GE VERNOVA

MiCOM P40 Agile

P442, P444

Addendum
Numerical Distance Protection IED

Hardware Version: M
Firmware Version: 92
Publication Reference: P44x-AD2-EN-1



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 furnished 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 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.

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

IT IS THE SOLE RESPONSIBILITY OF THE USER TO SECURE THEIR NETWORK AND ASSOCIATED DEVICES AGAINST CYBER SECURITY INTRUSIONS OR ATTACKS. GE VERNOVA AND ITS AFFILIATES ARE NOT LIABLE FOR ANY DAMAGES AND/OR LOSSES ARISING FROM OR RELATED TO SUCH SECURITY INTRUSION OR ATTACKS.

Contents

Chapter 1 Introduction 1

1.1 Scope of this addendum 2
1.1.1 IED Compatibility 2
1.2 Ordering Options 3

Chapter 2 Safety Information 4

2.1 Chapter Overview 5
2.2 Health and Safety 6
2.3 Symbols 7
2.4 Installation, Commissioning and Servicing 8
2.4.1 Lifting Hazards 8
2.4.2 Electrical Hazards 8
2.4.3 UL/CSA/CUL Requirements 9
2.4.4 Fusing Requirements 9
2.4.5 Equipment Connections 10
2.4.6 Protection Class 1 Equipment Requirements 10
2.4.7 Pre-energisation Checklist 11
2.4.8 Peripheral Circuitry 11
2.4.9 Upgrading/Servicing 13
2.5 Decommissioning and Disposal 14
2.6 Regulatory Compliance 15
2.6.1 EMC Compliance: 2014/30/EU 15
2.6.2 LVD Compliance: 2014/35/EU 15
2.6.3 R&TTE Compliance: 2014/53/EU 15
2.6.4 UL/CUL Compliance 15

Chapter 3 Hardware Design 16

3.1 Chapter Overview 17
3.2 Hardware Architecture 18
3.2.1 Coprocessor Hardware Architecture 18
3.3 Mechanical Implementation 20
3.3.1 Housing Variants 20
3.3.2 List of Boards 21
3.4 Front Panel 22
3.4.1 Front Panel 22
3.4.1.1 Front Panel Compartments 22
3.4.1.2 HMI Panel 23
3.4.1.3 Keypad 24
3.4.1.4 USB Port 24
3.4.1.5 Fixed Function LEDs 25
3.4.1.6 Function Keys 25
3.4.1.7 Programable LEDs 25
3.5 Rear Panel 26
3.5.1 Terminal Block Ingress Protection 27
3.6 Boards and Modules 28
3.6.1 PCBs 28
3.6.2 Subassemblies 28
3.6.3 Main Processor Board 29
3.6.4 Power Supply Board 30
3.6.4.1 Watchdog 32
3.6.4.2 Rear Serial Port 33
3.6.5 Input Module - 1 Transformer Board 34

3.6.5.1 Input Module Circuit Description 35
3.6.5.2 Frequency Response 36
3.6.5.3 Transformer Board 37
3.6.5.4 Input Board 38
3.6.6 Standard Output Relay Board 40
3.6.7 High Break Output Relay Board 42
3.6.8 IRIG-B Board 45
3.6.9 Fibre Optic Board 46
3.6.10 Rear Communication Board 47
3.6.10.1 Redundant Ethernet Board (Hardware Option R/S/T) 48
3.6.10.2 Single Ethernet Board (Hardware Option U) 49
3.6.10.3 Redundant Ethernet Board (Hardware Option W/Y) 51
3.6.10.4 Retrofit of Ethernet Cards Hardware Option R/S/T with Hardware Option U/W/Y 52
3.6.11 IEC61850-9-2LE Ethernet Board 54
3.6.12 Coprocessor Board 55

Chapter 4 Software Design 56

4.1 Chapter Overview 57
4.2 Sofware Design Overview 58
4.3 System Level Software 59
4.3.1 Real Time Operating System 59
4.3.2 System Services Software 59
4.3.3 Self-Diagnostic Software 59
4.3.4 Startup Self-Testing 59
4.3.4.1 System Boot 59
4.3.4.2 System Level Software Initialisation 60
4.3.4.3 Platform Software Initialisation and Monitoring 60
4.3.5 Continuous Self-Testing 60
4.4 Platform Software 61
4.4.1 Record Logging 61
4.4.2 Settings Database 61
4.4.3 Interfaces 61
4.5 Protection and Control Functions 62
4.5.1 Acquisition of Samples 62
4.5.2 Frequency Tracking 62
4.5.3 Direct Use of Sampled Values 62
4.5.4 Fourier Signal Processing 62
4.5.5 Programmable Scheme Logic 63
4.5.6 Event Recording 64
4.5.7 Disturbance Recorder 64
4.5.8 Fault Locator 64
4.5.9 Function Key Interface 64

Chapter 5 Configuration 65

5.1 Chapter Overview 66
5.2 Settings Application Software 67
5.3 Using the HMI Panel 68
5.3.1 Navigating the HMI Panel 69
5.3.2 Getting Started 69
5.3.3 Default Display 70
5.3.4 Default Display Navigation 71
5.3.5 Password Entry 72
5.3.6 Processing Alarms and Records 72
5.3.7 Menu Structure 73
5.3.8 Changing the Settings 74

5.3.9 Direct Access (The Hotkey menu) 75
5.3.9.1 Setting Group Selection Using Hotkeys 75
5.3.9.2 Control Inputs 75
5.3.9.3 Circuit Breaker Control 76
5.3.9.4 Function Keys 76
5.4 Date and Time Configuration 78
5.4.1 Using an SNTP Signal 78
5.4.2 Using an IRIG-B Signal 78
5.4.3 Using an IEEE 1588 PTP Signal 78
5.4.4 Without a Timing Source Signal 79
5.4.5 Time Zone Compensation 79
5.4.6 Daylight Saving Time Compensation 80
5.5 Settings Group Selection 81

Chapter 6 Communications 82

6.1 Chapter Overview 83
6.2 Communication Interfaces 84
6.3 Serial Communication 85
6.3.1 USB Front Port 85
6.3.2 EIA(RS)485 Bus 85
6.3.2.1 EIA(RS)485 Biasing Requirements 86
6.3.3 K-Bus 86
6.4 Ethernet Communication 88
6.5 Redundancy Protocols 89
6.5.1 Parallel Redundancy Protocol (PRP) 89
6.5.1.1 PRP Networks 89
6.5.1.2 Network Elements 89
6.5.2 High-Availability Seamless Redundancy (HSR) 90
6.5.2.1 HSR Multicast Topology 90
6.5.2.2 HSR Unicast Topology 91
6.5.2.3 HSR Application in the Substation 92
6.5.3 Rapid Spanning Tree Protocol (RSTP) 92
6.5.4 Failover 93
6.6 Simple Network Management Protocol (SNMP) 94
6.6.1 SNMP Management Information Bases 94
6.6.2 Main Processor MIBS Structure 94
6.6.3 Redundant Ethernet Board MIB Structure 95
6.6.4 Accessing the MIB 99
6.6.5 Main Processor SNMP Configuration 99
6.7 Data Protocols 101
6.7.1 Courier 101
6.7.1.1 Physical Connection and Link Layer 101
6.7.1.2 Courier Database 102
6.7.1.3 Settings Categories 102
6.7.1.4 Setting Changes 102
6.7.1.5 Event Extraction 102
6.7.1.6 Disturbance Record Extraction 104
6.7.1.7 Programmable Scheme Logic Settings 104
6.7.1.8 Time Synchronisation 105
6.7.1.9 Courier Configuration 105
6.7.2 IEC 60870-5-103 106
6.7.2.1 Physical Connection and Link Layer 107
6.7.2.2 Initialisation 107
6.7.2.3 Time Synchronisation 107
6.7.2.4 Configurable IEC 60870-5-103 Signal List 107
6.7.2.5 Spontaneous Events 108
6.7.2.6 General Interrogation (GI) 108

6.7.2.7	Cyclic Measurements	108
6.7.2.8	Commands	108
6.7.2.9	Test Mode	109
6.7.2.10	Disturbance Records	109
6.7.2.11	Command/Monitor Blocking	109
6.7.2.12	IEC 60870-5-103 Configuration	109
6.7.3	DNP 3.0	110
6.7.3.1	Physical Connection and Link Layer	110
6.7.3.2	Object 1 Binary Inputs	111
6.7.3.3	Object 10 Binary Outputs	111
6.7.3.4	Object 20 Binary Counters	112
6.7.3.5	Object 30 Analogue Input	113
6.7.3.6	Object 40 Analogue Output	113
6.7.3.7	Object 50 Time Synchronisation	113
6.7.3.8	DNP3 Device Profile	113
6.7.3.9	DNP3 Configuration	121
6.7.4	IEC 61850	122
6.7.4.1	Benefits of IEC 61850	123
6.7.4.2	IEC 61850 Interoperability	123
6.7.4.3	The IEC 61850 Data Model	123
6.7.4.4	IEC 61850 in MiCOM IEDs	124
6.7.4.5	IEC 61850 Data Model Implementation	125
6.7.4.6	IEC 61850 Communication Services Implementation	125
6.7.4.7	IEC 61850 Peer-to-peer (GOOSE) communications	125
6.7.4.8	GOOSE Message Validation	125
6.7.4.9	Mapping GOOSE Messages to Virtual Inputs	125
6.7.4.10	Ethernet Functionality	126
6.7.4.11	IEC 61850 Configuration	126
6.7.4.12	Selection of the IEC 61850 Edition	127
6.7.4.13	IEC 61850 Edition 2	128
6.8	**Read Only Mode**	**132**
6.8.1	IEC 60870-5-103 Protocol Blocking	132
6.8.2	Courier Protocol Blocking	132
6.8.3	IEC 61850 Protocol Blocking	133
6.8.4	Read-Only Settings	133
6.8.5	Read-Only DDB Signals	133
6.9	**Time Synchronisation using the Communication Protocols**	**134**
6.10	**Time Synchronisation**	**135**
6.10.1	IRIG-B	135
6.10.1.1	IRIG-B Implementation	136
6.10.2	SNTP	136
6.10.2.1	Loss of SNTP Server Signal Alarm	136
6.10.3	IEEE 1588 Precision time Protocol	136
6.10.3.1	Accuracy and Delay Calculation	137
6.10.3.2	PTP Domains	137
6.11	**Board Variants**	**138**
6.12	**Configuring IP Addresses**	**139**
6.12.1	Configuring the IED IP Address	139
6.12.2	Configuring the REB IP Address	139
6.12.2.1	Configuring the Last Octet (SHP, DHP, RSTP)	140
6.13	**Redundant Ethernet Configurator**	**143**
6.13.1	Connecting the IED to a PC	143
6.13.2	Installing the Configurator	143
6.13.3	Starting the Configurator	144
6.13.4	Device Identification	144
6.13.5	Selecting the Device Mode	144
6.13.6	Filter by Board Type	144
6.13.7	Password Confguration	144

6.13.8 IP Address Configuration 144
6.13.9 SNTP IP Address Configuration 145
6.13.10 Check MAC Table for Connected Equipment 145
6.13.11 PRP Configuration 145
6.13.12 HSR Configuration 145
6.13.13 RSTP Configuration 146
6.13.14 Bridge parameters 146
6.13.15 Port Parameters 146
6.13.16 Port States 147
6.13.17 Failover Configuration 147
6.13.18 Filtering Database 147
6.13.19 End of Session 148
6.14 General Functions for Redundant Ethernet Boards 149
6.14.1 Forwarding 149

Chapter 7 Cybersecurity 150

7.1 Disclaimer 151
7.2 Overview 152
7.3 The Need for Cybersecurity 153
7.4 Standards 154
7.4.1 NERC Compliance 154
7.4.1.1 CIP 002 155
7.4.1.2 CIP 003 155
7.4.1.3 CIP 004 155
7.4.1.4 CIP 005 155
7.4.1.5 CIP 006 156
7.4.1.6 CIP 007 156
7.4.1.7 CIP 008 156
7.4.1.8 CIP 009 156
7.4.2 IEEE 1686-2013 156
7.5 Cyber-Security Implementation 158
7.5.1 Initial Setup 158
7.6 Roles and Permissions 159
7.6.1 Roles 159
7.6.2 Permissions 160
7.7 Authentication 162
7.7.1 Authentication Methods 162
7.7.2 Bypass 162
7.7.3 Login 163
7.7.3.1 Front Panel Login 164
7.7.3.2 MiCOM S1 Login 164
7.7.3.3 Warning Banner 164
7.7.3.4 Login Failed 164
7.7.4 User Sessions 165
7.7.5 User Locking Policy 166
7.7.6 Logout 166
7.7.6.1 Front Panel Logout 166
7.7.6.2 MiCOM S1 Logout 167
7.7.7 Device Users 167
7.7.8 Password Policy 167
7.7.9 Change Password 167
7.7.10 RADIUS 167
7.7.10.1 RADIUS Users 168
7.7.10.2 RADIUS Client 168
7.7.10.3 RADIUS Server Settings 169
7.7.10.4 RADIUS Accounting 169

7.7.10.5 RADIUS Client-Server Validation 170
7.7.11 Recovery 170
7.7.11.1 Restore to Local Factory Default 170
7.7.11.2 Password Reset Procedure 170
7.7.11.3 Access Level DDBs 172
7.7.12 Disabling Physical Ports 172
7.7.13 Disabling Logical Ports 172
7.8 Security Event Management 174
7.8.1 Security Events: Courier 174
7.8.2 Syslog 176
7.8.3 Syslog Client 177
7.8.4 Syslog Functionality 177

Chapter 8 Installation 179

8.1 Chapter Overview 180
8.2 Handling the Goods 181
8.2.1 Receipt of the Goods 181
8.2.2 Unpacking the Goods 181
8.2.3 Storing the Goods 181
8.2.4 Dismantling the Goods 181
8.3 Mounting the Device 182
8.3.1 Flush Panel Mounting 182
8.3.2 Rack Mounting 182
8.4 Cables and Connectors 184
8.4.1 Terminal Blocks 184
8.4.2 Power Supply Connections 185
8.4.3 Earth Connnection 185
8.4.4 Current Transformers 185
8.4.5 Voltage Transformer Connections 186
8.4.6 Watchdog Connections 186
8.4.7 EIA(RS)485 and K-Bus Connections 186
8.4.8 IRIG-B Connection 186
8.4.9 Opto-input Connections 186
8.4.10 Output Relay Connections 187
8.4.11 Ethernet Metallic Connections 187
8.4.12 Ethernet Fibre Connections 187
8.4.13 USB Connection 187
8.4.14 GPS Fibre Connection 187
8.4.15 Fibre Communication Connections 188
8.5 Case Dimensions 189
8.5.1 Case Dimensions 40TE 189
8.5.2 Case Dimensions 60TE 190
8.5.3 Case Dimensions 80TE 191

Chapter 9 Commissioning Instructions 192

9.1 Chapter Overview 193
9.2 General Guidelines 194
9.3 Commissioning Test Menu 195
9.3.1 Opto I/P Status Cell (Opto-input Status) 195
9.3.2 Relay O/P Status Cell (Relay Output Status) 195
9.3.3 Test Port Status Cell 195
9.3.4 Monitor Bit 1 to 8 Cells 195
9.3.5 Test Mode Cell 196
9.3.6 Test Pattern Cell 196
9.3.7 Contact Test Cell 196

9.3.8	Test LEDs Cell	196
9.3.9	Test Autoreclose Cell	196
9.3.10	Red and Green LED Status Cells	197
9.4	**Commissioning Equipment**	**198**
9.4.1	Recommended Commissioning Equipment	198
9.4.2	Essential Commissioning Equipment	198
9.4.3	Advisory Test Equipment	199
9.5	**Product Checks**	**200**
9.5.1	Product Checks with the IED De-energised	200
9.5.1.1	Visual Inspection	200
9.5.1.2	Current Transformer Shorting Contacts	201
9.5.1.3	Insulation	201
9.5.1.4	External Wiring	201
9.5.1.5	Watchdog Contacts	201
9.5.1.6	Power Supply	202
9.5.2	Pxxx_CI_ProductChecksEnergised	202
9.5.2.1	Watchdog Contacts	202
9.5.2.2	Test LCD	202
9.5.2.3	Date and Time	203
9.5.2.4	Test LEDs	203
9.5.2.5	Test Alarm and Out-of-Service LEDs	203
9.5.2.6	Test Trip LED	204
9.5.2.7	Test User-programmable LEDs	204
9.5.2.8	Test Opto-inputs	204
9.5.2.9	Test Output Relays	204
9.5.2.10	Test Serial Communication Port RP1	204
9.5.2.11	Test Serial Communication Port RP2	206
9.5.2.12	Test Ethernet Communication	207
9.5.3	Secondary Injection Tests	207
9.5.3.1	Test Current Inputs	207
9.5.3.2	Test Voltage Inputs	207
9.6	**Setting Checks**	**209**
9.6.1	Apply Application-specific Settings	209
9.6.1.1	Transferring Settings from a Settings File	209
9.6.1.2	Entering settings using the HMI	209
9.7	**IEC 61850 Edition 2 Testing**	**211**
9.7.1	Using IEC 61850 Edition 2 Test Modes	211
9.7.1.1	IED Test Mode Behaviour	211
9.7.1.2	Sampled Value Test Mode Behaviour	211
9.7.2	Simulated Input Behaviour	212
9.7.3	Testing Examples	213
9.7.3.1	Test Procedure for Real Values	213
9.7.3.2	Test Procedure for Simulated Values - No Plant	214
9.7.3.3	Test Procedure for Simulated Values - With Plant	214
9.7.3.4	Contact Test	215
9.8	**Correct Distance Function Operation**	**216**
9.8.1	Functional Tests: Start, Control & Distance Characteristic Limits	216
9.8.1.1	Measurements Check	216
9.8.1.2	Default Simulation Principle	221
9.8.1.3	Check and Test of the Starting Characteristics	227
9.9	**Distance Scheme Test (if Activated in MiCOM S1 Agile)**	**234**
9.9.1	Control	234
9.10	**Loss of Guard/Loss of Carrier Test**	**235**
9.11	**Weak Infeed Mode Test**	**236**
9.12	**Protection Operation During Fuse Failure**	**238**
9.13	**Demonstrate Correct Overcurrent Function Operation**	**239**
9.13.1	Connect The Test Circuit	239
9.13.2	Perform The Test	239

9.13.3 Check The Operating Time 240
9.14 Check Trip and Auto-reclose Cycle 241
9.15 Protection Timing Checks 242
9.15.1 Overcurrent Check 242
9.15.2 Connecting the Test Circuit 242
9.15.3 Performing the Test 242
9.15.4 Check the Operating Time 242
9.16 Onload Checks 244
9.16.1 Confirm Current Connections 244
9.16.2 Confirm Voltage Connections 244
9.16.3 On-load Directional Test 245
9.17 Final Checks 246

Chapter 10 Maintenance and Troubleshooting 247

10.1 Chapter Overview 248
10.2 Maintenance 249
10.2.1 Maintenance Checks 249
10.2.1.1 Alarms 249
10.2.1.2 Opto-isolators 249
10.2.1.3 Output Relays 249
10.2.1.4 Measurement Accuracy 249
10.2.2 Replacing the Device 250
10.2.3 Repairing the Device 251
10.2.4 Removing the front panel 251
10.2.5 Replacing PCBs 252
10.2.5.1 Replacing the main processor board 252
10.2.5.2 Replacement of communications boards 253
10.2.5.3 Replacement of the input module 254
10.2.5.4 Replacement of the power supply board 254
10.2.5.5 Replacement of the I/O boards 255
10.2.6 Recalibration 255
10.2.7 Supercapacitor Discharged 255
10.2.8 Cleaning 256
10.3 Troubleshooting 257
10.3.1 Self-Diagnostic Software 257
10.3.2 Power-up Errors 257
10.3.3 Error Message or Code on Power-up 257
10.3.4 Out of Service LED on at power-up 258
10.3.5 Error Code during Operation 259
10.3.6 Mal-operation during testing 259
10.3.6.1 Failure of Output Contacts 259
10.3.6.2 Failure of Opto-inputs 259
10.3.6.3 Incorrect Analogue Signals 260
10.3.7 PSL Editor Troubleshooting 260
10.3.7.1 Diagram Reconstruction 260
10.3.7.2 PSL Version Check 260
10.3.8 Repair and Modification Procedure 261

Chapter 11 Technical Specifications 262

11.1 Chapter Overview 263
11.2 Technical Data 264
11.2.1 Input/Output (I/O) 264
11.3 Interfaces 265
11.3.1 Front USB Port 265
11.3.2 Rear Serial Port 1 265

