIONING TEST MENU

The IED provides several test facilities under the *COMMISSION TESTS* menu heading. There are menu cells that allow you to monitor the status of the opto-inputs, output relay contacts, internal Digital Data Bus (DDB) signals and user-programmable LEDs. This section describes these commissioning test facilities.

21.3.1 OPTO I/P STATUS CELL (OPTO-INPUT STATUS)

This cell can be used to monitor the status of the opto-inputs while they are sequentially energised with a suitable DC voltage. The cell is a binary string that displays the status of the opto-inputs where '1' means energised and '0' means de-energised. If you move the cursor along the binary numbers, the corresponding label text is displayed for each logic input.

21.3.2 RELAY O/P STATUS CELL (RELAY OUTPUT STATUS)

This cell can be used to monitor the status of the relay outputs. The cell is a binary string that displays the status of the relay outputs where '1' means energised and '0' means de-energised. If you move the cursor along the binary numbers, the corresponding label text is displayed for each relay output.

The cell indicates the status of the output relays when the IED is in service. You can check for device damage by comparing the status of the output contacts with their associated bits.

Note:
*When the **Test Mode** cell is set to `Contacts Blocked`, the relay output status indicates which contacts would operate if the IED was in-service. It does not show the actual status of the output relays, as they are blocked.*

21.3.3 TEST PORT STATUS CELL

This cell displays the status of the DDB signals that have been allocated in the ***Monitor Bit*** cells. If you move the cursor along the binary numbers, the corresponding DDB signal text string is displayed for each monitor bit.

By using this cell with suitable monitor bit settings, the state of the DDB signals can be displayed as various operating conditions or sequences are applied to the IED. This allows you to test the Programmable Scheme Logic (PSL).

21.3.4 MONITOR BIT 1 TO 8 CELLS

The eight Monitor Bit cells allows you to select eight DDB signals that can be observed in the Test Port Status cell or downloaded via the front port.

Each Monitor Bit cell can be assigned to a particular DDB signal. You set it by entering the required DDB signal number from the list of available DDB signals.

The pins of the monitor/download port used for monitor bits are as follows:

Monitor Bit	1	2	3	4	5	6	7	8
Monitor/Download Port Pin	11	12	15	13	20	21	23	24

The signal ground is available on pins 18, 19, 22 and 25.



Caution:
The monitor/download port is not electrically isolated against induced voltages on the communications channel. It should therefore only be used for local communications.

21.3.5 TEST MODE CELL

This cell allows you to perform secondary injection testing. It also lets you test the output contacts directly by applying menu-controlled test signals.

To go into test mode, select the `Test Mode` option in the ***Test Mode*** cell. This takes the IED out of service causing an alarm condition to be recorded and the ***Out of Service*** LED to illuminate. This also freezes any information stored in the *CB CONDITION* column. In IEC 60870-5-103 versions, it changes the Cause of Transmission (COT) to Test Mode.

In Test Mode, the output contacts are still active. To disable the output contacts you must select the `Contacts Blocked` option.

Once testing is complete, return the device back into service by setting the ***Test Mode*** Cell back to `Disabled`.



Caution:
When the cell is in Test Mode, the Scheme Logic still drives the output relays, which could result in tripping of circuit breakers. To avoid this, set the *Test Mode* cell to `Contacts Blocked`.

Note:
`Test mode` *and* `Contacts Blocked` *mode can also be selected by energising an opto-input mapped to the Test Mode signal, and the Contact Block signal respectively.*

21.3.6 TEST PATTERN CELL

The ***Test Pattern*** cell is used to select the output relay contacts to be tested when the ***Contact Test*** cell is set to `Apply Test`. The cell has a binary string with one bit for each user-configurable output contact, which can be set to '1' to operate the output and '0' to not operate it.

21.3.7 CONTACT TEST CELL

When the `Apply Test` command in this cell is issued, the contacts set for operation change state. Once the test has been applied, the command text on the LCD will change to ***No Operation*** and the contacts will remain in the Test state until reset by issuing the `Remove Test` command. The command text on the LCD will show ***No Operation*** after the `Remove Test` command has been issued.

Note:
*When the **Test Mode** cell is set to* `Contacts Blocked` *the **Relay O/P Status** cell does not show the current status of the output relays and therefore cannot be used to confirm operation of the output relays. Therefore it will be necessary to monitor the state of each contact in turn.*

21.3.8 TEST LEDS CELL

When the `Apply Test` command in this cell is issued, the user-programmable LEDs illuminate for approximately 2 seconds before switching off, and the command text on the LCD reverts to ***No Operation***.

21.3.9 TEST AUTORECLOSE CELL

Where the IED provides an auto-reclose function, this cell will be available for testing the sequence of circuit breaker trip and auto-reclose cycles.

The `Trip 3 Pole` option in the ***Test Autoreclose*** cell causes the device to perform the first three phase trip/ reclose cycle so that associated output contacts can be checked for operation at the correct times during the cycle.

Once the trip output has operated the command text will revert to *No Operation* whilst the rest of the auto-reclose cycle is performed. To test subsequent three-phase autoreclose cycles, you repeat the *Trip 3 Pole* command. You can also test the single phases with *Trip Pole A*, *Trip Pole B* and *Trip Pole C*.

Note:
The default settings for the programmable scheme logic has the AR Trip Test signals mapped to the Trip Input signals. If the programmable scheme logic has been changed, it is essential that these signals retain this mapping for the Test Autoreclose facility to work.

21.3.10 LOOPBACK MODE

Loopback Mode can be used to test InterMiCOM^{64} signalling.

Note:
If the cell is set to Internal, only the IED software is checked. If the cell is set to External, both the software and hardware are checked.

When the device is switched into Loopback Mode, it automatically uses generic addresses 0-0. It responds as if it is connected to a remote device. The sent and received IM^{64} signals continue to be routed to and from the signals defined in the programmable logic.

Note:
Loopback mode can also be selected by energising an opto-input mapped to the Loopback signal.

21.3.11 IM64 TEST PATTERN

This cell is used with the ***IM64 Test Mode*** cell to set a 16-bit pattern (8 bits per channel), which is transmitted whenever the ***IM64 Test Mode*** cell is set to *Enabled*. The ***IM64 TestPattern*** cell has a binary string with one bit for each user-defined Inter-MiCOM command. These can be set to '1' to operate the IM64 output under test conditions and '0' for no operation.

21.3.12 IM64 TEST MODE

When the *Enable* command in this cell is issued, the InterMiCOM^{64} commands change to reflect the state of the values set in the ***IM64 TestPattern*** cell. If the cell is set to Disabled, the InterMiCOM^{64} commands reflect the state of the signals generated by the protection and control functions.

21.3.13 RED AND GREEN LED STATUS CELLS

These cells contain binary strings that indicate which of the user-programmable red and green LEDs are illuminated when accessing from a remote location. A '1' indicates that a particular LED is illuminated.

Note:
*When the status in both **Red LED Status** and **Green LED Status** cells is '1', this indicates the LEDs illumination is yellow.*

21.4 COMMISSIONING EQUIPMENT

Specialist test equipment is required to commission this product. We recognise three classes of equipment for commissioning :

- Recommended
- Essential
- Advisory

Recommended equipment constitutes equipment that is both necessary, and sufficient, to verify correct performance of the principal protection functions.

Essential equipment represents the minimum necessary to check that the product includes the basic expected protection functions and that they operate within limits.

Advisory equipment represents equipment that is needed to verify satisfactory operation of features that may be unused, or supplementary, or which may, for example, be integral to a distributed control/automation scheme. Operation of such features may, perhaps, be more appropriately verified as part of a customer defined commissioning requirement, or as part of a system-level commissioning regime.

21.4.1 RECOMMENDED COMMISSIONING EQUIPMENT

The minimum recommended equipment is a multifunctional three-phase AC current and voltage injection test set featuring :

- Controlled three-phase AC current and voltage sources,
- Transient (dynamic) switching between pre-fault and post-fault conditions (to generate delta conditions),
- Dynamic impedance state sequencer (capable of sequencing through 4 impedance states),
- Integrated or separate variable DC supply (0 - 250 V)
- Integrated or separate AC and DC measurement capabilities (0-440V AC, 0-250V DC)
- Integrated and/or separate timer,
- Integrated and/or separate test switches.

In addition, you will need :

- A portable computer, installed with appropriate software to liaise with the equipment under test (EUT). Typically this software will be proprietary to the product's manufacturer (for example MiCOM S1 Agile).
- Suitable electrical test leads.
- Electronic or brushless insulation tester with a DC output not exceeding 500 V
- Continuity tester
- Verified application-specific settings files

For products that use fibre-optic communications to implement unit protection schemes :

- Fibre optic test leads (minimum 2). 10m minimum length, multimode 50/125 µm or 62.5µm, OR single mode (according to the model variant) terminated with connectors as required by the product.
- Fibre-optic power meter
- P59x commissioning instructions

21.4.2 ESSENTIAL COMMISSIONING EQUIPMENT

As an absolute minimum, the following equipment is required:

- AC current source coupled with AC voltage source
- Variable DC supply (0 - 250V)

- Multimeter capable of measuring AC and DC current and voltage (0-440V AC, 0-250V DC)
- Timer
- Test switches
- Suitable electrical test leads
- Continuity tester

For products that use fibre-optic communications to implement unit protection schemes :

- Fibre optic test leads (minimum 2). 10m minimum length, multimode 50/125 µm or 62.5µm, OR single mode (according to the model variant) terminated with connectors as required by the product.
- Fibre-optic power meter

Note:
If the AC test source that you are using is not capable of dynamic fault simulation (cannot dynamically switch from load to fault conditions) you must use the product's static test mode feature

Note:
To do this, in COMMISSION TESTS, set ***Static Test Mode*** *to* `Enabled`.

21.4.3 ADVISORY TEST EQUIPMENT

Advisory test equipment may be required for extended commissioning procedures:

- Current clamp meter
- Multi-finger test plug:
  - P992 for test block type P991
  - MMLB for test block type MMLG blocks
- Electronic or brushless insulation tester with a DC output not exceeding 500 V
- KITZ K-Bus - EIA(RS)232 protocol converter for testing EIA(RS)485 K-Bus port
- EIA(RS)485 to EIA(RS)232 converter for testing EIA(RS)485 Courier/IEC60870-5-103/DNP3 port
- A portable printer (for printing a setting record from the portable PC) and or writeable, detachable memory device
- Phase angle meter
- Phase rotation meter
- Fibre-optic power meter.
- Fibre optic test leads (minimum 2). 10m minimum length, multimode 50/125 µm or 62.5µm terminated with BFOC (ST) 2.5 connectors for testing the fibre-optic RP1 port.

21.5 PRODUCT CHECKS

These product checks are designed to ensure that the device has not been physically damaged prior to commissioning, is functioning correctly and that all input quantity measurements are within the stated tolerances.

If the application-specific settings have been applied to the IED prior to commissioning, you should make a copy of the settings. This will allow you to restore them at a later date if necessary. This can be done by:

- Obtaining a setting file from the customer.
- Extracting the settings from the IED itself, using a portable PC with appropriate setting software.

If the customer has changed the password that prevents unauthorised changes to some of the settings, either the revised password should be provided, or the original password restored before testing.

Note:
If the password has been lost, a recovery password can be obtained from GE Vernova.

21.5.1 PRODUCT CHECKS WITH THE IED DE-ENERGISED



Warning:
The following group of tests should be carried out without the auxiliary supply being applied to the IED and, if applicable, with the trip circuit isolated.

The current and voltage transformer connections must be isolated from the IED for these checks. If a P991 test block is provided, the required isolation can be achieved by inserting test plug type P992. This open circuits all wiring routed through the test block.

Before inserting the test plug, you should check the scheme diagram to ensure that this will not cause damage or a safety hazard (the test block may, for example, be associated with protection current transformer circuits). The sockets in the test plug, which correspond to the current transformer secondary windings, must be linked before the test plug is inserted into the test block.



Warning:
Never open-circuit the secondary circuit of a current transformer since the high voltage produced may be lethal and could damage insulation.

If a test block is not provided, the voltage transformer supply to the IED should be isolated by means of the panel links or connecting blocks. The line current transformers should be short-circuited and disconnected from the IED terminals. Where means of isolating the auxiliary supply and trip circuit (for example isolation links, fuses and MCB) are provided, these should be used. If this is not possible, the wiring to these circuits must be disconnected and the exposed ends suitably terminated to prevent them from being a safety hazard.

21.5.1.1 VISUAL INSPECTION



Warning:
Check the rating information under the top access cover on the front of the IED.



Warning:
Check that the IED being tested is correct for the line or circuit.



Warning:
Record the circuit reference and system details.



Warning:
Check the CT secondary current rating and record the CT tap which is in use.

Carefully examine the IED to see that no physical damage has occurred since installation.

Ensure that the case earthing connections (bottom left-hand corner at the rear of the IED case) are used to connect the IED to a local earth bar using an adequate conductor.

21.5.1.2 CURRENT TRANSFORMER SHORTING CONTACTS

Check the current transformer shorting contacts to ensure that they close when the heavy-duty terminal block is disconnected from the current input board.

The heavy-duty terminal blocks are fastened to the rear panel using four crosshead screws. These are located two at the top and two at the bottom.

Note:
Use a magnetic bladed screwdriver to minimise the risk of the screws being left in the terminal block or lost.

Pull the terminal block away from the rear of the case and check with a continuity tester that all the shorting switches being used are closed.

21.5.1.3 INSULATION

Insulation resistance tests are only necessary during commissioning if explicitly requested.

Isolate all wiring from the earth and test the insulation with an electronic or brushless insulation tester at a DC voltage not exceeding 500 V. Terminals of the same circuits should be temporarily connected together.

The insulation resistance should be greater than 100 MΩ at 500 V.

On completion of the insulation resistance tests, ensure all external wiring is correctly reconnected to the IED.

21.5.1.4 EXTERNAL WIRING



Caution:
Check that the external wiring is correct according to the relevant IED and scheme diagrams. Ensure that phasing/phase rotation appears to be as expected.

21.5.1.5 WATCHDOG CONTACTS

Using a continuity tester, check that the Watchdog contacts are in the following states:

Terminals	Contact State with Product De-energised
11 - 12 on power supply board	Closed
13 - 14 on power supply board	Open

21.5.1.6 POWER SUPPLY

Depending on its nominal supply rating, the IED can be operated from either a DC only or an AC/DC auxiliary supply. The incoming voltage must be within the operating range specified below.

Without energising the IED measure the auxiliary supply to ensure it is within the operating range.

Nominal Supply Rating DC	Nominal Supply Rating AC RMS	DC Operating Range	AC Operating Range
24 - 54 V	N/A	19 to 65 V	N/A
48 - 125 V	30 - 100 V	37 to 150 V	24 - 110 V
110 - 250 V	100 - 240 V	87 to 300 V	80 to 265 V

Note:
The IED can withstand an AC ripple of up to 15% of the upper rated voltage on the DC auxiliary supply.



Warning:
Do not energise the IED or interface unit using the battery charger with the battery disconnected as this can irreparably damage the power supply circuitry.



Caution:
Energise the IED only if the auxiliary supply is within the specified operating ranges. If a test block is provided, it may be necessary to link across the front of the test plug to connect the auxiliary supply to the IED.

21.5.2 PXXX_CI_PRODUCTCHECKSENERGISED



Warning:
The current and voltage transformer connections must remain isolated from the IED for these checks. The trip circuit should also remain isolated to prevent accidental operation of the associated circuit breaker.

The following group of tests verifies that the IED hardware and software is functioning correctly and should be carried out with the supply applied to the IED.

21.5.2.1 WATCHDOG CONTACTS

Using a continuity tester, check that the Watchdog contacts are in the following states when energised and healthy.

Terminals	Contact State with Product Energised
11 - 12 on power supply board	Open
13 - 14 on power supply board	Closed

21.5.2.2 TEST LCD

The Liquid Crystal Display (LCD) is designed to operate in a wide range of substation ambient temperatures. For this purpose, the IEDs have an ***LCD Contrast*** setting. The contrast is factory pre-set, but it may be necessary to adjust the contrast to give the best in-service display.

To change the contrast, you can increment or decrement the ***LCD Contrast*** cell in the *CONFIGURATION* column.



Caution:
Before applying a contrast setting, make sure that it will not make the display so light or dark such that menu text becomes unreadable. It is possible to restore the visibility of a display by downloading a setting file, with the LCD Contrast set within the typical range of 7 - 11.

21.5.2.3 DATE AND TIME

The date and time is stored in memory, which is backed up by a supercapacitor.

The method for setting the date and time depends on whether an IRIG-B signal is being used or not. The IRIG-B signal will override the time, day and month settings, but not the initial year setting. For this reason, you must ensure you set the correct year, even if the device is using IRIG-B to maintain the internal clock.

You set the Date and Time by one of the following methods:

- Using the front panel to set the ***Date and Time*** cells respectively
- By sending a courier command to the ***Date/Time*** cell (Courier reference 0801)

Note:
If the auxiliary supply fails, the time and date will be maintained by the supercapacitor. Therefore, when the auxiliary supply is restored, you should not have to set the time and date again. To test this, remove the IRIG-B signal, and then remove the auxiliary supply. Leave the device de-energised for approximately 30 seconds. On re energisation, the time should be correct.

When using IRIG-B to maintain the clock, the IED must first be connected to the satellite clock equipment (usually an RT430), which should be energised and functioning.

1. Set the IRIG-B Sync cell in the *DATE AND TIME* column to `Enabled`.
2. Ensure the IED is receiving the IRIG-B signal by checking that cell IRIG-B Status reads `Active`.
3. Once the IRIG-B signal is active, adjust the time offset of the universal co coordinated time (satellite clock time) on the satellite clock equipment so that local time is displayed.
4. Check that the time, date and month are correct in the Date/Time cell. The IRIG-B signal does not contain the current year so it will need to be set manually in this cell.
5. Reconnect the IRIG-B signal.

If the time and date is not being maintained by an IRIG-B signal, ensure that the IRIG-B Sync cell in the *DATE AND TIME* column is set to `Disabled`.

1. Set the date and time to the correct local time and date using Date/Time cell or using the serial protocol.

21.5.2.4 TEST LEDS

On power-up, all LEDs should first flash yellow. Following this, the green "Healthy" LED should illuminate indicating that the device is healthy.

The IED's non-volatile memory stores the states of the alarm, the trip, and the user-programmable LED indicators (if configured to latch). These indicators may also illuminate when the auxiliary supply is applied.

If any of these LEDs are ON then they should be reset before proceeding with further testing. If the LEDs successfully reset (the LED goes off), no testing is needed for that LED because it is obviously operational.

Note:
In most cases, alarms related to the communications channels will not reset at this stage.

21.5.2.5 TEST ALARM AND OUT-OF-SERVICE LEDS

The alarm and out of service LEDs can be tested using the *COMMISSION TESTS* menu column.

1. Set the ***Test Mode*** cell to `Contacts Blocked`.
2. Check that the out of service LED illuminates continuously and the alarm LED flashes.

It is not necessary to return the ***Test Mode*** cell to `Disabled` at this stage because the test mode will be required for later tests.

21.5.2.6 TEST TRIP LED

The trip LED can be tested by initiating a manual circuit breaker trip. However, the trip LED will operate during the setting checks performed later. Therefore no further testing of the trip LED is required at this stage.

21.5.2.7 TEST USER-PROGRAMMABLE LEDS

To test these LEDs, set the Test LEDs cell to `Apply Test`. Check that all user-programmable LEDs illuminate.

21.5.2.8 TEST OPTO-INPUTS

This test checks that all the opto-inputs on the IED are functioning correctly.

The opto-inputs should be energised one at a time. For terminal numbers, please see the external connection diagrams in the "Wiring Diagrams" chapter. Ensuring correct polarity, connect the supply voltage to the appropriate terminals for the input being tested.

The status of each opto-input can be viewed using either the ***Opto I/P Status*** cell in the *SYSTEM DATA* column, or the ***Opto I/P Status*** cell in the *COMMISSION TESTS* column.

A '1' indicates an energised input and a '0' indicates a de-energised input. When each opto-input is energised, one of the characters on the bottom line of the display changes to indicate the new state of the input.

21.5.2.9 TEST OUTPUT RELAYS

This test checks that all the output relays are functioning correctly.

1. Ensure that the IED is still in test mode by viewing the ***Test Mode*** cell in the *COMMISSION TESTS* column. Ensure that it is set to `Contacts Blocked`.
2. The output relays should be energised one at a time. To select output relay 1 for testing, set the Test Pattern cell as appropriate.
3. Connect a continuity tester across the terminals corresponding to output relay 1 as shown in the external connection diagram.
4. To operate the output relay set the Contact Test cell to `Apply Test`.
5. Check the operation with the continuity tester.
6. Measure the resistance of the contacts in the closed state.
7. Reset the output relay by setting the Contact Test cell to `Remove Test`.
8. Repeat the test for the remaining output relays.
9. Return the IED to service by setting the Test Mode cell in the *COMMISSION TESTS* menu to `Disabled`.

21.5.2.10 TEST SERIAL COMMUNICATION PORT RP1

You need only perform this test if the IED is to be accessed from a remote location with a permanent serial connection to the communications port. The scope of this test does not extend to verifying operation with connected equipment beyond any supplied protocol converter. It verifies operation of the rear communication port (and if applicable the protocol converter) and varies according to the protocol fitted.

21.5.2.10.1 CHECK PHYSICAL CONNECTIVITY

The rear communication port RP1 is presented on terminals 16, 17 and 18 of the power supply terminal block. Screened twisted pair cable is used to make a connection to the port. The cable screen should be connected to pin 16 and pins 17 and 18 are for the communication signal:

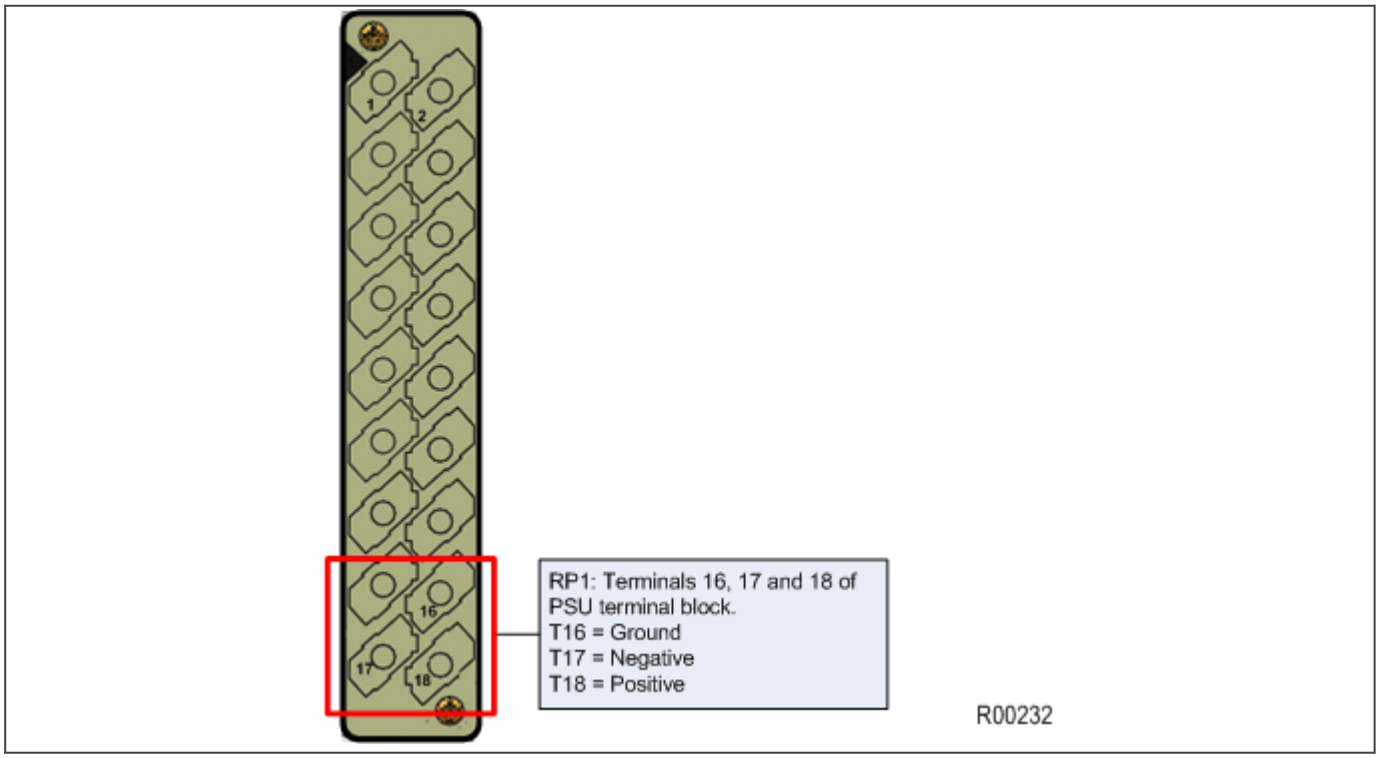


Figure 216: RP1 physical connection

For K-Bus applications, pins 17 and 18 are not polarity sensitive and it does not matter which way round the wires are connected. EIA(RS)485 is polarity sensitive, so you must ensure the wires are connected the correct way round (pin 18 is positive, pin 17 is negative).

If K-Bus is being used, a Kitz protocol converter (KITZ101, KITZ102 OR KITZ201) will have been installed to convert the K-Bus signals into RS232. Likewise, if RS485 is being used, an RS485-RS232 converter will have been installed. In the case where a protocol converter is being used, a laptop PC running appropriate software (such as MiCOM S1 Agile) can be connected to the incoming side of the protocol converter. An example for K-bus to RS232 conversion is shown below. RS485 to RS232 would follow the same principle, only using a RS485-RS232 converter. Most modern laptops have USB ports, so it is likely you will also require a RS232 to USB converter too.

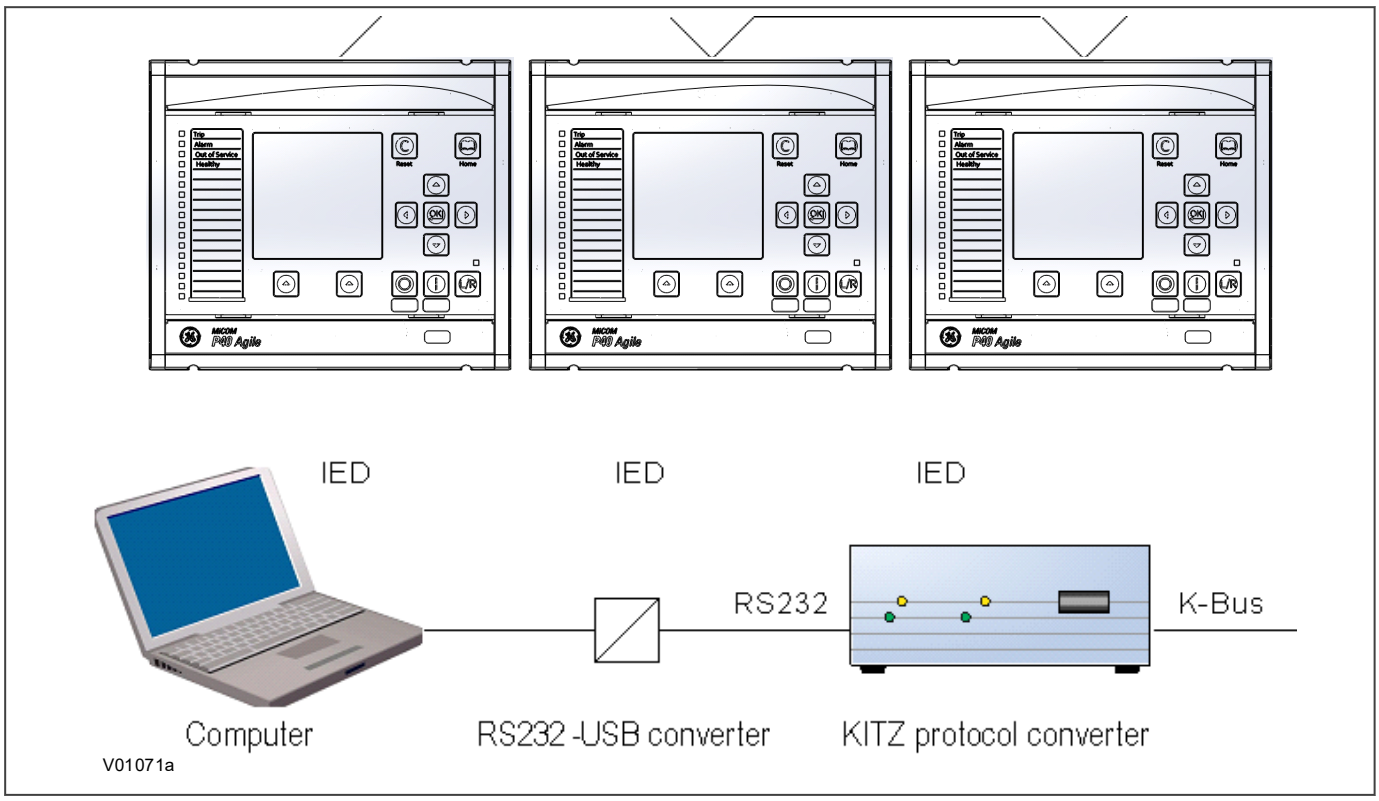


Figure 217: Remote communication using K-bus

Fibre connection

Some models have an optional fibre optic communications port fitted (on a separate communications board). The communications port to be used is selected by setting the Physical Link cell in the *COMMUNICATIONS* column, the values being `Copper` or `K-Bus` for the RS485/K-bus port and `Fibre Optic` for the fibre optic port.

21.5.2.10.2 CHECK LOGICAL CONNECTIVITY

The logical connectivity depends on the chosen data protocol, but the principles of testing remain the same for all protocol variants:

1. Ensure that the communications baud rate and parity settings in the application software are set the same as those on the protocol converter.
2. For Courier models, ensure that you have set the correct RP1 address
3. Check that communications can be established with this IED using the portable PC/Master Station.

21.5.2.11 TEST SERIAL COMMUNICATION PORT RP2

RP2 is an optional second serial port board providing additional serial connectivity. It provides two 9-pin D-type serial port connectors SK4 and SK5. Both ports are configured as DTE (Date Terminal Equipment) ports. That means they can be connected to communications equipment such as a modem with a straight-through cable.

SK4 can be configured as an EIA(RS232), EIA(RS485), or K-Bus connection for Courier protocol only, whilst SK5 is fixed to EIA(RS)232 for InterMiCOM signalling only.

It is not the intention of this test to verify the operation of the complete communication link between the IED and the remote location, just the IED's rear communication port and, if applicable, the protocol converter.

The only checks that need to be made are as follows:

1. Set the ***RP2 Port Config*** cell in the *COMMUNICATIONS* column to the required physical protocol; (K-Bus, EIA(RS)485, or EIA(RS)232.
2. Set the IED's Courier address to the correct value (it must be between 1 and 254).

21.5.2.12 TEST ETHERNET COMMUNICATION

For products that employ Ethernet communications, we recommend that testing be limited to a visual check that the correct ports are fitted and that there is no sign of physical damage.

If there is no board fitted or the board is faulty, a NIC link alarm will be raised (providing this option has been set in the ***NIC Link Report*** cell in the *COMMUNICATIONS* column).

21.5.3 SECONDARY INJECTION TESTS

Secondary injection testing is carried out to verify the integrity of the VT and CT readings. All devices leave the factory set for operation at a system frequency of 50 Hz. If operation at 60 Hz is required, you must set this in the Frequency cell in the *SYSTEM DATA* column.

The PMU must be installed and connected to a 1pps fibre optic synchronising signal and a demodulated IRIG-B signal, provided by a device such as a REASON RT430.

Connect the current and voltage outputs of the test set to the appropriate terminals of the first voltage and current channel and apply nominal voltage and current with the current lagging the voltage by 90 degrees.

21.5.3.1 TEST CURRENT INPUTS

This test verifies that the current measurement inputs are configured correctly.

1. Using secondary injection test equipment such as an Omicron, apply and measure nominal rated current to each CT in turn.
2. Check its magnitude using a multi-meter or test set readout. Check this value against the value displayed on the HMI panel (usually in *MEASUREMENTS 1* column).
3. Record the displayed value. The measured current values will either be in primary or secondary Amperes. If the Local Values cell in the *MEASURE'T SETUP* column is set to `Primary`, the values displayed should be equal to the applied current multiplied by the corresponding current transformer ratio (set in the *CT AND VT RATIOS* column). If the Local Values cell is set to Secondary, the value displayed should be equal to the applied current.

> *Note:*
> *If a PC connected to the IED using the rear communications port is being used to display the measured current, the process will be similar. However, the setting of the Remote Values cell in the MEASURE'T SETUP column will determine whether the displayed values are in primary or secondary Amperes.*

The measurement accuracy of the IED is +/- 1%. However, an additional allowance must be made for the accuracy of the test equipment being used.

21.5.3.2 TEST VOLTAGE INPUTS

This test verifies that the voltage measurement inputs are configured correctly.

1. Using secondary injection test equipment, apply and measure the rated voltage to each voltage transformer input in turn.
2. Check its magnitude using a multimeter or test set readout. Check this value against the value displayed on the HMI panel (usually in *MEASUREMENTS 1* column).
3. Record the value displayed. The measured voltage values will either be in primary or secondary Volts. If the Local Values cell in the *MEASURE'T SETUP* column is set to `Primary`, the values displayed should be

equal to the applied voltage multiplied by the corresponding voltage transformer ratio (set in the *CT AND VT RATIOS* column). If the Local Values cell is set to Secondary, the value displayed should be equal to the applied voltage.

Note:
If a PC connected to the IED using the rear communications port is being used to display the measured current, the process will be similar. However, the setting of the Remote Values cell in the MEASURE'T SETUP column will determine whether the displayed values are in primary or secondary Amperes.

The measurement accuracy of the IED is +/- 1%. However, an additional allowance must be made for the accuracy of the test equipment being used.

21.6 ELECTRICAL INTERMICOM COMMUNICATION LOOPBACK

If the IED is used in a scheme with standard InterMiCOM communication (Electrical Teleprotection), you need to configure a loopback for testing purposes.

21.6.1 SETTING UP THE LOOPBACK

The communication path may include various connectors and signal converters before leaving the substation. We therefore advise making the loopback as close as possible to where the communication link leaves the substation. This way, as much of the wiring as possible and all associated communication signal converters are included in the test.

1. Set *CONFIGURATION* > ***InterMiCOM*** to `Enabled`.
2. Set *INTERMICOM COMMS* > ***Ch Statistics*** and ***Ch Diagnostics*** to `Visible`.
3. Check that *INTERMICOM COMMS* > ***IM H/W Status*** displays OK. This means the InterMiCOM hardware is fitted and initialised.