11.3.3	Fibre Rear Serial Port 1	265
11.3.4	Rear Serial Port 2	265
11.3.5	Optional Rear Serial Port (SK5)	266
11.3.6	IRIG-B (Demodulated)	266
11.3.7	IRIG-B (Modulated)	266
11.3.8	Rear Ethernet Port Copper	266
11.3.9	Rear Ethernet Port Fibre (Hardware Option (R/S/T)	267
11.3.9.1	100 Base FX Receiver Characteristics	267
11.3.9.2	100 Base FX Transmitter Characteristics	267
11.3.10	Rear Ethernet Port Fibre (Hardware Option U/W/Y)	267
11.3.10.1	100 Base FX Receiver Characteristics	268
11.3.10.2	100 Base FX Transmitter Characteristics	268
11.4	**Measurements and Recording**	**269**
11.4.1	General	269
11.4.2	Disturbance Records	269
11.4.3	Event, Fault and Maintenance Records	269
11.4.4	Fault Locator	269
11.5	**Ratings**	**270**
11.5.1	AC Measuring Inputs	270
11.5.2	Current Transformer Inputs	270
11.5.3	Voltage Transformer Inputs	270
11.5.4	Nominal Burden	270
11.5.5	Supercapacitor	271
11.6	**Mechanical Specifications**	**272**
11.6.1	Physical Parameters	272
11.6.2	Enclosure Protection	272
11.6.3	Mechanical Robustness	272
11.6.4	Transit Packaging Performance	272
11.7	**Type Tests**	**273**
11.7.1	Insulation	273
11.7.2	Creepage Distances and Clearances	273
11.7.3	High Voltage (Dielectric) Withstand	273
11.7.4	Impulse Voltage Withstand Test	273
11.8	**Environmental Conditions**	**274**
11.8.1	Ambient Temperature Range	274
11.8.2	Temperature Endurance Test	274
11.8.3	Ambient Humidity Range	274
11.8.4	Corrosive Environments	274
11.9	**Electromagnetic Compatibility**	**275**
11.9.1	1 MHz Burst High Frequency Disturbance Test	275
11.9.2	Damped Oscillatory Test	275
11.9.3	Immunity to Electrostatic Discharge	275
11.9.4	Electrical Fast Transient or Burst Requirements	275
11.9.5	Surge Withstand Capability	275
11.9.6	Surge Immunity Test	276
11.9.7	Immunity to Radiated Electromagnetic Energy	276
11.9.8	Radiated Immunity from Digital Communications	276
11.9.9	Radiated Immunity from Digital Radio Telephones	276
11.9.10	Immunity to Conducted Disturbances Induced by Radio Frequency Fields	276
11.9.11	Magnetic Field Immunity	277
11.9.12	Conducted Emissions	277
11.9.13	Radiated Emissions	277
11.9.14	Power Frequency	277
11.10	**Regulatory Compliance**	**278**
11.10.1	EMC Compliance: 2014/30/EU	278
11.10.2	LVD Compliance: 2014/35/EU	278

11.10.3 UL/CUL Compliance 278

Appendix A Ordering Options 279

Appendix B Settings and Signals 280

Appendix C Wiring Diagrams 281

Table of Figures

Figure 1:	Hardware architecture	18
Figure 2:	Coprocessor hardware architecture	19
Figure 3:	Exploded view of IED	20
Figure 4:	Front panel (60TE)	22
Figure 5:	HMI panel	23
Figure 6:	Rear view of populated case	26
Figure 7:	Terminal block types	27
Figure 8:	Example - fitted IP2x shields (cabling omitted for clarity)	27
Figure 9:	Rear connection to terminal block	28
Figure 10:	Main processor board	29
Figure 11:	Power supply board	30
Figure 12:	Power supply assembly	31
Figure 13:	Power supply terminals	32
Figure 14:	Watchdog contact terminals	33
Figure 15:	Rear serial port terminals	34
Figure 16:	Input module - 1 transformer board	34
Figure 17:	Input module schematic	35
Figure 18:	Frequency response	36
Figure 19:	Transformer board	37
Figure 20:	Input board	38
Figure 21:	Standard relay output board - 8 contacts	40
Figure 22:	High Break relay output board	42
Figure 23:	High Break contact operation	43
Figure 24:	IRIG-B board	45
Figure 25:	Fibre optic board	46
Figure 26:	Rear communication board	47
Figure 27:	Redundant Ethernet board	48
Figure 28:	Ethernet board	50
Figure 29:	Redundant Ethernet board	51
Figure 30:	IEC 61850-9-2LE board	54
Figure 31:	Fully populated Coprocessor board	55
Figure 32:	Software Architecture	58
Figure 33:	Frequency Response (indicative only)	63
Figure 34:	Navigating the HMI	69
Figure 35:	Default display navigation	71
Figure 36:	RS485 biasing circuit	86
Figure 37:	Remote communication using K-Bus	87
Figure 38:	Example PRP redundant network	90

Figure 39:	HSR multicast topology	91
Figure 40:	HSR unicast topology	91
Figure 41:	HSR application in the substation	92
Figure 42:	IED attached to redundant Ethernet star or ring circuit	93
Figure 43:	Control input behaviour	112
Figure 44:	Data model layers in IEC61850	124
Figure 45:	Edition 2 system - backward compatibility	128
Figure 46:	Edition 1 system - forward compatibility issues	129
Figure 47:	Example of Standby IED	130
Figure 48:	Standby IED Activation Process	130
Figure 49:	GPS satellite timing signal	135
Figure 50:	Timing error using ring or line topology	137
Figure 51:	IED and REB IP address configuration	139
Figure 52:	Connection using (a) an Ethernet switch and (b) a media converter	143
Figure 53:	RADIUS server/client communication	168
Figure 54:	Rack mounting of products	183
Figure 55:	Terminal block types	184
Figure 56:	40TE case dimensions	189
Figure 57:	60TE case dimensions	190
Figure 58:	80TE case dimensions	191
Figure 59:	RP1 physical connection	205
Figure 60:	Remote communication using K-bus	206
Figure 61:	Simulated input behaviour	212
Figure 62:	Test example 1	213
Figure 63:	Test example 2	214
Figure 64:	Test example 3	215
Figure 65:	Control of VT & CT ratio's	217
Figure 66:	Measurement 1/LCD menu	218
Figure 67:		219
Figure 68:	Measurement setup/LCD menu	221
Figure 69:	Characteristic point determination (Rlim two-phase & Single-phase can be different)	222
Figure 70:	Example of Z-graph screen (Rio format can be created as well)	222
Figure 71:	Evolving impedance from the load area to the final fault impedance in Zone1	223
Figure 72:	Single characteristic with P forward zone	224
Figure 73:		228
Figure 74:	LCD menu for a control of an input/output/monitor bits check	229
Figure 75:	Example: AN - lim Z1	231
Figure 76:	Example: AB - limR2	232
Figure 77:	Example: ABC-limZ4 (Reverse)	232

Figure 78:	Points limit of the characteristic to be tested (with Zp selected as a reverse zone)	233
Figure 79:	Winf2	236
Figure 80:		237
Figure 81:	Possible terminal block types	251
Figure 82:	Front panel assembly	253

CHAPTER 1

INTRODUCTION

1.1 SCOPE OF THIS ADDENDUM

This addendum describes the functional enhancements, which have occurred since the release of the last full technical manual and subsequent addenda. This addendum covers software versions 80, 82, 83 and 91, and includes the following features:

- IEC 61850 Edition 1/2 switching.
- IEC 61850 Edition 2 support for test modes for online testing.
- IEEE 1588 Precision Time Protocol - efficient time synchronising direct from the substation LAN.
- Editable logical nodes/devices - customise the IEC 61850 modelling; maximum interoperability.
- Role based access control (RBAC) for centralised authentication.
- Authorization and account management via RADIUS, and directly on the relay.
- Security event management via syslog.
- Duplicate GOOSE rejection – defense against incorrect publishing of out-of-sequence or duplicated GOOSE messages by other devices on the network.
- SNMP version 2c and cybersecure v3 - network management tools can monitor protection IEDs.
- New Ethernet board support – improved traffic density handling assists in deploying bandwidth-hungry schemes for autotransformer switching
- Supercapacitor replaces backup battery
- USB type B port replaces front panel I/O

This addendum should be read alongside the last full technical manual covering this product:

- P44x/EN M/Hb6 - software version 72

1.1.1 IED COMPATIBILITY

This product version includes the following options:

- Black and silver front panel
- Front panel USB type B port
- Internal supercapacitor

Functional parity between legacy white and the black/silver front panel IEDs is maintained using an internal supercapacitor, which replaces the lithium battery. A front panel USB type B port replaces front panel serial and parallel ports.

Note:
To maintain software compatibility, IEDs will refer to the 'Battery' when a supercapacitor is fitted, as this provides backup battery functionality in the black and silver front panel versions.

Note:
For ease of navigation, this document includes full chapters applicable to software 91.

1.2 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.

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 5
Health and Safety 6
Symbols 7
Installation, Commissioning and Servicing 8
Decommissioning and Disposal 14
Regulatory Compliance 15

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 harmonized 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 17
Hardware Architecture 18
Mechanical Implementation 20
Front Panel 22
Rear Panel 26
Boards and Modules 28

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.

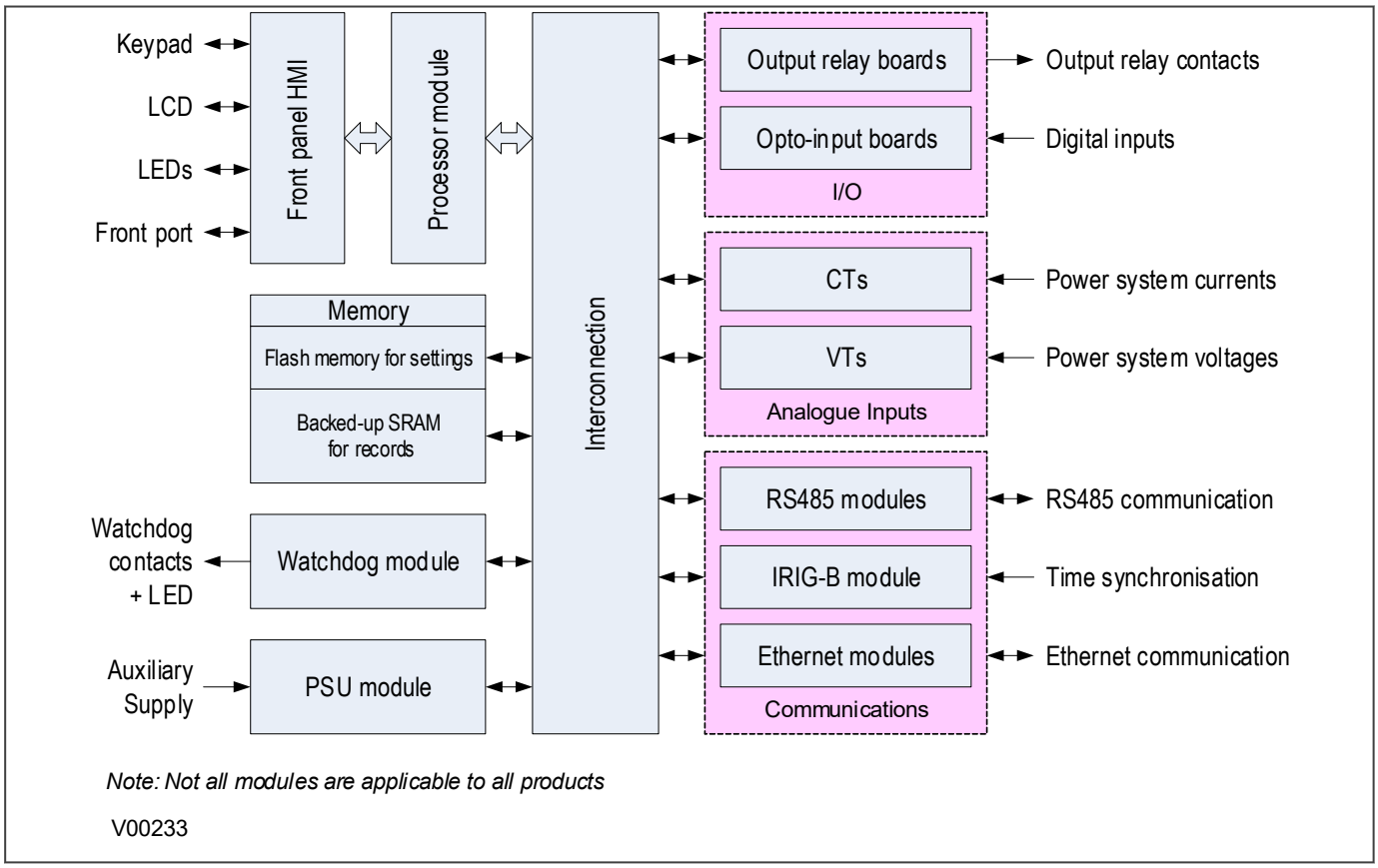


Figure 1: Hardware architecture

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.

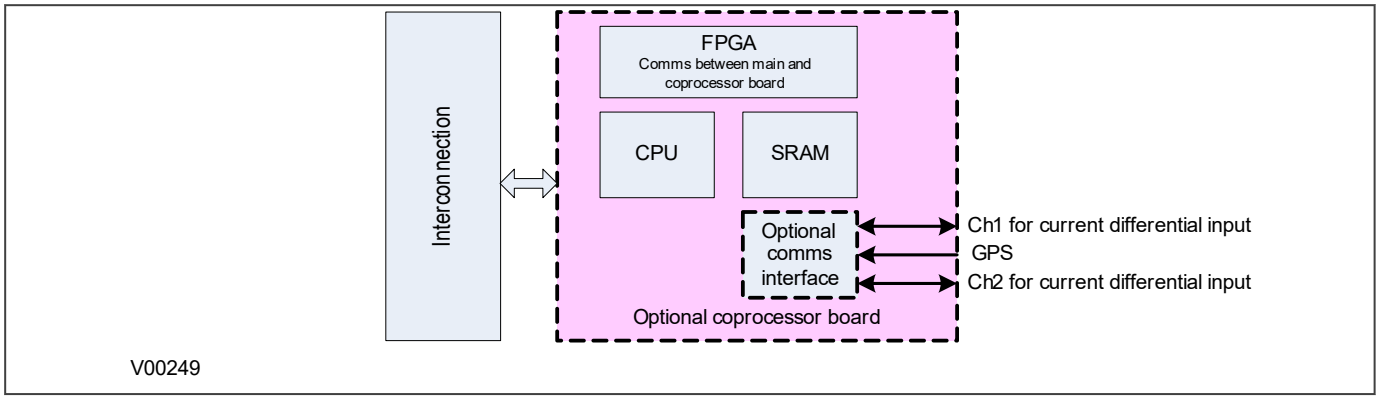


Figure 2: Coprocessor hardware architecture

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.

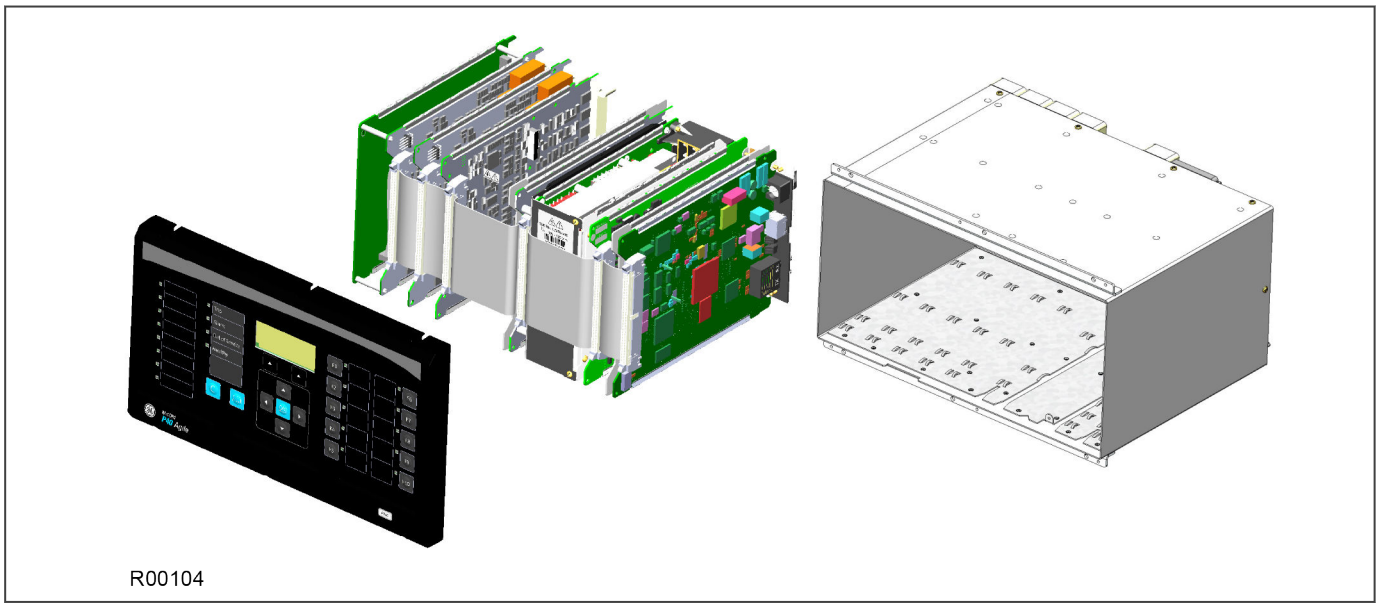


Figure 3: Exploded view of IED

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
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
IEC 61850 9-2LE board	Ethernet board for accepting IEC 61850 sampled values
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 on-board 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)
Output relay output board	Standard output relay board
High-break output relay board	Output relay board with high breaking capacity relays

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 4: 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 HMI PANEL

The keypad provides full access to the device functionality using a range of menu options. The information is displayed on the LCD.The LCD is a high resolution monochrome display with 16 characters by 3 lines and controllable back light.

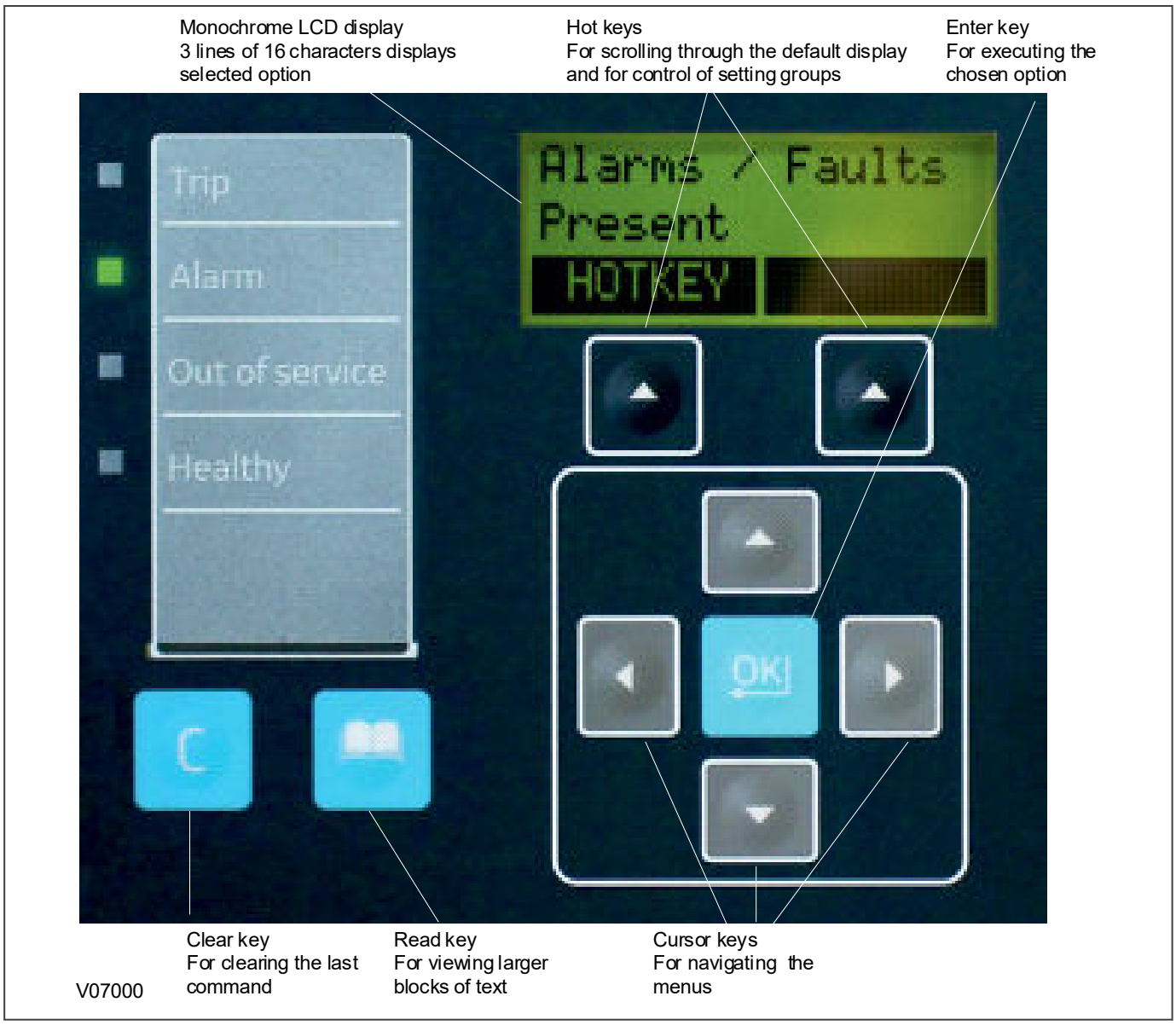
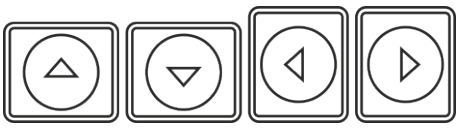


Figure 5: HMI panel

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

3.4.1.3 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.	

3.4.1.3.1 LIQUID CRYSTAL DISPLAY

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

3.4.1.4 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.

3.4.1.5 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.

3.4.1.6 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.

3.4.1.7 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.

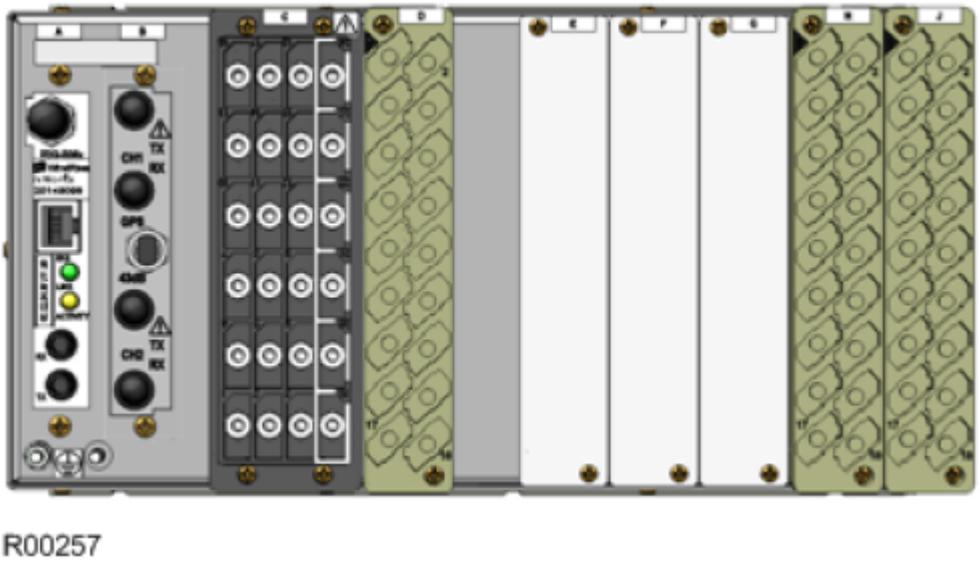


Figure 6: Rear view of populated case

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 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, 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

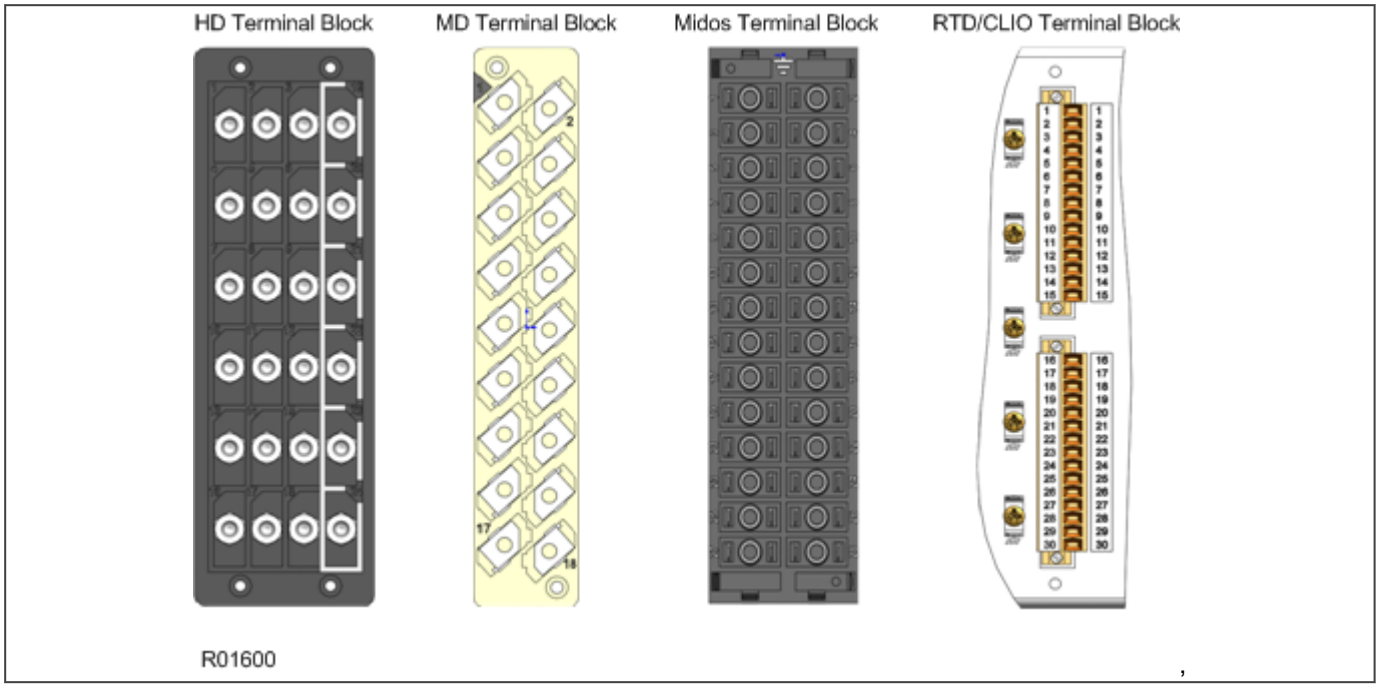


Figure 7: Terminal block types

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.

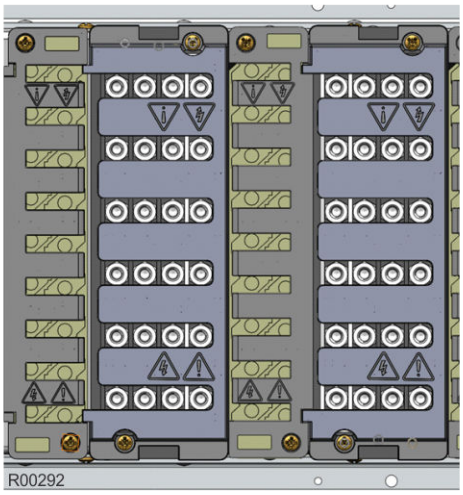


Figure 8: Example - fitted IP2x shields (cabling omitted for clarity)

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)

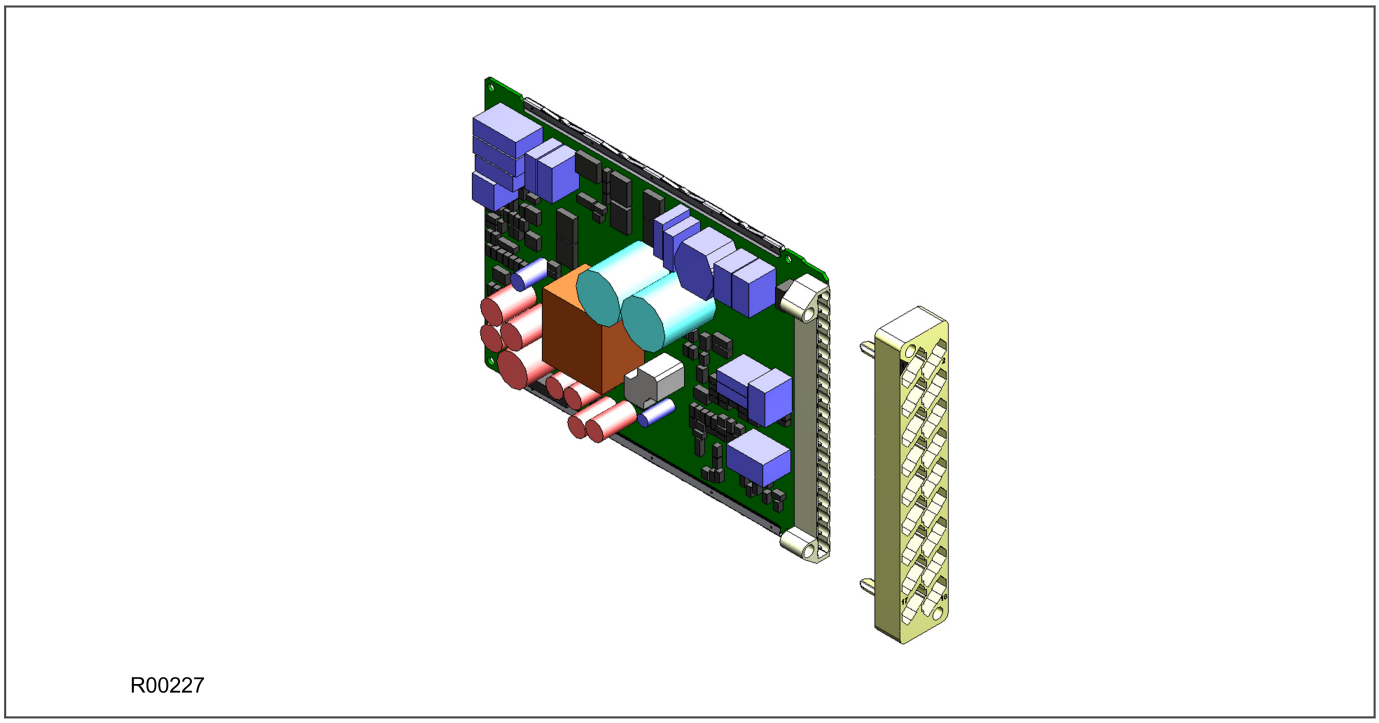


Figure 9: Rear connection to terminal block

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

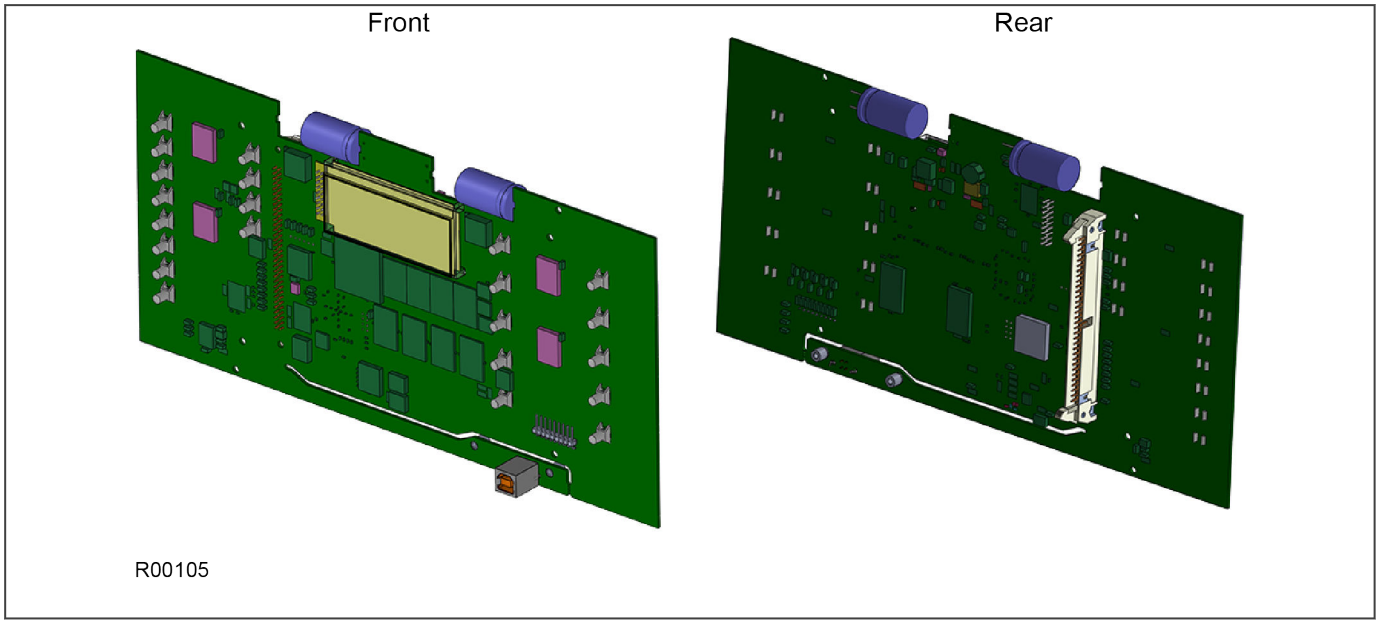


Figure 10: Main processor board

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

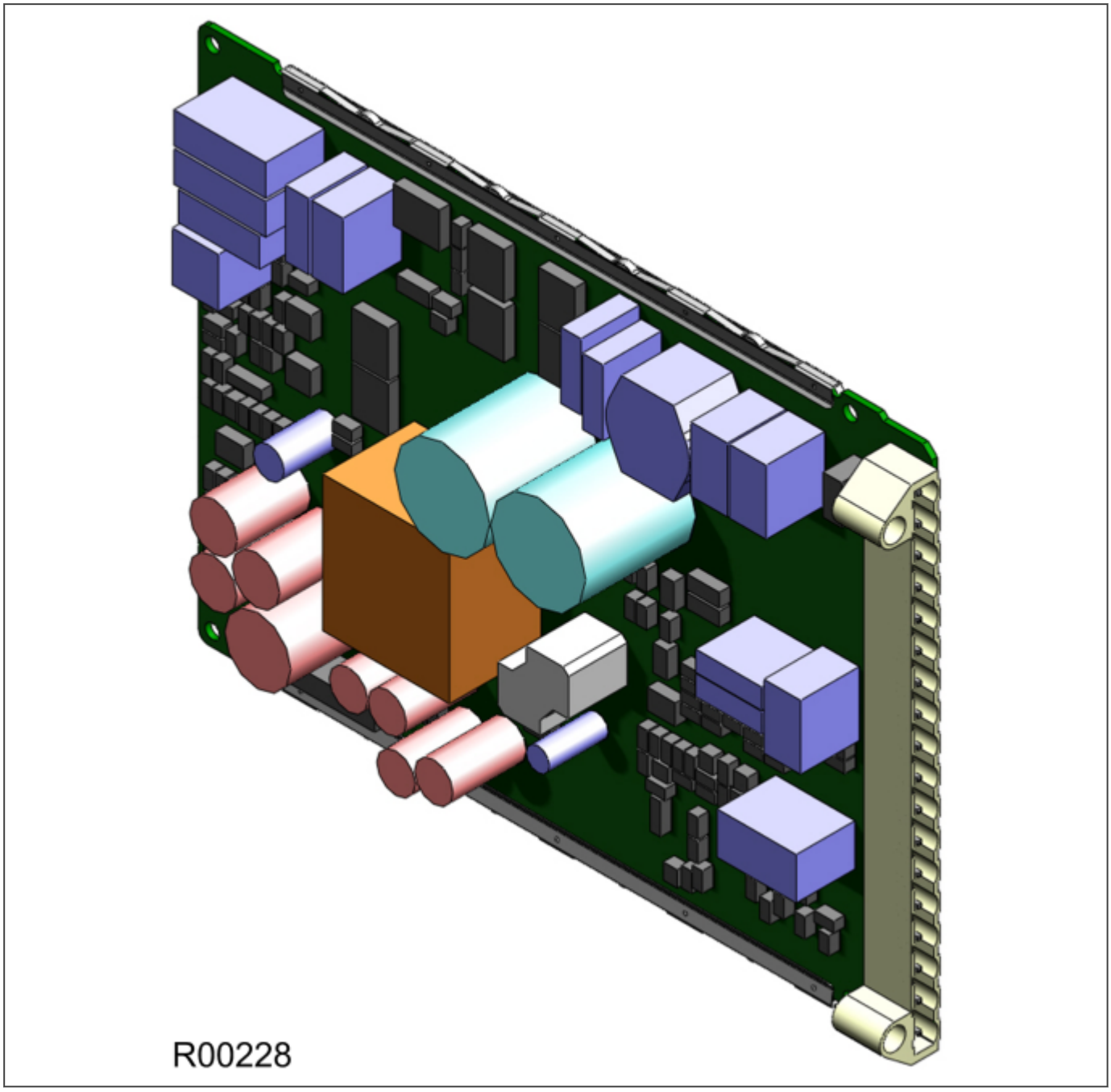


Figure 11: Power supply board

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.

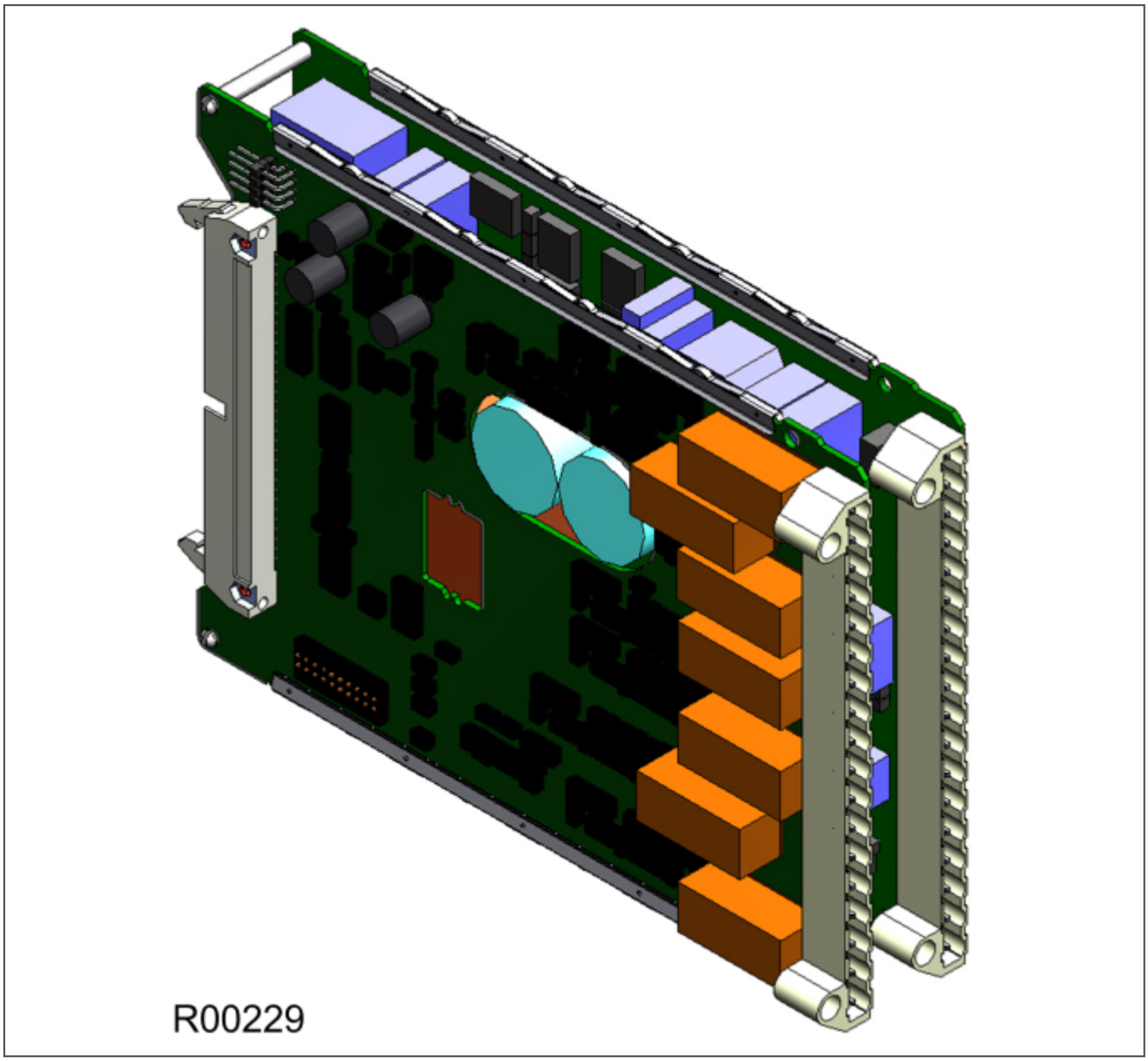


Figure 12: Power supply assembly

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.