21.6.2 LOOPBACK TEST

INTERMICOM COMMS > ***Loopback Mode*** allows you to test the InterMiCOM channel. In normal service it must be disabled. *INTERMICOM COMMS* > ***Loopback Status*** shows the status of the InterMiCOM loopback mode.

Note:
If INTERMICOM COMMS > ***Loopback Mode*** *is set to* `Internal`*, only the internal software of the device is checked. This is useful for testing functionality if no communications connections are made. Use the 'External' setting during commissioning because it checks both the software and hardware. When the IED is switched into either Internal or External Loopback Mode it automatically inhibits InterMiCOM messages to the PSL by setting all eight InterMiCOM message command states to zero.*

Set *INTERMICOM COMMS* > ***Loopback Mode*** to `External` and form a communications loopback by connecting the transmit signal (pin 2) to the receive signal (pin 3).

Note:
The DCD signal must be held high (by connecting pin 1 to pin 4) if the connected equipment does not support DCD.

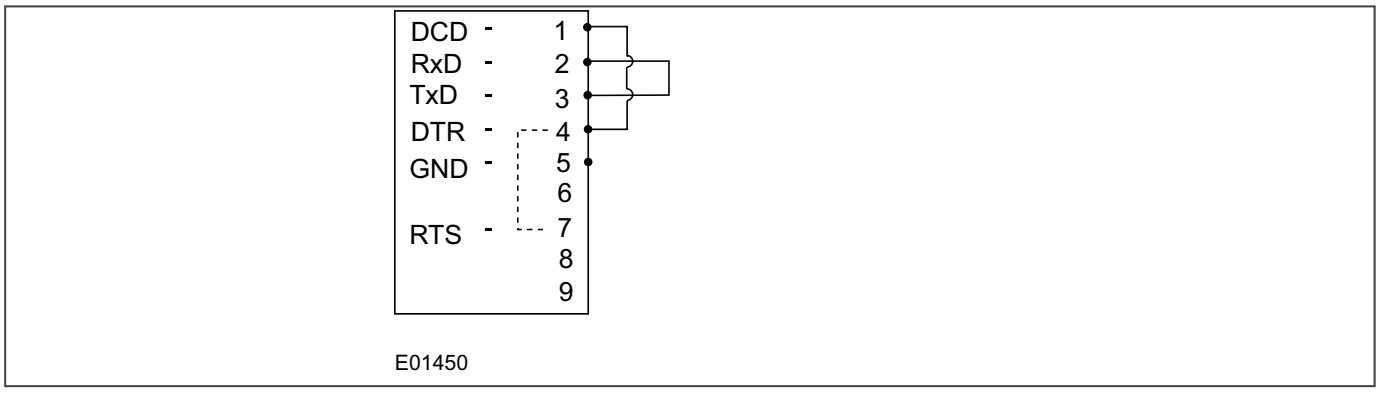


Figure 218: InterMicom loopback testing

The loopback mode is shown on the front panel by an Alarm LED and the message IM Loopback on the LCD.

Check that all connections are correct and the software is working correctly.

Check that *INTERMICOM COMMS* > ***Loopback Status*** shows OK.

21.6.2.1 INTERMICOM COMMAND BITS

To test the InterMiCOM command bits, go to the *INTERMICOM COMMS* column and do the following:

1. Enter any test pattern in the ***Test Pattern*** cell in the by scrolling through and changing selected bits between 1 and 0. The entered pattern is transmitted through the loopback.
2. Check that the ***IM Output Status*** cell matches the applied Test Pattern.
3. Check that all 8 bits in the ***IM Input Status*** cell are zero.

21.6.2.2 INTERMICOM CHANNEL DIAGNOSTICS

Check that the following cells in the *INTERMICOM COMMS* column all read **OK**.

- ***Data CD Status***
- ***FrameSync Status***
- ***Message Status***
- ***Channel Status***

21.6.2.3 SIMULATING A CHANNEL FAILURE

1. Simulate a failure of the communications link by breaking a connection and checking that some of these cells show **Fail**.
2. Restore the communications loopback and ensure that the four diagnostic cells display **OK.**

Note:
*Some or all of these cells show **Fail** depending on the communications configuration and the way the link has failed.*

21.7 INTERMICOM 64 COMMUNICATION

If the IED is used in a scheme with InterMiCOM^{64} communication, you need to configure a loopback for testing purposes.

IM64 is fibre-based. Several different fibre-optic interfaces are available. In general, 1550 nm single-mode fibres, or 1300 nm single-mode or multimode fibres are used for direct connection. 850 nm multimode fibres are generally used with multiplexing telecommunications equipment.

Note:
It is important that fibres used for testing are correct for the specified interface(s).

Optical fibres should be terminated with BFOC2.5 (ST2.5) connectors. For multimode applications use 50/125 µm core fibre. Make sure fibre test leads used for measurements are long enough for mode stripping (a method of reducing loss within the core). We recommend a minimum length of 10 m (30ft) for this.

If Current Differential protection is used, set *CONFIGURATION* > ***Current Diff*** to `Enable`.

If Current Differential protection is not used, set *CONFIGURATION* > ***InterMiCOM64*** to `Enable`.



Warning:
NEVER look directly into the transmit port or the end of an optical fibre, as this could severely damage your eyes.

21.7.1 CHECKING THE INTERFACE

Before carrying out the loopback test, you need to check that the interface is transmitting a suitable signal. To check this ...

1. Set *COMMISSION TESTS*> ***Loopback Mode*** to `External`.
2. Using an appropriate fibre-optic cable, connect the Channel 1 transmitter (TX1) to an optical power meter. Check that the average power transmitted is within the range given in the following table.
3. Record the transmit power level.
4. Repeat for Channel 2 if applicable.
5. Measure the received power strength at remote ends.

Power	850 nm Multi-Mode	1300 nm Multi-Mode	1300/1550 nm Single-Mode
Minimum transmitter power (average value)	-19 dBm	-6 dBm	-6 dBm
Receiver sensitivity (average power)	-32 dBm	-49 dBm	-49 dBm

Note:
*If CONFIGURATION > **InterMiCOM64** is set to `Enable`, the signals normally sent and received by and from the communications interface are routed to and from the signals defined in the Programmable Scheme Logic. If, however, COMMISSION TESTS > **IM64 Test Mode** is set to `Enabled`, an IM64 test pattern is transmitted instead.*

21.7.2 SETTING UP THE LOOPBACK

Set up a communications loopback for each of the two channels.

Where direct fibre connections are used (or where multiplexer channels conforming to the IEEE C37.94 standard are used), connect an appropriate fibre-optic cable from the channel transmitter to the channel receiver port on the rear of the device.

If the communications use P59x interface devices, connect the appropriate optical fibre(s) between the channel transmitter(s) on the IED used to make connection to the P59x optical receiver(s). Then commission the relevant P59x devices.

21.7.3 LOOPBACK TEST

1. Set *COMMISSION TESTS* > ***IM64 Test Mode*** to `Enabled`, and use *COMMISSION TESTS* > ***Test Pattern*** to set a bit pattern sent using the InterMiCOM^{64} loopback.
2. Check that *MEASUREMENTS 4* > ***IM64 Rx Status*** matches the test pattern set. The communication statistics show the number of valid and erroneous messages received.

Note:
The propagation delay measurement is not valid in this mode of operation. The IED responds as if it is connected to a remote IED. It indicates a loopback alarm which can only be cleared by setting COMMISSION TESTS > ***Loopback Mode*** *to* `Disabled`*.*

Note:
In loopback mode the signals sent and received through the protection communications interface continue to be routed to and from the signals defined in the programmable logic.

Note:
*A test pattern can also be sent to the remote end to test the whole InterMiCOM communication path. To do this, set COMMISSION TESTS >****IM64 Test Mode*** *to* `Enable` *and connect two ends. Take special care because the test pattern is executed using PSL at the remote end.*

21.8 SETTING CHECKS

The setting checks ensure that all of the application-specific settings (both the IED's function and Programmable Scheme Logic settings) have been correctly applied.

> *Note:*
> *If applicable, the trip circuit should remain isolated during these checks to prevent accidental operation of the associated circuit breaker.*

21.8.1 APPLY APPLICATION-SPECIFIC SETTINGS

There are two different methods of applying the settings to the IED

- Transferring settings to the IED from a pre-prepared setting file using MiCOM S1 Agile
- Enter the settings manually using the IED's front panel HMI

21.8.1.1 TRANSFERRING SETTINGS FROM A SETTINGS FILE

This is the preferred method for transferring function settings. It is much faster and there is a lower margin for error.

1. Connect a PC running the Settings Application Software to the IED's front port, or a rear Ethernet port. Alternatively connect to the rear Courier communications port, using a KITZ protocol converter if necessary.
2. Power on the IED
3. Enter the IP address of the device if it is Ethernet enabled
4. Right-click the appropriate device name in the System Explorer pane and select **Send**
5. In the **Send to** dialog select the setting files and click **Send**

> *Note:*
> *The device name may not already exist in the system shown in **System Explorer**. In this case, perform a **Quick Connect** to the IED, then manually add the settings file to the device name in the system. Refer to the Settings Application Software help for details of how to do this.*

21.8.1.2 ENTERING SETTINGS USING THE HMI

1. Starting at the default display, press the Down cursor key to show the first column heading.
2. Use the horizontal cursor keys to select the required column heading.
3. Use the vertical cursor keys to view the setting data in the column.
4. To return to the column header, either press the Up cursor key for a second or so, or press the **Cancel** key once. It is only possible to move across columns at the column heading level.
5. To return to the default display, press the Up cursor key or the Cancel key from any of the column headings. If you use the auto-repeat function of the Up cursor key, you cannot go straight to the default display from one of the column cells because the auto-repeat stops at the column heading.
6. To change the value of a setting, go to the relevant cell in the menu, then press the **Enter** key to change the cell value. A flashing cursor on the LCD shows that the value can be changed. You may be prompted for a password first.
7. To change the setting value, press the vertical cursor keys. If the setting to be changed is a binary value or a text string, select the required bit or character to be changed using the left and right cursor keys.

8. Press the **Enter** key to confirm the new setting value or the **Clear** key to discard it. The new setting is automatically discarded if it is not confirmed within 15 seconds.
9. For protection group settings and disturbance recorder settings, the changes must be confirmed before they are used. When all required changes have been entered, return to the column heading level and press the down cursor key. Before returning to the default display, the following prompt appears.

```
Update settings?
ENTER or CLEAR
```

10. Press the **Enter** key to accept the new settings or press the **Clear** key to discard the new settings.

Note:
If the menu time-out occurs before the setting changes have been confirmed, the setting values are also discarded.
Control and support settings are updated immediately after they are entered, without the Update settings prompt.
It is not possible to change the PSL using the IED's front panel HMI.



Caution:
Where the installation needs application-specific PSL, the relevant .psl files, must be transferred to the IED, for each and every setting group that will be used. If you do not do this, the factory default PSL will still be resident. This may have severe operational and safety consequences.

21.9 IEC 61850 EDITION 2 TESTING

21.9.1 USING IEC 61850 EDITION 2 TEST MODES

In a conventional substation, functionality typically resides in a single device. It is usually easy to physically isolate these functions, as the hardwired connects can simply be removed. Within a digital substation architecture however, functions may be distributed across many devices. This makes isolation of these functions difficult, because there are no physical wires that can be disconnected on a Ethernet network. Logical isolation of the various functions is therefore necessary.

With devices that support IEC 61850 Edition 2, it is possible to use a test mode to conduct online testing, which helps with the situation. The advantages of this are as follows:

- The device can be placed into a test mode, which can disable the relay outputs when testing the device with test input signals.
- Specific protection and control functions can be logically isolated.
- GOOSE messages can be tagged so that receiving devices can recognise they are test signals.
- An IED receiving simulated GOOSE or Sampled Value messages from test devices can differentiate these from normal process messages, and be configured to respond appropriately.

21.9.1.1 IED TEST MODE BEHAVIOUR

Test modes define how the device responds to test messages, and whether the relay outputs are activated or not. You can select the mode of operation by:

- Using the front panel HMI, with the setting ***IED Test Mode*** under the *COMMISSION TESTS* column.
- Using an IEC 61850 control service to ***System/LLN0.Mod***
- Using an opto-input via PSL with the signal ***Block Contacts***

The following table summarises the IED behaviour under the different modes:

IED Test Mode Setting	Result
Disabled	Normal IED behaviour
Test	Protection remains enabled Output from the device is still active IEC 61850 message output has the 'quality' parameter set to 'test' The device only responds to IEC61850 MMS messages from the client with the 'test' flag set
Contacts Blocked	Protection remains enabled Output from the device is disabled IEC 61850 message output has quality set to ‘test’ The device only responds to IEC 61850 MMS messages from the client with the 'test' flag set

Setting the Test or Contacts Blocked mode puts the whole IED into test mode. The IEC 61850 data object ***Beh*** in all Logical Nodes (except LPHD and any protection Logical Nodes that have Beh = 5 (off) due to the function being disabled) will be set to 3 (test) or 4 (test/blocked) as applicable.

21.9.1.2 SAMPLED VALUE TEST MODE BEHAVIOUR

The SV Test Mode defines how the device responds to test sampled value messages. You can select the mode of operation by using the front panel HMI, with the setting ***SV Test Mode*** under the *IEC 61850-9.2LE* column.

The following table summarises the behaviour for sampled values under the different modes:

SV Test Mode Setting	Result
Disabled	• Normal IED behaviour • All sampled value data frames received with an IEC 61850 Test quality bit set are treated as invalid • The IED will display the measurement values for sampled values with the Simulated flag set but the protection elements within the IED will be blocked
Enabled	• All sampled value data frames received are treated as good, no matter if they have an IEC 61850-9-2 Simulated flag set or not

21.9.2 SIMULATED INPUT BEHAVIOUR

Simulated GOOSE messages and sampled value streams can be used during testing.

The ***Subscriber Sim*** setting in the *COMMISSION TESTS* column controls whether a device listens to simulated signals or to real ones. An IEC 61850 control service to System/LPHD.Sim can also be used to change this value.

The device may be presented with both real signals and test signals. An internal state machine is used to control how the device switches between signals:

- The IED will continue subscribing to the 'real' GOOSE1 (in green) until it receives the first simulated GOOSE 1 (in red). This will initiate subscription changeover.
- After changeover to this new state, the IED will continue to subscribe to the simulated GOOSE 1 message (in red). Even if this simulated GOOSE 1 message disappears, the real GOOSE 1 message (in green) will still not be processed. This means all Virtual Inputs derived from the GOOSE 1 message will go to their default state.
- The only way to bring the IED out of this state is to set the ***Subscriber Sim*** setting back to False. The IED will then immediately stop processing the simulated messages and start processing real messages again.
- During above steps, IED1 will continuously process the real GOOSE 2 and GOOSE 3 messages as normal because it has not received any simulated messages for these that would initiate a changeover.

The process is represented in the following figure:

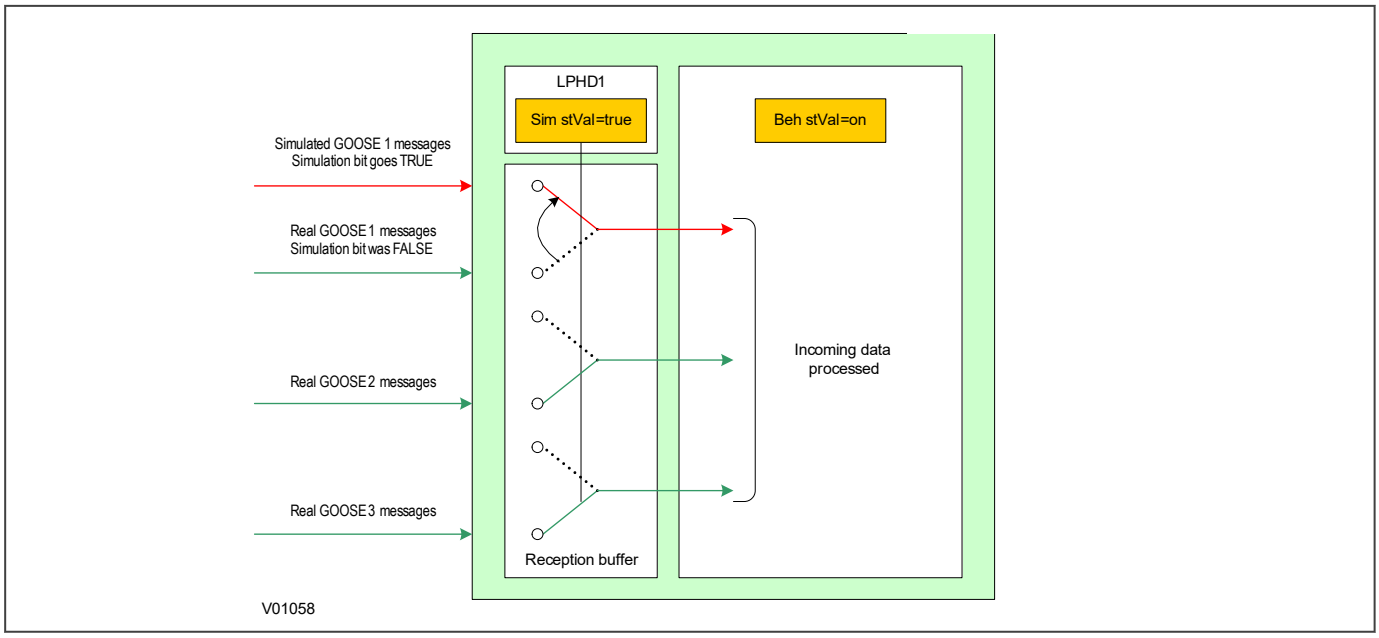


Figure 219: Simulated input behaviour

21.9.3 TESTING EXAMPLES

These examples show how you test the IED with and without simulated values. Depending on the IED Test Mode, it may respond by operating plant (for example by tripping the circuit breaker) or it may not operate plant.

21.9.3.1 TEST PROCEDURE FOR REAL VALUES

This procedure is for testing with real values without operating plant.

1. Set device into 'Contacts Blocked' Mode
   Select *COMMISSION TESTS* → ***IED Test Mode*** → `Contacts Blocked`
2. Confirm new behaviour has been enabled
   View *COMMISSION TESTS* → ***IED Mod/Beh***, and check that it shows `Test-blocked`
3. Set device into Simulation Listening Mode
   Select *COMMISSION TESTS* → ***Subscriber Sim*** = `Disabled`
4. If using sampled values set the sampled values test mode
   Select *IEC 61850-9.2LE* → ***SV Test Mode*** → `Disabled`
5. Inject real signals using a test device connected to the merging units. The device will continue to listen to 'real' GOOSE messages and ignore simulated messages received.
6. Verify function based on test signal outputs
   Binary outputs (e.g. CB trips) will not operate. All transmitted GOOSE and MMS data items will be tagged with the 'quality' parameter set to 'test', so that the receiver understands that they have been issued by a device under test and can respond accordingly. This is summarised in the following diagram

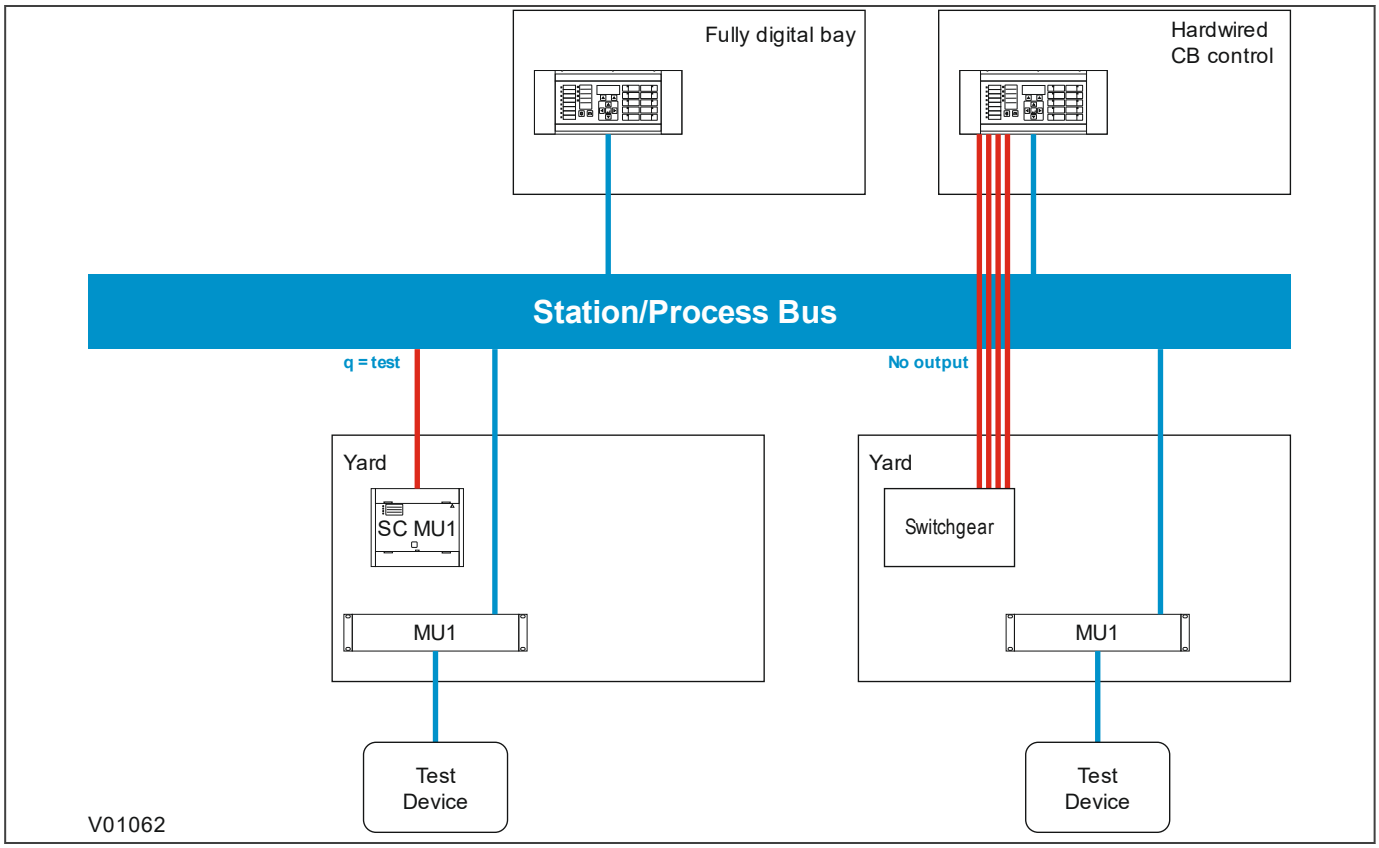


Figure 220: Test example 1

21.9.3.2 TEST PROCEDURE FOR SIMULATED VALUES - NO PLANT

This procedure is for testing with simulated values without operating plant.

1. Set device into 'Contacts Blocked' Mode
   Select *COMMISSION TESTS* → ***IED Test Mode*** → `Contacts Blocked`
2. Confirm new behaviour has been enabled
   View *COMMISSION TESTS* → ***IED Mod/Beh***, and check that it shows `test-blocked`
3. Set device into Simulation Listening Mode
   Select *COMMISSION TESTS* → ***Subscriber Sim*** = `Enabled`
4. If using sampled values set the sampled values test mode
   Select *IEC 61850-9.2LE* → ***SV Test Mode*** → `Enabled`
5. Inject simulated signals using a test device connected to the Ethernet network. The device will continue to listen to 'real' GOOSE messages until a simulated message is received. Once the simulated messages are received, the corresponding 'real' messages are ignored until the device is taken out of test mode. Each message is treated separately, but sampled values are considered as a single message.
6. Verify function based on test signal outputs
   Binary outputs (e.g. CB trips) will not operate. All transmitted GOOSE and MMS data items will be tagged with the 'quality' parameter set to 'test', so that the receiver understands that they have been issued by a device under test and can respond accordingly. This is summarised in the following diagram

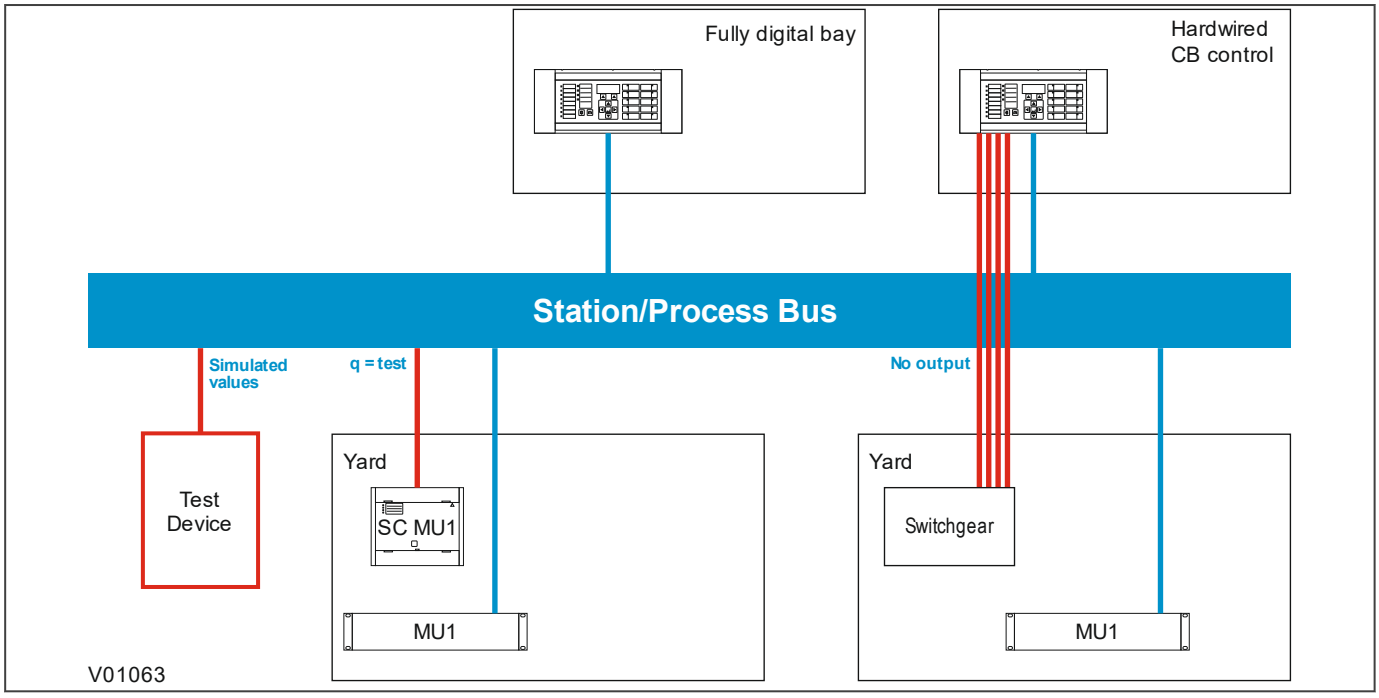


Figure 221: Test example 2

21.9.3.3 TEST PROCEDURE FOR SIMULATED VALUES - WITH PLANT

This procedure is for testing with simulated values with operating plant.

1. Set device into 'Contacts Blocked' Mode
   Select *COMMISSION TESTS* → ***IED Test Mode*** → `Test`
2. Confirm new behaviour has been enabled
   View *COMMISSION TESTS* → ***IED Mod/Beh***, and check that it shows `Test`
3. Set device into Simulation Listening Mode

Select *COMMISSION TESTS* → ***Subscriber Sim*** = `Enabled`

4. If using sampled values set the sampled values test mode

   Select *IEC 61850-9.2LE* → ***SV Test Mode*** → `Enabled`

5. Inject simulated signals using a test device connected to the Ethernet network.

   The device will continue to listen to 'real' GOOSE messages until a simulated message is received. Once the simulated messages are received, the corresponding 'real' messages are ignored until the device is taken out of IED test mode. Each message is treated separately, but sampled values are considered as a single message.

6. Verify function based on test signal outputs.

   Binary outputs (e.g. CB trips) will operate as normal. All transmitted GOOSE and MMS data items will be tagged with the 'quality' parameter set to 'test', so that the receiver understands that they have been issued by a device under test and can respond accordingly. This is summarised in the following diagram:

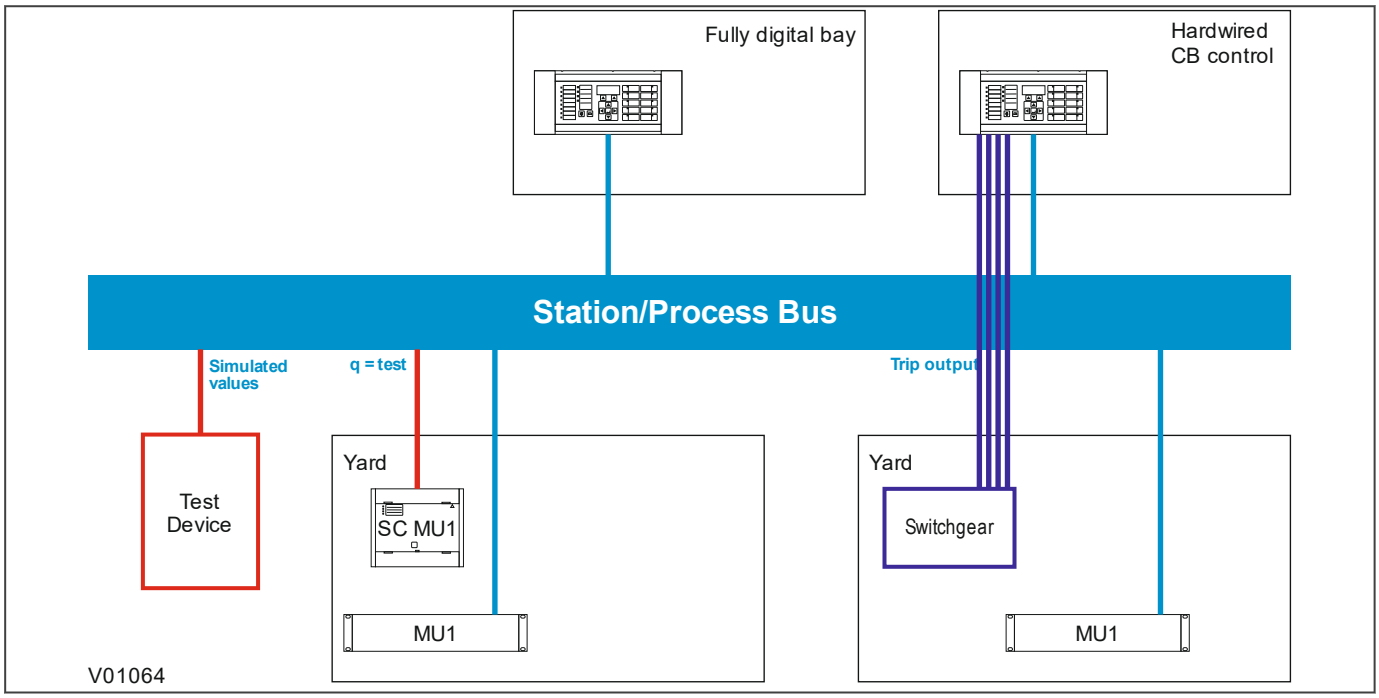


Figure 222: Test example 3

21.9.3.4 CONTACT TEST

The ***Apply Test*** command in this cell is used to change the state of the contacts set for operation.

If the device has been put into 'Contact Blocked' mode using an input signal (via the ***Block Contacts*** DDB signal) then the ***Apply Test*** command will not execute. This is to prevent a device that has been blocked by an external process having its contacts operated by a local operator using the HMI.

If the ***Block Contacts*** DDB is not set and the ***Apply Test*** command in this cell is issued, contacts change state and the command text on the LCD changes to `No Operation`. The contacts remain in the Test state until reset by issuing the ***Remove Test*** command. The command text on the LCD shows `No Operation` after the ***Remove Test*** command has been issued.

Note:
*When the **IED Test Mode** cell is set to Contacts Blocked, the **Relay O/P Status** cell does not show the current status of the output relays so cannot be used to confirm operation of the output relays. Therefore it is necessary to monitor the state of each contact in turn.*

21.10 CURRENT DIFFERENTIAL PROTECTION

21.10.1 CURRENT DIFFERENTIAL BIAS CHARACTERISTIC

The multi-ended line differential characteristic is defined by four settings:

- ***Phase Is1***: The basic differential current setting which determines the minimum pick-up level of the protection.
- ***Phase k1***: The lower percentage bias setting used when the bias current is below the Phase Is2 setting. This provides stability for small CT mismatches, while ensuring good sensitivity to resistive faults under heavy load conditions.
- ***Phase Is2***: A bias current threshold setting, above which the higher percentage bias setting Phase k2 is used.
- ***Phase k2***: The higher percentage bias setting used to improve protection stability under heavy through fault current conditions.

The differential protection characteristic is shown below:

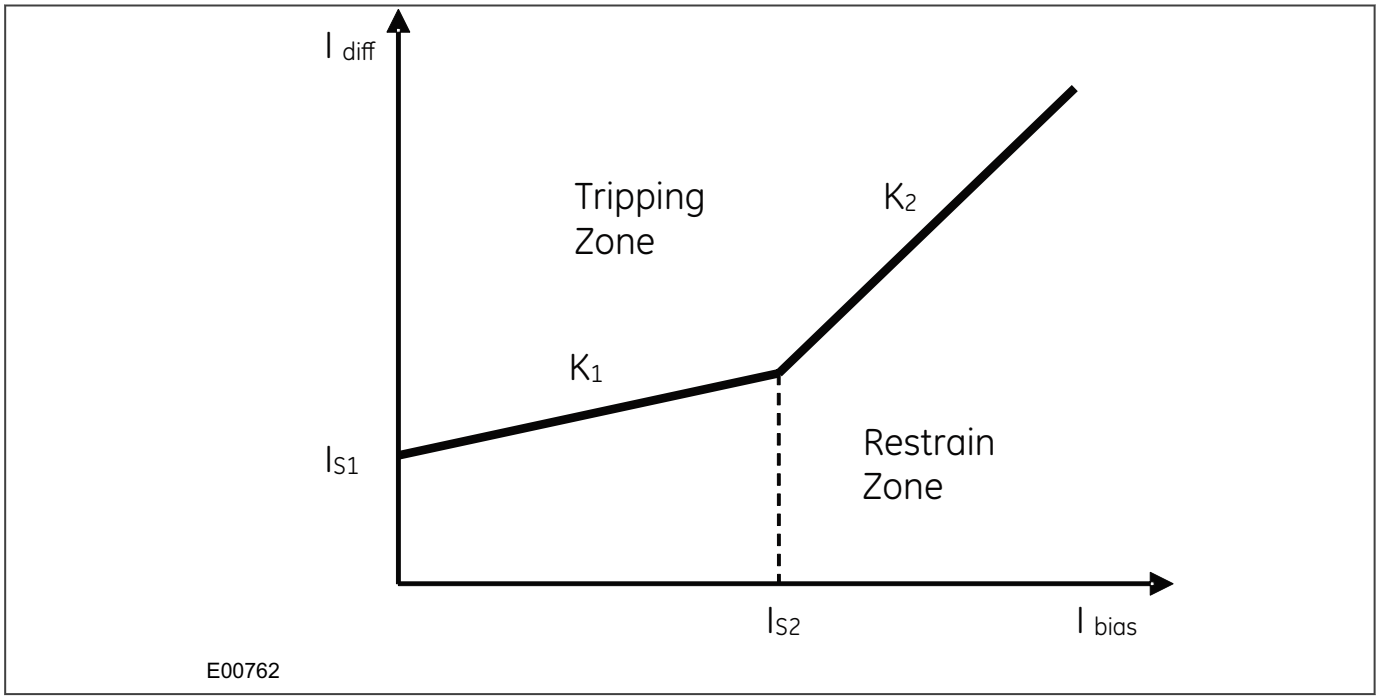


Figure 223: Current differential bias characteristics

21.10.2 CURRENT DIFFERENTIAL BIAS TESTING

1. In the *CONFIGURATION* column, disable all protection elements other than the one being tested.
2. Make a note of which elements need to be re-enabled after testing.
3. Set the device to loopback mode, isolating it from the remote end.
4. Connect the test circuit shown below. Alternatively, use an injection test set to supply Ia and Ib

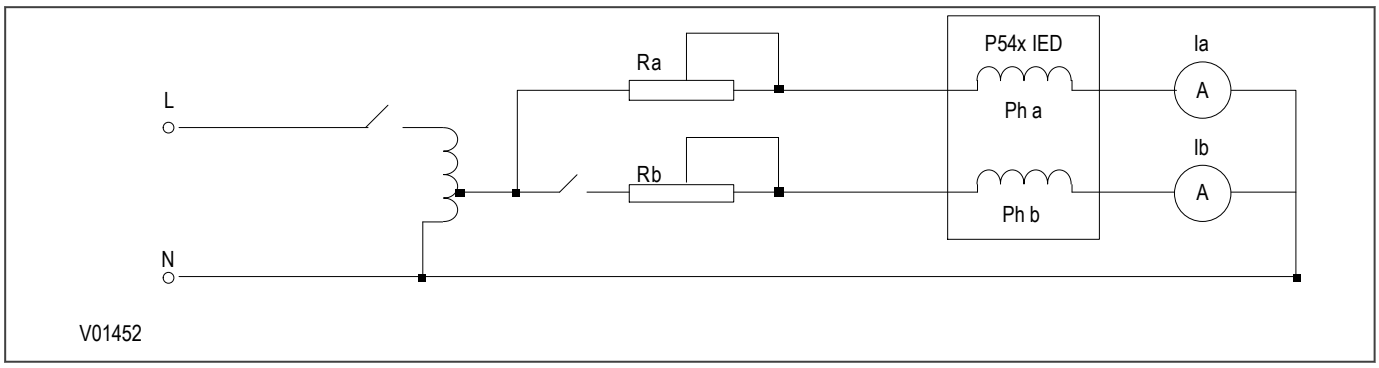


Figure 224: Test circuit connection diagram

21.10.2.1 LOWER SLOPE

If three LEDs have been assigned to provide phase segregated trip information (Trip A, Trip B and Trip C), these may be used to indicate correct operation per-phase. If LEDs are not used, use monitor options, as follows.

1. Go to *COMMISSION TESTS* > ***Monitor Bit***. Change cells 1, 2 and 3 to the values 523, 524 and 525 respectively. The ***Test Port Status*** cell then displays the status of Trip Output A (DDB 523), Trip Output B (DDB 524) and Trip Output C (DDB 525), with the rightmost bit representing Phase A Trip. From now on monitor the ***Test Port Status*** cell.
2. Make sure that the IED is in loopback mode by setting the Loopback Mode cell to External and applying a loop-back, either by direct fibre or using a P59x. Alternatively you can set the ***Test Loopback*** cell to `Internal`.
3. Adjust the variac and the resistor to give a bias current of 1pu in the A-phase (1A into terminals 3-2 for 1A applications, or 5A into terminals 1-2 for 5A applications).

   The device trips, contacts associated with the A-phase operate, and bit 1 (rightmost) of the ***Test Port Status*** cell is set to 1. Some LEDs, including the yellow alarm LED, switch OFF, but ignore these for the moment.
4. When the current in the A Phase is established, close the switch and slowly increase the current in the B phase from zero until Phase B trips (bit 2 of the ***Test Port Status*** cell is set to 1).

For the initial conditions where the magnitude of the bias current in phase A = 1 pu, record the phase B current magnitude and check that it corresponds to the following.

Connection Type	Magnitude of Current in Phase B
2-terminal & dual redundant	0.25 pu +/-10%
>2-terminal	0.216 pu +/-10%

Assumption: Is1 = 0.2 pu, k1 = 30%, Is2 = 2.0 pu

For other differential settings or current injected into A phase (Ia), the following formula can be used (enter slope in pu form, which is. percentage/100):

Connection Type	Magnitude of Differential Current in Phase B
2-terminal & dual redundant	0.5 x (Is1 + (Ia x k1)) pu +/- 10%
>2-terminal	0.333 x (Is1 + (1.5 x Ia x k1)) pu +/- 10

Assumption: Ia < Is2

Switch OFF the AC supply, read and clear all alarms.

21.10.2.2 UPPER SLOPE

1. Repeat the lower slope test but with the bias current set in the A-phase to 3 pu.
2. When the current in the A Phase is established, close the switch and slowly increase the current in the B phase from zero until phase B trips (bit 2 of the ***Test Port Status*** cell is set to 1).

For the initial conditions where the magnitude of the bias current in phase A = 3 pu, record the phase B current magnitude and check that it corresponds to the information below.

Connection Type	k2	Magnitude of Differential Current in Phase B
2-terminal & dual redundant	150%	1.15 pu +/- 10%
2-terminal & dual redundant	100%	0.9 pu +/- 10%
>2-terminal	150%	1.51 pu +/- 10%
>2-terminal	100%	1.1 pu +/- 10%

Assumption: Is1 = 0.2 pu, k1 = 30%, Is2 = 2.0 pu, k2 as above

For other differential settings or current injected into A phase (Ia), the formula below can be used (enter slopes in pu form, which is percentage/100):

Connection Type	Magnitude of Differential Current in Phase B
2-terminal & dual redundant	0.5 x [(Ia x k2) – {(k2 – k1) x Is2\- } + Is1] pu +/- 20%
>2-terminal	0.333 x [(1.5 x Ia x k2) – {(k2 – k1) x Is2\- } + Is1] pu +/- 20%

Assumption: Ia > IS2

Switch OFF the ac supply and reset the alarms.

Note:
For 5 A applications, keep the duration of current injections short to avoid overheating of the variac or injection test set.

21.10.3 CURRENT DIFFERENTIAL OPERATION AND CONTACT ASSIGNMENT

Phase A

1. Retaining the same test circuit as before, prepare for an instantaneous injection of 3 pu current in the A phase, with no current in the B phase (B phase switch open).
2. Set a timer to start when the fault injection is applied, and to stop when the trip occurs.
3. To verify the correct output contact mapping, use the trip contacts that would be expected to trip the circuit breaker(s), as shown below. For two breaker applications, stop the timer once both CB1 and CB2 trip contacts have closed. This can be achieved by connecting the contacts in series to stop the timer.

	Single Breaker	Two Circuit Breakers
Three Pole Tripping	Any Trip	Any Trip (CB1) and Any Trip (CB2)
Single Pole Tripping	Trip A	Trip A (CB1) and Trip A (CB2)

Phase B

1. Reconfigure the test equipment to inject fault current into the B phase.
2. Repeat the test, this time ensuring that the breaker trip contacts relative to B phase operation close correctly.
3. Record the B phase trip time.
4. Switch OFF the ac supply and reset the alarms

Phase C

1. Repeat the above procedure for the C phase.
2. Switch OFF the ac supply and reset the alarms.

The average of the recorded operating times for the three phases should be less than 40 ms for 50 Hz, and less than 35 ms for 60 Hz when set for instantaneous operation.

> *Note:*
> *For applications using magnetising inrush current restraint, use a test current higher than the Inrush High setting to obtain fast operating times. A setting of at least twice the Inrush High setting is recommended.*

The expected operating time is typically within +/- 5% (for IDMT) or +/-2% (for DT) of that for the curve equation plus the “instantaneous” delay quoted above.

When the tests are completed, restore the original settings of any elements which were disabled for testing purposes. Use the *CONFIGURATION* column.

21.11 PROTECTION TIMING CHECKS

There is no need to check every protection function. Only one protection function needs to be checked as the purpose is to verify the timing on the processor is functioning correctly.

21.11.1 DEPENDENCY CONDITIONS

Some protection elements can be set to have dependencies on the availability of the protection communication channel(s) and on the status of the voltage transformer supervision function (VTS).

If you are testing a distance model, the distance protection can be permanently enabled, or it can be set so that it is only enabled in the event of a failure of the protection communications channel(s).

The overcurrent and earth faults elements can be permanently enabled, or can be set so that they are only enabled:

- in the event of a failure of the protection communications channel(s)
- in the event of a VTS alarm
- according to a logical combination of both conditions.

If these elements are enabled with a dependency upon the above conditions, it is necessary to simulate the condition to test the correct operation of the protection function.

A communications failure can be simulated by setting the Test Loopback cell to Disabled and checking that the IED raises a Comms Fail alarm.

At the end of the test, clear the communications alarms and reset the statistics.

A VTS alarm can be raised by applying a 3-phase voltage to the VT inputs and then removing one phase voltage for a duration exceeding the VTS Time Delay setting.

At the end of the tests, clear the VTS alarm.

21.11.2 OVERCURRENT CHECK

If the overcurrent protection function is being used, test the overcurrent protection for stage 1.

1. Check for any possible dependency conditions and simulate as appropriate.
2. In the *CONFIGURATION* column, disable all protection elements other than the one being tested.
3. Make a note of which elements need to be re-enabled after testing.
4. Connect the test circuit.
5. Perform the test.
6. Check the operating time.

21.11.3 CONNECTING THE TEST CIRCUIT

1. Use the PSL to determine which output relay will operate when an overcurrent trip occurs.
2. Use the output relay assigned to ***Trip Output A***.
3. Use the PSL to map the protection stage under test directly to an output relay.

> *Note:*
> *If using the default PSL, use output relay 3 as this is already mapped to the DDB signal* ***Trip Command Out****.*

4. Connect the output relay so that its operation will trip the test set and stop the timer.
5. Connect the current output of the test set to the A-phase current transformer input.

   If the ***I>1 Directional*** cell in the *OVERCURRENT* column is set to `Directional Fwd`, the current should flow out of terminal 2. If set to `Directional Rev`, it should flow into terminal 2.

If the ***I>1 Directional*** cell in the *OVERCURRENT* column has been set to `Directional Fwd` or `Directional Rev`, the rated voltage should be applied to terminals 20 and 21.

6. Ensure that the timer starts when the current is applied.

Note:
If the timer does not stop when the current is applied and stage 1 has been set for directional operation, the connections may be incorrect for the direction of operation set. Try again with the current connections reversed.

21.11.4 PERFORMING THE TEST

1. Ensure that the timer is reset.
2. Apply a current of twice the setting shown in the ***I>1 Current Set*** cell in the *OVERCURRENT* column.
3. Note the time displayed when the timer stops.
4. Check that the red trip LED has illuminated.

21.11.5 CHECK THE OPERATING TIME

Check that the operating time recorded by the timer is within the range shown below.

For all characteristics, allowance must be made for the accuracy of the test equipment being used.

Characteristic	Operating Time at Twice Current Setting and Time Multiplier/Time Dial Setting of 1.0	
	Nominal (Seconds)	Range (Seconds)
DT	I>1 Time Delay setting	Setting ±2%
IEC S Inverse	10.03	9.53 - 10.53
IEC V Inverse	13.50	12.83 - 14.18
IEC E Inverse	26.67	24.67 - 28.67
UK LT Inverse	120.00	114.00 - 126.00
IEEE M Inverse	3.8	3.61 - 4.0
IEEE V Inverse	7.03	6.68 - 7.38
IEEE E Inverse	9.50	9.02 - 9.97
US Inverse	2.16	2.05 - 2.27
US ST Inverse	12.12	11.51 - 12.73

Note:
With the exception of the definite time characteristic, the operating times given are for a Time Multiplier Setting (TMS) or Time Dial Setting (TDS) of 1. For other values of TMS or TDS, the values need to be modified accordingly.
For definite time and inverse characteristics there is an additional delay of up to 0.02 second and 0.08 second respectively. You may need to add this the IED's acceptable range of operating times.



Caution:
On completion of the tests, you must restore all settings to customer specifications.

21.12 SYSTEM CHECK AND CHECK SYNCHRONISM

This function performs a comparison between the line voltage and the bus voltage.

There are two voltage inputs to compare:

- one from the voltage transformer input from the line side of the circuit breaker (Main VT)
- one from the VT on the bus side of the circuit breaker (CS VT).

In most cases the line VT input is three phase, whereas the bus VTs are single phase.

The bus VT inputs are normally single phase so the system voltage checks are made on single phases and the VT may be connected to either a phase-to-phase or phase to neutral voltage.

For these reasons, the IED has to be programmed with the appropriate connection. The ***CS Input*** setting in the *CT AND VT RATIOS* column can be set to A-N, B-N, C-N, A-B, B-C or C-A according to the application.

The single-phase bus VT inputs each have associated phase shift and voltage magnitude compensation settings to compensate for healthy voltage angle and magnitude differences between the check sync VT input and the selected main VT reference phase. These are:

- ***CS VT Ph Shift*** and ***CS VT Mag***

Any voltage measurements or comparisons using bus VT inputs are made using the compensated values.

Each circuit breaker controlled can have two stages of check synchronism enabled according to the settings:

- ***System Checks***, ***CS1 Status*** and ***CS2 Status***

When the system voltage check conditions are satisfied, the relevant DDB signals are asserted high as follows:

- DDB (883): Check Sync 1 OK
- DDB (884): Check Sync 2 OK

These DDB signals should be mapped to the monitor/download port and used to indicate that the system check synchronism condition has been satisfied.

21.12.1 CHECK SYNCHRONISM PASS

1. Taking note of the check synchronism settings, identify the appropriate VT input terminals and inject voltage signals that should satisfy the system voltage check synchronism criteria.
2. Check that the DDB signals are asserted high.

21.12.2 CHECK SYNCHRONISM FAIL

1. Change the voltage signals so that the criteria are not satisfied
2. Check that the appropriate DDB signals are driven low

21.13 CHECK TRIP AND AUTORECLOSE CYCLE

If the auto-reclose function is being used, the circuit breaker trip and auto reclose cycle can be tested automatically by using the application-specific settings.

To test the trip and close operation without operating the breaker, the following conditions must be satisfied:

- The ***CB Healthy*** DDB signal should either not be mapped, or if it is mapped it must be asserted high.
- The CB status inputs (52A, etc.) should either not be mapped, or if they are mapped they should be activated to mimic the circuit breaker operation.
- Some models can be configured for single-pole tripping. If configured for single pole tripping, either set *CT/VT RATIO* > ***VT Connected*** to `No`, or apply appropriate voltage signals to prevent the pole dead logic from converting to 3-pole tripping.

1. To test the first three-phase auto-reclose cycle, set *COMMISSION TESTS* > ***Test Autoreclose*** to `Trip 3 Pole`. The IED performs a trip/reclose cycle.
2. Repeat this operation to test the subsequent three-phase auto-reclose cycles.
3. Check all output relays (used for such as circuit breaker tripping and closing, or blocking other devices) operate at the correct times during the trip/close cycle.

Check the auto-reclose cycles for single phase trip conditions one at a time by sequentially setting *COMMISSION TESTS* > ***Test Autoreclose*** to `Trip Pole A`, `Trip Pole B` and `Trip Pole C`.

21.14 END-TO-END COMMUNICATION TESTS

If the IED is being used in a scheme with InterMiCOM^{64} communications you must perform end-to-end testing of the protection communications channels.

In this section all loopbacks are removed and satisfactory communications between line ends of the IEDs in the scheme are confirmed.

Note:
End-to-end communication requires a working telecommunication channel between line ends (which may be a multiplexed link or may be a direct connection). If the telecommunication channel is not available, it is not possible to establish end-to end communication. Unless otherwise directed by local operational practise, follow the instructions in this section so the scheme is ready for full operation when the telecommunications channels become available.

Note:
The trip circuit should remain isolated during these checks to prevent accidental operation of the associated circuit breaker.

21.14.1 REMOVE LOCAL LOOPBACKS

As well as removing the loopback, this section checks that all wiring and optical fibre are reconnected. If P591, P592 or P593 interface units are installed the application-specific settings are also applied.

1. Check the alarm records to ensure that no communications failure alarms have occurred while the loopback test was in progress. If it was necessary to 'fail' the communications while testing the non-current differential elements, observe the communications behaviour for a few minutes before removing the loopbacks.
2. After you are satisfied with the communications behaviour in loopback, set *COMMISSION TESTS* > ***Test Mode*** and ***Test Loopback*** to `Disabled`.

Note:
Most of the required optical signal power levels have already been measured and recorded. If all signalling uses P59x interface units, no further measurements are required. If, however, C37.94 direct fibre communications are used, further measurements are needed.

21.14.1.1 RESTORING DIRECT FIBRE CONNECTIONS

When restoring direct fibre connections, check the optical power level received from the remote IED(s).

1. Remove the loopback test fibres and at both ends of each channel used, reconnect the fibre optic cables for communications between IEDs.
2. For each channel fitted, remove the fibre connecting to the optical receiver (RX).
3. Using an optical power meter measure the strength of the signal received from the remote IED. The measurements should be within -25.4 dBm and -16.8 dBm for 850 nm fibre connections and between -37 dBm and -7 dBm for 1300 nm fibre connections
4. Record the received power level(s).
5. Reconnect the fibre(s) to the IED receiver(s).



Warning:
NEVER look directly into the transmit port or the end of an optical fibre, as this could severely damage your eyes.

21.14.1.2 RESTORING C37.94 FIBRE CONNECTIONS

When restoring C37.94 fibre connections, check the optical power level received from both the IED and the C37.94 multiplexer.

1. Remove the loopback test fibres and at both ends of each channel used.
2. Reconnect the fibre optic cables for communications between IEDs and the C37.94 compatible multiplexer.
3. Check that the value received from the IED at the C37.94 multiplexer, as well as that received by the IED from the C37.94 multiplexer are between -25.4 dBm (min) and -16.8 dBm (max).
4. Record the received power level(s).
5. Reconnect the fibre(s) to the IED receiver(s).



Warning:
NEVER look directly into the transmit port or the end of an optical fibre, as this could severely damage your eyes.

21.14.2 REMOVE REMOTE LOOPBACKS

Remove loopbacks at remote terminal connected to channel 1 and channel 2 by repeating the instructions for local loopback removal.

21.14.3 VERIFY COMMUNICATION BETWEEN IEDS

Communications statistics and status – non GPS synchronised.

1. Reset any alarm indications and check that no further communications failure alarms are raised.
2. Check channel status and propagation delays in *MEASUREMENTS 4* column for channel 1 (and channel 2 where fitted).
3. Check that the first two bits in ‘Channel Status’ (Rx and Tx) are displaying ‘1’ (11********** where * indicates a ‘don’t care’ state).
4. Clear the statistics and record the number of valid messages and the number of errored messages after a minimum period of 1 hour.
5. Check that the ratio of errored/good messages is better than 10-4.
6. Record the measured message propagation delays for channel 1, and channel 2 (if fitted).

21.15 ONLOAD CHECKS



Warning:
Onload checks are potentially very dangerous and may only be carried out by qualified and authorised personnel.

Onload checks can only be carried out if there are no restrictions preventing the energisation of the plant, and the other devices in the group have already been commissioned.

Remove all test leads and temporary shorting links, then replace any external wiring that has been removed to allow testing.



Warning:
If any external wiring has been disconnected for the commissioning process, replace it in accordance with the relevant external connection or scheme diagram.

21.15.1 CONFIRM VOLTAGE CONNECTIONS

1. Using a multimeter, measure the voltage transformer secondary voltages to ensure they are correctly rated.
2. Check that the system phase rotation is correct using a phase rotation meter.
3. Compare the values of the secondary phase voltages with the measured voltage magnitude values, which can be found in the *MEASUREMENTS 1* menu column.

Cell in MEASUREMENTS 1 Column	Corresponding VT Ratio in CT/VT RATIOS Column
VAB MAGNITUDE *VBC MAGNITUDE* *VCA MAGNITUDE* *VAN MAGNITUDE* *VBN MAGNITUDE* *VCN MAGNITUDE*	Main VT Primary/Main VT Sec'y
C/S Voltage Mag	CS VT Primary/CS VT Secondary

If the ***Local Values*** cell is set to `Secondary`, the values displayed should be equal to the applied secondary voltage. The values should be within 1% of the applied secondary voltages. However, an additional allowance must be made for the accuracy of the test equipment being used.

If the ***Local Values*** cell is set to `Primary`, the values displayed should be equal to the applied secondary voltage multiplied the corresponding voltage transformer ratio set in the *CT & VT RATIOS* column. The values should be within 1% of the expected values, plus an additional allowance for the accuracy of the test equipment being used.

21.15.2 CONFIRM CURRENT CONNECTIONS

1. Measure the current transformer secondary values for each input either by:
   a. reading from the device's HMI panel (providing it has first been verified by a secondary injection test)
   b. using a current clamp meter
2. Check that the current transformer polarities are correct by measuring the phase angle between the current and voltage, either against a phase meter already installed on site and known to be correct or by determining the direction of power flow by contacting the system control centre.
3. Ensure the current flowing in the neutral circuit of the current transformers is negligible.

If the ***Local Values*** cell is set to `Secondary`, the values displayed should be equal to the applied secondary voltage. The values should be within 1% of the applied secondary voltages. However, an additional allowance must be made for the accuracy of the test equipment being used.

If the ***Local Values*** cell is set to `Primary`, the values displayed should be equal to the applied secondary voltage multiplied the corresponding voltage transformer ratio set in the *CT & VT RATIOS* column. The values should be within 1% of the expected values, plus an additional allowance for the accuracy of the test equipment being used.

21.15.3 MEASURE CAPACITIVE CHARGING CURRENT

1. With the feeder energised from one end only, compare the local and remote measured currents in the *MEASUREMENTS 3* column to confirm that the feeder capacitive charging current is similar to that expected on all three phases.
2. Check that GROUP 1 *CURRENT DIFF* > ***Phase Is1*** is set higher than 2.5 times the capacitive charging current. If this is not the case, notify those concerned of the setting required to ensure stability under normal operating conditions.

21.15.4 CHECK DIFFERENTIAL CURRENT

With the feeder supplying load current, check that the measurements in the *MEASUREMENTS 3* column are as expected and that the differential current is similar to the value of capacitive charging current previously measured for all.

21.15.5 CHECK CURRENT TRANSFORMER POLARITY

The load current should be high enough to be certain that the main current transformers are connected with the same polarity to each device in the group. On cable circuits with high line capacitance, it is possible that the load current could be masked by the capacitive charging current.

1. If necessary reverse the connections to the main current transformers and check that the 'A' current differential in *MEASUREMENTS 3* > ***IA Differential*** cell is significantly higher than for the normal connection. If the differential current falls with the connection reversed, the main current transformers may not be correct and should be thoroughly checked.
2. Repeat the test for phases B and C using the IB Differential and IC Differential cells respectively.

21.15.6 ON-LOAD DIRECTIONAL TEST

This test ensures that directional overcurrent and fault locator functions have the correct forward/reverse response to fault and load conditions. For this test you must first know the actual direction of power flow on the system. If you do not already know this you must determine it using adjacent instrumentation or protection already in-service.

- For load current flowing in the Forward direction (power export to the remote line end), the ***A Phase Watts*** cell in the *MEASUREMENTS 2* column should show positive power signing.
- For load current flowing in the Reverse direction (power import from the remote line end), the ***A Phase Watts*** cell in the *MEASUREMENTS 2* column should show negative power signing.

> *Note:*
> *This check applies only for Measurement Modes 0 (default), and 2. This should be checked in the MEASURE'T SETUP column (**Measurement Mode** = 0 or 2). If measurement modes 1 or 3 are used, the expected power flow signing would be opposite to that shown above.*

In the event of any uncertainty, check the phase angle of the phase currents with respect to their phase voltage.

21.16 FINAL CHECKS

1. Remove all test leads and temporary shorting leads.
2. If you have had to disconnect any of the external wiring in order to perform the wiring verification tests, replace all wiring, fuses and links in accordance with the relevant external connection or scheme diagram.
3. The settings applied should be carefully checked against the required application-specific settings to ensure that they are correct, and have not been mistakenly altered during testing.
4. Ensure that all protection elements required have been set to `Enabled` in the *CONFIGURATION* column.
5. Ensure that the IED has been restored to service by checking that the ***Test Mode*** cell in the *COMMISSION TESTS* column is set to `Disabled`.
6. If the IED is in a new installation or the circuit breaker has just been maintained, the circuit breaker maintenance and current counters should be zero. These counters can be reset using the ***Reset All Values*** cell. If the required access level is not active, the device will prompt for a password to be entered so that the setting change can be made.
7. If the menu language has been changed to allow accurate testing it should be restored to the customer's preferred language.
8. If a P991/MMLG test block is installed, remove the P992/MMLB test plug and replace the cover so that the protection is put into service.
9. Ensure that all event records, fault records, disturbance records, alarms and LEDs and communications statistics have been reset.

Note:
Remember to restore the language setting to the customer's preferred language on completion.

CHAPTER 22

MAINTENANCE AND TROUBLESHOOTING

22.1 CHAPTER OVERVIEW

The Maintenance and Troubleshooting chapter provides details of how to maintain and troubleshoot products based on the Px4x and P40Agile platforms. Always follow the warning signs in this chapter. Failure to do so may result injury or defective equipment.



Caution:
Before carrying out any work on the equipment you should be familiar with the contents of the Safety Section or the Safety Guide SFTY/4LM and the ratings on the equipment's rating label.

The troubleshooting part of the chapter allows an error condition on the IED to be identified so that appropriate corrective action can be taken.

If the device develops a fault, it is usually possible to identify which module needs replacing. It is not possible to perform an on-site repair to a faulty module.

If you return a faulty unit or module to the manufacturer or one of their approved service centres, you should include a completed copy of the Repair or Modification Return Authorisation (RMA) form.

This chapter contains the following sections:

Chapter Overview 493

Maintenance 494

Troubleshooting 502

22.2 MAINTENANCE

22.2.1 MAINTENANCE CHECKS

In view of the critical nature of the application, GE Vernova products should be checked at regular intervals to confirm they are operating correctly. GE Vernova products are designed for a life in excess of 20 years.

The devices are self-supervising and so require less maintenance than earlier designs of protection devices. Most problems will result in an alarm, indicating that remedial action should be taken. However, some periodic tests should be carried out to ensure that they are functioning correctly and that the external wiring is intact. It is the responsibility of the customer to define the interval between maintenance periods. If your organisation has a Preventative Maintenance Policy, the recommended product checks should be included in the regular program. Maintenance periods depend on many factors, such as:

- The operating environment
- The accessibility of the site
- The amount of available manpower
- The importance of the installation in the power system
- The consequences of failure

Although some functionality checks can be performed from a remote location, these are predominantly restricted to checking that the unit is measuring the applied currents and voltages accurately, and checking the circuit breaker maintenance counters. For this reason, maintenance checks should also be performed locally at the substation.



Caution:
Before carrying out any work on the equipment you should be familiar with the contents of the Safety Section or the Safety Guide SFTY/4LM and the ratings on the equipment's rating label.

22.2.1.1 ALARMS

First check the alarm status LED to see if any alarm conditions exist. If so, press the Read key repeatedly to step through the alarms.

After dealing with any problems, clear the alarms. This will clear the relevant LEDs.

22.2.1.2 OPTO-ISOLATORS

Check the opto-inputs by repeating the commissioning test detailed in the Commissioning chapter.

22.2.1.3 OUTPUT RELAYS

Check the output relays by repeating the commissioning test detailed in the Commissioning chapter.

22.2.1.4 MEASUREMENT ACCURACY

If the power system is energised, the measured values can be compared with known system values to check that they are in the expected range. If they are within a set range, this indicates that the A/D conversion and the calculations are being performed correctly. Suitable test methods can be found in Commissioning chapter.

Alternatively, the measured values can be checked against known values injected into the device using the test block, (if fitted) or injected directly into the device's terminals. Suitable test methods can be found in the Commissioning chapter. These tests will prove the calibration accuracy is being maintained.

22.2.2 REPLACING THE DEVICE

If your product should develop a fault while in service, depending on the nature of the fault, the watchdog contacts will change state and an alarm condition will be flagged. In the case of a fault, you can replace either the complete device or just the faulty PCB, identified by the in-built diagnostic software.

If possible you should replace the complete device, as this reduces the chance of damage due to electrostatic discharge and also eliminates the risk of fitting an incompatible replacement PCB. However, we understand it may be difficult to remove an installed product and you may be forced to replace the faulty PCB on-site. The case and rear terminal blocks are designed to allow removal of the complete device, without disconnecting the scheme wiring.



Caution:
Replacing PCBs requires the correct on-site environment (clean and dry) as well as suitably trained personnel.



Caution:
If the repair is not performed by an approved service centre, the warranty will be invalidated.



Caution:
Before carrying out any work on the equipment, you should be familiar with the contents of the Safety Information section of this guide or the Safety Guide SFTY/4LM, as well as the ratings on the equipment's rating label. This should ensure that no damage is caused by incorrect handling of the electronic components.



Warning:
Before working at the rear of the device, isolate all voltage and current supplying it.

Note:
The current transformer inputs are equipped with integral shorting switches which will close for safety reasons, when the terminal block is removed.

To replace the complete device:

1. Carefully disconnect the cables not connected to the terminal blocks (e.g. IRIG-B, fibre optic cables, earth), as appropriate, from the rear of the device.
2. Remove the terminal block screws using a magnetic screwdriver to minimise the risk of losing the screws or leaving them in the terminal block.
3. Without exerting excessive force or damaging the scheme wiring, pull the terminal blocks away from their internal connectors.
4. Remove the terminal block screws that fasten the device to the panel and rack. These are the screws with the larger diameter heads that are accessible when the access covers are fitted and open.
5. Withdraw the device from the panel and rack. Take care, as the device will be heavy due to the internal transformers.
6. To reinstall the device, follow the above instructions in reverse, ensuring that each terminal block is relocated in the correct position and the chassis ground, IRIG-B and fibre optic connections are replaced. The terminal blocks are labelled alphabetically with 'A' on the left hand side when viewed from the rear.

Once the device has been reinstalled, it should be re-commissioned as set out in the Commissioning chapter.

Caution:
If the top and bottom access covers have been removed, some more screws with smaller diameter heads are made accessible. Do NOT remove these screws, as they secure the front panel to the device.

Note:
There are four possible types of terminal block: RTD/CLIO input, heavy duty, medium duty, and MiDOS. The terminal blocks are fastened to the rear panel with slotted or cross-head screws depending on the type of terminal block. Not all terminal block types are present on all products.

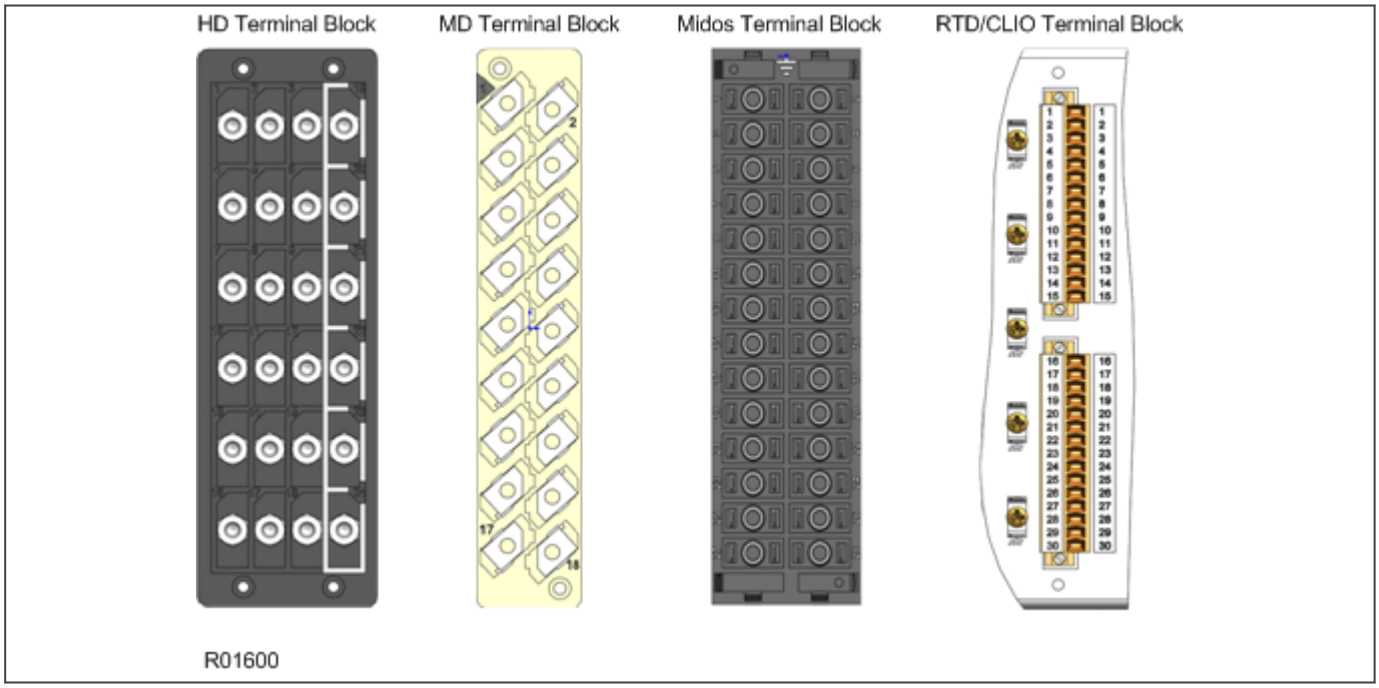


Figure 225: Possible terminal block types

22.2.3 REPAIRING THE DEVICE

If your product should develop a fault while in service, depending on the nature of the fault, the watchdog contacts will change state and an alarm condition will be flagged. In the case of a fault, either the complete unit or just the faulty PCB, identified by the in-built diagnostic software, should be replaced.