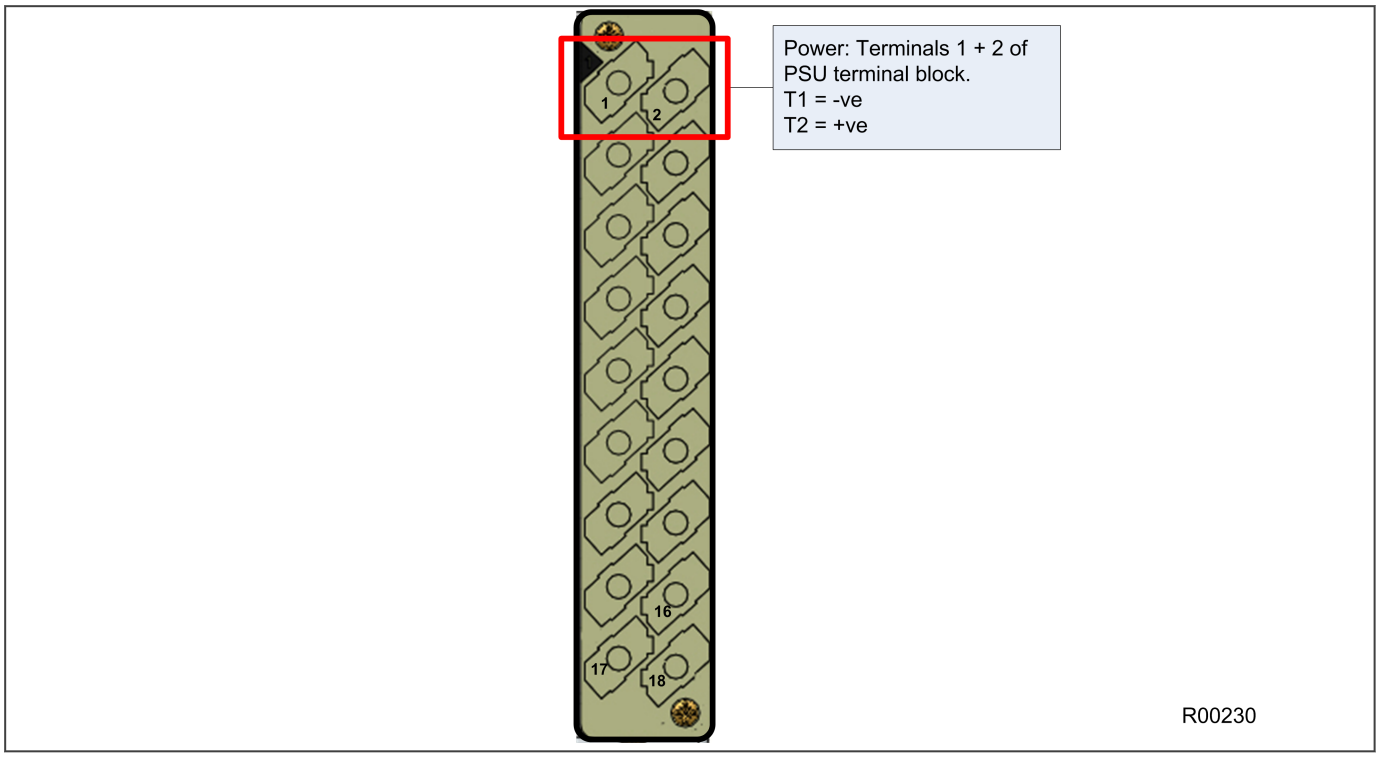


Figure 13: Power supply terminals

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.

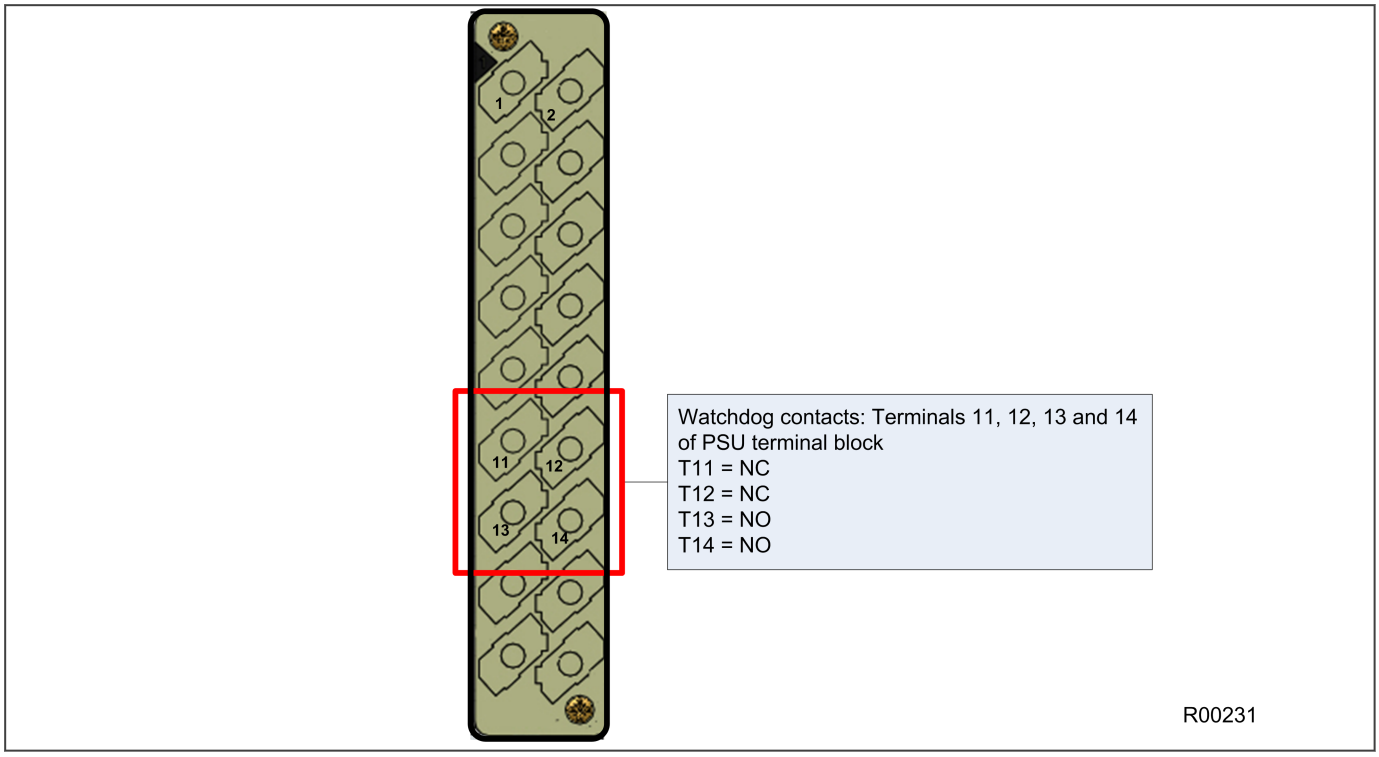


Figure 14: Watchdog contact terminals

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

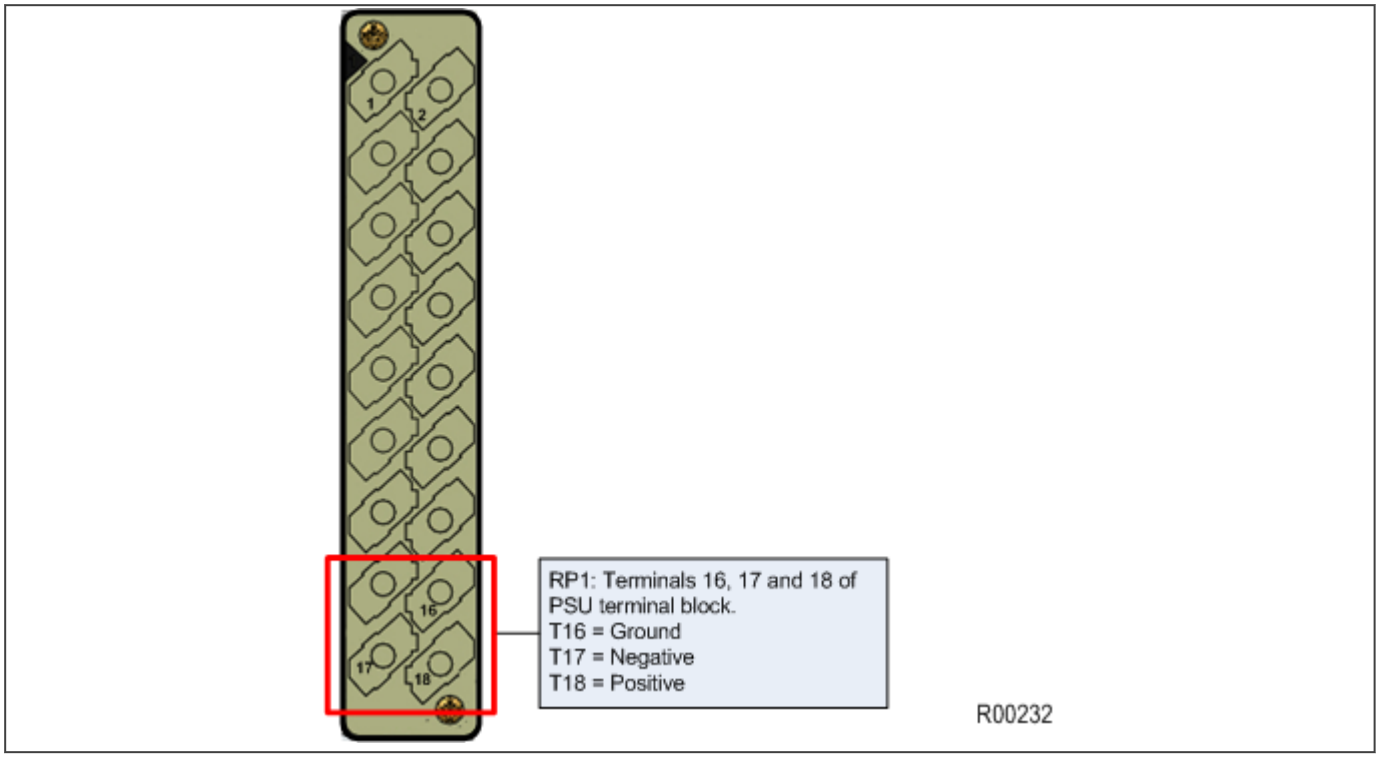


Figure 15: Rear serial port terminals

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

3.6.5 INPUT MODULE - 1 TRANSFORMER BOARD

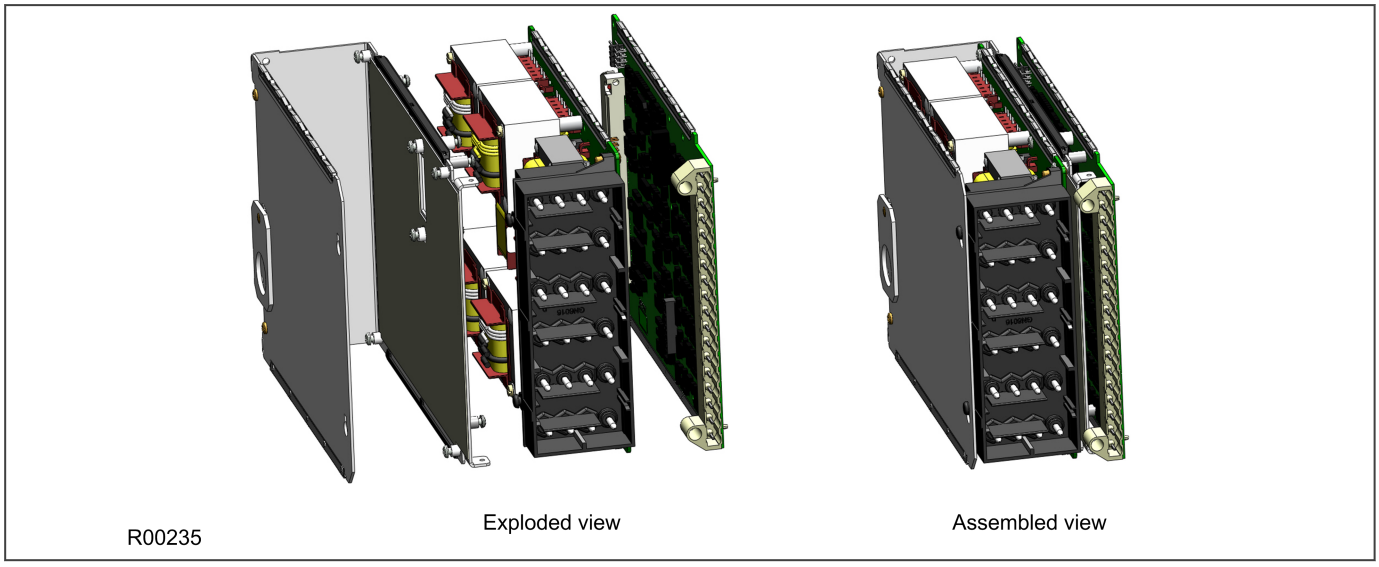


Figure 16: Input module - 1 transformer board

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

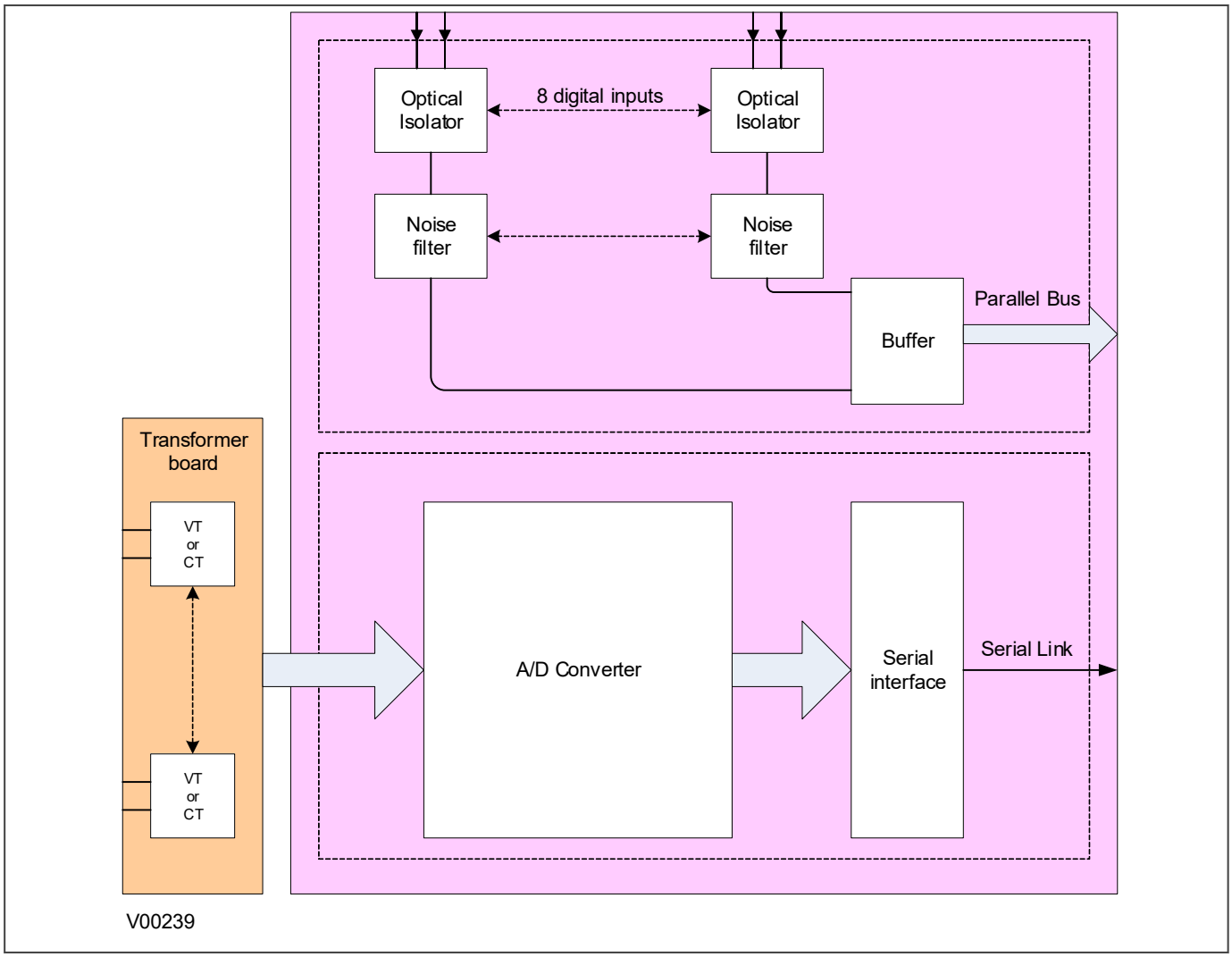


Figure 17: Input module schematic

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 FREQUENCY RESPONSE

With the exception of the RMS measurements, all other measurements and protection functions are based on the Fourier-derived fundamental component. The fundamental component is extracted by using a 24 sample Discrete Fourier Transform (DFT). This gives good harmonic rejection for frequencies up to the 23rd harmonic. The 23rd is the first predominant harmonic that is not attenuated by the Fourier filter and this is known as an 'Alias'. However, the Alias is attenuated by approximately 85% by an additional, analogue, 'anti-aliasing' filter (low pass filter). The combined affect of the anti-aliasing and Fourier filters is shown below.

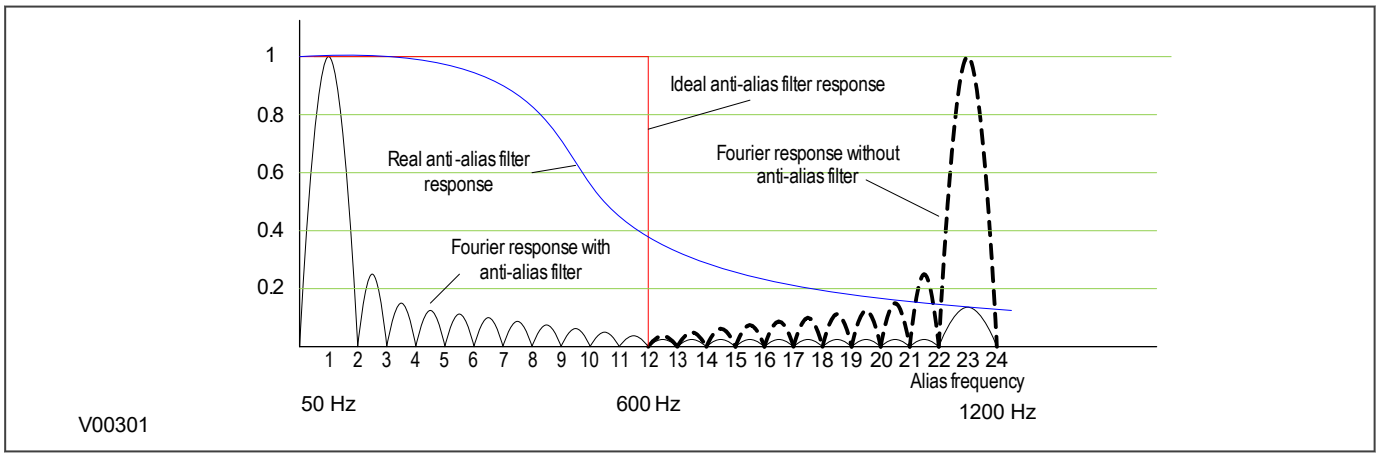


Figure 18: Frequency response

For power frequencies that are not equal to the selected rated frequency, the harmonics are attenuated to zero amplitude. For small deviations of +/-1 Hz, this is not a problem but to allow for larger deviations, frequency tracking is used.

Frequency tracking automatically adjusts the sampling rate of the analog to digital conversion to match the applied signal. In the absence of a suitable signal to amplitude track, the sample rate defaults to the selected rated frequency (Fn). If the signal is in the tracking range of 45 to 66 Hz, the relay locks onto the signal and the measured frequency coincides with the power frequency. The outputs for harmonics up to the 23rd are zero. The device frequency tracks off any voltage or current in the order VA/VB/VC/IA/IB/IC down to 10% Vn for voltage and 5%In for current.

3.6.5.3 TRANSFORMER BOARD

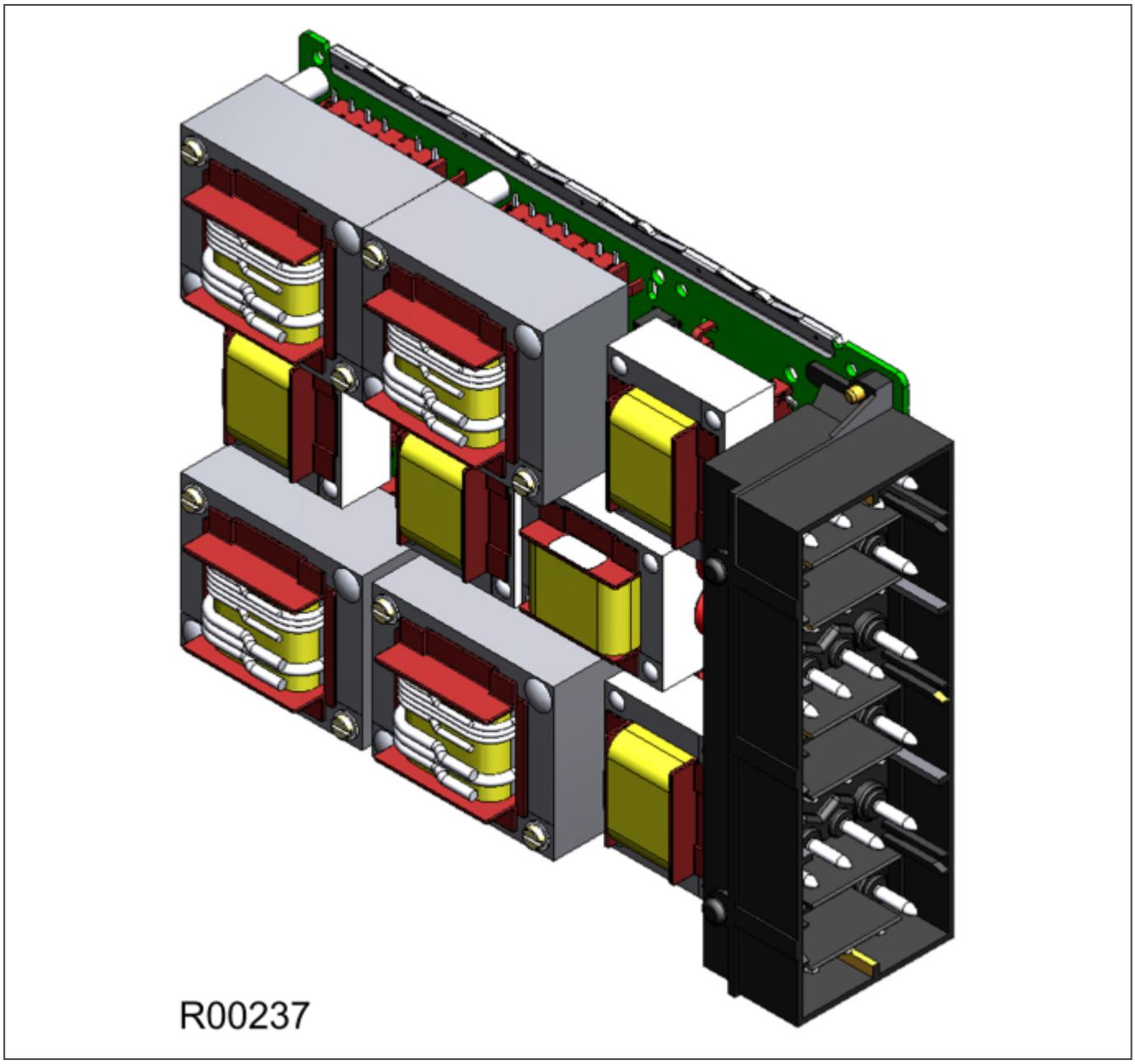


Figure 19: Transformer board

The transformer board hosts the current and voltage transformers. These are used to step down the currents and voltages originating from the power systems' current and voltage transformers to levels that can be used by the devices' electronic circuitry. In addition to this, the on-board CT and VT transformers provide electrical isolation between the unit and the power system.

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

For terminal connections, please refer to the wiring diagrams.

3.6.5.4 INPUT BOARD

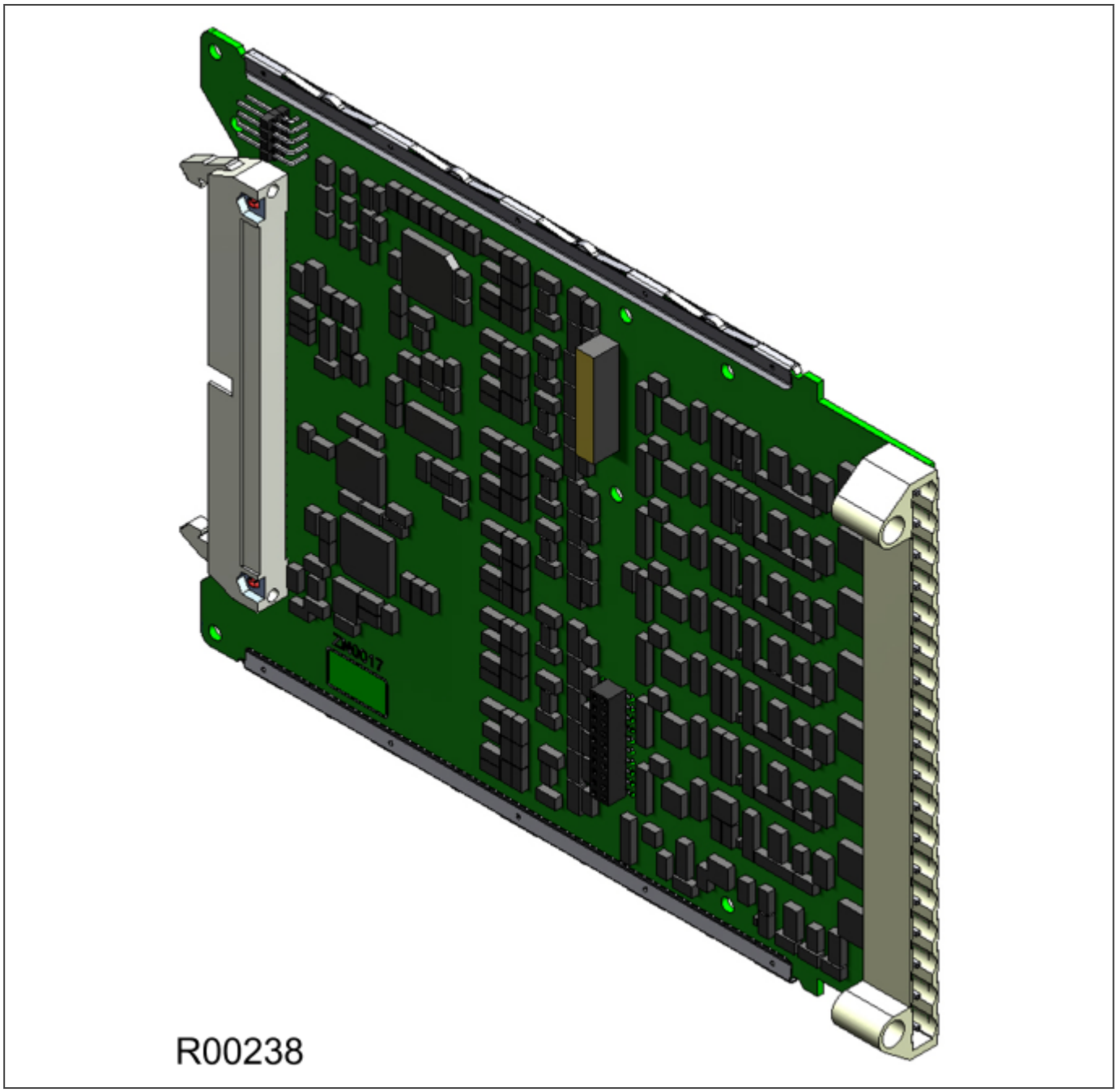


Figure 20: Input board

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

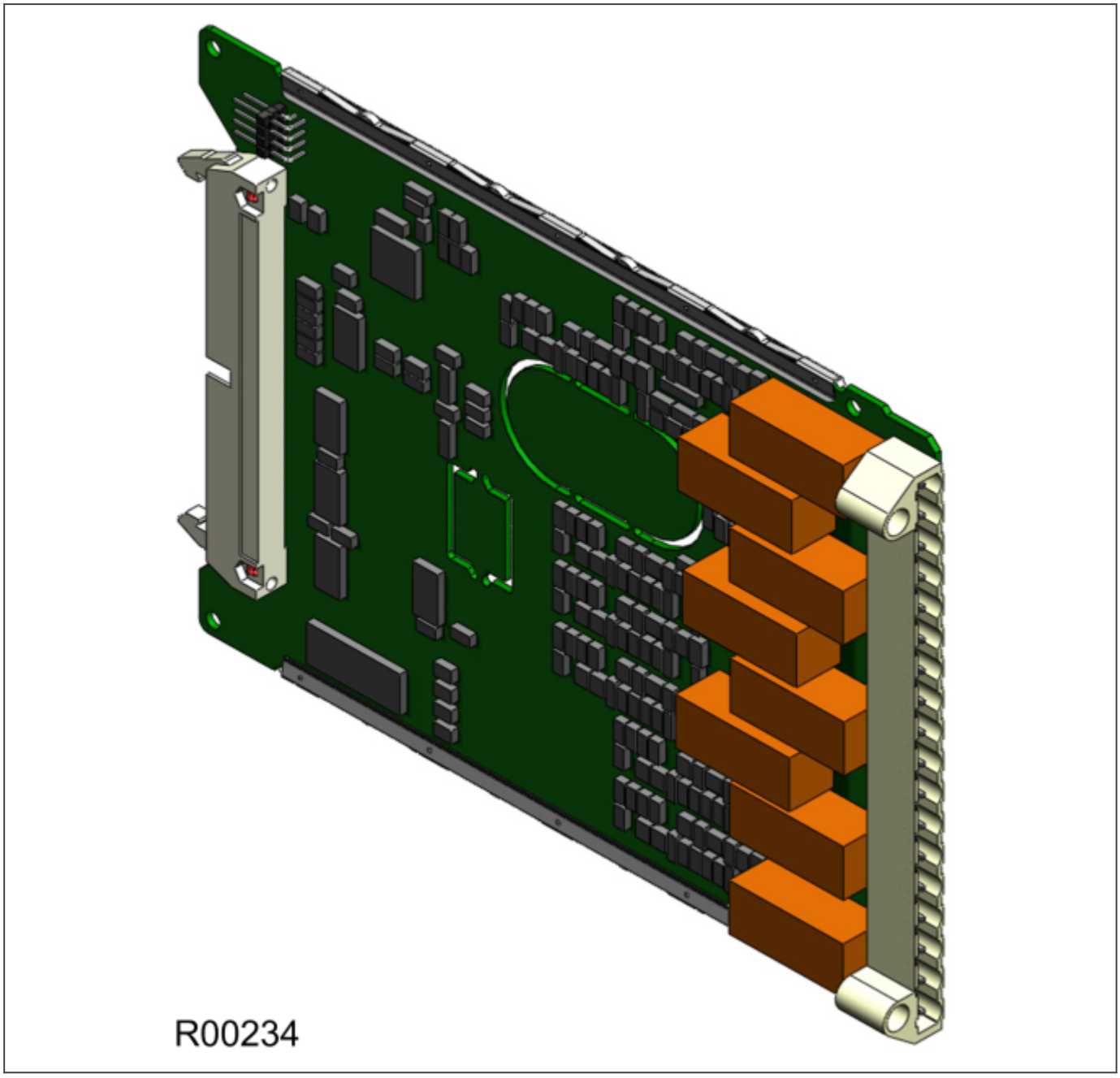


Figure 21: Standard relay output board - 8 contacts

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 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 HIGH BREAK OUTPUT RELAY BOARD

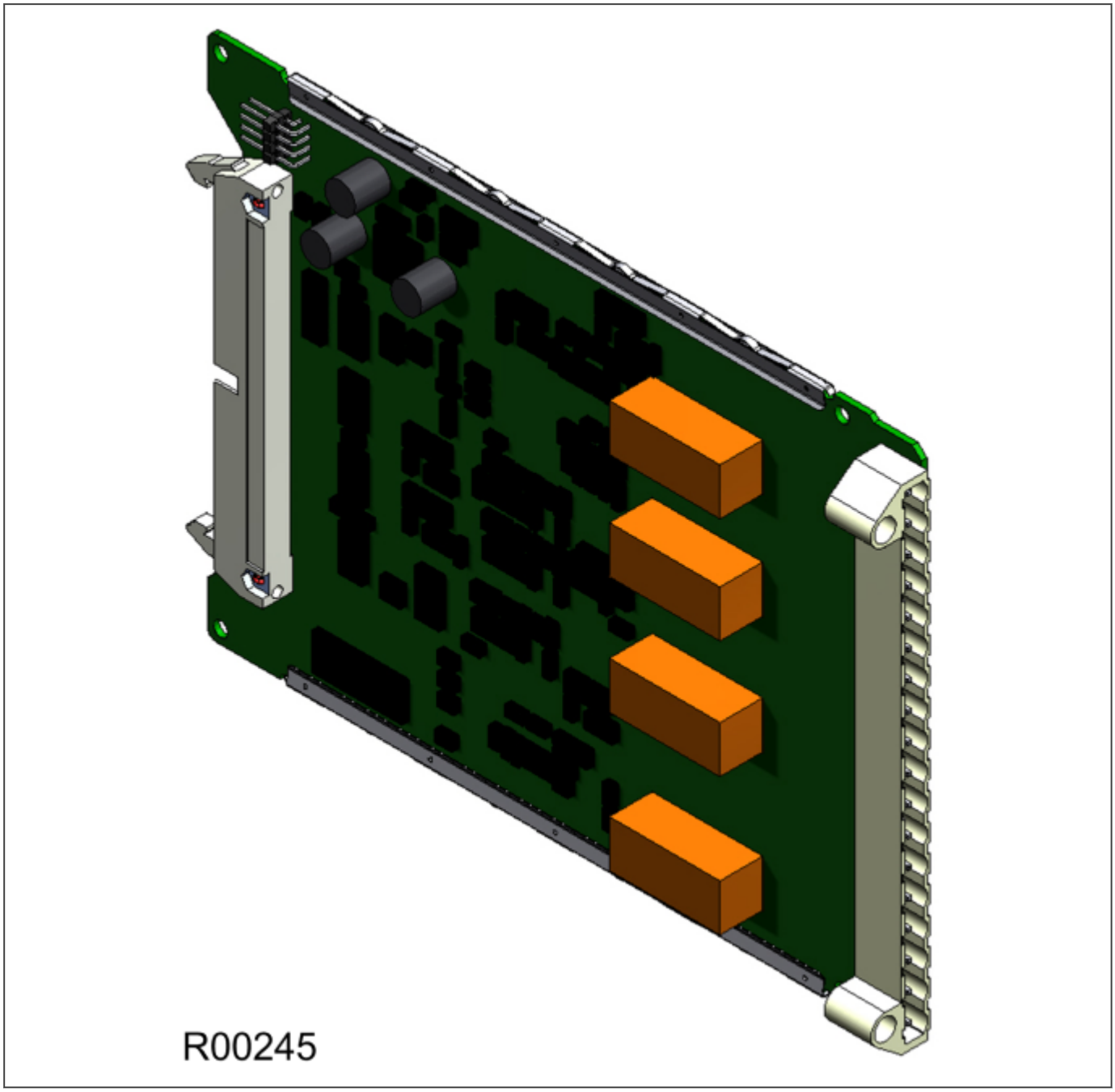


Figure 22: High Break relay output board

A High Break output relay board is available as an option. It comprises four normally open output contacts, which are suitable for high breaking loads.

A High Break contact consists of a high capacity relay with a MOSFET in parallel with it. The MOSFET has a varistor placed across it to provide protection, which is required when switching off inductive loads. This is because the stored energy in the inductor causes a high reverse voltage that could damage the MOSFET, if not protected.

When there is a control input command to operate an output contact the miniature relay is operated at the same time as the MOSFET. The miniature relay contact closes in nominally 3.5 ms and is used to carry the continuous load current. The MOSFET operates in less than 0.2 ms, but is switched off after 7.5 ms.

When the control input is reset, the MOSFET is again turned on for 7.5 mS. The miniature relay resets in nominally 3.5 ms before the MOSFET. This means the MOSFET is used to break the load. The MOSFET absorbs the energy when breaking inductive loads and so limits the resulting voltage surge. This contact arrangement is for switching DC circuits only.

The board number is:

- ZN0042 001

High Break Contact Operation

The following figure shows the timing diagram for High Break contact operation.

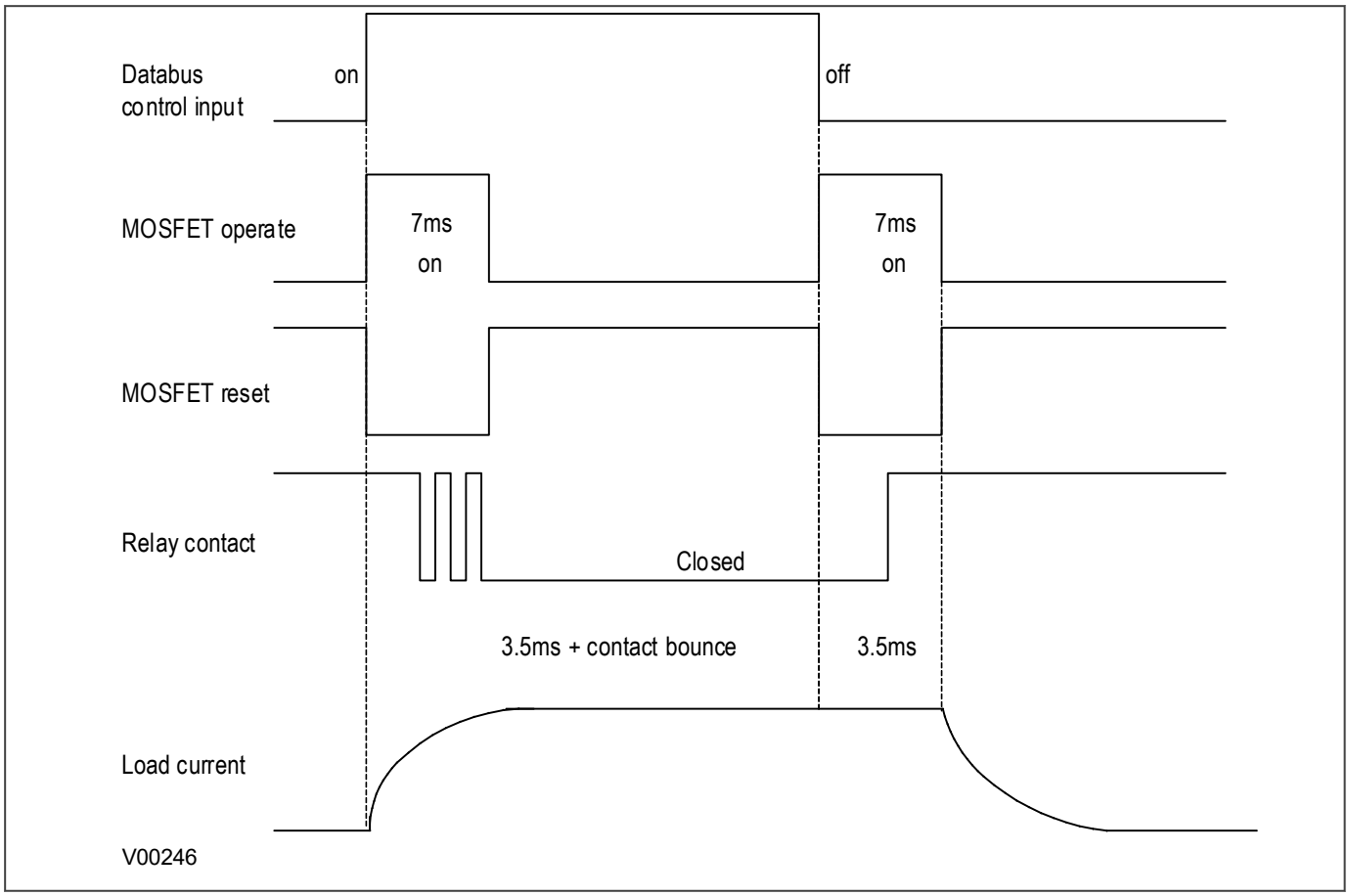


Figure 23: High Break contact operation

High Break Contact Applications

- Efficient scheme engineering

  In traditional hard wired scheme designs, High Break capability could only be achieved using external electromechanical trip relays. Instead, these internal High Break contacts can be used thus reducing space requirements.
- Accessibility of CB auxiliary contacts

  It is common practise to use circuit breaker 52a (CB Closed) auxiliary contacts to break the trip coil current on breaker opening, thereby easing the duty on the protection contacts. In some cases (such as operation of disconnectors, or retrofitting), it may be that 52a contacts are either unavailable or unreliable. In such cases, High Break contacts can be used to break the trip coil current in these applications.
- Breaker fail

In the event of failure of the local circuit breaker (stuck breaker), or defective auxiliary contacts (stuck contacts), it is incorrect to use 52a contact action. The interrupting duty at the local breaker then falls on the relay output contacts, which may not be rated to perform this duty. High Break contacts should be used in this case to avoid the risk of burning out relay contacts.