Replacement of printed circuit boards and other internal components must be undertaken by approved Service Centres. Failure to obtain the authorisation of after-sales engineers prior to commencing work may invalidate the product warranty.

We recommend that you entrust any repairs to Automation Support teams, which are available world-wide.

22.2.4 REMOVING THE FRONT PANEL

Warning:
Before removing the front panel to replace a PCB, you must first remove the auxiliary power supply and wait 5 seconds for the internal capacitors to discharge. You should also isolate voltage and current transformer connections and trip circuit.



Caution:
Before removing the front panel, you should be familiar with the contents of the Safety Information section of this guide or the Safety Guide SFTY/4LM, as well as the ratings on the equipment's rating label.

To remove the front panel:

1. Open the top and bottom access covers. You must open the hinged access covers by more than 90° before they can be removed.
2. If fitted, remove the transparent secondary front cover.
3. Apply outward pressure to the middle of the access covers to bow them and disengage the hinge lug, so the access cover can be removed. The screws that fasten the front panel to the case are now accessible.
4. Undo and remove the screws. The 40TE case has four cross-head screws fastening the front panel to the case, one in each corner, in recessed holes. The 60TE/80TE cases have an additional two screws, one midway along each of the top and bottom edges of the front plate.
5. When the screws have been removed, pull the complete front panel forward to separate it from the metal case. The front panel is connected to the rest of the circuitry by a 64-way ribbon cable.
6. The ribbon cable is fastened to the front panel using an IDC connector; a socket on the cable and a plug with locking latches on the front panel. Gently push the two locking latches outwards which eject the connector socket slightly. Remove the socket from the plug to disconnect the front panel.



Caution:
Do not remove the screws with the larger diameter heads which are accessible when the access covers are fitted and open. These screws hold the device in its mounting (panel or cubicle).



Caution:
The internal circuitry is now exposed and is not protected against electrostatic discharge and dust ingress. Therefore ESD precautions and clean working conditions must be maintained at all times.

22.2.5 REPLACING PCBS

1. To replace any of the PCBs, first remove the front panel.
2. Once the front panel has been removed, the PCBs are accessible. The numbers above the case outline identify the guide slot reference for each printed circuit board. Each printed circuit board has a label stating the corresponding guide slot number to ensure correct relocation after removal. To serve as a reminder of the slot numbering there is a label on the rear of the front panel metallic screen.
3. Remove the 64-way ribbon cable from the PCB that needs replacing
4. Remove the PCB in accordance with the board-specific instructions detailed later in this section.

Note:
To ensure compatibility, always replace a faulty PCB with one of an identical part number.

22.2.5.1 REPLACING THE MAIN PROCESSOR BOARD

The main processor board is situated in the front panel. This board contains application-specific settings in its non-volatile memory. You may wish to take a backup copy of these settings. This could save time in the re-commissioning process.

To replace the main processor board:

1. Remove front panel.
2. Place the front panel with the user interface face down and remove the six screws from the metallic screen, as shown in the figure below. Remove the metal plate.
3. Remove the screws that hold the main processor board in position.
4. Carefully disconnect the ribbon cable. Take care as this could easily be damaged by excessive twisting.
5. Replace the main processor board
6. Reassemble the front panel using the reverse procedure. Make sure the ribbon cable is reconnected to the main processor board and that all eight screws are refitted.
7. Refit the front panel.
8. Refit and close the access covers then press the hinge assistance T-pieces so they click back into the front panel moulding.
9. Once the unit has been reassembled, carry out the standard commissioning procedure as defined in the Commissioning chapter.

Note:
After replacing the main processor board, all the settings required for the application need to be re-entered. This may be done either manually or by downloading a settings file.

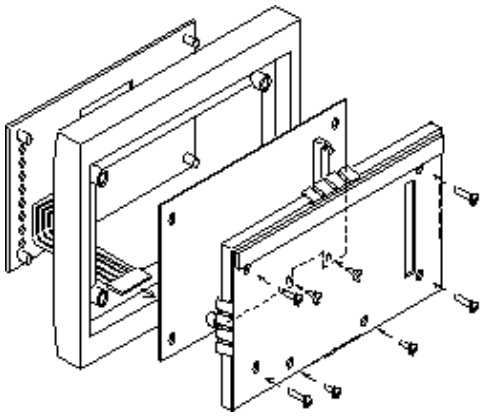


Figure 226: Front panel assembly

22.2.5.2 REPLACEMENT OF COMMUNICATIONS BOARDS

Most products will have at least one communications board of some sort fitted. There are several different boards available offering various functionality, depending on the application. Some products may even be fitted with two boards of different types.

To replace a faulty communications board:

1. Remove front panel.
2. Disconnect all connections at the rear.
3. The board is secured in the device case by two screws, one at the top and another at the bottom. Remove these screws carefully as they are not captive in the rear panel.
4. Gently pull the communications board forward and out of the case.

5. Before fitting the replacement PCB check that the number on the round label next to the front edge of the PCB matches the slot number into which it will be fitted. If the slot number is missing or incorrect, write the correct slot number on the label.
6. Fit the replacement PCB carefully into the correct slot. Make sure it is pushed fully back and that the securing screws are refitted.
7. Reconnect all connections at the rear.
8. Refit the front panel.
9. Refit and close the access covers then press the hinge assistance T-pieces so they click back into the front panel moulding.
10. Once the unit has been reassembled, commission it according to the Commissioning chapter.

22.2.5.3 REPLACEMENT OF THE INPUT MODULE

Depending on the product, the input module consists of two or three boards fastened together and is contained within a metal housing. One board contains the transformers and one contains the analogue to digital conversion and processing electronics. Some devices have an additional auxiliary transformer contained on a third board.

To replace an input module:

1. Remove front panel.
2. The module is secured in the case by two screws on its right-hand side, accessible from the front, as shown below. Move these screws carefully as they are not captive in the front plate of the module.
3. On the right-hand side of the module there is a small metal tab which brings out a handle (on some modules there is also a tab on the left). Grasp the handle(s) and pull the module firmly forward, away from the rear terminal blocks. A reasonable amount of force is needed due to the friction between the contacts of the terminal blocks.
4. Remove the module from the case. The module may be heavy, because it contains the input voltage and current transformers.
5. Slot in the replacement module and push it fully back onto the rear terminal blocks. To check that the module is fully inserted, make sure the v-shaped cut-out in the bottom plate of the case is fully visible.
6. Refit the securing screws.
7. Refit the front panel.
8. Refit and close the access covers then press the hinge assistance T-pieces so they click back into the front panel moulding.
9. Once the unit has been reassembled, commission it according to the Commissioning chapter.



Caution:
With non-mounted IEDs, the case needs to be held firmly while the module is withdrawn. Withdraw the input module with care as it suddenly comes loose once the friction of the terminal blocks is overcome.

Note:
If individual boards within the input module are replaced, recalibration will be necessary. We therefore recommend replacement of the complete module to avoid on-site recalibration.

22.2.5.4 REPLACEMENT OF THE POWER SUPPLY BOARD



Caution:
Before removing the front panel, you should be familiar with the contents of the Safety Information section of this guide or the Safety Guide SFTY/4LM, as well as the ratings on the equipment's rating label.

The power supply board is fastened to an output relay board with push fit nylon pillars. This doubled-up board is secured on the extreme left hand side, looking from the front of the unit.

1. Remove front panel.
2. Pull the power supply module forward, away from the rear terminal blocks and out of the case. A reasonable amount of force is needed due to the friction between the contacts of the terminal blocks.
3. Separate the boards by pulling them apart carefully. The power supply board is the one with two large electrolytic capacitors.
4. Before reassembling the module, check that the number on the round label next to the front edge of the PCB matches the slot number into which it will be fitted. If the slot number is missing or incorrect, write the correct slot number on the label
5. Reassemble the module with a replacement PCB. Push the inter-board connectors firmly together. Fit the four push fit nylon pillars securely in their respective holes in each PCB.
6. Slot the power supply module back into the housing. Push it fully back onto the rear terminal blocks.
7. Refit the front panel.
8. Refit and close the access covers then press the hinge assistance T-pieces so they click back into the front panel moulding.
9. Once the unit has been reassembled, commission it according to the Commissioning chapter.

22.2.5.5 REPLACEMENT OF THE I/O BOARDS

There are several different types of I/O boards, which can be used, depending on the product and application. Some boards have opto-inputs, some have relay outputs and others have a mixture of both.

1. Remove front panel.
2. Gently pull the board forward and out of the case
3. If replacing the I/O board, make sure the setting of the link above IDC connector on the replacement board is the same as the one being replaced.
4. Before fitting the replacement board check the number on the round label next to the front edge of the board matches the slot number into which it will be fitted. If the slot number is missing or incorrect, write the correct slot number on the label.
5. Carefully slide the replacement board into the appropriate slot, ensuring that it is pushed fully back onto the rear terminal blocks.
6. Refit the front panel.
7. Refit and close the access covers then press at the hinge assistance T-pieces so they click back into the front panel moulding.
8. Once the unit has been reassembled, commission it according to the Commissioning chapter.

22.2.6 RECALIBRATION

Recalibration is not needed when a PCB is replaced, unless it is one of the boards in the input module. If any of the boards in the input module is replaced, the unit must be recalibrated.

Although recalibration is needed when a board inside the input module is replaced, it is not needed if the input module is replaced in its entirety.

Although it is possible to carry out recalibration on site, this requires special test equipment and software. We therefore recommend that the work be carried out by the manufacturer, or entrusted to an approved service centre.

22.2.7 SUPERCAPACITOR DISCHARGED

The supercapacitor maintains charge for two weeks with the IED de-energised. When first energising the IED after this time there may be a Battery Alarm due to the supercapacitor voltage dropping below a pre-defined threshold.

The battery alarm will clear after approximately 30 minutes of IED being energised, and once cleared there will be enough charge in the supercapacitor to backup status data.

Note:
Events, disturbance and maintenance records will be lost if the supercapacitor is fully discharged.

22.2.8 CLEANING



Warning:
Before cleaning the device, ensure that all AC and DC supplies and transformer connections are isolated, to prevent any chance of an electric shock while cleaning.

Only clean the equipment with a lint-free cloth dampened with clean water. Do not use detergents, solvents or abrasive cleaners as they may damage the product's surfaces and leave a conductive residue.

22.3 TROUBLESHOOTING

22.3.1 SELF-DIAGNOSTIC SOFTWARE

The device includes several self-monitoring functions to check the operation of its hardware and software while in service. If there is a problem with the hardware or software, it should be able to detect and report the problem, and attempt to resolve the problem by performing a reboot. In this case, the device would be out of service for a short time, during which the 'Healthy' LED on the front of the device is switched OFF and the watchdog contact at the rear is ON. If the restart fails to resolve the problem, the unit takes itself permanently out of service; the 'Healthy' LED stays OFF and watchdog contact stays ON.

If a problem is detected by the self-monitoring functions, the device attempts to store a maintenance record to allow the nature of the problem to be communicated to the user.

The self-monitoring is implemented in two stages: firstly a thorough diagnostic check which is performed on boot-up, and secondly a continuous self-checking operation, which checks the operation of the critical functions whilst it is in service.

22.3.2 POWER-UP ERRORS

If the IED does not appear to power up, use the following to determine whether the fault is in the external wiring, auxiliary fuse, IED power supply module or IED front panel.

Test	Check	Action
1	Measure the auxiliary voltage on terminals 1 and 2. Verify the voltage level and polarity against the rating label on the front. Terminal 1 is –dc, 2 is +dc	If the auxiliary voltage is correct, go to test 2. Otherwise check the wiring and fuses in the auxiliary supply.
2	Check the LEDs and LCD backlight switch on at power-up. Also check the N/O (normally open) watchdog contact for closing.	If the LEDs and LCD backlight switch on, or the contact closes and no error code is displayed, the error is probably on the main processor board in the front panel. If the LEDs and LCD backlight do not switch on and the contact does not close, go to test 3.
3	Check the output (nominally 48 V DC).	If there is no field voltage, the fault is probably in the IED power supply module.

22.3.3 ERROR MESSAGE OR CODE ON POWER-UP

The IED performs a self-test during power-up. If it detects an error, a message appears on the LCD and the power-up sequence stops. If the error occurs when the IED application software is running, a maintenance record is created and the device reboots.

Test	Check	Action
1	Is an error message or code permanently displayed during power up?	If the IED locks up and displays an error code permanently, go to test 2. If the IED prompts for user input, go to test 4. If the IED reboots automatically, go to test 5.
2	Record displayed error, and then remove and re-apply IED auxiliary supply.	Record whether the same error code is displayed when the IED is rebooted. If no error code is displayed, contact the local service centre stating the error code and IED information. If the same code is displayed, go to test 3.

Test	Check	Action
3	Error Code Identification The following text messages (in English) are displayed if a fundamental problem is detected, preventing the system from booting: Bus Fail - address lines SRAM Fail - data lines FLASH Fail format error FLASH Fail checksum Code Verify Fail The following hex error codes relate to errors detected in specific IED modules:	These messages indicate that a problem has been detected on the IED's main processor board in the front panel.
3.1	0c140005/0c0d0000	Input Module (including opto-isolated inputs)
3.2	0c140006/0c0e0000	Output IED boards
3.3	The last four digits provide details on the actual error.	Other error codes relate to hardware or software problems on the main processor board. Contact GE Vernova with details of the problem for a full analysis.
4	The IED displays a message for corrupt settings and prompts for the default values to be restored for the affected settings.	The power-up tests have detected corrupted IED settings. Restore the default settings to allow the power-up to complete, and then reapply the application-specific settings.
5	The IED resets when the power-up is complete. A record error code is displayed	Error 0x0E080000, programmable scheme logic error due to excessive execution time. If the IED powers up successfully, check the programmable logic for feedback paths. Other error codes relate to software errors on the main processor board.

22.3.4 OUT OF SERVICE LED ON AT POWER-UP

Test	Check	Action	
1	Using the IED menu, confirm the Commission Test or Test Mode setting is Enabled. If it is not Enabled, go to test 2.	If the setting is Enabled, disable the test mode and make sure the Out of Service LED is OFF.	
2	Select the *VIEW RECORDS* column then view the last maintenance record from the menu.	Check for the H/W Verify Fail maintenance record. This indicates a discrepancy between the IED model number and the hardware. Examine the ***Maint Data***; cell. This indicates the causes of the failure using bit fields: Bit Meaning	
		0	The application type field in the model number does not match the software ID
		1	The application field in the model number does not match the software ID
		2	The variant 1 field in the model number does not match the software ID
		3	The variant 2 field in the model number does not match the software ID
		4	The protocol field in the model number does not match the software ID
		5	The language field in the model number does not match the software ID
		6	The VT type field in the model number is incorrect (110 V VTs fitted)
		7	The VT type field in the model number is incorrect (440 V VTs fitted)
		8	The VT type field in the model number is incorrect (no VTs fitted)

22.3.5 ERROR CODE DURING OPERATION

The IED performs continuous self-checking. If the IED detects an error it displays an error message, logs a maintenance record and after a short delay resets itself. A permanent problem (for example due to a hardware fault) is usually detected in the power-up sequence. In this case the IED displays an error code and halts. If the problem was transient, the IED reboots correctly and continues operation. By examining the maintenance record logged, the nature of the detected fault can be determined.

22.3.6 MAL-OPERATION DURING TESTING

22.3.6.1 FAILURE OF OUTPUT CONTACTS

An apparent failure of the relay output contacts can be caused by the configuration. Perform the following tests to identify the real cause of the failure. The self-tests verify that the coils of the output relay contacts have been energised. An error is displayed if there is a fault in the output relay board.

Test	Check	Action
1	Is the Out of Service LED ON?	If this LED is ON, the device may be in test mode or the protection has been disabled due to a hardware verify error.
2	Examine the Contact status in the Commissioning section of the menu.	If the relevant bits of the contact status are operated, go to test 4; if not, go to test 3.
3	Examine the fault record or use the test port to check the protection element is operating correctly.	If the protection element does not operate, check the test is correctly applied. If the protection element operates, check the programmable logic to make sure the protection element is correctly mapped to the contacts.
4	Using the Commissioning or Test mode function, apply a test pattern to the relevant relay output contacts. Consult the correct external connection diagram and use a continuity tester at the rear of the device to check the relay output contacts operate.	If the output relay operates, the problem must be in the external wiring to the device. If the output relay does not operate the output relay contacts may have failed (the self-tests verify that the relay coil is being energised). Ensure the closed resistance is not too high for the continuity tester to detect.

22.3.6.2 FAILURE OF OPTO-INPUTS

The opto-isolated inputs are mapped onto the IED's internal DDB signals using the programmable scheme logic. If an input is not recognised by the scheme logic, use the ***Opto I/P Status*** cell in the *COMMISSION TESTS* column to check whether the problem is in the opto-input itself, or the mapping of its signal to the scheme logic functions.

If the device does not correctly read the opto-input state, test the applied signal. Verify the connections to the opto-input using the wiring diagram and the nominal voltage settings in the *OPTO CONFIG* column. To do this:

1. Select the nominal voltage for all opto-inputs by selecting one of the five standard ratings in the ***Global Nominal V*** cell.
2. Select `Custom` to set each opto-input individually to a nominal voltage.
3. Using a voltmeter, check that the voltage on its input terminals is greater than the minimum pick-up level (See the Technical Specifications chapter for opto pick-up levels).

If the signal is correctly applied, this indicates failure of an opto-input, which may be situated on standalone opto-input board, or on an opto-input board that is part of the input module. Separate opto-input boards can simply be replaced. If, however, the faulty opto-input board is part of the input module, the complete input module should be replaced. This is because the analogue input module cannot be individually replaced without dismantling the module and recalibration of the IED.

22.3.6.3 INCORRECT ANALOGUE SIGNALS

If the measured analogue quantities do not seem correct, use the measurement function to determine the type of problem. The measurements can be configured in primary or secondary terms.

1. Compare the displayed measured values with the actual magnitudes at the terminals.
2. Check the correct terminals are used.
3. Check the CT and VT ratios set are correct.
4. Check the phase displacement to confirm the inputs are correctly connected.

22.3.7 COPROCESSOR BOARD FAILURES

If a coprocessor board is used, this may cause the IED to report one or more of the following alarms:

- Signalling failure alarm (on its own)
- C diff failure (on its own)
- Signalling failure and C diff failure together
- Incompatible IED
- Comms changed
- IEEE C37.94 fail

22.3.7.1 SIGNALLING FAILURE ALARM (ON ITS OWN)

This indicates that there is a problem with one of the fibre-optic signalling channels. This alarm can occur in dual redundant or three terminal schemes. The fibre may have been disconnected, the device may have been incorrectly configured at one of the ends, or there is a problem with the communications equipment. Further information about the status of the signalling channels can be found in *MEASUREMENTS 4* column.

22.3.7.2 C DIFF FAILURE ALARM (ON ITS OWN)

This indicates there is a problem with the Coprocessor board. As a result the current differential/distance protection is not available and backup protection will operate, if configured to do so. Further information can be found in the maintenance records.

22.3.7.3 SIGNALLING FAILURE AND C DIFF FAILURE ALARMS TOGETHER

This indicates that there is a problem with one or both fibre-optic signalling channels. The fibre may have been disconnected, the device may have been incorrectly configured at one of the ends, or there is a problem with the communications equipment. As a result the current differential protection is not available and backup protection will operate, if configured to do so. Further information about the status of the signalling channels can be found in *MEASUREMENTS 4* column.

22.3.7.4 INCOMPATIBLE IED

This occurs if the IEDs trying to communicate with each other are of incompatible types.

22.3.7.5 COMMS CHANGED

This indicates that the ***Comms Mode*** setting has been changed without a subsequent power off and on.

22.3.7.6 IEEE C37.94 FAIL

This indicates a Signal Lost, a Path Yellow (indicating a fault on the communications channel) or a mismatch in the number of N*64 channels used on either channel 1 or channel 2. Further information can be found in the *MEASUREMENTS 4* column.

22.3.8 PSL EDITOR TROUBLESHOOTING

A failure to open a connection could be due to one or more of the following:

- The IED address is not valid (this address is always 1 for the front port)
- Password in not valid
- Communication set-up (COM port, Baud rate, or Framing) is not correct
- Transaction values are not suitable for the IED or the type of connection
- The connection cable is not wired correctly or broken
- The option switches on any protocol converter used may be incorrectly set

22.3.8.1 DIAGRAM RECONSTRUCTION

Although a scheme can be extracted from an IED, a facility is provided to recover a scheme if the original file is unobtainable.

A recovered scheme is logically correct but much of the original graphical information is lost. Many signals are drawn in a vertical line down the left side of the canvas. Links are drawn orthogonally using the shortest path from A to B. Any annotation added to the original diagram such as titles and notes are lost.

Sometimes a gate type does not appear as expected. For example, a single-input AND gate in the original scheme appears as an OR gate when uploaded. Programmable gates with an inputs-to-trigger value of 1 also appear as OR gates

22.3.8.2 PSL VERSION CHECK

The PSL is saved with a version reference, time stamp and CRC check (Cyclic Redundancy Check). This gives a visual check whether the default PSL is in place or whether a new application has been downloaded.

22.3.9 REPAIR AND MODIFICATION PROCEDURE

Please follow these steps to return an Automation product to us:

1. Get the Repair and Modification Return Authorisation (RMA) form
   An electronic version of the RMA form is available from the following:
   GA.support@gevernova.com
2. Fill in the RMA form
   Fill in only the white part of the form.
   Please ensure that all fields marked **(M)** are completed such as:
   - Equipment model
   - Model No. and Serial No.
   - Description of failure or modification required (please be specific)
   - Value for customs (in case the product requires export)
   - Delivery and invoice addresses
   - Contact details
3. Send the RMA form to your local contact
   For a list of local service contacts worldwide, email us at:
   GA.support@gevernova.com
4. The local service contact provides the shipping information
   Your local service contact provides you with all the information needed to ship the product:
   - Pricing details
   - RMA number
   - Repair centre address

If required, an acceptance of the quote must be delivered before going to the next stage.

5. Send the product to the repair centre
   - Address the shipment to the repair centre specified by your local contact
   - Make sure all items are packaged in an anti-static bag and foam protection
   - Make sure a copy of the import invoice is attached with the returned unit
   - Make sure a copy of the RMA form is attached with the returned unit
   - E-mail or fax a copy of the import invoice and airway bill document to your local contact.

CHAPTER 23

TECHNICAL SPECIFICATIONS

23.1 CHAPTER OVERVIEW

This chapter describes the technical specifications of the product.

This chapter contains the following sections:

Chapter Overview 509
Interfaces 510
Protection Functions 515
Monitoring, Control and Supervision 520
Measurements and Recording 522
Ratings 523
Input/Output Connections 526
Mechanical Specifications 528
Type Tests 529
Environmental Conditions 530
Electromagnetic Compatibility 531
Regulatory Compliance 534

23.2 INTERFACES

23.2.1 FRONT USB PORT

Front USB Port	
Use	For local connection to laptop for configuration purposes and firmware downloads
Connector	USB type B
Isolation	Isolation to ELV level
Constraints	Maximum cable length 5 m

23.2.2 REAR SERIAL PORT 1

Rear Serial Port 1 (RP1)	
Use	For SCADA communications (multi-drop)
Standard	EIA(RS)485, K-bus
Connector	General purpose block, M4 screws (2 wire)
Cable	Screened twisted pair (STP)
Supported Protocols *	Courier, IEC-60870-5-103, DNP3.0, MODBUS
Isolation	Isolation to SELV level
Constraints	Maximum cable length 1000 m

* Not all models support all protocols - see ordering options

23.2.3 FIBRE REAR SERIAL PORT 1

Optional Fibre Rear Serial Port (RP1)	
Main Use	Serial SCADA communications over fibre
Connector	IEC 874-10 BFOC 2.5 –(ST®) (1 each for Tx and Rx)
Fibre type	Multimode 50/125 µm or 62.5/125 µm
Supported Protocols	Courier, IEC870-5-103, DNP 3.0, MODBUS
Wavelength	850 nm

23.2.4 REAR SERIAL PORT 2

Optional Rear Serial Port (RP2)	
Use	For SCADA communications (multi-drop)
Standard	EIA(RS)485, K-bus, EIA(RS)232
Designation	SK4
Connector	9 pin D-type female connector
Cable	Screened twisted pair (STP)
Supported protocols	Courier
Isolation	Isolation to SELV level
Constraints	Maximum cable length 1000 m for RS485 and K-bus, 15 m for RS232

23.2.5 OPTIONAL REAR SERIAL PORT (SK5)

Optional Rear Serial Port for Teleprotection	
Use	For teleprotection in distance products
Standard	EIA(RS)232
Designation	SK5
Connector	9 pin D-type female connector
Cable	Screened twisted pair (STP)
Supported protocols	InterMiCOM (IM)
Isolation	Isolation to SELV level
Constraints	Maximum cable length 15 m

23.2.6 IRIG-B (DEMODULATED)

IRIG-B Interface (Demodulated)	
Use	External clock synchronisation signal
Standard	IRIG 200-98 format B00X
Connector	BNC
Cable type	50 ohm coaxial
Isolation	Isolation to SELV level
Input signal	TTL level
Input impedance	10 k ohm at dc
Accuracy	+/-1 ms

23.2.7 IRIG-B (MODULATED)

IRIG-B Interface (Modulated)	
Use	External clock synchronisation signal
Standard	IRIG 200-98 format B12X
Connector	BNC
Cable type	50 ohm coaxial
Isolation	Isolation to SELV level
Input signal	Peak to peak, 200 mV to 20 mV
Input impedance	6 k ohm at 1000 Hz
Accuracy	+/-1 ms

23.2.8 REAR ETHERNET PORT COPPER

Rear Ethernet Port using CAT 5/6/7 Wiring	
Main Use	Substation Ethernet communications
Standard	IEEE 802.3 100BaseTX
Connector	RJ45
Cable type	Screened twisted pair (STP)
Isolation	1.5 kV

Rear Ethernet Port using CAT 5/6/7 Wiring	
Supported Protocols	IEC 61850
Constraints	Maximum cable length 100 m

23.2.9 REAR ETHERNET PORT FIBRE (HARDWARE OPTION (R/S/T)

Rear Ethernet Port using Fibre-Optic Cabling	
Main Use	Substation Ethernet communications
Connector	IEC 874-10 BFOC 2.5 –(ST®) (1 each for Tx and Rx)
Standard	IEEE 802.3 100 BaseFX
Fibre type	Multimode 50/125 µm or 62.5/125 µm
Supported Protocols	IEC 61850
Optional Redundancy Protocols Supported	PRP (Parallel Redundancy Protocol) HSR (High-availability Seamless Redundancy) RSTP (Rapid Spanning Tree Protocol) Failover
Wavelength	1300 nm

23.2.9.1 100 BASE FX RECEIVER CHARACTERISTICS

Parameter	Sym	Min.	Typ.	Max.	Unit
Input Optical Power Minimum at Window Edge	PIN Min. (W)		-33.5	–31	dBm avg.
Input Optical Power Minimum at Eye Centre	PIN Min. (C)		-34.5	-31.8	Bm avg.
Input Optical Power Maximum	PIN Max.	-14	-11.8		dBm avg.

Conditions: TA = 0°C to 70°C

23.2.9.2 100 BASE FX TRANSMITTER CHARACTERISTICS

Parameter	Sym	Min.	Typ.	Max.	Unit
Output Optical Power BOL 62.5/125 µm NA = 0.275 Fibre EOL	PO	-19 -20	-16.8	-14	dBm avg.
Output Optical Power BOL 50/125 µm NA = 0.20 Fibre EOL	PO	-22.5 -23.5	-20.3	-14	dBm avg.
Optical Extinction Ratio				10 -10	% dB
Output Optical Power at Logic "0" State	PO			-45	dBm avg.

Conditions: TA = 0°C to 70°C

23.2.10 REAR ETHERNET PORT FIBRE (HARDWARE OPTION U/W/Y)

Rear Ethernet Port using Fibre-optic Cabling	
Main Use	Substation Ethernet communications
Connector	IEC 874-10 BFOC 2.5 - (LC®) (1 each for Tx and Rx)
Standard	IEEE 802.3 100 BaseFX

Rear Ethernet Port using Fibre-optic Cabling	
Fibre type	Multimode 50/125 µm (OM2 or OM3) or 62.5/125 µm (OM1)
Supported Protocols	Courier (tunnelled), IEC 61850, PTP, SNTP, SNMP, RADIUS, syslog
Redundancy Protocols Supported	PRP (Parallel Redundancy Protocol) HSR (High-availability Seamless Redundancy) RSTP (Rapid Spanning Tree Protocol) Failover
Wavelength	1310 nm

23.2.10.1 100 BASE FX RECEIVER CHARACTERISTICS

Parameter	Sym	Min.	Typ.	Max.	Unit
Input optical power minimum at window edge	PIN Min. (W)	-31.0		-12.0	dBm avg.
Input optical power minimum at eye centre	PIN Min. (C)		-34.5	-31.8	Bm avg.
Input optical power maximum	PIN Max.	-14	-11.8		dBm avg.

Note:
Conditions: TA = 0°C to 70°C

23.2.10.2 100 BASE FX TRANSMITTER CHARACTERISTICS

Parameter	Sym	Min.	Typ.	Max.	Unit
Output optical power BOL 62.5/125 µm NA = 0.275 Fibre EOL	PO	-20	-17.0	-14.0	dBm avg.
Output optical power BOL 50/125 µm NA = 0.20 Fibre EOL	PO	-24.0	-21.0	-17.0	dBm avg.
Optical extinction ratio	ER	10			dB
Output optical power at logic "0" state	$P_{O(off)}$			-45	dBm avg.

Note:
Conditions: TA = 0°C to 70°C

23.2.11 FIBRE TELEPROTECTION INTERFACE

Fibre Teleprotection Interface	
Main use	Teleprotection communications
Connectors (2)	BFOC 2.5 –(ST®)
Standard	IEC 874-10
Protocol	InterMicom 64
Fibre type	Multimode 50/125 µm or 62.5/125 µm or single-mode 9/125 µm
Wavelength	850 nm or 1300 nm (multimode), 1300 nm or 1500 nm (single mode)
Minimum reception level	-28 dBm
Accuracy	Better than +/- 50 ns for maximum absolute error between actual GPS time and rising edge of 1 PPS signal

Optical Budget

	850nm MM	1300 nm MM	1300 nm SM	1550 nm SM
Minimum transmit output level (average power)	-19 dBm	-6 dBm	-6 dBm	-6 dBm
Receiver sensitivity (average power)	-32 dBm	-49 dBm	-49 dBm	-49 dBm
Optical budget	13 dB	43 dB	43 dB	43 dB
Less safety margin (3 dB)	10 dB	40 dB	40 dB	40 dB
Typical cable loss	2.6 dB/km	0.8 dB/km	0.4 dB/km	0.3 dB/km
Maximum transmission distance	3.8 km	50 km	100 km	130 km
Typical transmitter optical power	-16 dBm	-	-	-
Maximum receiver optical power	-11 dBm	-	-	-

Note:
This optical interface has been designed and tested for compliance with IEEE C37.94.

23.3 PROTECTION FUNCTIONS

23.3.1 PHASE CURRENT DIFFERENTIAL PROTECTION

Accuracy	
Pick-up	Formula +/- 10%
Drop-off	0.75 x Formula +/- 10%
IDMT characteristic shape	+/- 5% or 40 ms, whichever is greater
DT operation	+/- 2% or 20 ms, whichever is greater
2 Terminal instantaneous operating times * Typical operating time at 2x pickup value Typical operating time at 3x pickup value Typical operating time at 5x and above pickup value Probability of achieving tripping time	 < 25 ms < 21 ms < 18 ms 98.00%
4 & 6 Terminal instantaneous operating times * Typical operating time at 2x pickup value Typical operating time at 3x pickup value and above Probability of achieving tripping time	 < 33 ms < 28 ms 98.00%
Reset time	<60 ms
Repeatability	+/- 2.5%
Characteristic	UK curves IEC 60255-3 – 1998 US curves IEEE C37.112 – 1996
Current transformer ratio compensation	No affect on accuracy
High set characteristic setting	No affect on accuracy

* Reference conditions:

- Standard output contact is used
- Default setting value is used for testing (Is1 = 0.2, K1= 30%, K2=150 %, Is2= 2).
- The operating time quoted is for a maximum time slot setting of 12.
- The operating time claim is based upon current injection at one end of the scheme and is for the IED with injected current.
- Probability estimation is based on a sample size (number of cases) of 100 test cases.

* Notes:

2 Terminal:

- Sub-cycle operation at 3x pick-up value and above can be achieved by using high-speed high-break contacts.
- The inter-tripping to remote ends can add an additional 8 ms to the tripping time quoted above.

4 & 6 Terminal:

- The inter-tripping to remote ends is included in the tripping time quoted above.

23.3.2 FIBRE TELEPROTECTION TRANSFER TIMES

The table below shows the minimum and maximum transfer time for InterMiCOM64 (IM64). The times are measured from opto initialisation (with no opto filtering) to relay standard output and include a small propagation delay for back-back test.

IDiff IM64 indicates InterMiCOM64 signals working in conjunction with the differential protection fibre optic communications channel. IM64 indicates InterMiCOM64 signals working as a standalone feature.

Configuration	Signals	Permissive Op Times (ms)	Direct Op Times (ms)	MaxCh1 Prop Delay Measured
IM64 at 56kbps	8	18-21	21-24	1.6ms
IM64 at 64kbps	8	18-21	21-24	1.3ms
IM64 at 128kbps	24	17-20	20-23	1.4ms
IDiff IM64 at 56kbps	8	24-26	29-31	3.3ms
IDiff IM64 at 64kbps	8	24-26	29-31	2.9ms
IDiff IM64 at 128kbps	32	20-26	24-31	1.9ms

23.3.3 AUTORECLOSE AND CHECK SYNYCHRONISM

Accuracy	
Timers	+/-20 ms or 2%, whichever is greater

23.3.4 PHASE OVERCURRENT PROTECTION

Accuracy	
IDMT pick-up	1.05 x Setting +/-5%
DT pick-up	Setting +/-5%
Drop-off (IDMT and DT)	0.95 x setting +/-5%
IDMT operate time	+/-5% or 40 ms, whichever is greater *
IEEE reset time	+/-5% or 40 ms, whichever is greater **
DT operate time	+/-2% or 25 ms, whichever is greater (non-directional) * +/-2% or 40 ms, whichever is greater (directional) *
DT reset time	+/-5% or 40 ms, whichever is greater **
Repeatability	<5%
Characteristic UK	IEC 60255-151: 2009
Characteristic US	IEEE C37.112 1996

23.3.4.1 PHASE OVERCURRENT DIRECTIONAL PARAMETERS

Accuracy	
Directional boundary pickup (RCA +/-90%)	+/-2° ◆
Directional boundary hysteresis	<2°
Directional boundary repeatability	<2%

23.3.5 EARTH FAULT PROTECTION

Accuracy	
IDMT pick-up	1.05 x Setting +/-5%
DT pick-up	Setting +/-5%, or 20 mA, whichever is greater
Drop-off (IDMT and DT)	0.9 x setting +/-5%
IDMT Operate	+/-5% or 40 ms, whichever is greater*
IEEE reset	+/-10% or 40 ms, whichever is greater

Accuracy	
Repeatability	< 5%
DT operate	+/-2% or 50 ms, whichever is greater
DT reset	+/- 5% or 50 ms, whichever is greater

Note:
Reference conditions: TMS = 1, TD = 1, IN> = 1A, operating range = 2-20In.

23.3.5.1 EARTH FAULT DIRECTIONAL PARAMETERS

Zero Sequence Polarising Accuracy	
Directional boundary pick-up (RCA +/- 90°)	+/-2°
Hysteresis	<3°
N> pick-up	Setting +/-10%
VN> drop-off	0.9 x Setting +/-10%

Negative Sequence Polarising Accuracy	
Directional boundary pick-up (RCA +/- 90°)	+/-2°
Hysteresis	<3°
VN2> pick-up	Setting+/-10%
VN2> drop-off	0.9 x Setting +/-10%
IN2> pick-up	Setting+/-10%
IN2> drop-off	0.9 x Setting +/-10%

23.3.6 SENSITIVE EARTH FAULT PROTECTION

IDMT pick-up	1.05 x Setting +/-5%
DT Pick-up	Setting +/- 5%
Drop-off (IDMT + DT)	0.95 x Setting +/-5%
IDMT operate	+/- 5% or 70 ms, whichever is greater (1.05 - 2) Is +/- 5% or 40 ms, whichever is greater (2 - 20) Is
DT operate	+/- 2% or 70 ms, whichever is greater (1.05 - 2) Is +/- 2% or 50 ms, whichever is greater (2 - 20) Is
DT reset	Setting +/- 5% or 50 ms, whichever is greater
Repeatability	< 5%

Note:
SEF claims apply to SEF input currents of no more than 2 x In. For input ranges above 2 x In, the claim is not supported.

23.3.6.1 SENSITIVE EARTH FAULT PROTECTION DIRECTIONAL ELEMENT

Wattmetric SEF	
Pick-up P = 0 W	ISEF > +/-5% or 5 mA

Wattmetric SEF	
Pick-up P > 0 W	P > +/-5%
Drop-off P = 0 W	0.95 x ISEF> +/- 5% or 5 mA
Drop-off P > 0 W	0.9 x P> +/- 5% or 5 mA
Boundary accuracy	+/-5% with hysteresis < 1°
Repeatability	< 1%

23.3.7 RESTRICTED EARTH FAULT PROTECTION

Low Impedance REF	
Pick-up	Setting formula +/- 5%
Drop-off	0.8 x Setting formula +/-5%
Operating time	<60 ms
Repeatability	<5%

High Impedance REF	
High set pick-up	Setting +/-10%
High set operating time	<30 ms
Repeatability	<5%

23.3.8 NEGATIVE SEQUENCE OVERCURRENT PROTECTION

IDMT pick-up	1.05 x Setting +/-5%
DT pick-up	Setting +/-5%
Drop-off (IDMT and DT)	0.95 x Setting +/-5%
IDMT operate time	+/-5% or 40 ms, whichever is greater *
DT operate time	+/-2% or 60 ms, whichever is greater **
DT Reset time	Setting +/-5%

23.3.8.1 NEGATIVE SEQUENCE OVERCURRENT PROTECTION DIRECTIONAL PARAMETERS

Directional boundary pick-up (RCA+/-90%)	+/-2° ◆
Directional boundary hysteresis	<1°
Directional boundary repeatability	<1%

23.3.9 CIRCUIT BREAKER FAIL AND UNDERCURRENT PROTECTION

I< Pick-up	Setting +/-10% or 0.025 In, whichever is greater
I< Drop-off	Setting +/-5% or 20 mA, whichever is greater
Operate time	<12 ms ‡

Timers	+/-2% or 20 ms, whichever is greater
Reset time	<15 ms

Note:
‡ Operating time measured with applied current of 20% above thermal setting.

23.3.10 BROKEN CONDUCTOR PROTECTION

Pick-up	Setting +/- 2.5%
Drop-off	0.95 x Setting +/- 2.5%
DT operate	+/- 2% or 40 ms, whichever is greater
Reset time	<25 ms

23.3.11 THERMAL OVERLOAD PROTECTION

Thermal alarm pick-up	Calculated trip time +/-10%
Thermal overload pick-up	Calculated trip time +/-10%
Cooling time accuracy	+/-15% of theoretical
Repeatability	<5%

Note:
*‡ **CS VT Ph Shift** setting = 0°.*
** Reference conditions: Injected value is 2 x pick-up value or more, effective range (0.1 - 20In).*
*** Reference conditions: Injected value instantaneously reduced to 0 (zero) from 2 x pick-up value.*
♦ Reference conditions: Tested with nominal voltage or current.

23.4 MONITORING, CONTROL AND SUPERVISION

23.4.1 VOLTAGE TRANSFORMER SUPERVISION

Fast block operation	< 1 cycle
Fast block reset	< 1.5 cycles
Time delay	+/- 2% or 20 ms, whichever is greater

23.4.2 STANDARD CURRENT TRANSFORMER SUPERVISION

IN> Pick-up	Setting +/-5%
VN< Pick-up	Setting +/-5%
IN> Drop-off	0.9 x setting +/-5%
VN< Drop-off	1.05 x setting +/-5% or 1 V, whichever is greater
Time delay operation	Setting +/-2% or 30 ms, whichever is greater
CTS block operation	<1 cycle
CTS reset	<35 ms

23.4.3 DIFFERENTIAL CURRENT TRANSFORMER SUPERVISION

Accuracy	
I1> Pick-up	Setting +/- 5%
I1> Drop-off	0.9 x setting +/- 5%
I2/I1> Pick-up	Setting +/- 5%
I2/I1> Drop-off	0.9 x setting +/-5%
I2/I1>> Pick-up	Setting +/- 5%
I2/I1 >> Drop-off	0.9 x setting +/-5%
Time delay operation	Setting +/-2% or 20 ms, whichever is greater
CTS block diff operation	<1 cycle
CTS reset	<35 ms

23.4.4 CB STATE AND CONDITION MONITORING

Accuracy	
Timers	+/-40 ms or 2%, whichever is greater
Broken current accuracy	+/-5%
Reset time	<30 ms

23.4.5 PSL TIMERS

Output conditioner timer	Setting +/-2% or 50 ms, whichever is greater
Dwell conditioner timer	Setting +/-2% or 50 ms, whichever is greater
Pulse conditioner timer	Setting +/-2% or 50 ms, whichever is greater

23.5 MEASUREMENTS AND RECORDING

23.5.1 GENERAL

General Measurement Accuracy	
Current (0.05 to 3 In)	+/-0.5% between 0.2 - 2 In Else +/-1.0% or 4mA whichever is greater (1A input) Else +/-1.0% or 20mA whichever is greater (5A input)
Voltage (0.05 to 2 Vn)	+/-0.5% between 0.2 - 2 Vn Else +/-1.0% or 100mV whichever is greater
Phase	+/-2° at rated voltage and current
Frequency (45 to 65 Hz)	+/-0.025 Hz
Power (W) (0.2 to 2 Vn and 0.05 to 3 In)	+/-5.0% of reading at unity power factor
Reactive power (Vars) (0.2 to 2 Vn and 0.05 to 3 In)	+/-5.0% of reading at zero power factor
Apparent power (VA) (0.2 to 2 Vn and 0.05 to 3 In)	+/-.0% of reading
Energy (Wh) (0.2 to 2 Vn and 0.2 to 3 In)	+/-5.0% of reading at unity power factor
Energy (Varh) (0.2 to 2 Vn and 0.2 to 3In)	+/-5.0% of reading at zero power factor

23.5.2 DISTURBANCE RECORDS

Disturbance Records Measurement Accuracy	
Minimum record duration	0.1 s
Maximum record duration	10.5 s
Minimum number of records at 10.5 seconds	100
Magnitude and relative phases accuracy	+/- 5% of applied quantities
Duration accuracy	+/- 2%
Trigger position accuracy	+/- 2% (minimum Trigger 100 ms)

23.5.3 EVENT, FAULT AND MAINTENANCE RECORDS

Event, Fault & Maintenance Records	
Record location	Supercapacitor backed memory
Viewing method	Front panel display or Settings Application Software
Extraction method	Extracted via the USB port
Number of Event records	Up to 1024 time tagged event records (newest overwrites oldest)
Number of Fault Records	Up to 15
Number of Maintenance Records	Up to 10
Event time stamp resolution	1 ms

23.5.4 FAULT LOCATOR

Accuracy	
Fault Location	+/-5% of line length Reference conditions: solid fault applied on line

23.6 RATINGS

23.6.1 AC MEASURING INPUTS

AC Measuring Inputs	
Nominal frequency	50 Hz or 60 Hz (settable)
Operating range	45 to 65 Hz
Phase rotation	ABC or CBA

23.6.2 CURRENT TRANSFORMER INPUTS

AC Current Inputs	
Nominal current (In)	1A or 5A
Nominal burden per phase	< 0.2 VA at 5A nominal < 0.04 VA at 1A nominal
AC current thermal withstand (5A input)	20 A (continuous operation) 150 A (for 10 s) 500 A (for 1 s)
AC current thermal withstand (1A input)	4 A (continuous operation) 30 A (for 10 s) 100 A (for 1 s)
Linearity	Linear up to 64 × In (non-offset)

23.6.3 VOLTAGE TRANSFORMER INPUTS

AC Voltage Inputs	
Nominal voltage (Vn)	100 V to 120 V (ph-ph)
Nominal burden per VT input *1	<0.003 VA @ 69.3 V (ph-n) <0.01 VA @ 138.6 V (ph-n)
Linearity for each VT input	Linear up to 200 Vac rms
Continuous rating for each VT input	240 Vac rms
10 seconds rating for each VT input	312 Vac rms

Note:
*Reference Conditions: * = Overfrequency operating range 50/60 Hz and over temperature range 20° +/-5°C.*

23.6.4 AUXILIARY SUPPLY VOLTAGE

Nominal operating range	CORTEC option (DC only) 24 to 48 V DC CORTEC option (rated for AC or DC operation) 48 to 110 V DC 40 to 100 V AC rms CORTEC option (rated for AC or DC operation) 110 to 250 V DC 100 to 240 V AC rms

Maximum operating range	CORTEC option (DC only) 19 to 65 V DC CORTEC option (rated for AC or DC operation) 37 to 150 V DC 32 to 110 V AC rms CORTEC option (rated for AC or DC operation) 87 to 300 V DC 80 to 265 V AC rms
Frequency range for AC supply	45 to 65 Hz
Ripple	<15% for a DC supply (compliant with IEC 60255-26:2013)
Power up time	<11 seconds

23.6.5 NOMINAL BURDEN

Quiescent burden	11 W or 22 VA
2nd rear communications port	1.25 W or 2.5 VA
Each relay output burden	0.13 W or 0.25 VA per output relay
Each opto-input burden (24 – 27 V)	0.065 W or 0.13 VA max
Each opto-input burden (30 – 34 V)	0.065 W or 0.13 VA max
Each opto-input burden (48 – 54 V)	0.125 W or 0.25 VA max
Each opto-input burden (110 – 125 V)	0.36 W or 0.72 VA max
Each opto-input burden (220 – 250 V)	0.9 W or 1.8 VA max

23.6.6 POWER SUPPLY INTERRUPTION

Standard	IEC 60255-26:2013 (DC and AC)
24 - 48V DC Supply 100% interruption without de-energising	20 ms at 24 V (half and full load) 50 ms at 36 V (half and full load) 100 ms at 48 V (half and full load)
48 - 110V DC Supply 100% interruption without de-energising	20 ms at 37 V (half and full load) 50 ms at 60 V (half and full load) 100 ms at 72 V (half load) 100 ms at 85 V (full load) 200 ms at 110 V (half and full load)
110 - 250V DC Supply 100% interruption without de-energising	20 ms at 87 V (half load) 50 ms at 110 V (half load) 50 ms at 98 V (full load) 100 ms at 160 V (half load) 100 ms at 135 V (full load) 200 ms at 210 V (half load) 200 ms at 174 V (full load)
40 - 100V AC Supply 100% voltage dip without de-energising	50 ms at 32 V (half load) 10 ms at 32 V (full load)
100 - 240V AC Supply 100% voltage dip without de-energising	50 ms at 80 V (full and half load)

Note:
Maximum loading = all inputs/outputs energised.
Quiescent or 1/2 loading = 1/2 of all inputs/outputs energised.

23.6.7 SUPERCAPACITOR

Discharge time	>14 days

23.7 INPUT/OUTPUT CONNECTIONS

23.7.1 ISOLATED DIGITAL INPUTS

Opto-isolated Digital Inputs (Opto-inputs)	
Compliance	ESI 48-4
Rated nominal voltage	24 to 250 V dc
Operating range	19 to 265 V dc
Withstand	300 V dc
Recognition time with half-cycle ac immunity filter removed	<2 ms
Recognition time with filter on	<12 ms

23.7.1.1 NOMINAL PICKUP AND RESET THRESHOLDS

Nominal Battery Voltage	Logic Levels: 60-80% DO/PU	Logic Levels: 50-70% DO/PU
24/27 V	Logic 0 <16.2 V, Logic 1 >19.2 V	Logic 0 <12 V, Logic 1 >16.8 V
30/34	Logic 0 <20.4 V, Logic 1 >24 V	Logic 0 <15 V, Logic 1 >21 V
48/54	Logic 0 <32.4 V, Logic 1 >38.4 V	Logic 0 <24 V, Logic 1 >33.6 V
110/125	Logic 0 <75 V, Logic 1 >88 V	Logic 0 <55 V, Logic 1 >77 V
220/250	Logic 0 <150 V, Logic 1 >176 V	Logic 0 <110 V, Logic 1 >154 V

Note:
Filter is required to make the opto-inputs immune to induced AC voltages.

In addition to the above thresholds, some models of this product provide the following threshold levels for FSK applications:

- For 220/250 voltage inputs: Logic 0 < 145V, Logic 1 > 165V

23.7.2 STANDARD OUTPUT CONTACTS

Compliance	In accordance with IEC 60255-1:2009
Use	General purpose relay outputs for signalling, tripping and alarming
Rated voltage	300 V
Maximum continuous current	10 A
Short duration withstand carry	30 A for 3 s 250 A for 30 ms
Make and break, dc resistive	50 W
Make and break, dc inductive	62.5 W (L/R = 50 ms)
Make and break, ac resistive	2500 VA resistive (cos phi = unity)
Make and break, ac inductive	2500 VA inductive (cos phi = 0.7)
Make and carry, dc resistive	30 A for 3 s, 10000 operations (subject to a maximum load of 7500W))
Make, carry and break, dc resistive	4 A for 1.5 s, 10000 operations (subject to the above limit for make and break, dc resistive load)

Make, carry and break, dc inductive	0.5 A for 1 s, 10000 operations (subject to the above limit for make and break, dc inductive load)
Make, carry and break ac resistive	30 A for 200 ms, 2000 operations (subject to the above limits)
Make, carry and break ac inductive	10 A for 1.5 s, 10000 operations (subject to the above limits)
Loaded contact	10000 operations min.
Unloaded contact	100000 operations min.
Operate time	<5 ms
Reset time	<10 ms

23.7.3 HIGH BREAK OUTPUT CONTACTS

Compliance	In accordance with IEC 60255-1:2009
Use	For applications requiring high rupture capacity
Rated voltage	300 V
Maximum continuous current	10 A DC
Short duration withstand carry	30 A DC for 3 s 250 A for 30 ms
Make and break, dc resistive	7500 W
Make and break, dc inductive	2500 W (L/R = 50 ms)
Make and carry, dc resistive	30 A for 3 s, 10000 operations (subject to the above limits)
Make, carry and break, dc resistive	30 A for 3 s, 5000 operations (subject to the above limit for make and break, dc resistive load) 30 A for 200 ms, 10000 operations (subject to the above limit for make and break, dc resistive load)
Make, carry and break, dc inductive	10 A for 40 ms, 10000 operations (subject to the above limit for make and break, dc inductive load) 10 A for 20 ms (250 V, 4 shots per second, subject to the above limit for make and break, dc inductive load)
Loaded contact	10,000 operations minimum.
Unloaded contact	100,000 operations minimum.
Operate time	<0.2 ms
Reset time	<8 ms
MOV Protection	Maximum voltage 330 V DC

23.7.4 WATCHDOG CONTACTS

Use	Non-programmable contacts for relay healthy/relay fail indication
Breaking capacity, dc resistive	30 W
Breaking capacity, dc inductive	15 W (L/R = 40 ms)
Breaking capacity, ac inductive	375 VA inductive (cos phi = 0.7)

23.8 MECHANICAL SPECIFICATIONS

23.8.1 PHYSICAL PARAMETERS

Case Types*	40TE 60TE 80TE
Weight (40TE case)	7 kg - 8 kg (depending on chosen options)
Weight (60TE case)	9 kg - 12 kg (depending on chosen options)
Weight (80TE case)	13 kg - 16 kg (depending on chosen options)
Dimensions in mm (w x h x l) (40TE case)	W: 206.0 mm H: 177.0 mm D: 243.1 mm
Dimensions in mm (w x h x l) (60TE case)	W: 309.6 mm H: 177.0 mm D: 243.1 mm
Dimensions in mm (w x h x l) (80TE case)	W 413.2 mm H 177.0 mm D 243.1 mm
Mounting	Panel, rack, or retrofit

Note:
** Case size is product dependent.*

23.8.2 ENCLOSURE PROTECTION

Against dust and dripping water (front face)	IP52 as per IEC 60529:1989/A2:2013
Protection against dust (whole case)	IP50 as per IEC 60529:1989/A2:2013
Protection for sides of the case (safety)	IP30 as per IEC 60529:1989/A2:2013
Protection for rear of the case (safety)	IP10 as per IEC 60529:1989/A2:2013

23.8.3 MECHANICAL ROBUSTNESS

Vibration test per EN 60255-21-1:1998	Response: class 2, Endurance: class 2
Shock and bump immunity per EN 60255-21-2:1988	Shock response: class 2, Shock withstand: class 1, Bump withstand: class 1
Seismic test per EN 60255-21-3: 1993	Class 2

23.8.4 TRANSIT PACKAGING PERFORMANCE

Primary packaging carton protection	ISTA 1C
Vibration tests	3 orientations, 7 Hz, amplitude 5.3 mm, acceleration 1.05g
Drop tests	10 drops from 610 mm height on multiple carton faces, edges and corners

23.9 TYPE TESTS

23.9.1 INSULATION

Compliance	IEC 60255-27: 2013
Insulation resistance	>100 M ohm at 500 V DC (Using only electronic/brushless insulation tester)

23.9.2 CREEPAGE DISTANCES AND CLEARANCES

Compliance	IEC 60255-27: 2013
Pollution degree	3
Overvoltage category	III
Impulse test voltage (not RJ45)	5 kV
Impulse test voltage (RJ45)	1 kV

23.9.3 HIGH VOLTAGE (DIELECTRIC) WITHSTAND

IEC compliance	IEC 60255-27: 2013
Between all independent circuits	2 kV ac rms for 1 minute
Between independent circuits and protective earth conductor terminal	2 kV ac rms for 1 minute
Between all case terminals and the case earth	2 kV ac rms for 1 minute
Across open watchdog contacts	1 kV ac rms for 1 minute
Across open contacts of changeover output relays	1 kV ac rms for 1 minute
Between all RJ45 contacts and protective earth	1 kV ac rms for 1 minute
Between all screw-type EIA(RS)485 contacts and protective earth	1 kV ac rms for 1 minute
ANSI/IEEE compliance	ANSI/IEEE C37.90-2005
Across open contacts of normally open output relays	1.5 kV ac rms for 1 minute
Across open contacts of normally open changeover output relays	1 kV ac rms for 1 minute
Across open watchdog contacts	1 kV ac rms for 1 minute

23.9.4 IMPULSE VOLTAGE WITHSTAND TEST

Compliance	IEC 60255-27: 2013
Between all independent circuits	Front time: 1.2 µs, Time to half-value: 50 µs, Peak value: 5 kV, 0.5 J
Between terminals of all independent circuits	Front time: 1.2 µs, Time to half-value: 50 µs, Peak value: 5 kV, 0.5 J
Between all independent circuits and protective earth conductor terminal	Front time: 1.2 µs, Time to half-value: 50 µs, Peak value: 5 kV, 0.5 J

Note:
Exceptions are communications ports and normally-open output contacts, where applicable.

23.10 ENVIRONMENTAL CONDITIONS

23.10.1 AMBIENT TEMPERATURE RANGE

Compliance	IEC 60255-27: 2013
Test method	IEC 60068-2-1:2007 and IEC 60068-2-2 2007
Operating temperature range	-25°C to +55°C (continuous)
Storage and transit temperature range	-25°C to +70°C (continuous)

23.10.2 TEMPERATURE ENDURANCE TEST

Temperature Endurance Test	
Test method	IEC 60068-2-1: 2007 and 60068-2-2: 2007
Operating temperature range	-40°C (96 hours) +70°C (96 hours)
Storage and transit temperature range	-40°C (96 hours) +70°C (96 hours)

23.10.3 AMBIENT HUMIDITY RANGE

Compliance	IEC 60068-2-78: 2012 and IEC 60068-2-30: 2005
Durability	56 days at 93% relative humidity and +40°C
Damp heat cyclic	Six (12 + 12) hour cycles, 93% RH, +25 to +55°C

23.10.4 CORROSIVE ENVIRONMENTS

Compliance, Industrial corrosive environment/poor environmental control	IEC 60068-2-42:2003, IEC 60068-2-43:2003, IEC 60068-2-52:1996
Sulphur Dioxide, IEC 60068-2-42:2003	21 days exposure to elevated concentrations (25ppm) of SO_2 at 75% relative humidity and +25°C
Hydrogen Sulphide, IEC 60068-2-43:2003	21 days exposure to elevated concentrations (10ppm) of H_2S at 75% relative humidity and +25°C
Salt Mist, IEC 60068-2-52:1996	7 days, KB severity 3

23.11 ELECTROMAGNETIC COMPATIBILITY

23.11.1 1 MHZ BURST HIGH FREQUENCY DISTURBANCE TEST

Compliance	IEC 60255-26:2013
Common-mode test voltage (level 3)	2.5 kV
Differential test voltage (level 3)	1.0 kV

23.11.2 DAMPED OSCILLATORY TEST

Compliance	EN61000-4-18: 2011: Level 3, 100 kHz and 1 MHz. Level 4: 3 MHz, 10 MHz and 30 MHz, IEC 60255-26:2013
Common-mode test voltage (level 3)	2.5 kV
Common-mode test voltage (level 4)	4.0 kV
Differential mode test voltage	1.0 kV

23.11.3 IMMUNITY TO ELECTROSTATIC DISCHARGE

Compliance	IEC 60255-26:2013, IEC 61000-4-2:2009
Class 4 Condition	15 kV discharge in air to user interface, display, and exposed metalwork
Class 3 Condition	8 kV discharge in air to all communication ports

23.11.4 ELECTRICAL FAST TRANSIENT OR BURST REQUIREMENTS

Compliance	IEC 60255-26:2013, IEC 61000-4-4:2012
Applied to communication inputs	Amplitude: 2 kV, burst frequency 5 kHz and 100 KHz (level 4)
Applied to power supply and all other inputs except for communication inputs	Amplitude: 4 kV, burst frequency 5 kHz and 100 KHz (level 4)

23.11.5 SURGE WITHSTAND CAPABILITY

Compliance	IEEE/ANSI C37.90.1: 2012
Condition 1	4 kV fast transient and 2.5 kV oscillatory applied common mode and differential mode to opto inputs, output relays, CTs, VTs, power supply
Condition 2	4 kV fast transient and 2.5 kV oscillatory applied common mode to communications, IRIG-B

23.11.6 SURGE IMMUNITY TEST

Compliance	IEC 60255-26:2013, IEC 61000-4-5:2014 + AMD1:2017

Pulse duration	Time to half-value: 1.2/50 µs
Between all groups and protective earth conductor terminal	Amplitude 4 kV
Between terminals of each group (excluding communications ports, where applicable)	Amplitude 2 kV

23.11.7 IMMUNITY TO RADIATED ELECTROMAGNETIC ENERGY

Compliance	IEC 60255-26:2013, IEC 61000-4-3:2006 + A2:2010
Frequency band	80 MHz to 3.0 GHz
Spot tests at	80, 160, 380, 450, 900, 1850, 2150 MHz
Test field strength	10 V/m
Test using AM	1 kHz @ 80%
Compliance	IEEE/ANSI C37.90.2: 2004
Frequency band	80 MHz to 1 GHz
Spot tests at	80, 160, 380, 450 MHz
Waveform	1 kHz @ 80% am and pulse modulated
Field strength	35 V/m

23.11.8 RADIATED IMMUNITY FROM DIGITAL COMMUNICATIONS

Compliance	IEC 61000-4-3:2006 + A2:2010
Frequency bands	800 to 960 MHz, 1.4 to 2.0 GHz
Test field strength	30 V/m
Test using AM	1 kHz/80%

23.11.9 RADIATED IMMUNITY FROM DIGITAL RADIO TELEPHONES

Compliance	IEC 60255-26:2013, IEC 61000-4-3:2006 + A2:2010
Frequency bands	900 MHz and 1.89 GHz
Test field strength	10 V/m

23.11.10 IMMUNITY TO CONDUCTED DISTURBANCES INDUCED BY RADIO FREQUENCY FIELDS

Compliance	IEC 60255-26:2013, IEC 61000-4-6:2013 Level 3
Frequency bands	150 kHz to 80 MHz
Test disturbance voltage	10 V rms
Test using AM	1 kHz @ 80%
Spot tests	27 MHz and 68 MHz

23.11.11 MAGNETIC FIELD IMMUNITY

Compliance	IEC 61000-4-8:2009 Level 5 IEC 61000-4-9:2016 Level 5 IEC 61000-4-10:2016 Level 5
IEC 61000-4-8 test	100 A/m applied continuously, 1000 A/m applied for 3 s
IEC 61000-4-9 test	1000 A/m applied in all planes
IEC 61000-4-10 test	100 A/m applied in all planes at 100 kHz/1 MHz with a burst duration of 2 seconds

23.11.12 CONDUCTED EMISSIONS

Compliance	IEC 60255-26:2013, EN 55032: 2015 + A1:2020
Power supply test 1	0.15 - 0.5 MHz, 79 dBµV (quasi peak) 66 dBµV (average)
Power supply test 2	0.5 - 30 MHz, 73 dBµV (quasi peak) 60 dBµV (average)
RJ45 test 1 (where applicable)	0.15 - 0.5 MHz, 97 dBµV (quasi peak) 84 dBµV (average)
RJ45 test 2 (where applicable)	0.5 - 30 MHz, 87 dBµV (quasi peak) 74 dBµV (average)

23.11.13 RADIATED EMISSIONS

Compliance	IEC 60255-26:2013
Test 1	30 - 230 MHz, 40 dBµV/m at 10 m measurement distance
Test 2	230 - 1 GHz, 47 dBµV/m at 10 m measurement distance
Test 3	1 - 2 GHz, 76 dBµV/m at 10 m measurement distance

23.11.14 POWER FREQUENCY

Compliance	IEC 60255-26:2013
Opto-inputs (compliance is achieved using the opto-input filter)	300 V common-mode (Class A) 150 V differential mode (Class A)

Note:
Compliance is achieved using the opto-input filter.

23.12 REGULATORY COMPLIANCE

Compliance with the European Commission Directive on EMC and LVD is demonstrated using a technical file.

CE

23.12.1 EMC COMPLIANCE: 2014/30/EU

The product specific Declaration of Conformity (DoC) lists the relevant harmonised standard(s) or conformity assessment used to demonstrate compliance with the EMC directive.

23.12.2 LVD COMPLIANCE: 2014/35/EU

The product specific Declaration of Conformity (DoC) lists the relevant harmonised standard(s) or conformity assessment used to demonstrate compliance with the LVD directive.

Safety related information, such as the installation I overvoltage category, pollution degree and operating temperature ranges are specified in the Technical Data section of the relevant product documentation and/or on the product labelling.

Unless otherwise stated in the Technical Data section of the relevant product documentation, the equipment is intended for indoor use only. Where the equipment is required for use in an outdoor location, it must be mounted in a specific cabinet or housing to provide the equipment with the appropriate level of protection from the expected outdoor environment.

23.12.3 R&TTE COMPLIANCE: 2014/53/EU

Radio and Telecommunications Terminal Equipment (R&TTE) directive 2014/53/EU.

Conformity is demonstrated by compliance to both the EMC directive and the Low Voltage directive, to zero volts.

23.12.4 UL/CUL COMPLIANCE

If marked with this logo, the product is compliant with the requirements of the Canadian and USA Underwriters Laboratories.