- Initiation of teleprotection

  The High Break contacts also offer fast making, which results in faster tripping. In addition, fast keying of teleprotection is a benefit. Fast keying bypasses the usual contact operation time, such that permissive, blocking and intertrip commands can be routed faster.



Warning:
These relay contacts are POLARITY SENSITIVE. External wiring must comply with the polarity requirements described in the external connection diagram to ensure correct operation.

3.6.8 IRIG-B BOARD

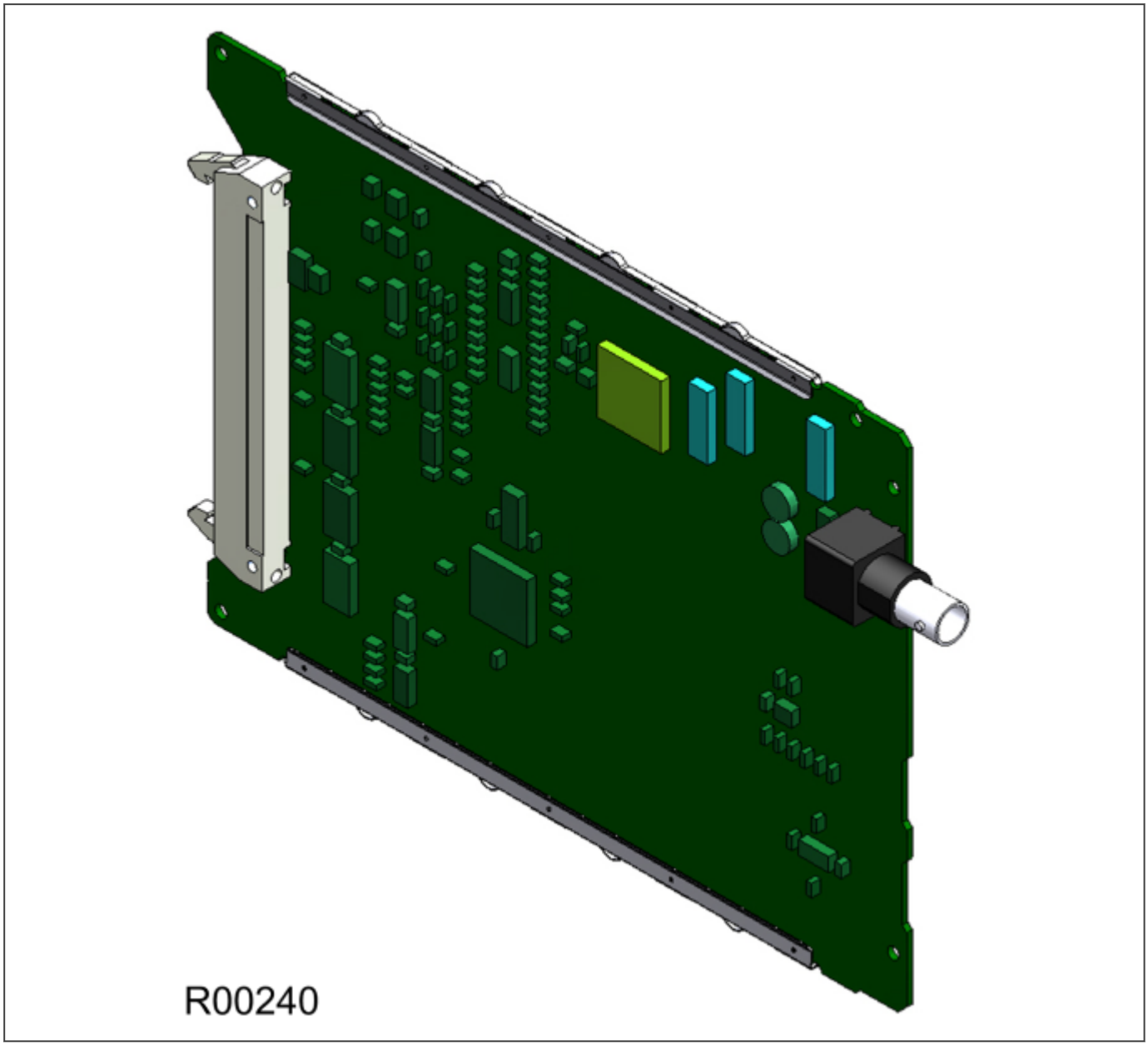


Figure 24: IRIG-B board

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.

3.6.9 FIBRE OPTIC BOARD

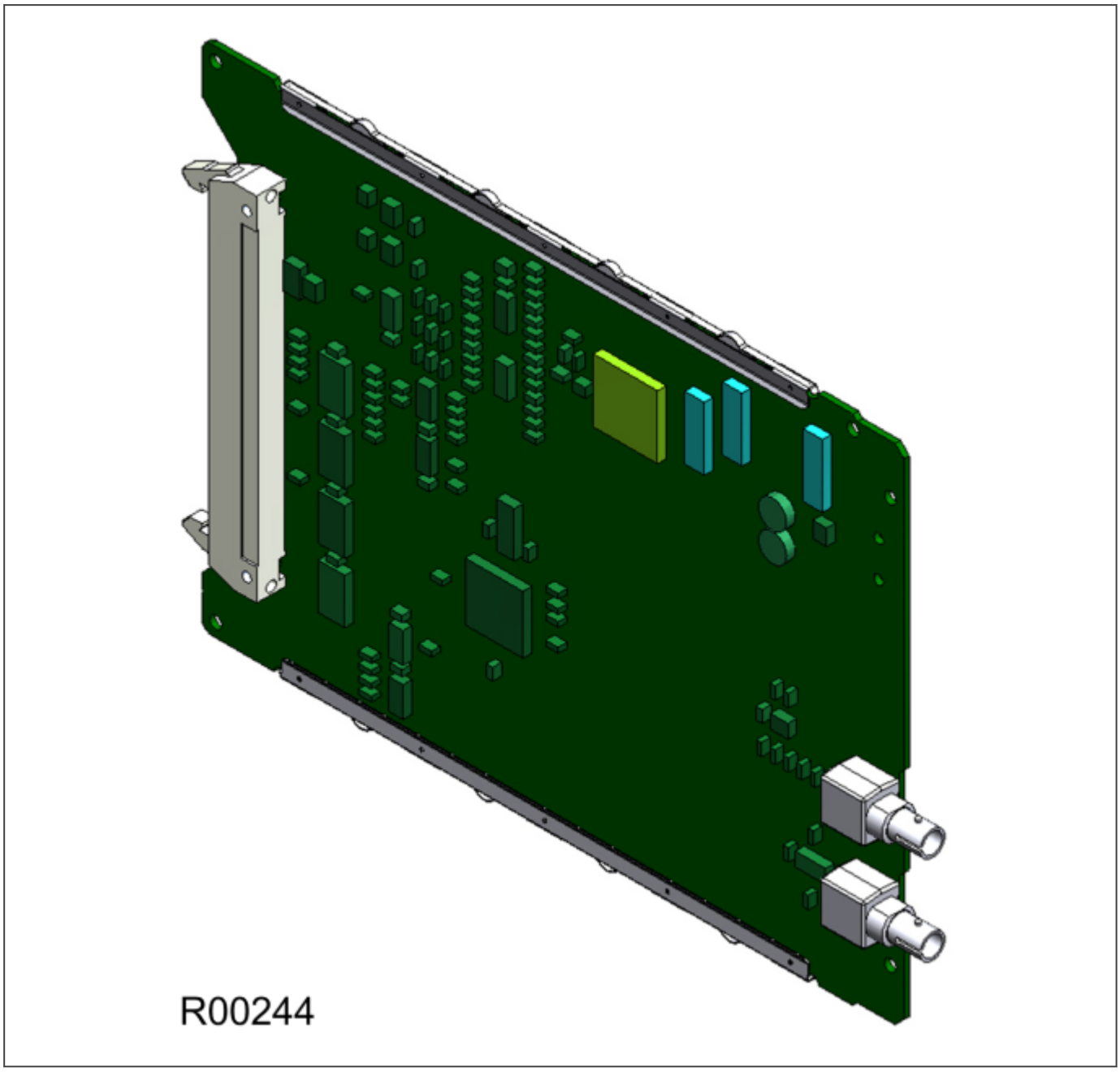


Figure 25: Fibre optic board

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:

3.6.10 REAR COMMUNICATION BOARD

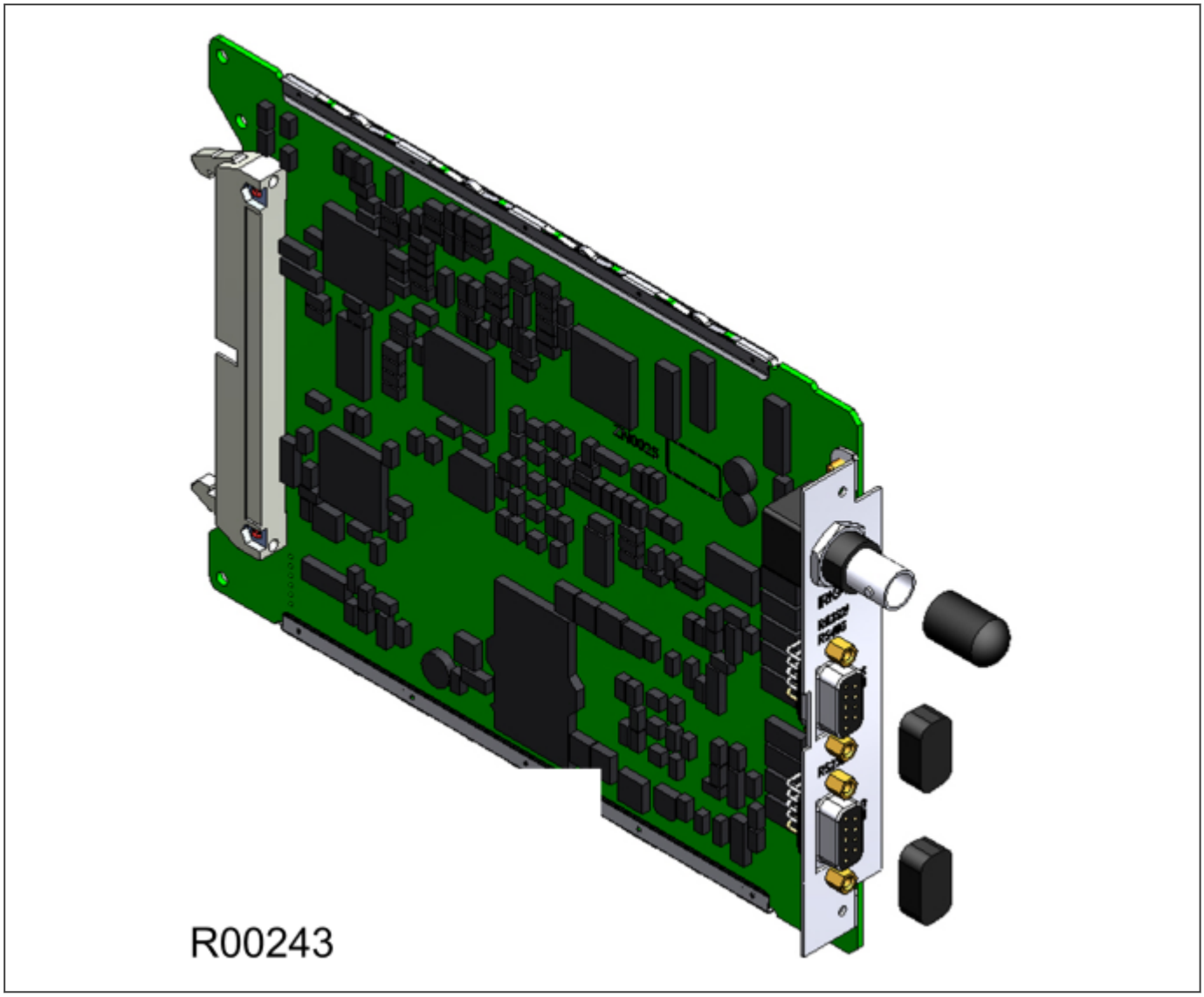


Figure 26: Rear communication board

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.

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

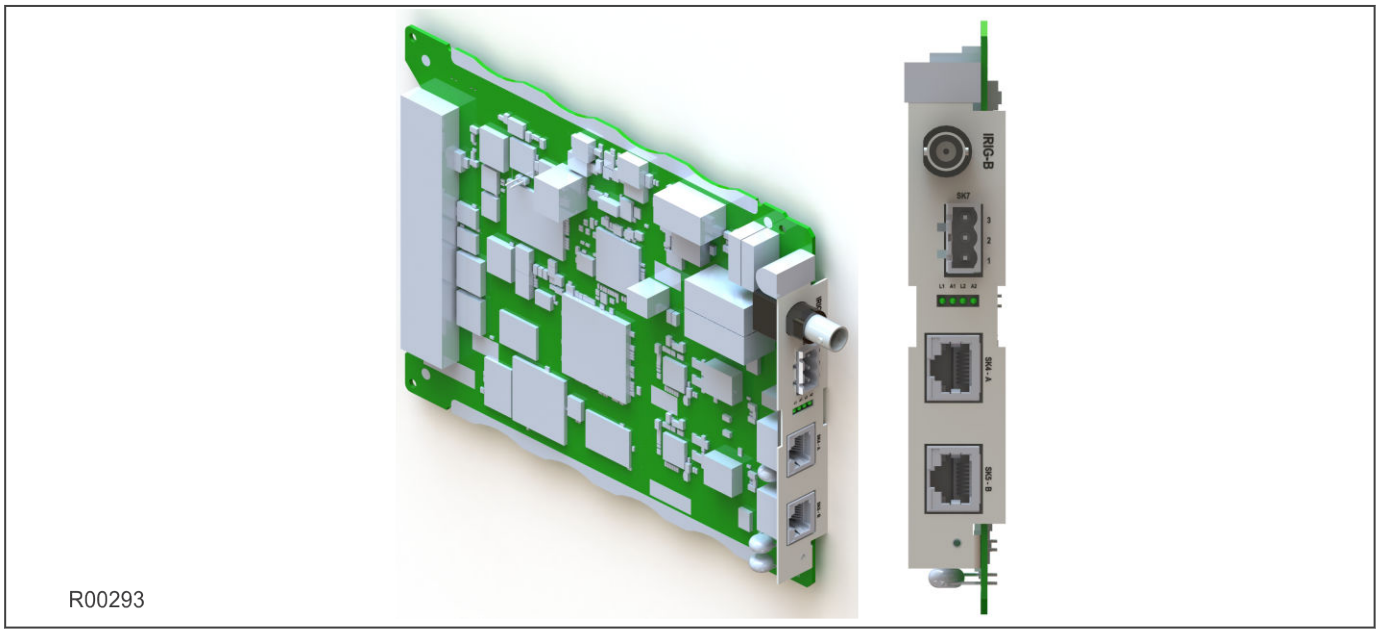


Figure 27: Redundant Ethernet board

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

3.6.10.2 SINGLE ETHERNET BOARD (HARDWARE OPTION U)

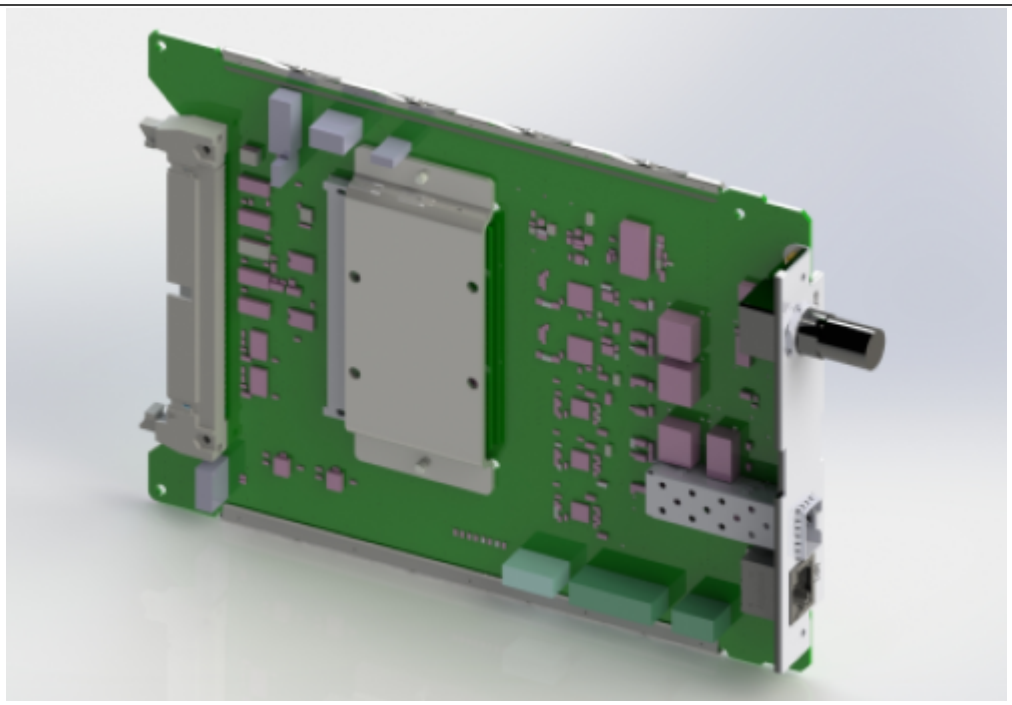




Figure 28: Ethernet board

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

3.6.10.3 REDUNDANT ETHERNET BOARD (HARDWARE OPTION W/Y)

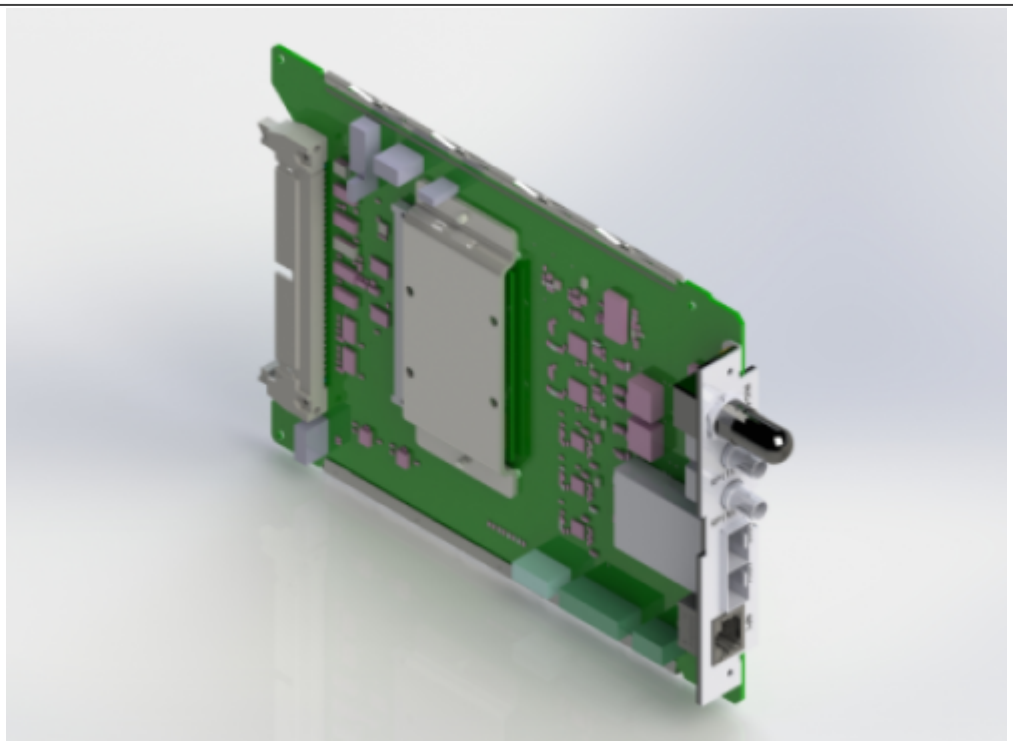




Figure 29: Redundant Ethernet board

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

3.6.10.4 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.

3.6.11 IEC61850-9-2LE ETHERNET BOARD

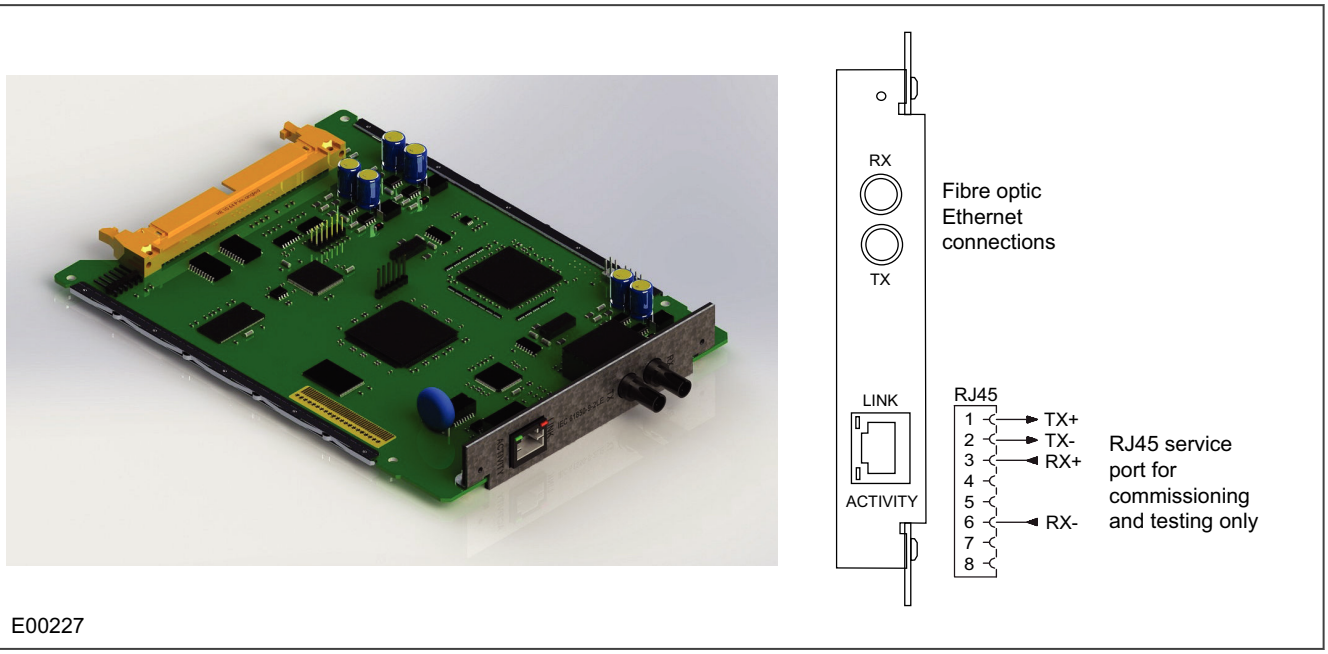


Figure 30: IEC 61850-9-2LE board

Optical Fibre Connectors

The board uses 1300 nm multi mode 100BaseFx with ST connectors.

RJ45 Connector

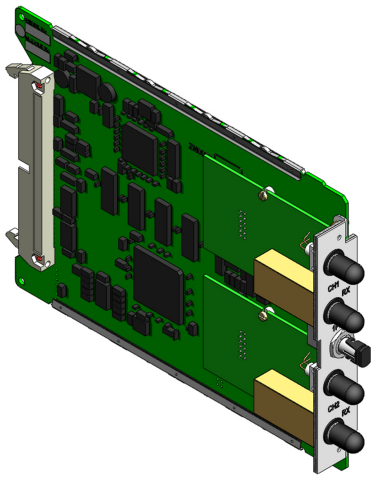
This is a service port for commissioning and testing only. Do not use this for permanent connections.

LEDs

LED	Function	On	Off	Flashing
Green	Link	Link ok	Link broken	
Yellow	Activity			Traffic

Note:
The 9-2LE interface fibre port does not support auto negotiation. Ensure the Ethernet port of the device connected to the 9-2 LE interface fibre port is set to 100Mbps full duplex.

3.6.12 COPROCESSOR BOARD



R00248

Figure 31: 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

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 57
Sofware Design Overview 58
System Level Software 59
Platform Software 61
Protection and Control Functions 62

4.2 SOFWARE DESIGN OVERVIEW

The device software can be conceptually categorized 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.

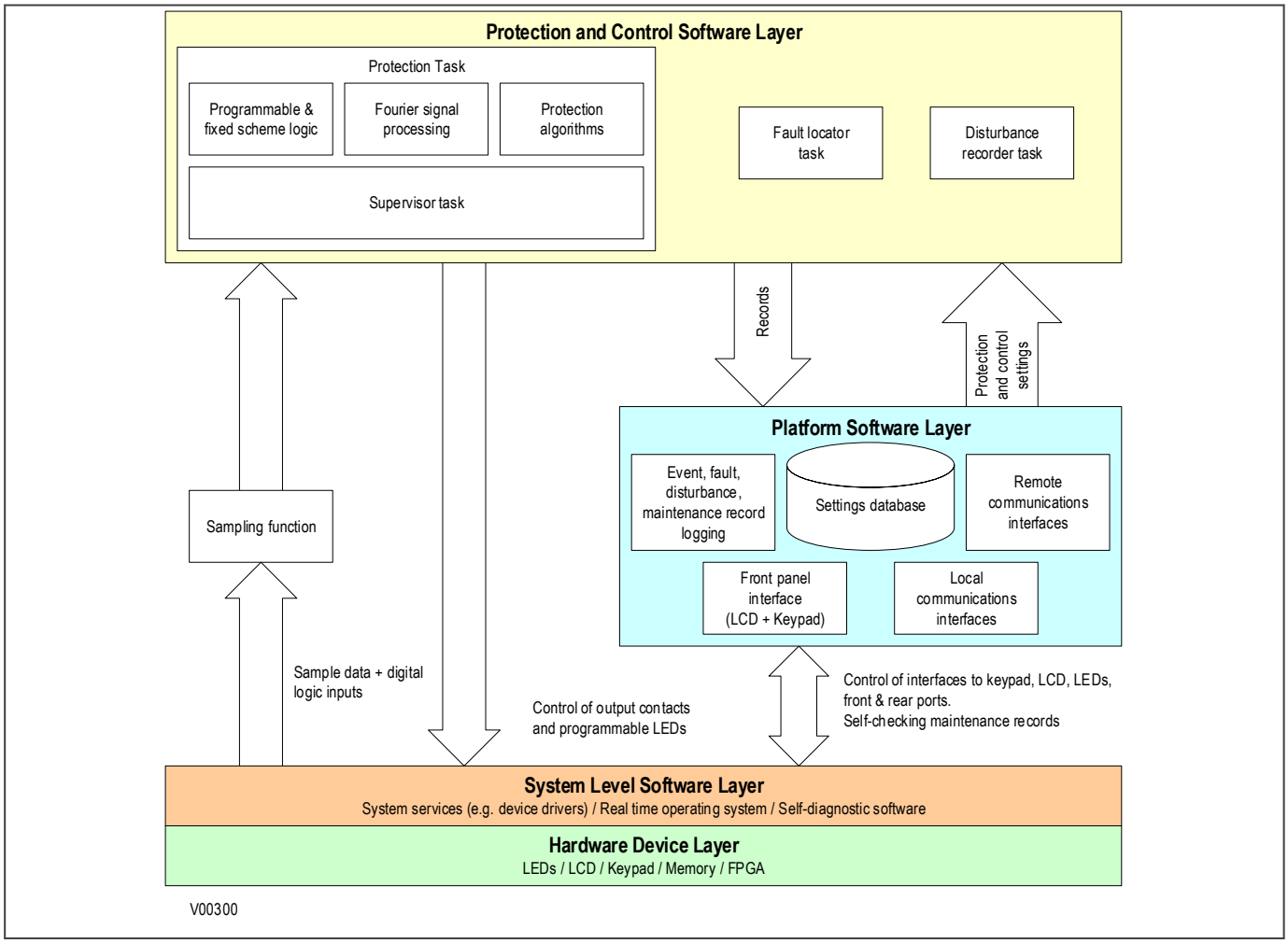


Figure 32: Software Architecture

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 initialization process initializes 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 initialization process the device checks the following:

- The status of the supercapacitor
- The integrity of the supercapacitor-backed SRAM that is used to store event, fault and disturbance records
- The operation of the LCD controller
- The watchdog operation

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

4.3.4.3 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 ACQUISITION OF SAMPLES

After initialization, the protection and control task waits until there are enough samples to process. The acquisition of samples on the main processor board is controlled by a ‘sampling function’ which is called by the system services software.

This sampling function takes samples from the input module and stores them in a two-cycle FIFO buffer. The sample rate is 24 samples per cycle. This results in a nominal sample rate of 1,200 samples per second for a 50 Hz system and 1,440 samples per second for a 60 Hz system. However the sample rate is not fixed. It tracks the power system frequency as described in the next section.

4.5.2 FREQUENCY TRACKING

The device provides a frequency tracking algorithm so that there are always 24 samples per cycle irrespective of frequency drift within a certain frequency range (see technical specifications). If the frequency falls outside this range, the sample rate reverts to its default rate of 1200 Hz for 50 Hz or 1440 Hz for 60 Hz.

The frequency tracking of the analog input signals is achieved by a recursive Fourier algorithm which is applied to one of the input signals. It works by detecting a change in the signal’s measured phase angle. The calculated value of the frequency is used to modify the sample rate being used by the input module, in order to achieve a constant sample rate per cycle of the power waveform. The value of the tracked frequency is also stored for use by the protection and control task.

The frequency tracks off any voltage or current in the order VA, VB, VC, IA, IB, IC, down to 10%Vn for voltage and 5%In for current.

4.5.3 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.

4.5.4 FOURIER SIGNAL PROCESSING

When the protection and control task is re-started by the sampling function, it calculates the Fourier components for the analog signals. Although some protection algorithms use some Fourier-derived harmonics (e.g. second harmonic for magnetizing inrush), most protection functions are based on the Fourier-derived fundamental components of the measured analog signals. The Fourier components of the input current and voltage signals are stored in memory so that they can be accessed by all of the protection elements’ algorithms.

The Fourier components are calculated using single-cycle Fourier algorithm. This Fourier algorithm always uses the most recent 24 samples from the 2-cycle buffer.

Most protection algorithms use the fundamental component. In this case, the Fourier algorithm extracts the power frequency fundamental component from the signal to produce its magnitude and phase angle. This can be represented in either polar format or rectangular format, depending on the functions and algorithms using it.

The Fourier function acts as a filter, with zero gain at DC and unity gain at the fundamental, but with good harmonic rejection for all harmonic frequencies up to the nyquist frequency. Frequencies beyond this nyquist frequency are known as alias frequencies, which are introduced when the sampling frequency becomes less than twice the frequency component being sampled. However, the Alias frequencies are significantly attenuated by an anti-aliasing filter (low pass filter), which acts on the analog signals before they are sampled. The ideal cut-off point of an anti-aliasing low pass filter would be set at:

(samples per cycle) x (fundamental frequency)/2

At 24 samples per cycle, this would be nominally 600 Hz for a 50 Hz system, or 720 Hz for a 60 Hz system.

The following figure shows the nominal frequency response of the anti-alias filter and the Fourier filter for a 24-sample single cycle fourier algorithm acting on the fundamental component:

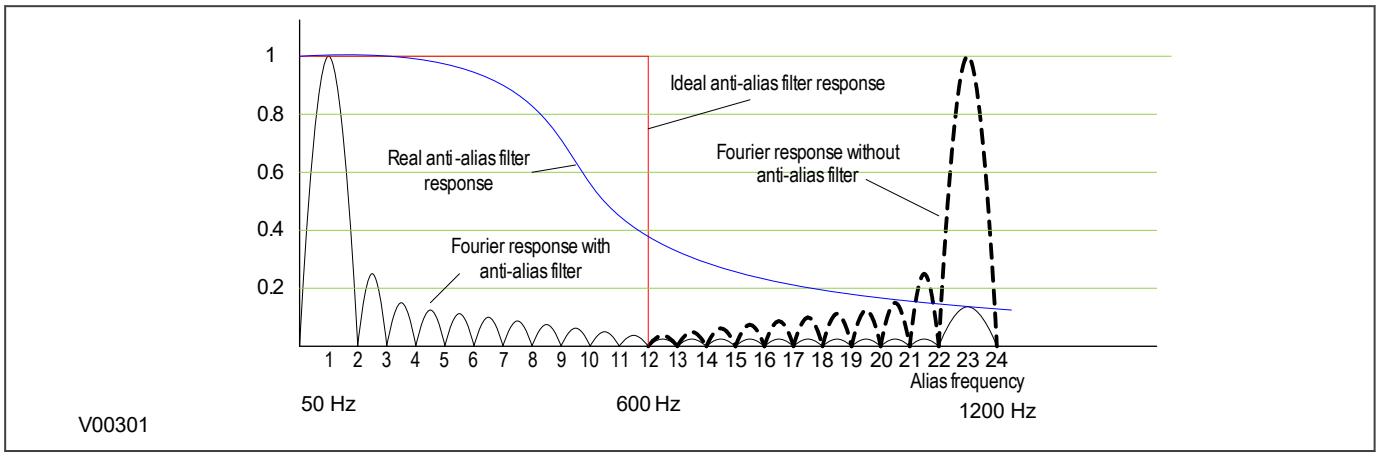


Figure 33: Frequency Response (indicative only)

4.5.5 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 relay 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.

4.5.6 EVENT RECORDING

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. When the supervisor task receives an event record, it instructs the platform software to create the appropriate log in non-volatile memory (backed-up SRAM). The operation of the record logging to backed-up SRAM is slower than the supervisor buffer. This means that the protection software is not delayed waiting for the records to be logged by the platform software. However, in the rare case when a large number of records to be logged are created in a short period of time, it is possible that some will be lost, if the supervisor buffer is full before the platform software is able to create a new log in backed-up SRAM. If this occurs then an event is logged to indicate this loss of information.

Maintenance records are created in a similar manner, with the supervisor task instructing the platform software to log a record when it receives a maintenance record message. However, it is possible that a maintenance record may be triggered by a fatal error in the relay in which case it may not be possible to successfully store a maintenance record, depending on the nature of the problem.

For more information, see the Monitoring and Control chapter.

4.5.7 DISTURBANCE RECORDER

The disturbance recorder operates as a separate task from the protection and control task. It can record the waveforms of the calibrated analog channels, plus the values of the digital signals. The recording time is user selectable up to a maximum of 10.5 seconds. The disturbance recorder is supplied with data by the protection and control task once per cycle, and collates the received data into the required length disturbance record. The disturbance records can be extracted using application software or the SCADA system, which can also store the data in COMTRADE format, allowing the use of other packages to view the recorded data.

For more information, see the Monitoring and Control chapter.

4.5.8 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.

4.5.9 FUNCTION KEY INTERFACE

The function keys interface directly into the PSL as digital input signals. A change of state is only recognized 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 relay 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 66
Settings Application Software 67
Using the HMI Panel 68
Date and Time Configuration 78
Settings Group Selection 81

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.

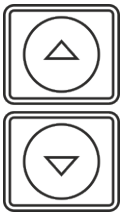
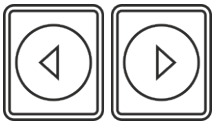
The software is designed to be intuitive, but help is available in an online help system and also the Settings Application Software user guide P40-M&CR-SAS-UG-EN-n, where 'Language' is a 2 letter code designating the language version of the user guide and 'n' is the latest version of the settings application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

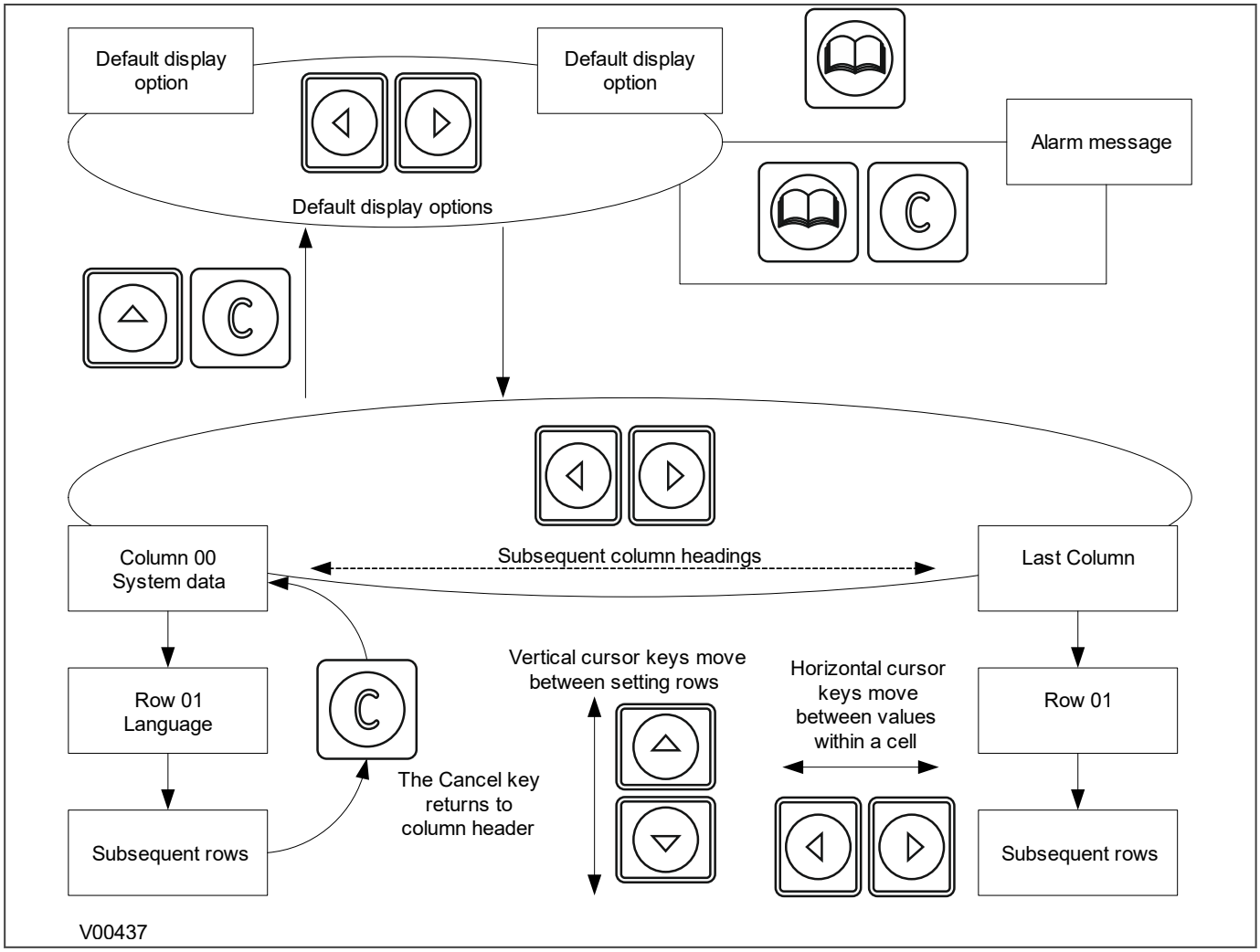


Figure 34: Navigating the HMI

5.3.2 GETTING STARTED

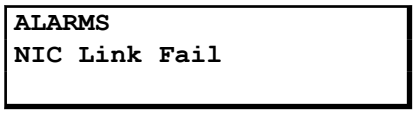
When you first start the IED, it will go through its power up procedure. After a few seconds it will settle down into one of the top level menus. There are two menus at this level:

- 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:

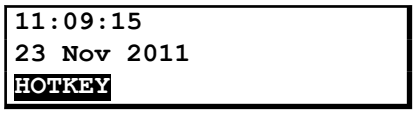
NERC Compliant banner

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.