The relevant UL file number and ID is shown on the equipment.

c UL us

APPENDIX A

ORDERING OPTIONS

Ordering Information

| Variants Order No. | | |

Variants Order No.														
Current Differential - 40TE with 3 Pole Autoreclose and Check Synchronising (up to 6 Ends Application)		**P54B**										**		
Nominal auxiliary voltage														
24-54 Vdc			7											
48-125 Vdc (40-100 Vac)			8											
110-250 Vdc (100-240 Vac)			9											
In/Vn Rating														
In = 1A/5A ; Vn = 100-120Vac				1										
Hardware Options	**Protocol Compatibilty**													
Standard - None	1, 3 & 4				1									
IRIG-B Only (Modulated)	1, 3 & 4				2									
IRIG-B (Modulated) & Fibre Optic Converter	1, 3 & 4				4									
Ethernet (100Mbit/s)	1, 3 & 4				6									
Second Rear Comms	1				7									
IRIG-B (Modulated) + Second Rear Comms	1				8									
Ethernet (100Mbit/s) plus IRIG-B (Modulated)	6, 7 & 8				A									
Ethernet (100Mbit/s) plus IRIG-B (Un-modulated)	6, 7 & 8				B									
InterMiCOM + Courier Rear Port + IRIG-B Modulated	1, 3 & 4				F									
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Modulated IRIG-B	6, 7 & 8				J									
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Un-modulated IRIG-B	6, 7 & 8				K									
***** For HSR - contact GE Vernova for details														
Product Options														
Ch1=850nm multi-mode, Ch2=850nm multi-mode, 8 Inputs and 8 Output Relays						A								
Ch1=1300nm single-mode, Ch2=not fitted (2 Terminal only), 8 Inputs and 8 Output Relays						B								
Ch1=1300nm single-mode, Ch2=1300nm single-mode, 8 Inputs and 8 Output Relays						C								
Ch1=1300nm multi-mode, Ch2=not fitted (2 Terminal only), 8 Inputs and 8 Output Relays						D								
Ch1=1300nm multi-mode, Ch2=1300nm multi-mode, 8 Inputs and 8 Output Relays						E								
Ch1=1550nm single-mode, Ch2=not fitted (2 Terminal only), 8 Inputs and 8 Output Relays						F								
Ch1=1550nm single-mode, Ch2=1550nm single-mode, 8 Inputs and 8 Output Relays						G								
Ch1=850nm multi-mode, Ch2=1300nm single-mode, 8 Inputs and 8 Output Relays						H								
Ch1=850nm multi-mode, Ch2=1300nm multi-mode, 8 Inputs and 8 Output Relays						J								
Ch1=850nm multi-mode, Ch2=1550nm single-mode, 8 Inputs and 8 Output Relays						K								
Ch1=1300nm single-mode, Ch2=850nm multi-mode, 8 Inputs and 8 Output Relays						L								
Ch1=1300nm multi-mode, Ch2=850nm multi-mode, 8 Inputs and 8 Output Relays						M								
Reserved for future single channel						N								
Reserved for future single channel						P								
Ch1 1550nm single-mode, Ch2 850nm multi-mode, 8 Inputs and 8 Output Relays						R								
Protocol Options														
K-Bus							1							
IEC60870-5-103 (VDEW)							3							
DNP3.0							4							
IEC61850 + Courier via rear RS485 port							6							
IEC61850 + IEC60870-5-103 via rear RS485 port							7							
DNP3.0 Over Ethernet with courier rear port K-Bus/RS485 protocol							8							
Mounting								S						
Flush/Panel Mounting with Harsh Env. Coating, with USB Port, Black and Silver Front Panel								S						
Flush/Panel Mounting with Harsh Environment Coating								P						
Language									0					
English, French, German, Spanish									0					
English, French, German, Italian (not yet available!)									4					
English, French, German, Russian									5					
English, Italian, Polish and Portuguese									7					
* Design Suffix G, J, K & M only														
** Design Suffix K and M with 42/52 software and later only														
*** Design Suffx M with 65/66/75/76 software														
Software Version												01		
Without Distance												01		
With Distance **(not on first release)**														
Customer Specific Options													0	
Standard version													0	
Customer version													A	
Hardware Version														P
CPU3 with increased main processor memory														P

Variants Order No.														
Current Differential - 60TE with 1/3 Pole Autoreclose and Check Synchronising (up to 6 Ends Application)	**P54C**											**		
Nominal Auxiliary Voltage														
24-54 Vdc		7												
48-125 Vdc (40-100 Vac)		8												
110-250 Vdc (100-240 Vac)		9												
In/Vn Rating														
In = 1A/5A ; Vn = 100-120Vac			1											

Hardware Options	**Protocol Compatibilty**													
Standard - None	1, 3 & 4			1										
IRIG-B Only (Modulated)	1, 3 & 4			2										
IRIG-B (Modulated) & Fibre Optic Converter	1, 3 & 4			4										
Ethernet (100Mbit/s)	1, 3 & 4			6										
Second Rear Comms	1			7										
IRIG-B (Modulated) + Second Rear Comms	1			8										
Ethernet (100Mbit/s) plus IRIG-B (Modulated)	6, 7 & 8			A										
Ethernet (100Mbit/s) plus IRIG-B (Un-modulated)	6, 7 & 8			B										
InterMiCOM + Courier Rear Port + IRIG-B Modulated	1, 3 & 4			F										
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Modulated IRIG-B	6, 7 & 8			J										
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Un-modulated IRIG-B	6, 7 & 8			K										
Single Ethernet 1 LC Duplex port + Universal IRIG-B + 1588	6 & 7			U										
Redundant Ethernet PRP/HSR/RSTP/Failover 2 RJ45 + Universal IRIG-B + 1588	6 & 7			W										
Redundant Ethernet PRP/HSR/RSTP/Failover 2 LC Duplex ports + Universal IRIG-B + 1588	6 & 7			Y										
***** For HSR - contact GE Vernova for details														

Product Options														
Ch1=850nm multi-mode, Ch2=850nm multi-mode, 16 Inputs and 16 Output Relays				A										
Ch1=1300nm single-mode, Ch2=not fitted (2 Terminal only), 16 Inputs and 16 Output Relays				B										
Ch1=1300nm single-mode, Ch2=1300nm single-mode, 16 Inputs and 16 Output Relays				C										
Ch1=1300nm multi-mode, Ch2=not fitted (2 Terminal only), 16 Inputs and 16 Output Relays				D										
Ch1=1300nm multi-mode, Ch2=1300nm multi-mode, 16 Inputs and 16 Output Relays				E										
Ch1=1550nm single-mode, Ch2=not fitted (2 Terminal only), 16 Inputs and 16 Output Relays				F										
Ch1=1550nm single-mode, Ch2=1550nm single-mode, 16 Inputs and 16 Output Relays				G										
Ch1=850nm multi-mode, Ch2=1300nm single-mode, 16 Inputs and 16 Output Relays				H										
Ch1=850nm multi-mode, Ch2=1300nm multi-mode, 16 Inputs and 16 Output Relays				J										
Ch1=850nm multi-mode, Ch2=1550nm single-mode, 16 Inputs and 16 Output Relays				K										
Ch1=1300nm single-mode, Ch2=850nm multi-mode, 16 Inputs and 16 Output Relays				L										
Ch1=1300nm multi-mode, Ch2=850nm multi-mode, 16 Inputs and 16 Output Relays				M										
Reserved for future single channel				N										
Reserved for future single channel				P										
Ch1=1550nm single-mode, Ch2 850nm multi-mode, 16 Inputs and 16 Output Relays				R										
Ch1=850nm multi-mode, Ch2=850nm multi-mode, 16 Inputs and 12 Outputs Relays (Including 4 High Break)				S										
Ch1=1300nm single-mode, Ch2=not fitted (2 Terminal only), 16 Inputs and 12 Output Relays (Including 4 High Break)				T										
Ch1=1300nm single-mode, Ch2=1300nm single mode, 16 Inputs and 12 Output Relays (Including 4 High Break)				U										
Ch1=1300nm multi-mode, Ch2=not fitted (2 Terminal only), 16 Inputs and 12 Output Relays (Including 4 High Break)				V										
Ch1=1300nm multi-mode, Ch2=1300nm multi-mode, 16 Inputs and 12 Output Relays (Including 4 High Break)				W										
Ch1=1550nm single-mode, Ch2=not fitted (2 Terminal only), 16 Inputs and 12 Output Relays (including 4 High Break)				X										
Reserved - was used for RWE special				Y										
Ch1=1550nm single-mode, Ch2=1550nm single-mode, 16 Inputs and 12 Output Relays (Including 4 High Break)				Z										
Ch1=850nm multi-mode, Ch2=1300nm single-mode, 16 Inputs and 12 Outputs (Including 4 High Break)				0										
Ch1=850nm multi-mode, Ch2=1300nm multi-mode, 16 Inputs and 12 Outputs (Including 4 High Break)				1										
Ch1=850nm multi-mode, Ch2=1550nm single-mode, 16 Inputs and 12 Output Relays (Including 4 High Break)				2										
Ch1=1300nm single-mode, Ch2=850nm multi-mode, 16 Inputs and 12 Output Relays (Including 4 High Break)				3										
Ch1=1300nm multi-mode, Ch2=850nm multi-mode, 16 Inputs and 12 Output Relays (Including 4 High Break)				4										
Ch1=1550nm single-mode, Ch2=850nm multi-mode, 16 Inputs and 12 Output Relays (Including 4 High Break)				5										
Reserved for future single channel				6										
Reserved for future single channel				7										
Protocol Options														
K-Bus					1									
IEC60870-5-103 (VDEW)					3									
DNP3.0					4									
IEC61850 + Courier via rear RS485 port					6									
IEC61850 + IEC60870-5-103 via rear RS485 port					7									
DNP3.0 Over Ethernet with courier rear port K-Bus/RS485 protocol					8									
Mounting														
Flush/Panel Mounting with Harsh Env. Coating, with USB Port, Black and Silver Front Panel						S								
Flush/Panel Mounting with Harsh Environment Coating						P								
Language														
English, French, German, Spanish							0							
English, French, German, Italian (not yet available!) English,							4							
French, German, Russian							5							
English, Italian, Polish and Portuguese							7							
* Design Suffix G, J, K & M only														
** Design Suffix K and M with 42/52 software and later only														
*** Design Suffx M with 65/66/75/76 software														
Software Version														
Without Distance												**		
With Distance **(not on first release)**														
Customer Specific Options														
Standard version													0	
Customer version													A	
Hardware Version														
XCPU3 with increased main processor memory														M

| Variants Order No. | | |

APPENDIX B

SETTINGS AND SIGNALS

Tables containing a full list of settings for each model are provided in a separate Excel file, attached as an embedded resource. If using Adobe Acrobat Reader, click on the button below to open the spreadsheet.

This manual must be opened with a PDF viewer capable of opening attachments, such as Adobe Acrobat Reader or Nitro PDF. If using Nitro PDF, attachments are shown in the attachment pane. To show or hide the attachments pane, look in the sidebar and click the attachments tab.

Note:
An Open File dialogue box may open with a warning message about potential harm from programs, macros or viruses. The file supplied does not contain any harmful content, and may be safely opened.

Settings and Signals_sw91

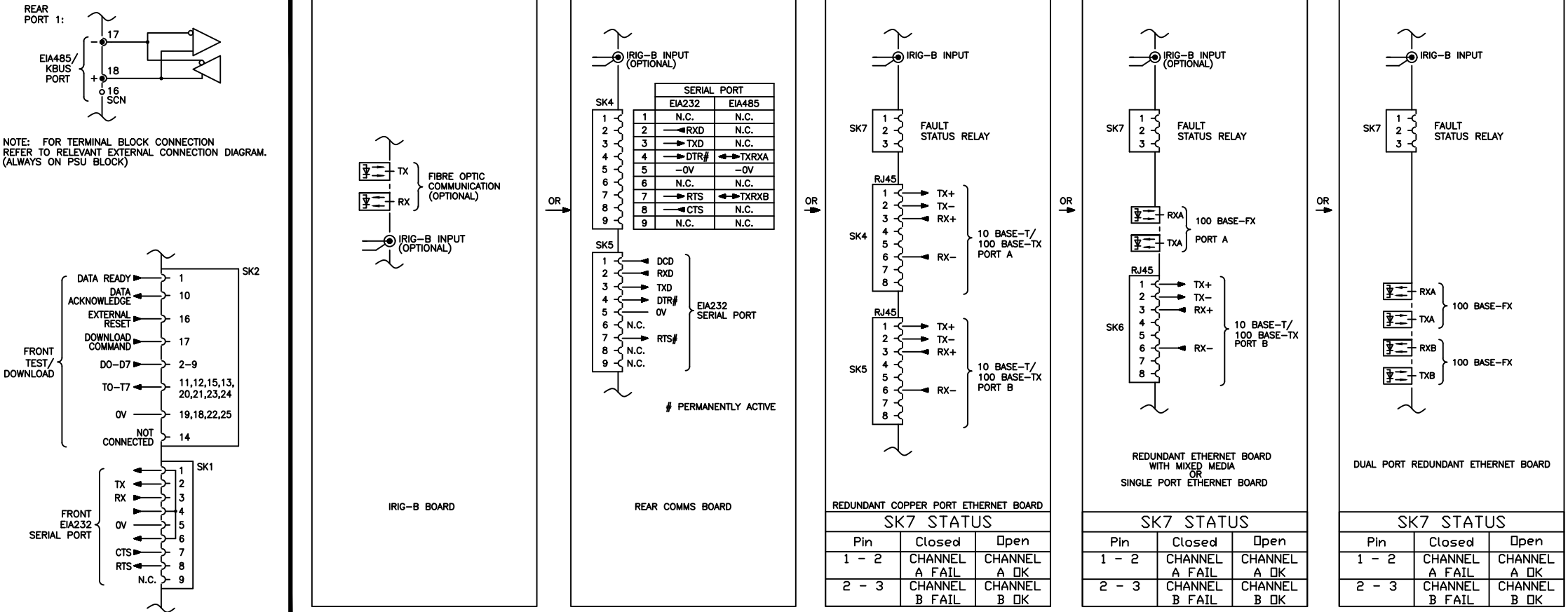
Settings and Signals_sw92

APPENDIX C

WIRING DIAGRAMS

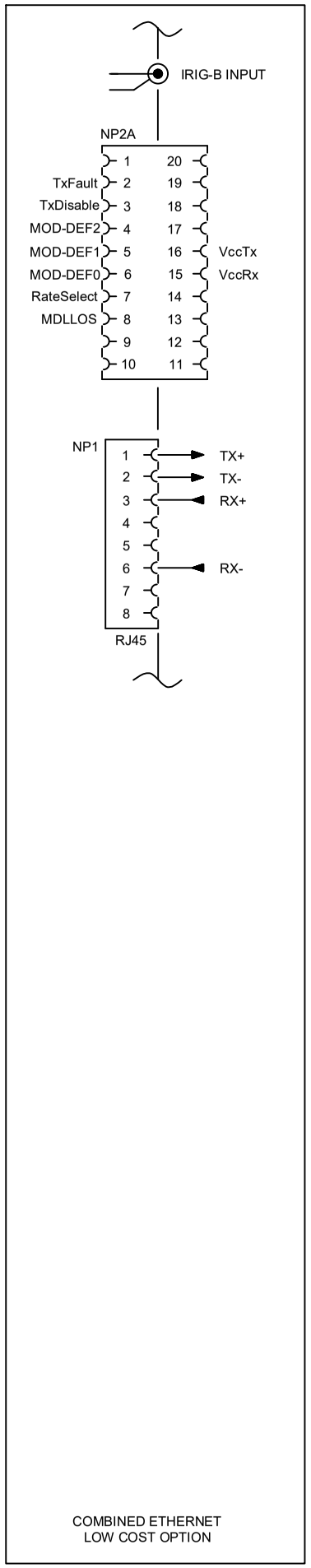
Model	CORTEC Option*	Input/Output Options and Case Size Compatibility	Drawing-Sheet	Issue
All	-	Comms Options MiCOM Px40 Platform	10Px4001-1 10Px4001-2	N B
P54A	A to R	Current Diff 1 Relay 8 Inputs, 8 Outputs (40TE)	10P54A01-1 10P54A01-2	E D
P54B	A to R	Current Diff 2 Relay 8 Inputs, 8 Outputs (40TE)	10P54B01-1 10P54A01-2	E D
P54C	A to R	Current Diff 2 Relay 16 Inputs, 16 Outputs & SEF (60TE)	10P54C01-1 10P54C01-2	E E
	S to Z, 0 to 5	Current Diff 3 Relay 16 Inputs, 12 Outputs + (4 High-Break) & SEF (60TE)	10P54C02-1 10P54C02-2	D E
P54E	S to Z, 0 to 5	Current Diff 2 Relay 24 Inputs, 24 Outputs + (8 High Break) & SEF (80TE)	10P54E01-1 10P54E01-2	E F
	A to H, J to M, R	Current Diff Relay 24 Inputs, 32 Outputs & SEF (80TE)	10P54E02-1 10P54E02-2	E D
	I, N to Q, 8 to 9	Current Diff Relay 32 Inputs, 32 Outputs & SEF (80TE)	10P54E03-1 10P54E03-2	D E

* When selecting the applicable wiring diagram(s), refer to the appropriate model CORTEC.

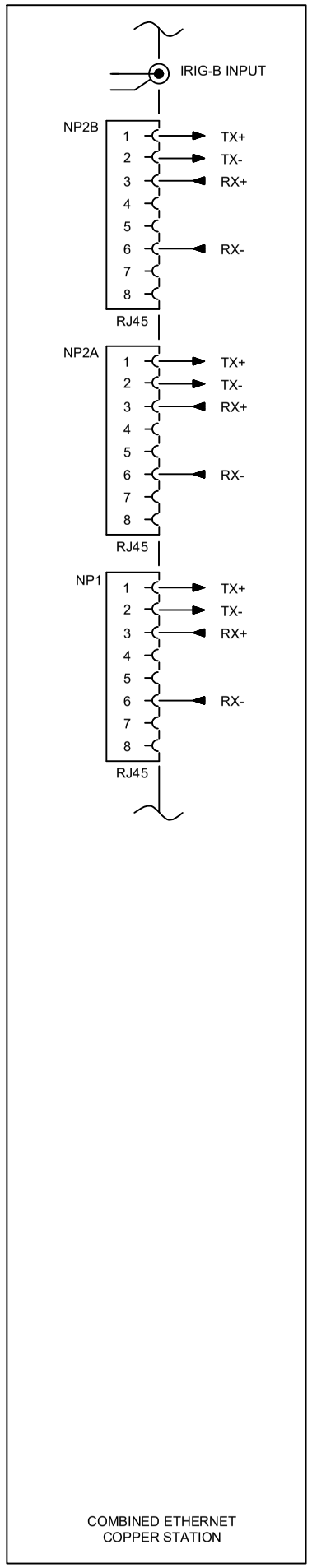


Issue: N	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: COMMS OPTIONS MICOM Px40 PLATFORM		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10PX4001**	PLM No: A20022917	Sht: 1
Date:	Chkd:				Next Sht: 2

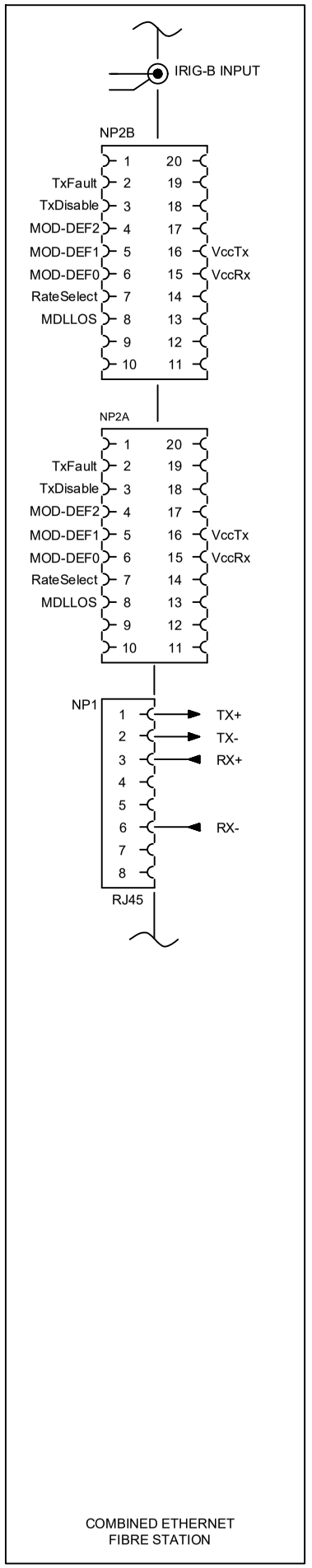
GE VERNOVA



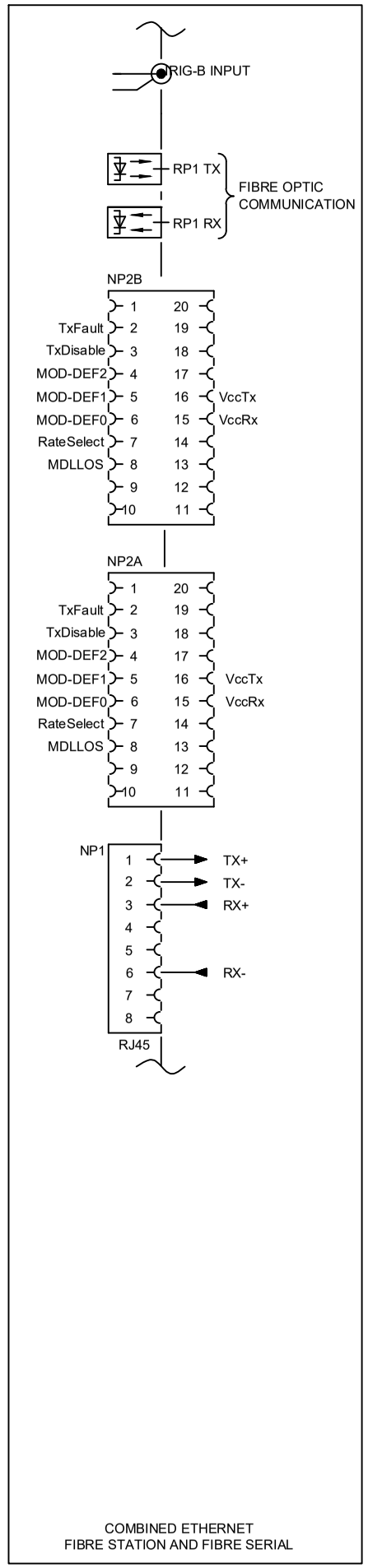
COMBINED ETHERNET
LOW COST OPTION



COMBINED ETHERNET
COPPER STATION

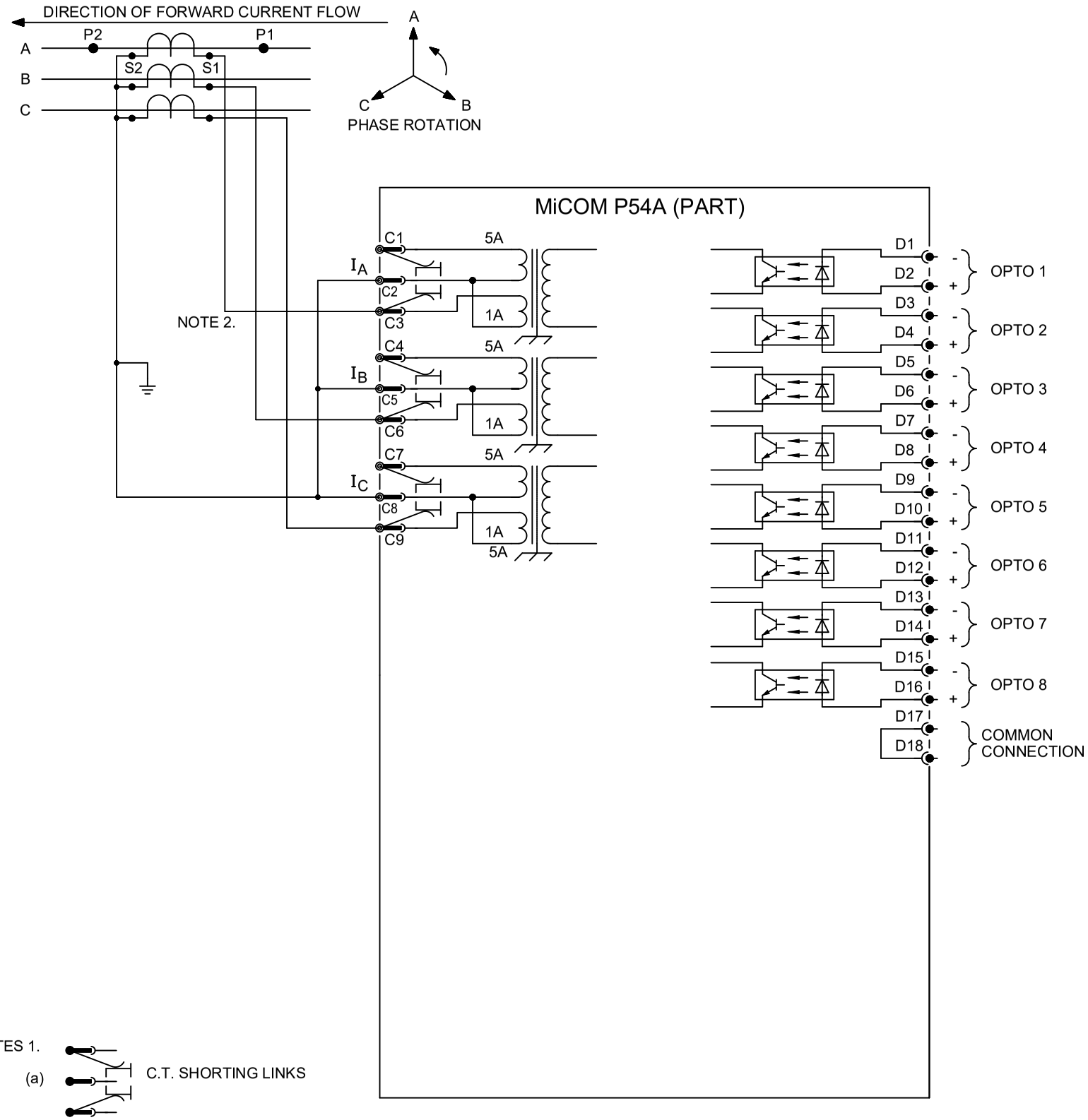


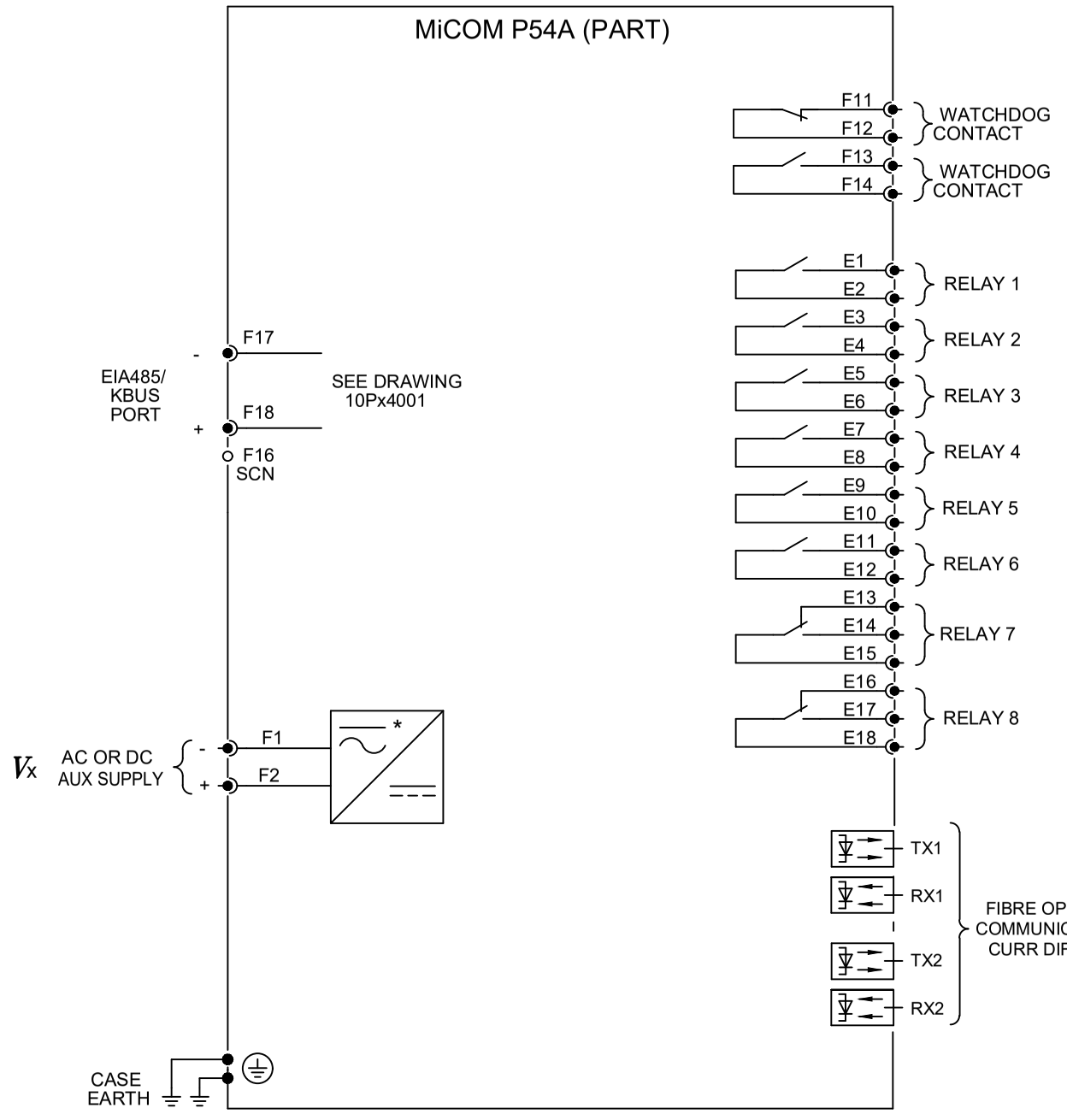
COMBINED ETHERNET
FIBRE STATION



COMBINED ETHERNET
FIBRE STATION AND FIBRE SERIAL

Issue: B	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM COMMS OPTIONS MICOM Px40			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10PX4001**	PLM No: A20095995	Sht: 2 Next Sht: -	GE VERNOVA
Date:	Chkd:					





* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

NOTES 1.

(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

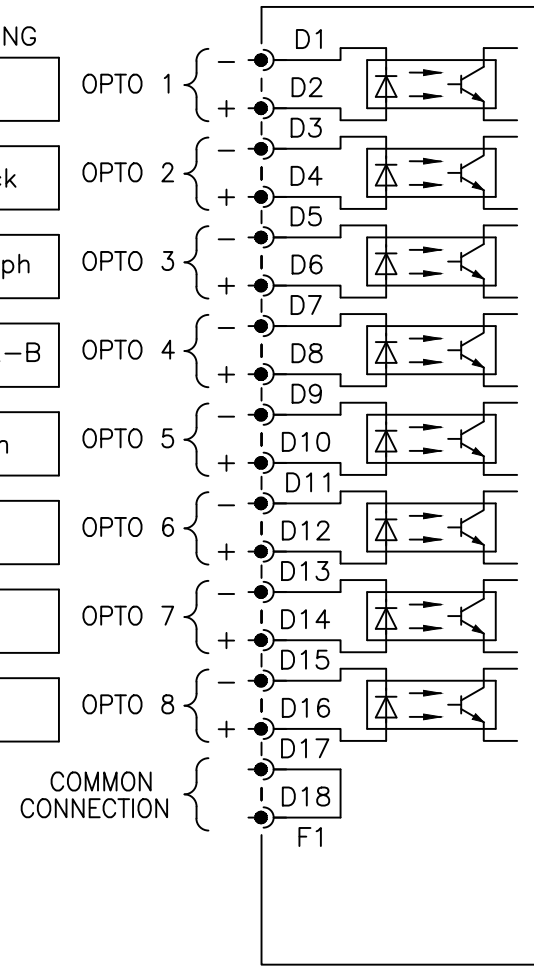
50 OHM BNC CONNECTOR

9-WAY & 25-WAY FEMALE D-TYPE SOCKET

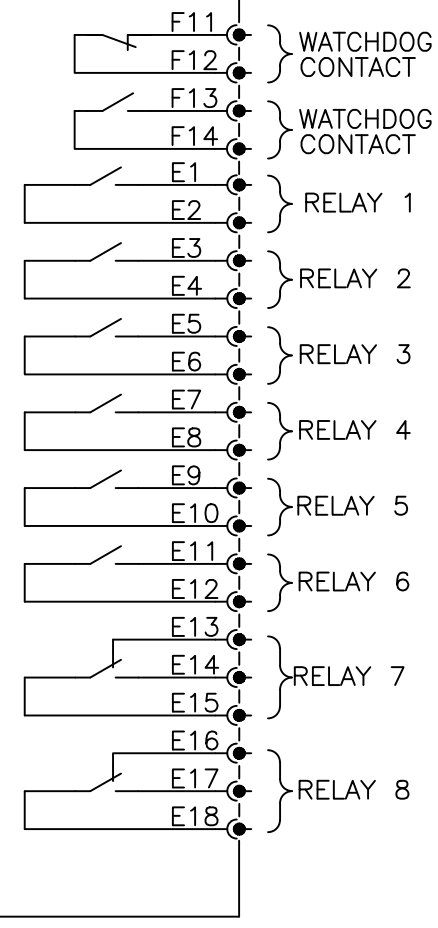
2. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
3. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 1 RELAY 8 INPUTS, 8 OUTPUTS (40TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54A01**	PLM No: A20065612	Sht: 1 Next Sht: 2	GE VERNOVA
Date:	Chkd:					

CUSTOMER SETTING	DEFAULT SETTING
	Inhibit Diff
	Recon Interlock
	External Trip 3ph
	CB Aux 3ph 52-B
	CB Close Man
	CB Healthy

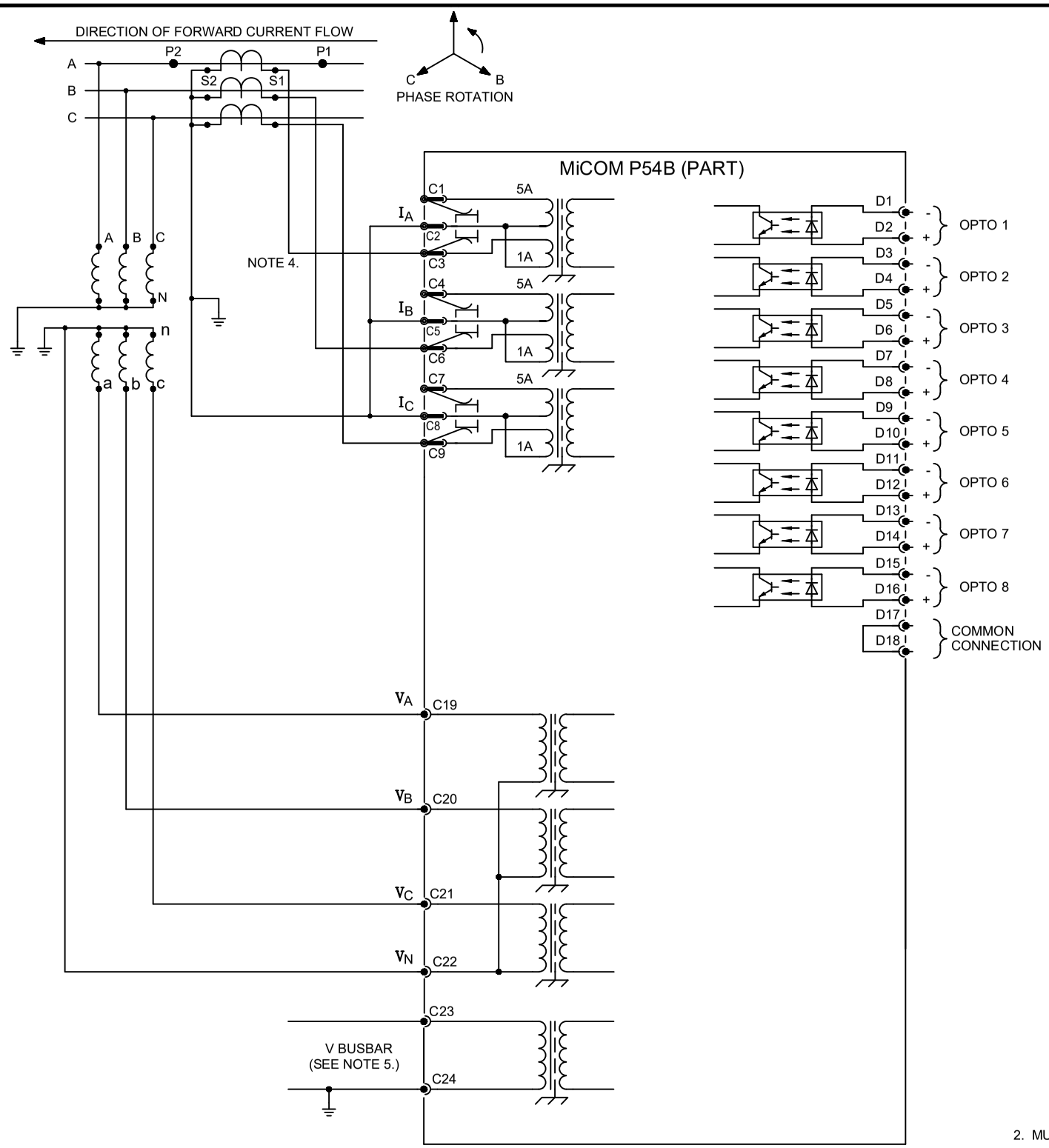


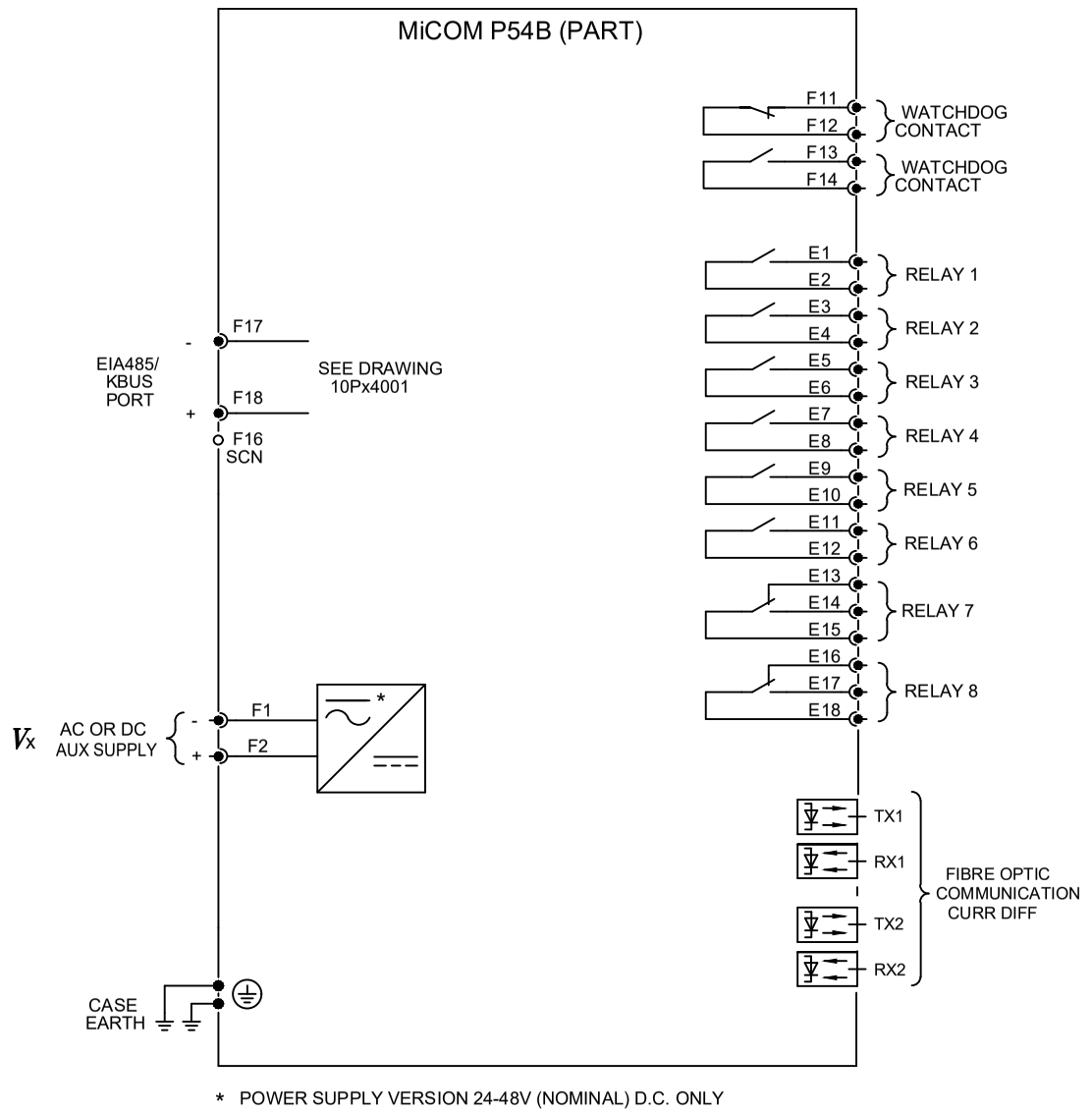
MiCOM P54A
(PART)



DEFAULT SETTING	CUSTOMER SETTING
Trip Diff	
SignalingFail	
Any trip	
General Alarm	
CB Fail Time 1	
Trip 3ph	

Issue: D	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 1 RELAY 8 INPUTS, 8 OUTPUTS (40TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54A01**	PLM No: A20065574	Sht: 2 / Next Sht: -
Date:	Chkd:				GE VERNOVA





* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

NOTES 1.

(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

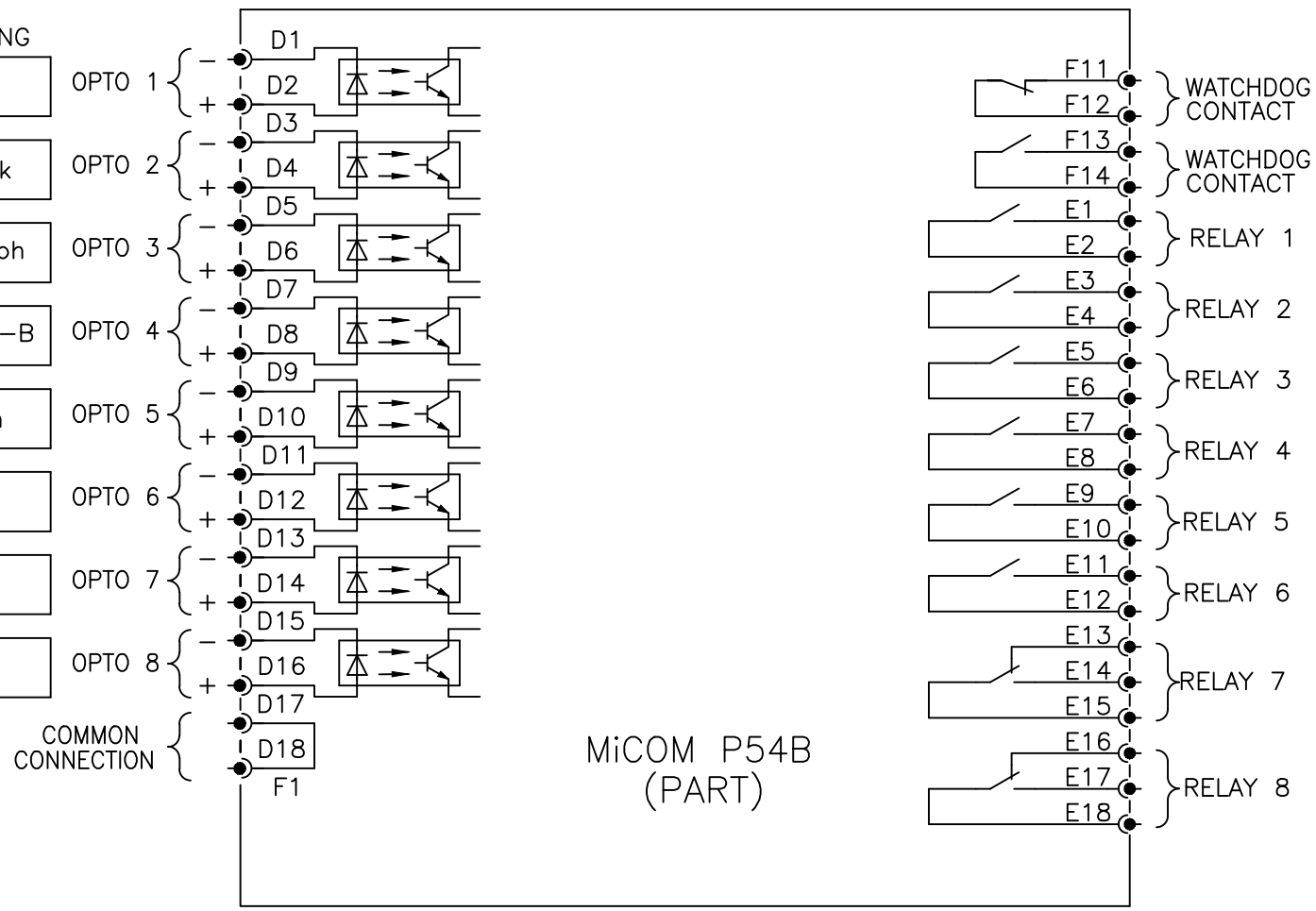
50 OHM BNC CONNECTOR

9-WAY & 25-WAY FEMALE D-TYPE SOCKET

2. MUTUAL CURRENT INPUT ONLY REQUIRED IF ENABLED IN FAULT LOCATOR.
3. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
4. FOR COMMS OPTIONS SEE DRAWING 10Px4001.
5. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.

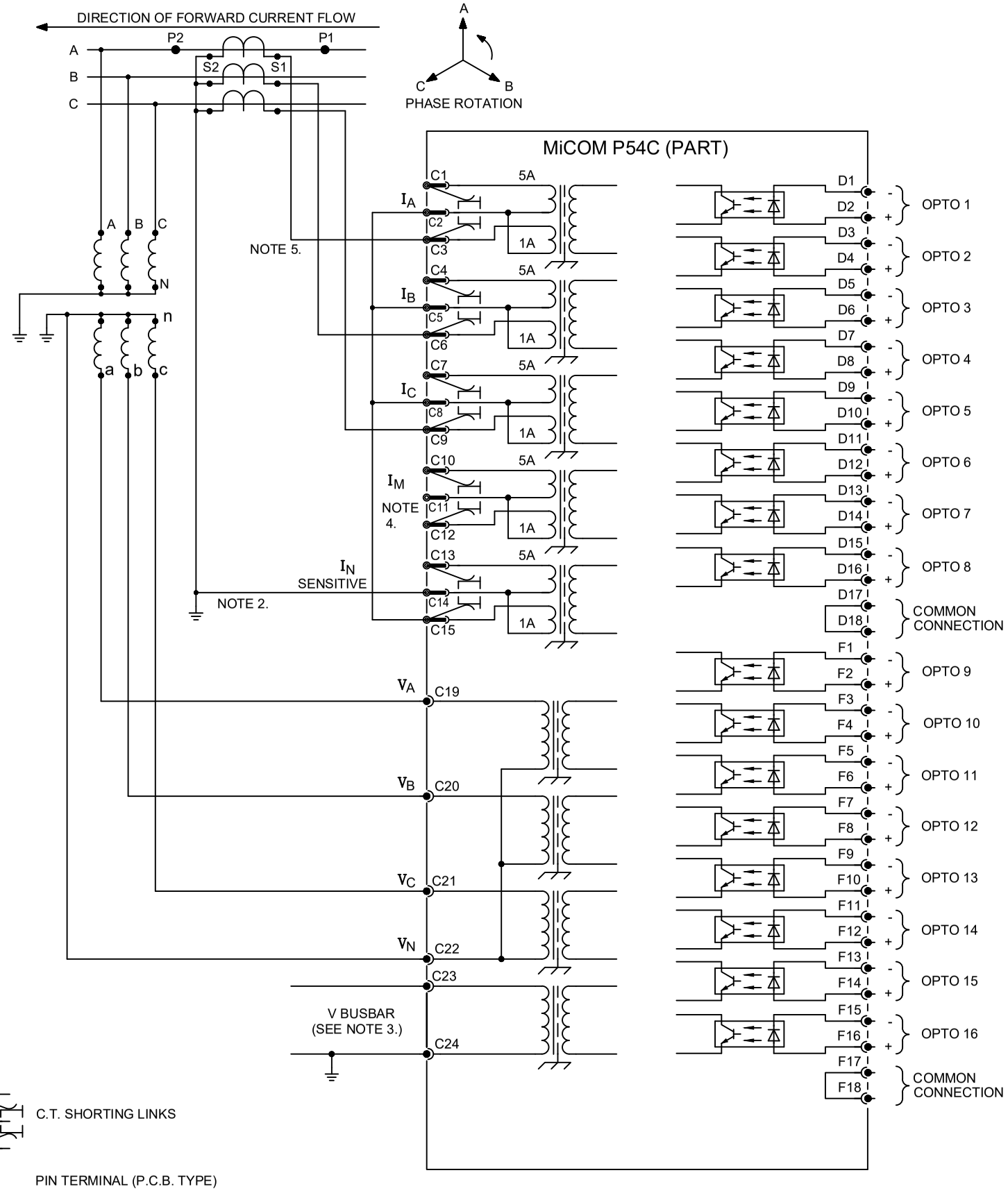
Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 2 RELAY 8 INPUTS, 8 OUTPUTS (40TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54B01**	PLM No: A20065393	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	

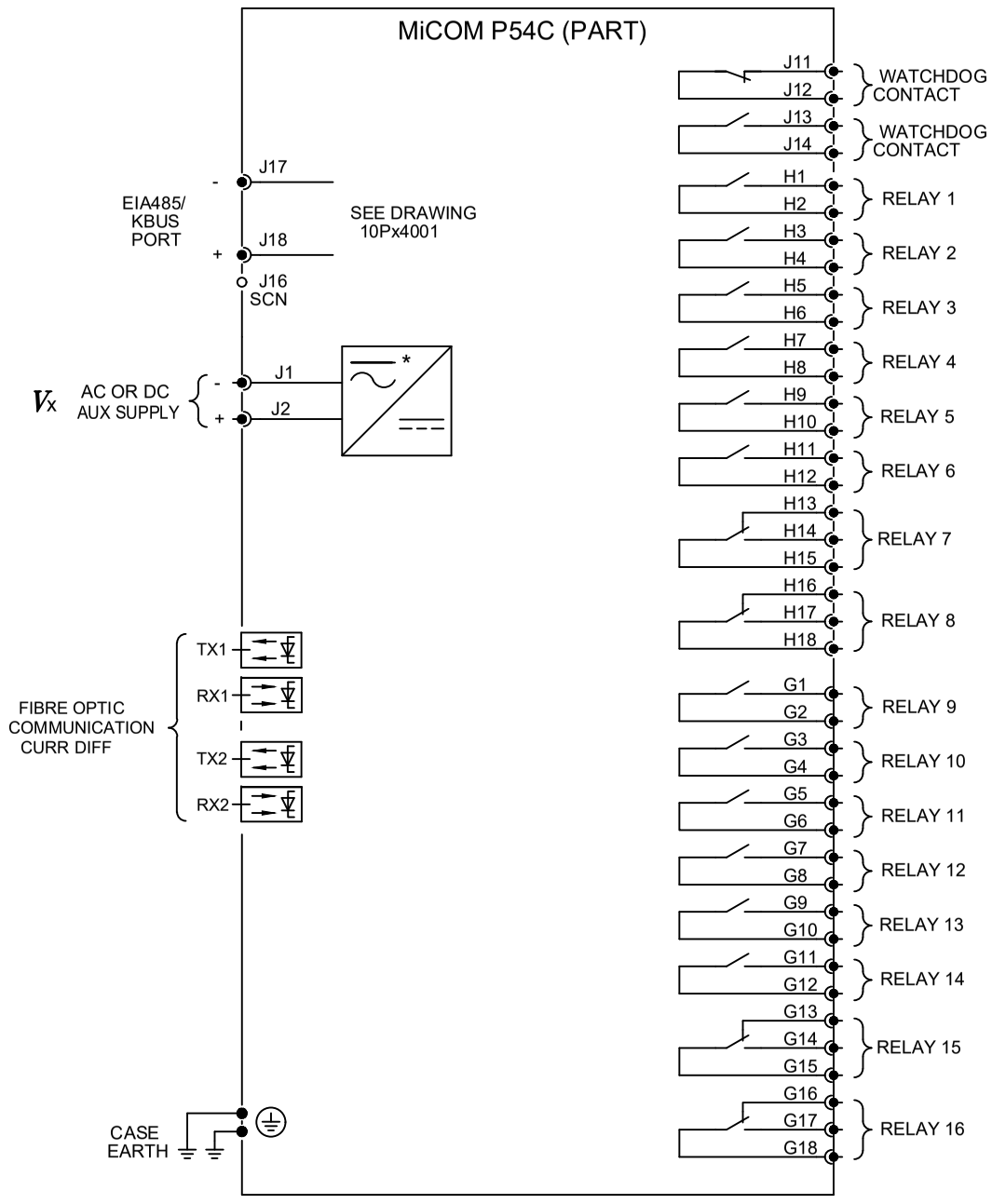
CUSTOMER SETTING	DEFAULT SETTING
	Inhibit Diff
	Recon Interlock
	External Trip 3ph
	CB Aux 3ph 52–B
	CL Close Man
	MCB/VTS
	CB Healthy
	BAR



DEFAULT SETTING	CUSTOMER SETTING
Trip Diff	
SignalingFail	
Any Trip	
General Alarm	
CB Fail Time1	
Trip 3ph	
AR in Prog	
AR Lockout	

Issue: D	Status: **Under Approval**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 2 RELAY 8 INPUTS, 8 OUTPUTS (40TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54B01**	PLM No: A20065407	Sht: 2 / Next Sht: -
Date:	Chkd:				GE VERNOVA





* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

NOTES 1.

(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

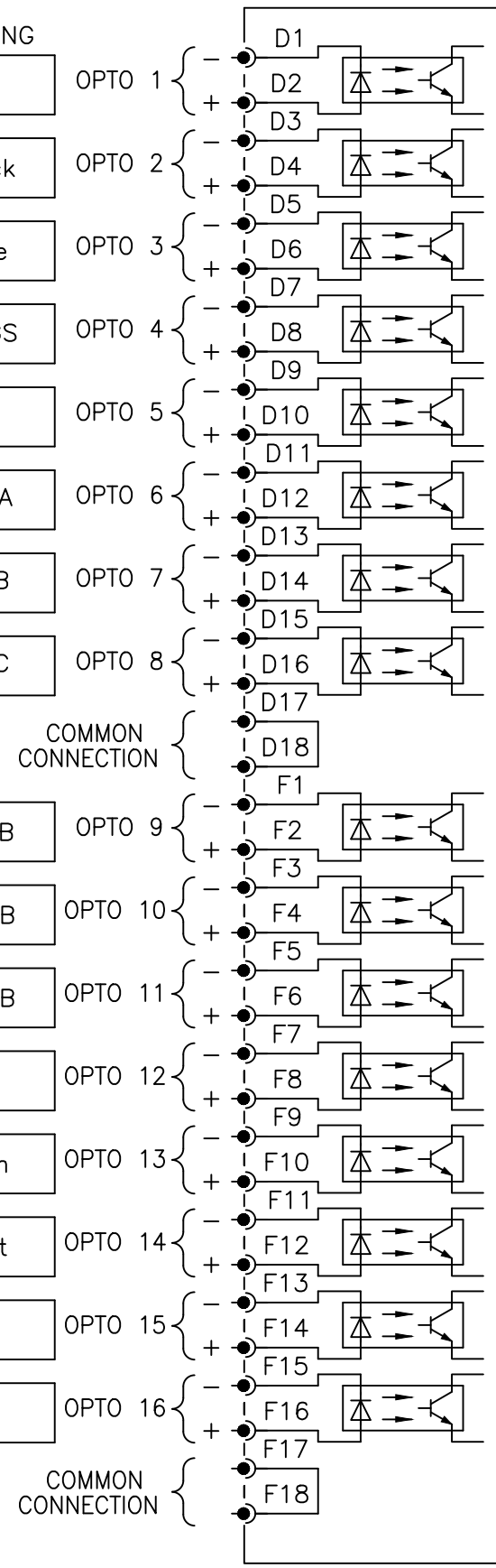
50 OHM BNC CONNECTOR

9-WAY & 25-WAY FEMALE D-TYPE SOCKET

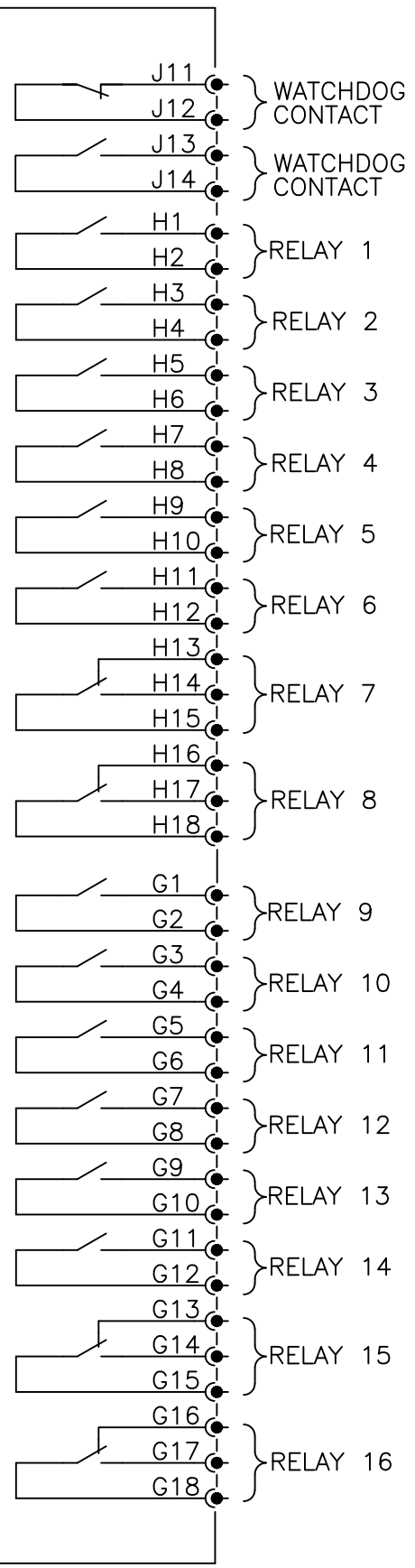
2. USED FOR SEF PROTECTION. I_N SENSITIVE SHOULD BE DRIVEN FROM A CORE BALANCE CT WHEN SENSITIVE SETTINGS ARE USED.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. MUTUAL CURRENT INPUT ONLY REQUIRED IF ENABLED IN FAULT LOCATOR.
5. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
6. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 2 RELAY 16 INPUTS, 16 OUTPUTS & SEF (60TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54C01**	PLM No: A20065570	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	

CUSTOMER SETTING	DEFAULT SETTING
	Inhibit Diff
	Recon Interlock
	Aid 1 Receive
	Aid 1 COS/LGS
	Reset LEDs
	External Trip A
	Exernal Trip B
	Exernal Trip C
	CB AuxA 52-B
	CB AuxB 52-B
	CB AuxC 52-B
	MCB/VTS
	CB Close Man
	Reset Lockout
	CB Healthy
	BAR

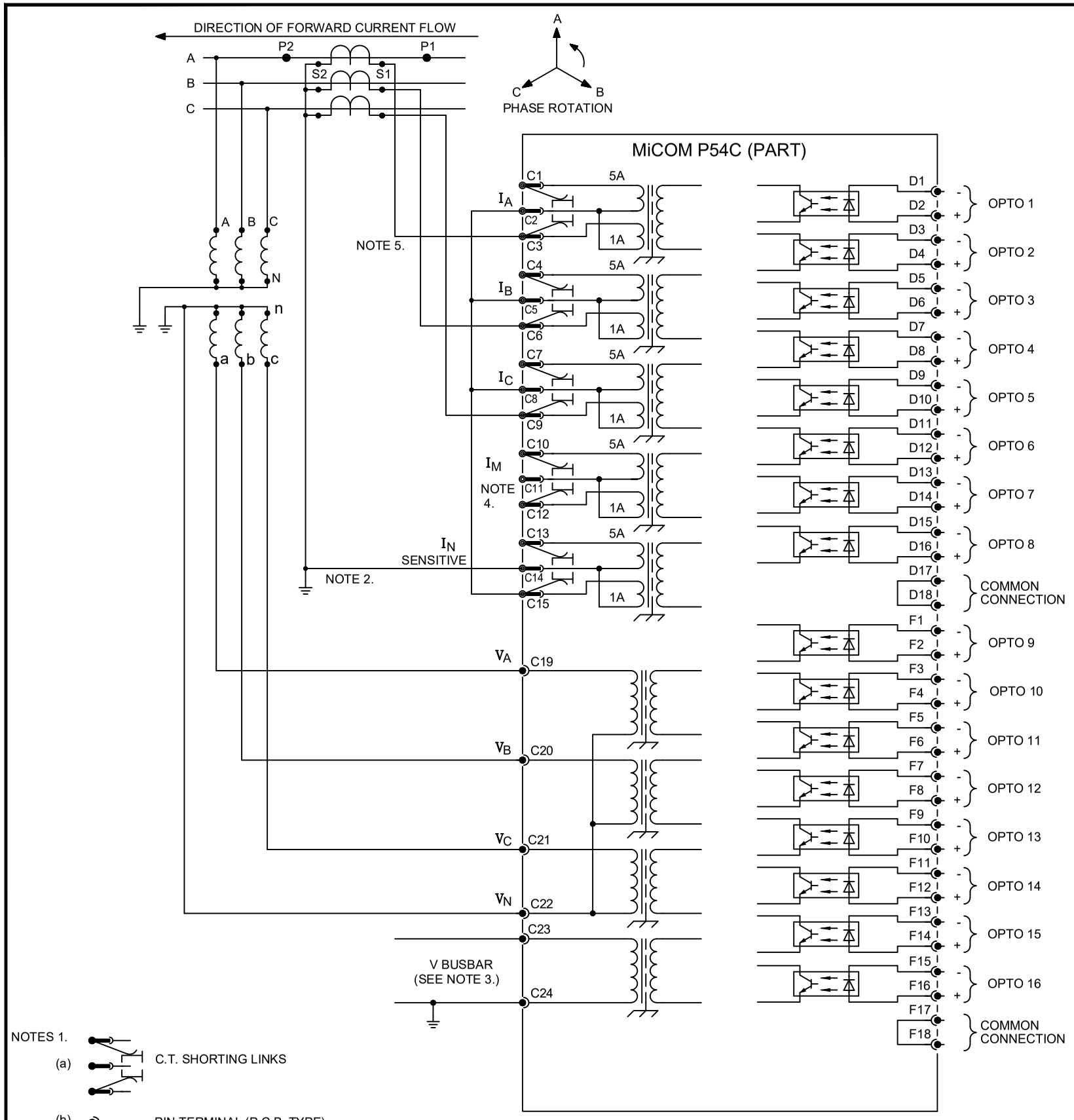


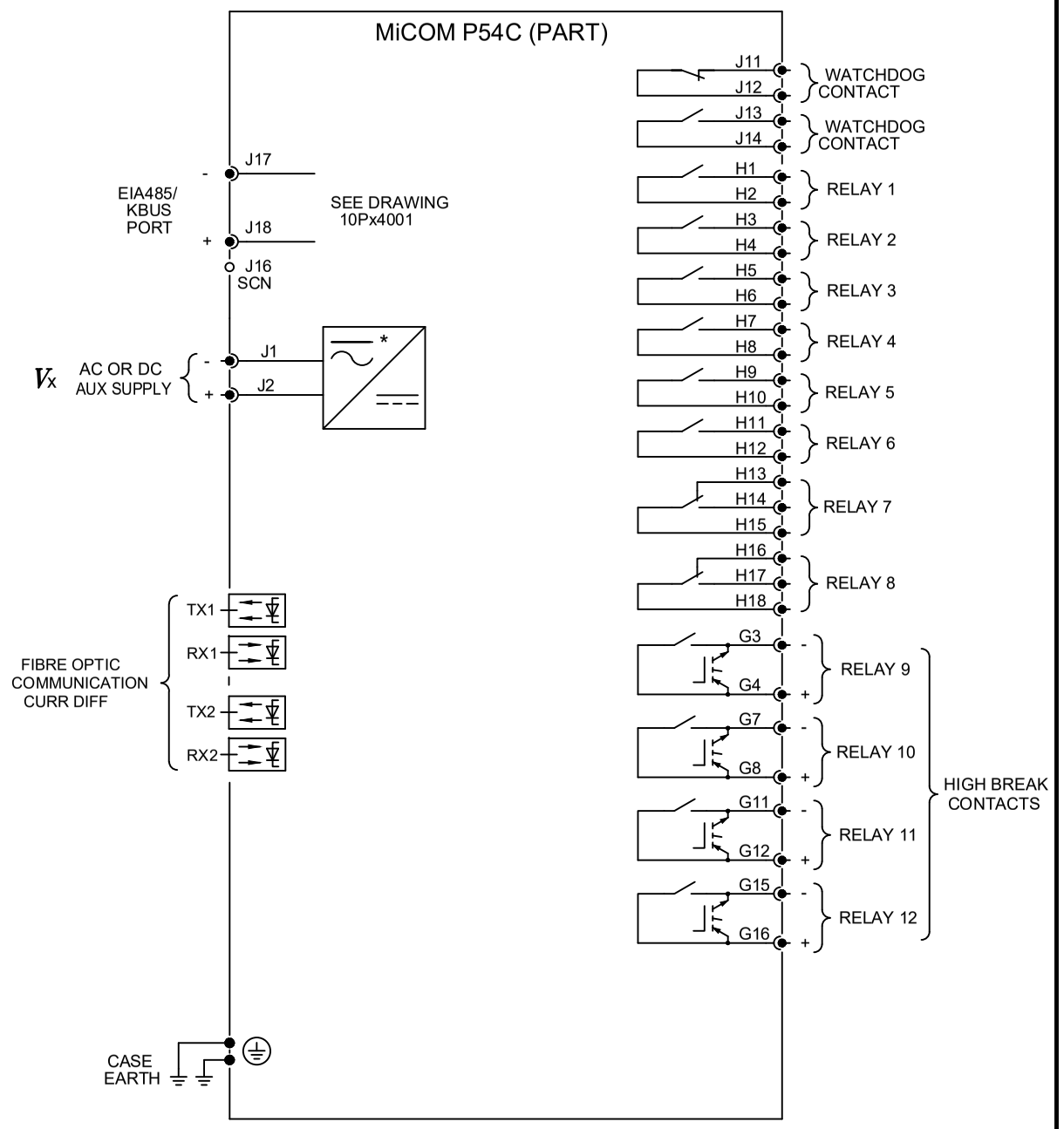
MiCOM P54C
(PART)



DEFAULT SETTING	CUSTOMER SETTING
Trip Diff	
SignalingFail	
Any Trip	
General Alarm	
IM64 1	
CB Fail Time1	
Cntl CB Close	
Cntl CB Trip	
Trip A	
Trip B	
Trip C	
Not used	
Not used	
Not used	
Not used	
Not used	

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 2 RELAY 16 INPUTS, 16 OUTPUTS & SEF (60TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54C01**	PLM No: A20065510	Sht: 2
Date:	Chkd:			Next Sht: -	GE VERNOVA





* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

NOTES 1.

(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

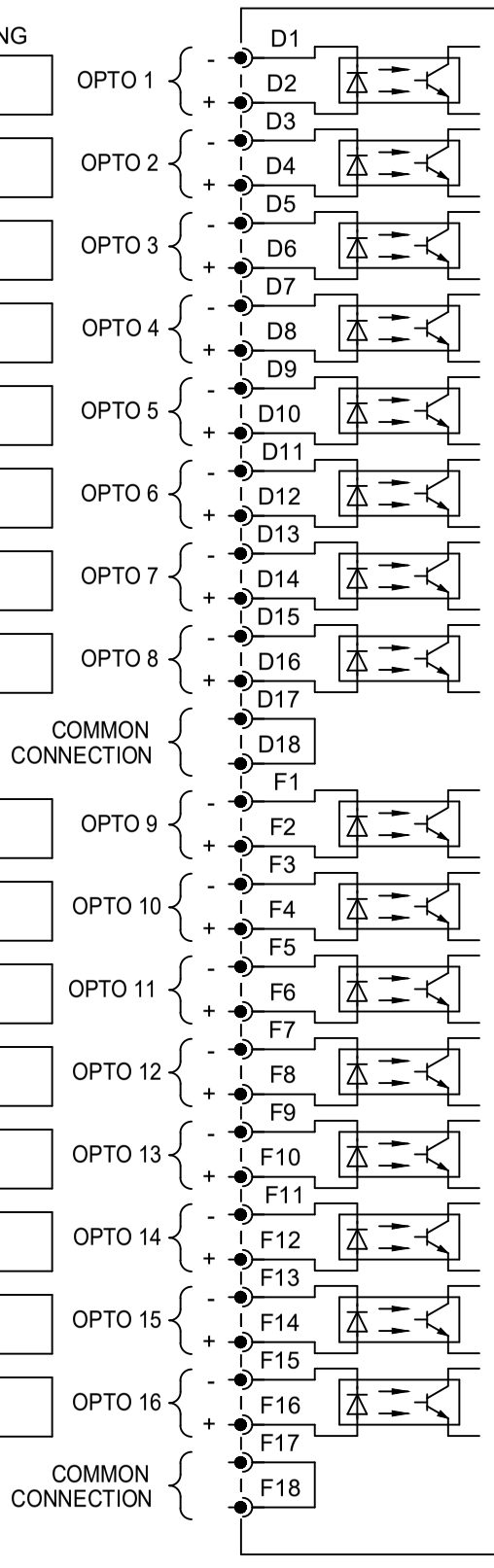
50 OHM BNC CONNECTOR

9-WAY & 25-WAY FEMALE D-TYPE SOCKET

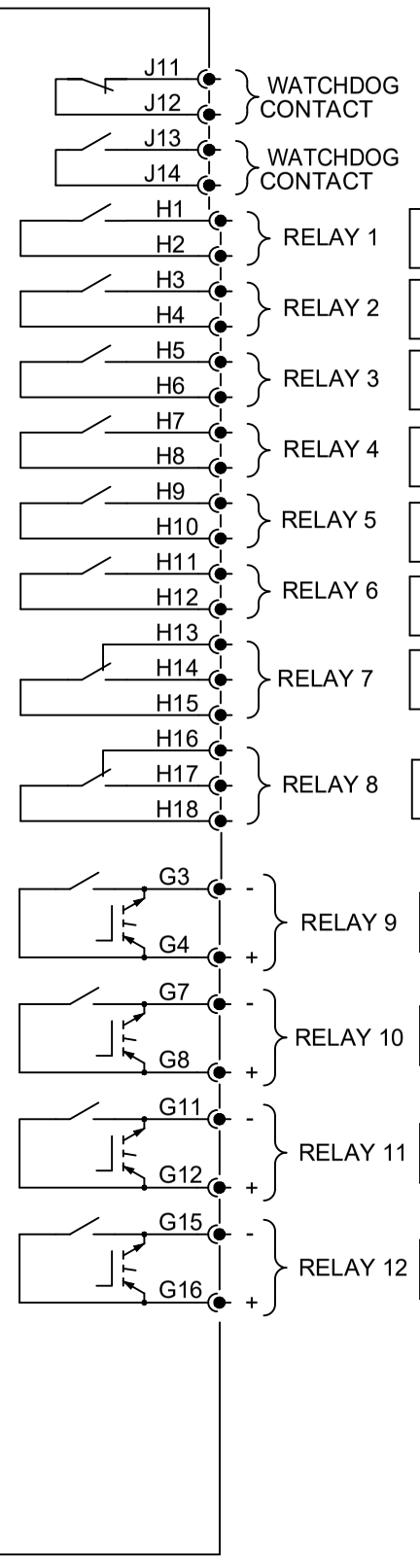
2. USED FOR SEF PROTECTION. I_N SENSITIVE SHOULD BE DRIVEN FROM A CORE BALANCE CT WHEN SENSITIVE SETTINGS ARE USED.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. MUTUAL CURRENT INPUT ONLY REQUIRED IF ENABLED IN FAULT LOCATOR.
5. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
6. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

Issue: D	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 3 RELAY 16 INPUTS, 12 OUTPUTS (4 HIGH BREAK) & SEF (60TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54C02**	PLM No: A20065380	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	

CUSTOMER SETTING	DEFAULT SETTING
	Inhibit Diff
	Recon Interlock
	Aid 1 Receive
	Aid 1 COS/LGS
	Reset LEDs
	External Trip A
	Exernal Trip B
	Exernal Trip C
	CB AuxA 52-B
	CB AuxB 52-B
	CB AuxC 52-B
	MCB/VTS
	CB Close Man
	Reset Lockout
	CB Healthy
	BAR



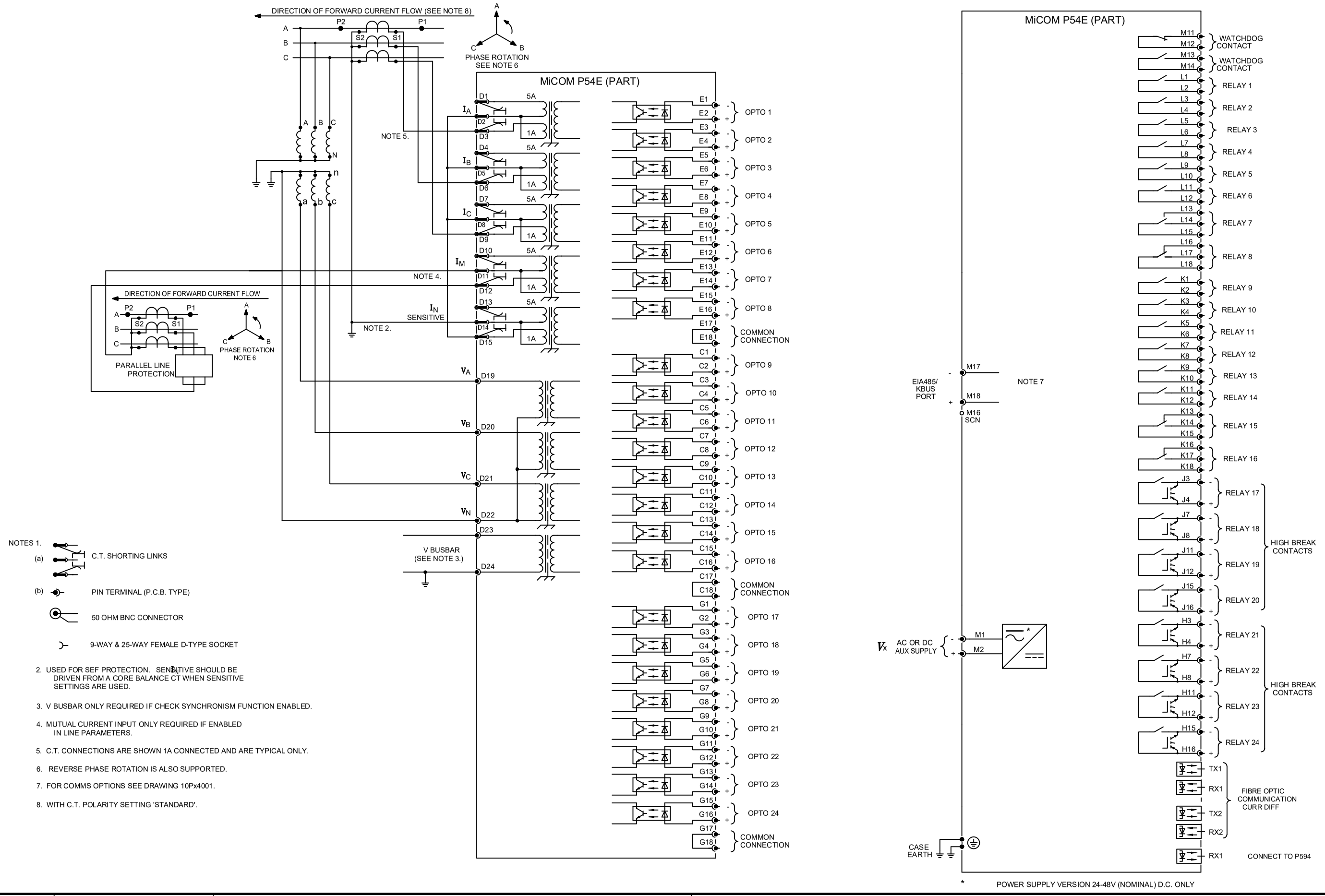
MiCOM P54C
(PART)



DEFAULT SETTING	CUSTOMER SETTING
Trip Diff	
SignalingFail	
Any Trip	
General Alarm	
IM64 1	
CB Fail Time1	
Cntl CB Close	
Trip A	
Trip B	
Trip C	
Any Trip	
Not used	

HIGH BREAK CONTACTS

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 3 RELAY 16 INPUTS, 12 OUTPUTS (4 HIGH BREAK) & SEF (60TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54C02**	PLM No: A20065472	Sht: 2
Date:	Chkd:			Next Sht: -	GE VERNOVA



NOTES 1.

(a) C.T. SHORTING LINKS

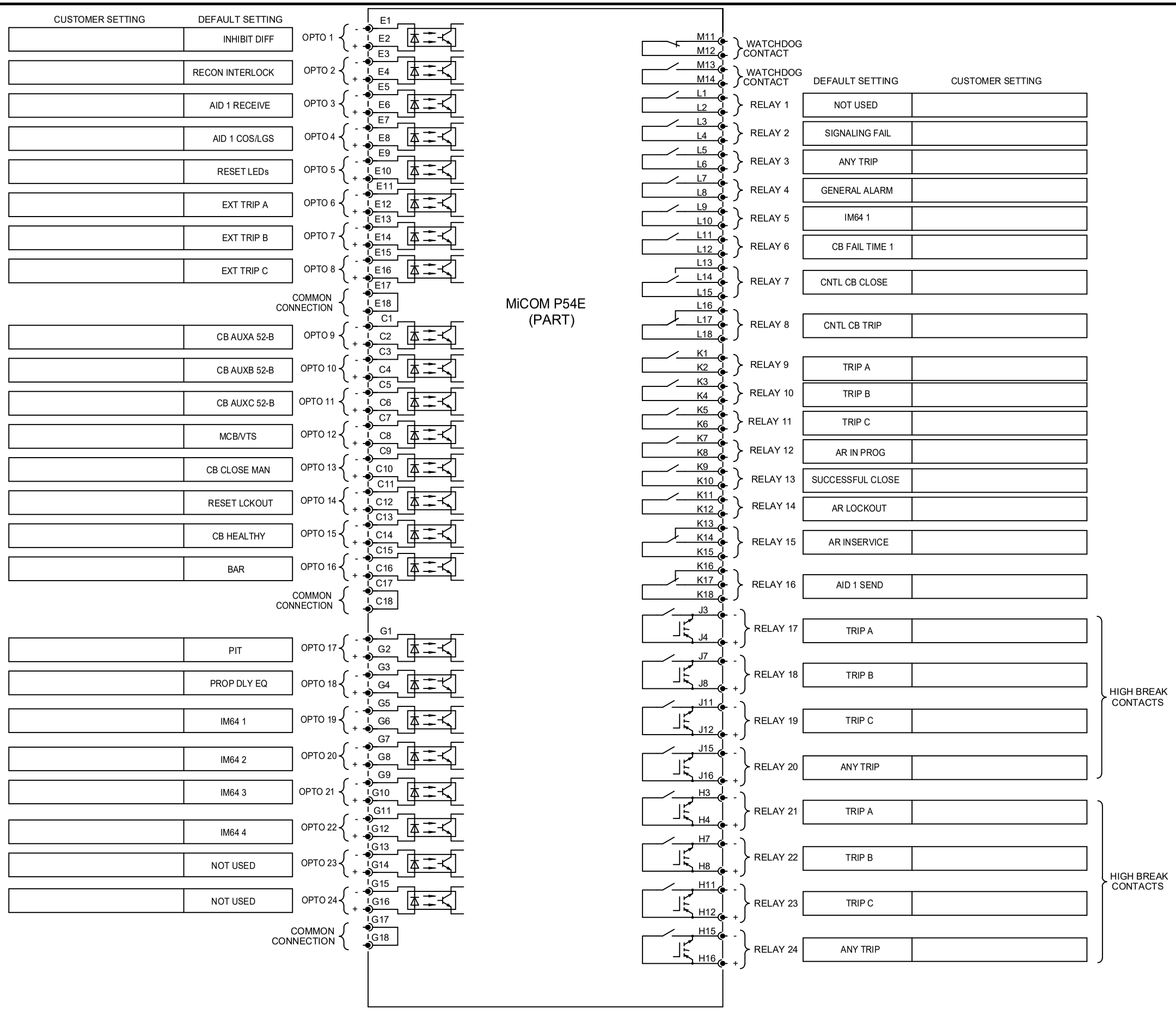
(b) PIN TERMINAL (P.C.B. TYPE)

50 OHM BNC CONNECTOR

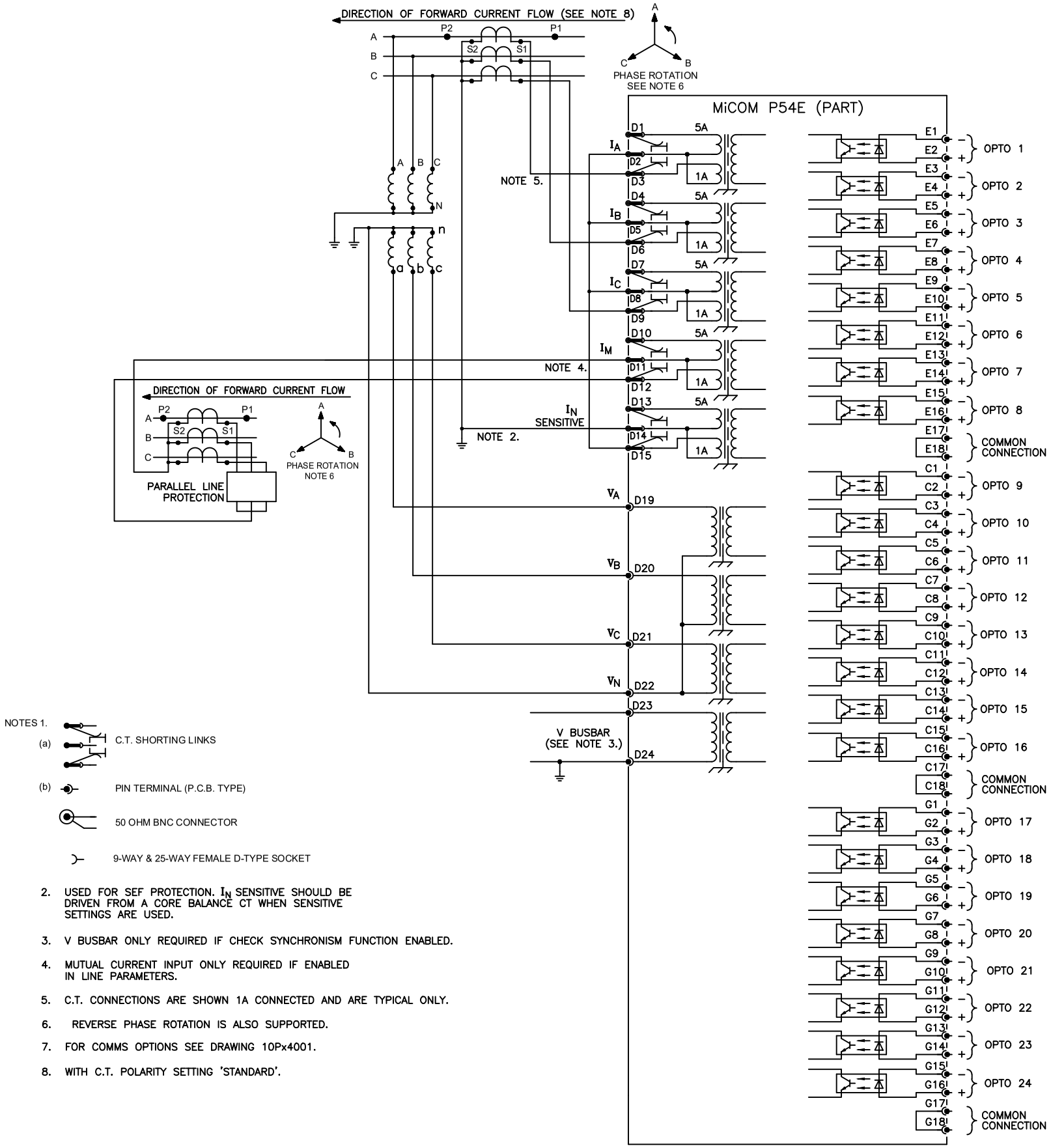
9-WAY & 25-WAY FEMALE D-TYPE SOCKET

2. USED FOR SEF PROTECTION. SENSITIVE SHOULD BE DRIVEN FROM A CORE BALANCE CT WHEN SENSITIVE SETTINGS ARE USED.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. MUTUAL CURRENT INPUT ONLY REQUIRED IF ENABLED IN LINE PARAMETERS.
5. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
6. REVERSE PHASE ROTATION IS ALSO SUPPORTED.
7. FOR COMMS OPTIONS SEE DRAWING 10Px4001.
8. WITH C.T. POLARITY SETTING 'STANDARD'.

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title:	EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF RELAY 24 INPUTS / 24 OUTPUTS (8 HIGH BREAK) & SEF (80TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54E01**	PLM No: A20065622	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	



Issue: F	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: CURRENT DIFF 2 RELAY 24 INPUTS / 24 OUTPUTS (8 HIGH BREAK) & SEF (80TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54E01**	PLM No: A20065615	Sht: 2	GE VERNOVA
Date:	Chkd:				Next Sht: -	



NOTES 1.

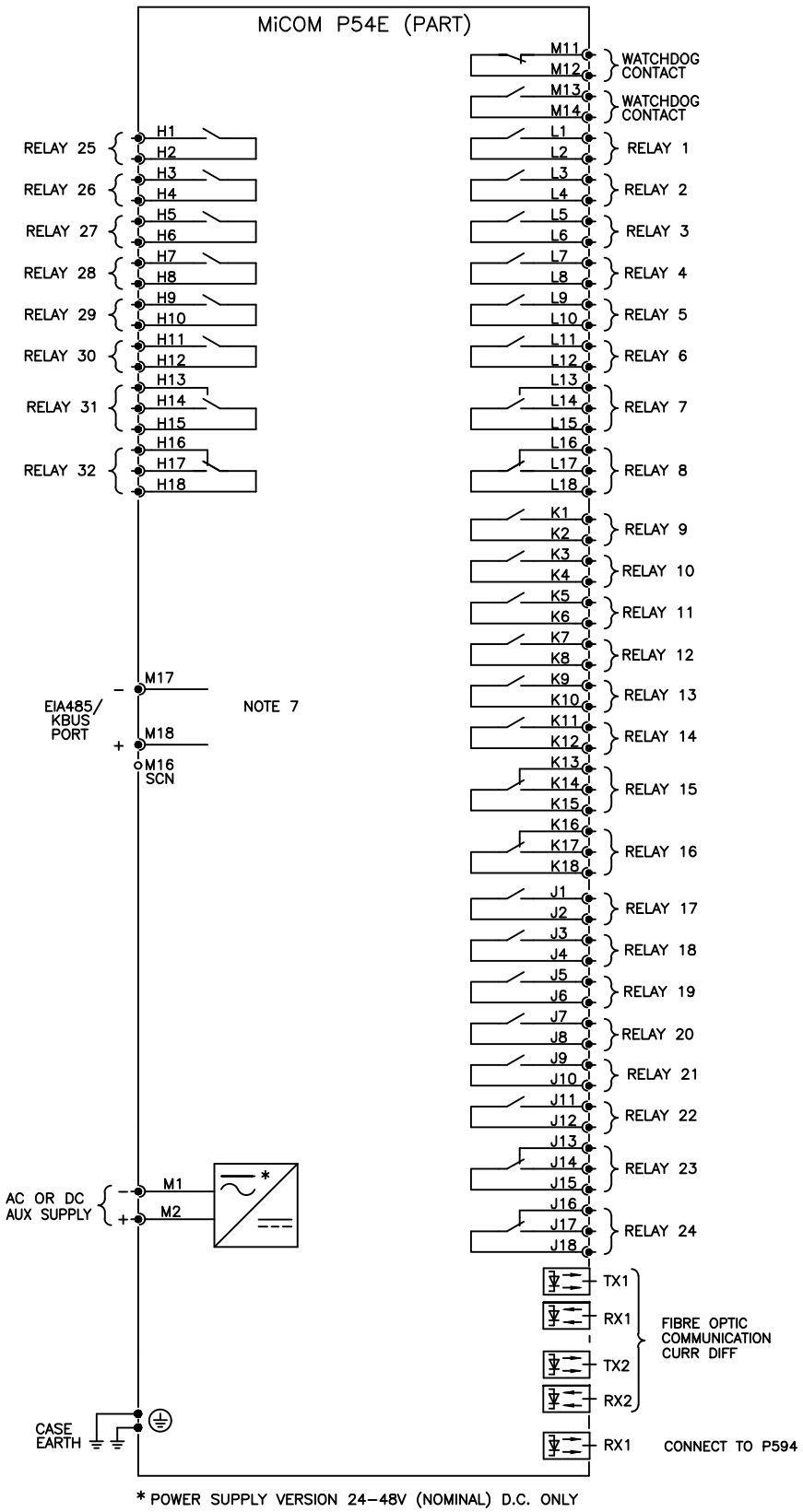
(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

50 OHM BNC CONNECTOR

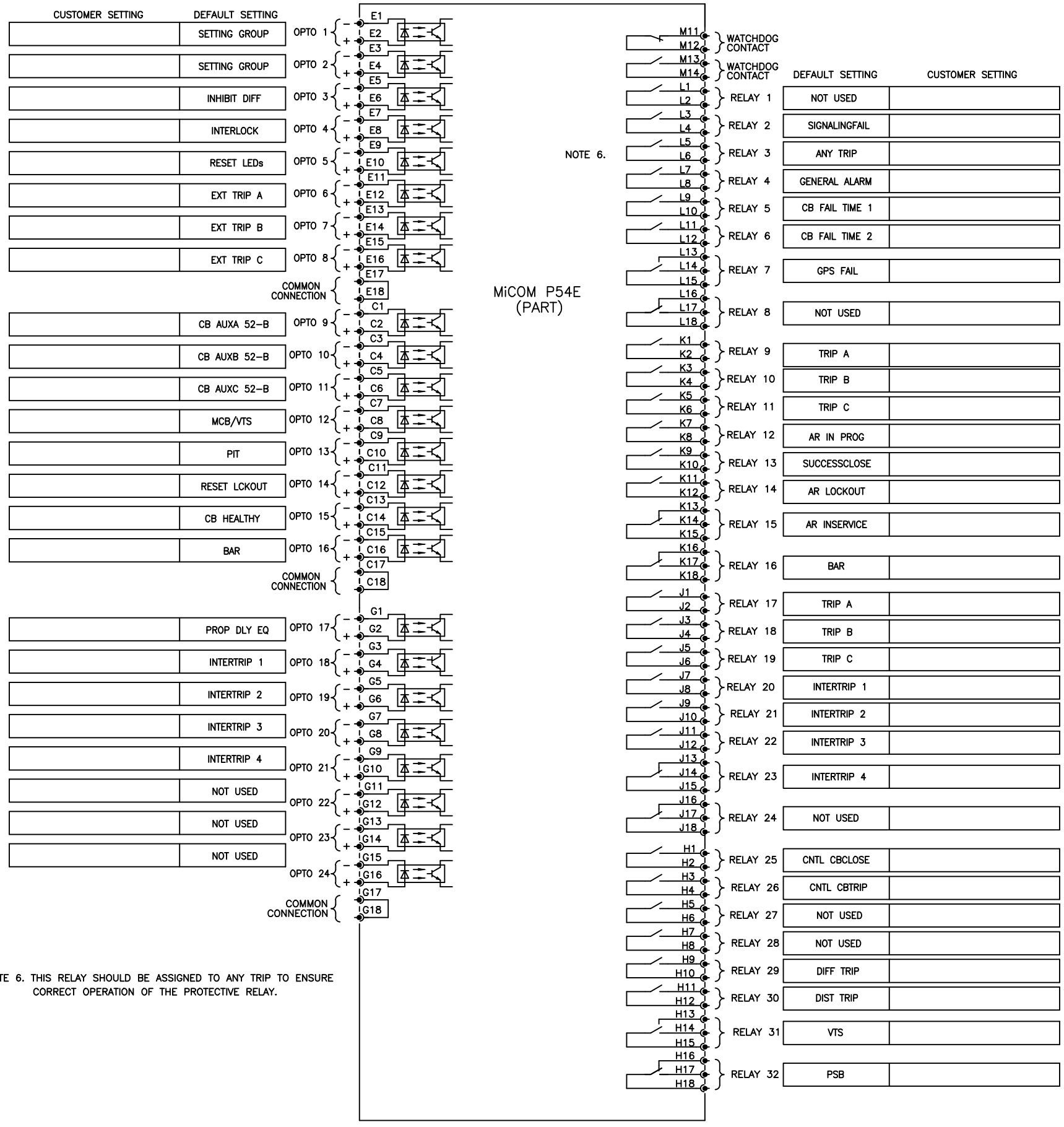
9-WAY & 25-WAY FEMALE D-TYPE SOCKET

2. USED FOR SEF PROTECTION. I_N SENSITIVE SHOULD BE DRIVEN FROM A CORE BALANCE CT WHEN SENSITIVE SETTINGS ARE USED.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. MUTUAL CURRENT INPUT ONLY REQUIRED IF ENABLED IN LINE PARAMETERS.
5. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
6. REVERSE PHASE ROTATION IS ALSO SUPPORTED.
7. FOR COMMS OPTIONS SEE DRAWING 10Px4001.
8. WITH C.T. POLARITY SETTING 'STANDARD'.



* POWER SUPPLY VERSION 24–48V (NOMINAL) D.C. ONLY

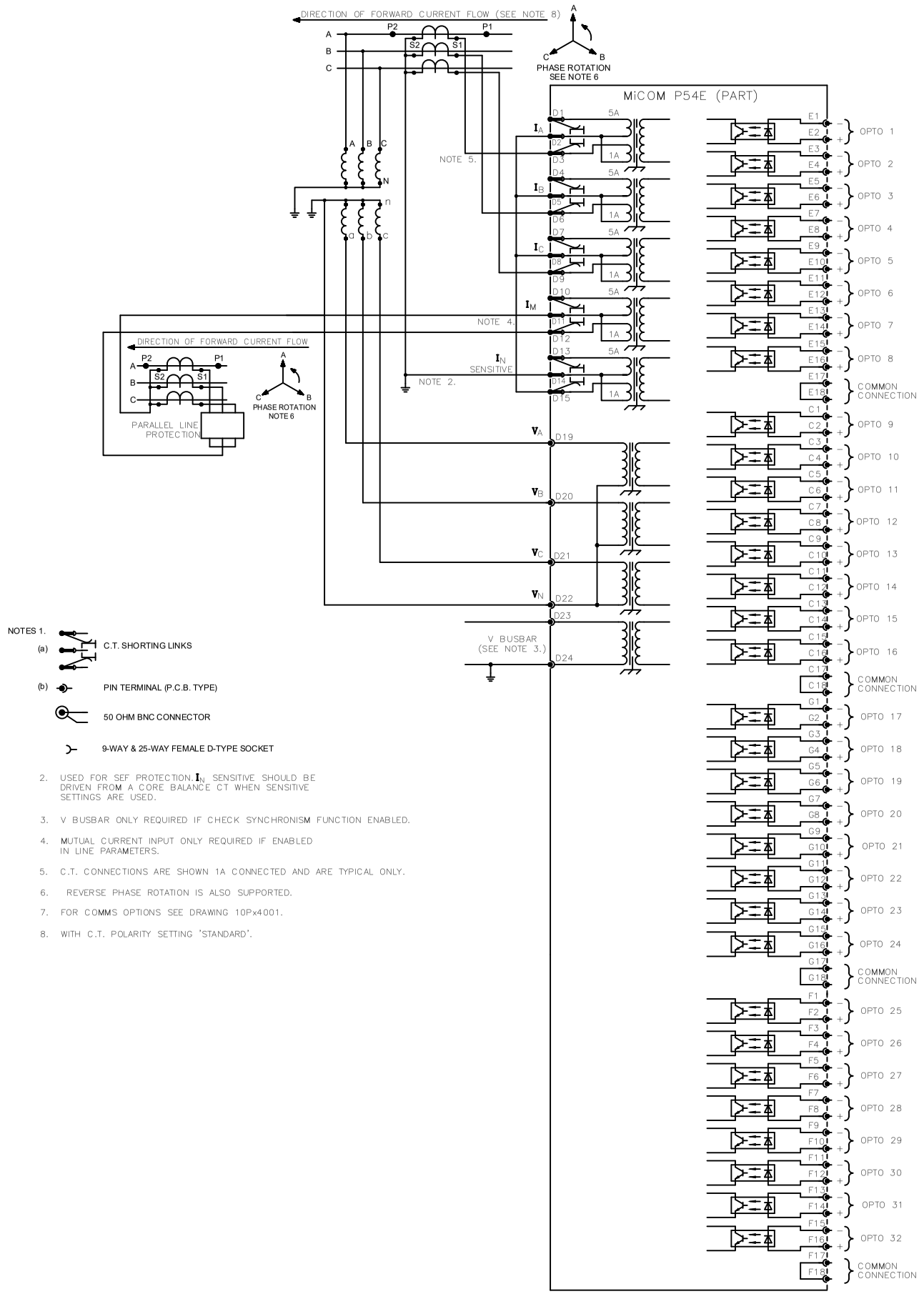
Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTRERNAL CONNECTION DIAG CURRENT DIFF RELAY 24 INPUTS, 32 OUTPUTS & SEF (80TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54E02**	PLM No: A20065449	Sht: 1 / Next Sht: 2
Date:	Chkd:				GE VERNOVA



NOTE 6. THIS RELAY SHOULD BE ASSIGNED TO ANY TRIP TO ENSURE CORRECT OPERATION OF THE PROTECTIVE RELAY.

Issue: D	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTRERNAL CONNECTION DIAG CURRENT DIFF RELAY 24 INPUTS, 32 OUTPUTS & SEF (80TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54E02**	PLM No: A20065551	Sht: 2
Date:	Chkd:				Next Sht: -

GE VERNOVA



NOTES 1.

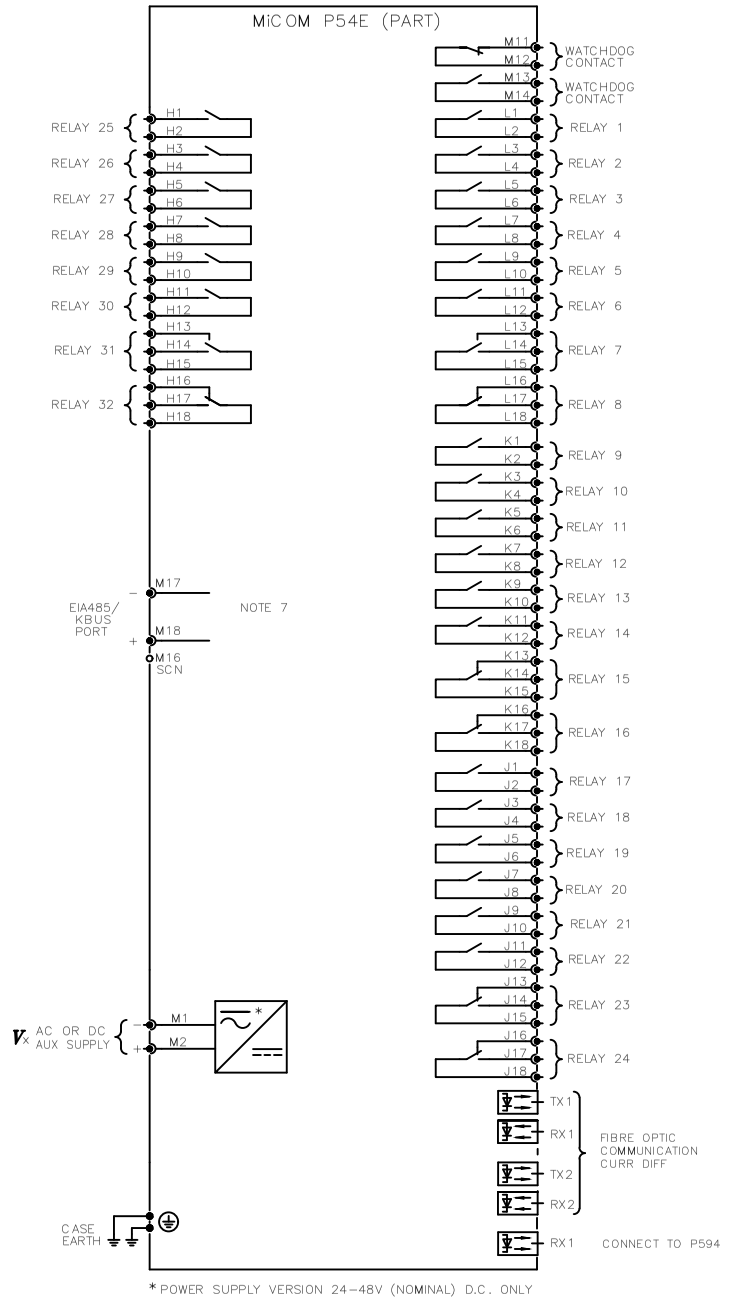
(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

50 OHM BNC CONNECTOR

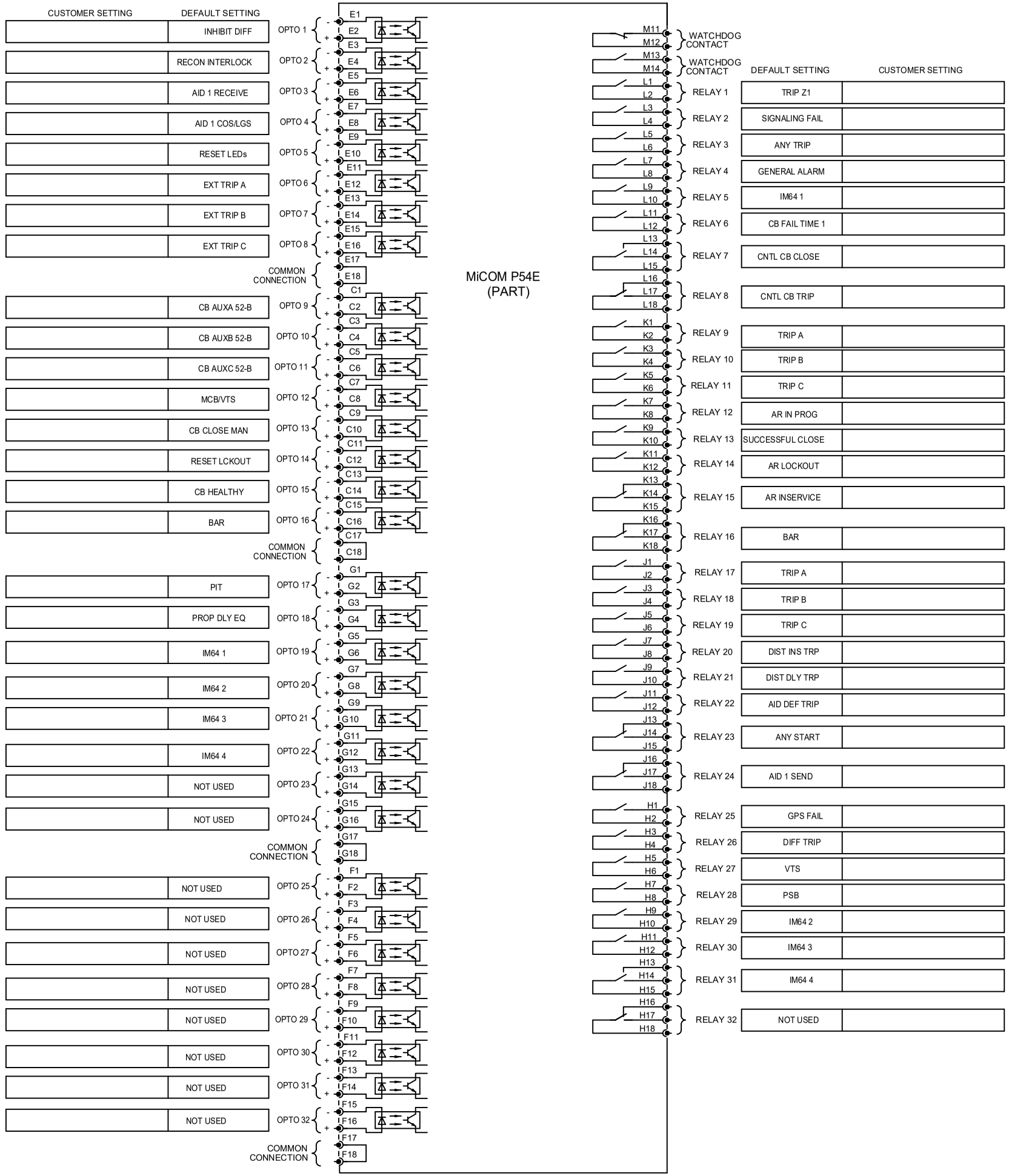
9-WAY & 25-WAY FEMALE D-TYPE SOCKET

2. USED FOR SEF PROTECTION. I_N SENSITIVE SHOULD BE DRIVEN FROM A CORE BALANCE CT WHEN SENSITIVE SETTINGS ARE USED.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. MUTUAL CURRENT INPUT ONLY REQUIRED IF ENABLED IN LINE PARAMETERS.
5. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
6. REVERSE PHASE ROTATION IS ALSO SUPPORTED.
7. FOR COMMS OPTIONS SEE DRAWING 10Px4001.
8. WITH C.T. POLARITY SETTING 'STANDARD'.



* POWER SUPPLY VERSION 24–48V (NOMINAL) D.C. ONLY

Issue: D	Status: **In Work**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAG CURRENT DIFF RELAY 32 INPUTS, 32 OUTPUTS & SEF (80TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54E03**	PLM No: A20065337	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	



Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAG CURRENT DIFF RELAY 32 INPUTS, 32 OUTPUTS & SEF (80TE)		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information of GEV. This document is loaned on the express condition that neither it nor the information contained therein shall be disclosed to others without the express written consent of GEV, and that the information shall be used by the recipient only as approved expressly by GEV. This document shall be returned to GEV upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations. © GE VERNOVA Company, GEV CONFIDENTIAL UNPUBLISHED WORK.	Drg No: **10P54E03**	PLM No: A20065512	Sht: 2
Date:	Chkd:				Next Sht: -

GE VERNOVA

APPENDIX D

HARDWARE/COMMUNICATIONS COMPATIBILITY MATRIX TABLES

A compatibility matrix table for MiCOM P54A-E Line Differential Protection Relays is provided in a separate Excel file, attached as an embedded resource. The matrix can be used to check communications compatibility between related devices. If using Adobe Acrobat Reader, click on the button below to open the spreadsheet.

This manual must be opened with a PDF viewer capable of opening attachments, such as Adobe Acrobat Reader or Nitro PDF. If using Nitro PDF, attachments are shown in the attachment pane. To show or hide the attachments pane, look in the sidebar and click the attachments tab.

Note:
An Open File dialogue box may open with a warning message about potential harm from programs, macros or viruses. The file supplied does not contain any harmful content, and may be safely opened.

Settings and Signals



GE VERNOVA

© 2026, GE Vernova and/or its affiliates. All rights reserved.