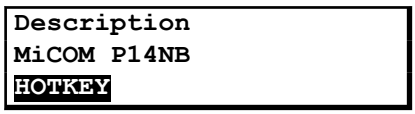
Date and time

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.

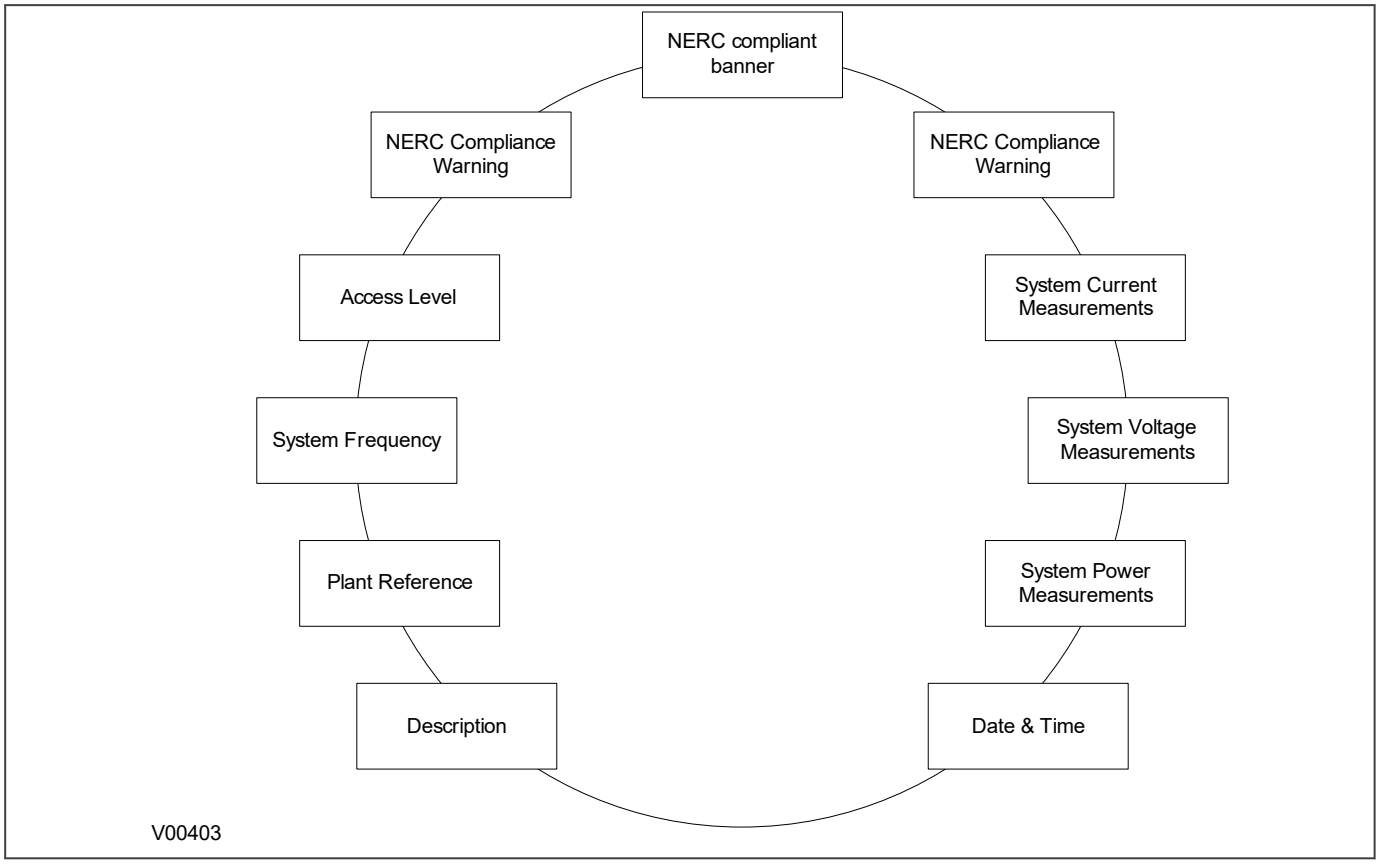


Figure 35: Default display navigation

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 ChangeMe1#.

```
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 attemps, 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

Setting	Column	Row	Description
…	…	…	
VIEW RECORDS	**01**	**00**	**Second Column definition**
Select Event [0...n]	01	01	First setting within second column
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

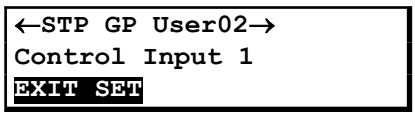
The control inputs are user-assignable functions. You can use the *CTRL I/P CONFIG* column to configure the control inputs for the hotkey menu. In order to do this, use the first setting ***Hotkey Enabled*** cell to enable or disable any of the 32 control inputs. You can then set each control input to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

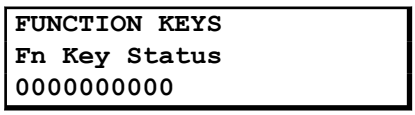
5.3.9.4 FUNCTION KEYS

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 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.

5.4.1 USING AN SNTP SIGNAL

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

5.4.2 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 energized 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-energized for approximately 30 seconds. On re-energization, the time should be correct.
7. Reconnect the IRIG-B signal.

5.4.3 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 energized 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.

5.4.4 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-energized for approximately 30 seconds. On re-energization, the time should be correct.

5.4.5 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.

5.4.6 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.

5.5 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

COMMUNICATIONS

6.1 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 83
Communication Interfaces 84
Serial Communication 85
Ethernet Communication 88
Redundancy Protocols 89
Simple Network Management Protocol (SNMP) 94
Data Protocols 101
Read Only Mode 132
Time Synchronisation using the Communication Protocols 134
Time Synchronisation 135
Board Variants 138
Configuring IP Addresses 139
Redundant Ethernet Configurator 143
General Functions for Redundant Ethernet Boards 149

6.2 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.

6.3 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 customization 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.

6.3.1 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.

6.3.2 EIA(RS)485 BUS

The RS485 two-wire connection provides a half-duplex, fully isolated serial connection to the IED. The connection is polarized 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.

6.3.2.1 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.

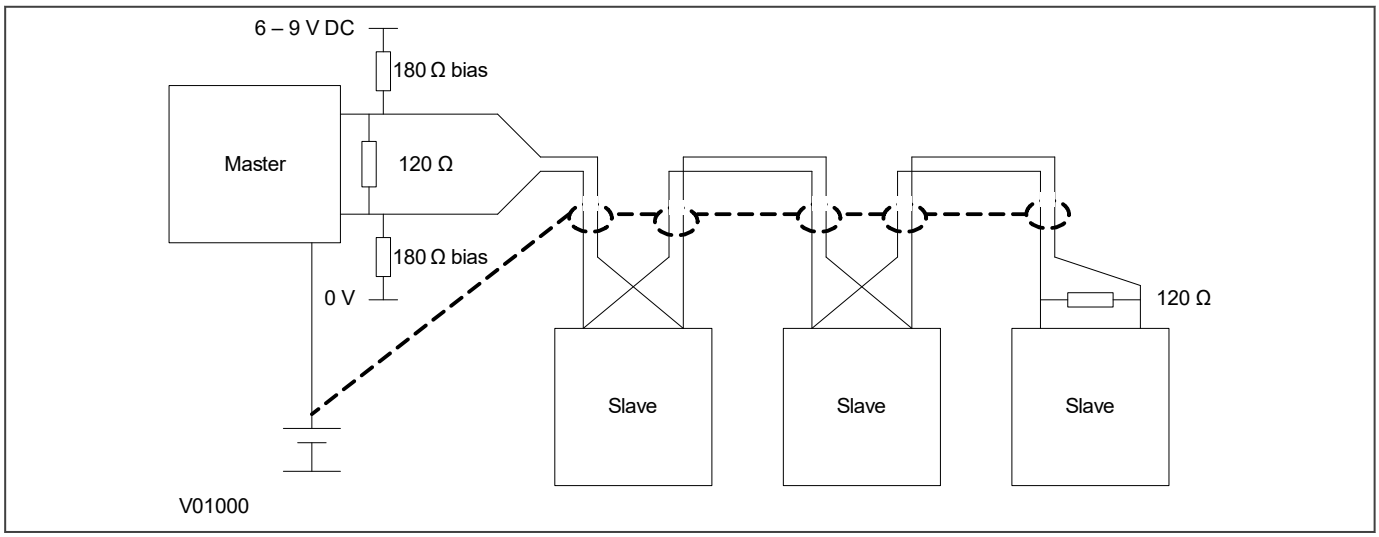


Figure 36: RS485 biasing circuit

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.

6.3.3 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.

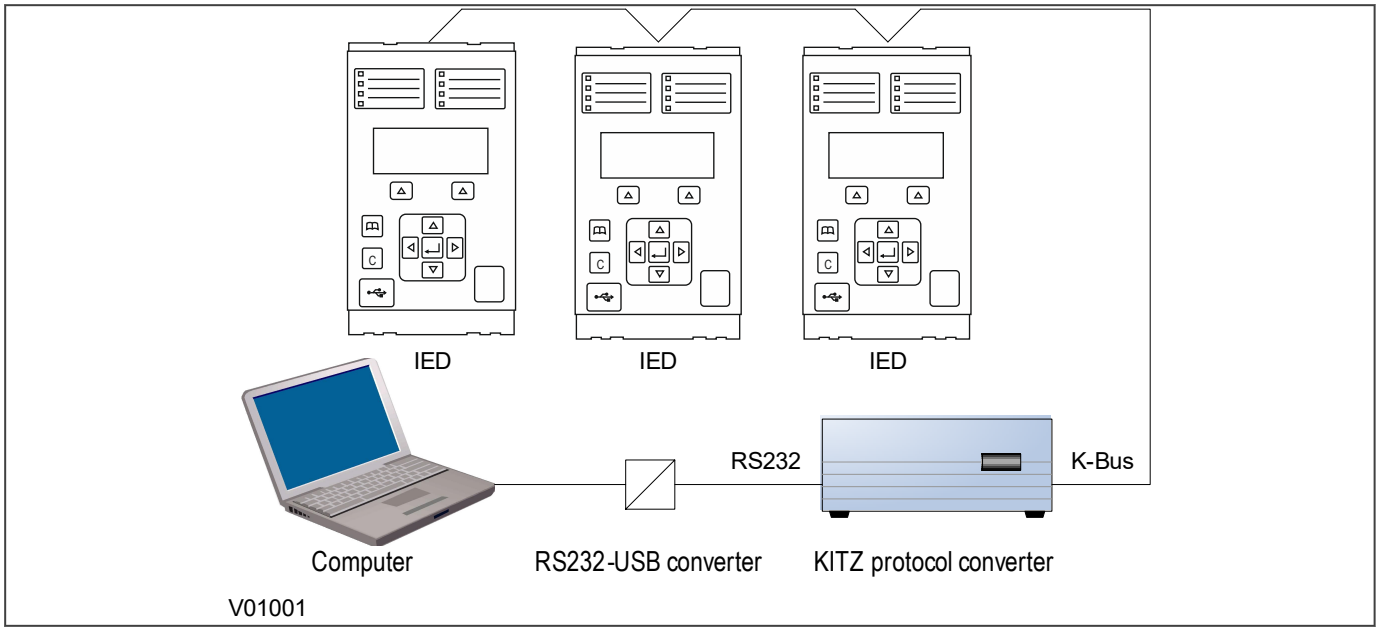


Figure 37: Remote communication using K-Bus

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.

6.4 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.

6.5 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 provides "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.

6.5.1 PARALLEL REDUNDANCY PROTOCOL (PRP)

Power system companies have traditionally used proprietary protocols for redundant communications. This is because standardized 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.

6.5.1.1 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.

6.5.1.2 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).

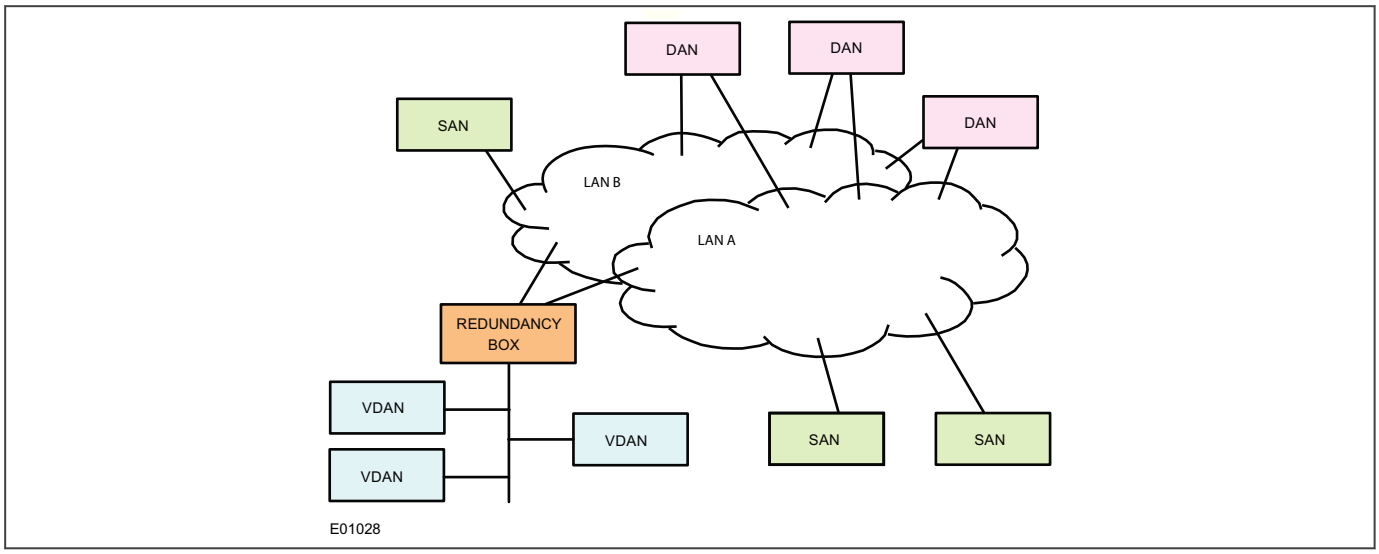


Figure 38: Example PRP redundant network

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.

6.5.2 HIGH-AVAILABILITY SEAMLESS REDUNDANCY (HSR)

HSR is standardized 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).

6.5.2.1 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.

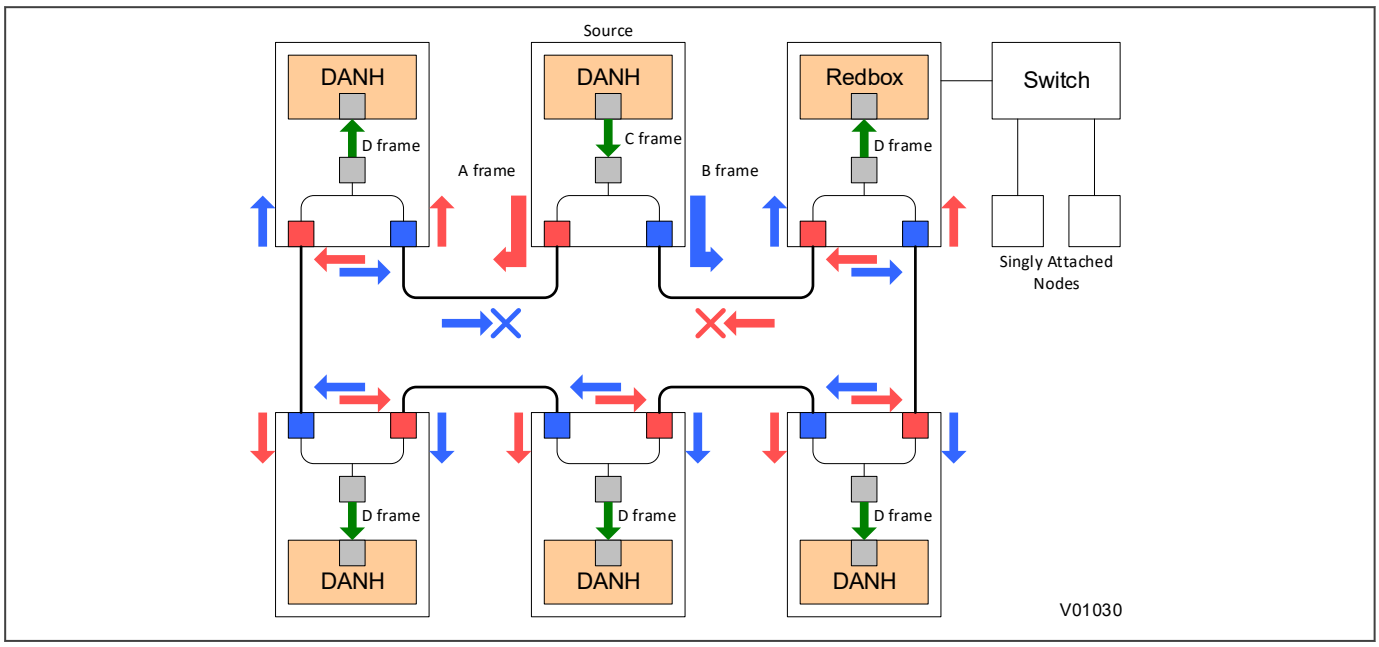


Figure 39: HSR multicast topology

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.

6.5.2.2 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.

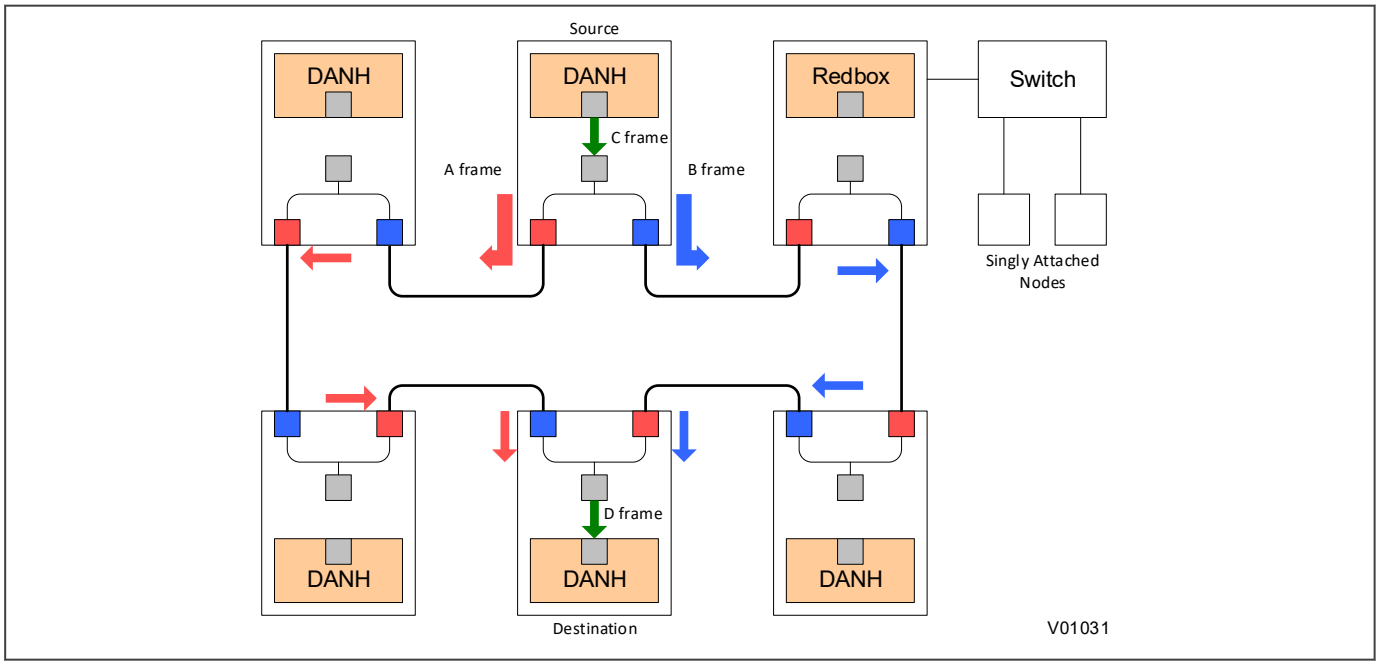


Figure 40: HSR unicast topology

For unicast frames, the whole bandwidth is available as both frames A & B stop at the destination node.

6.5.2.3 HSR APPLICATION IN THE SUBSTATION

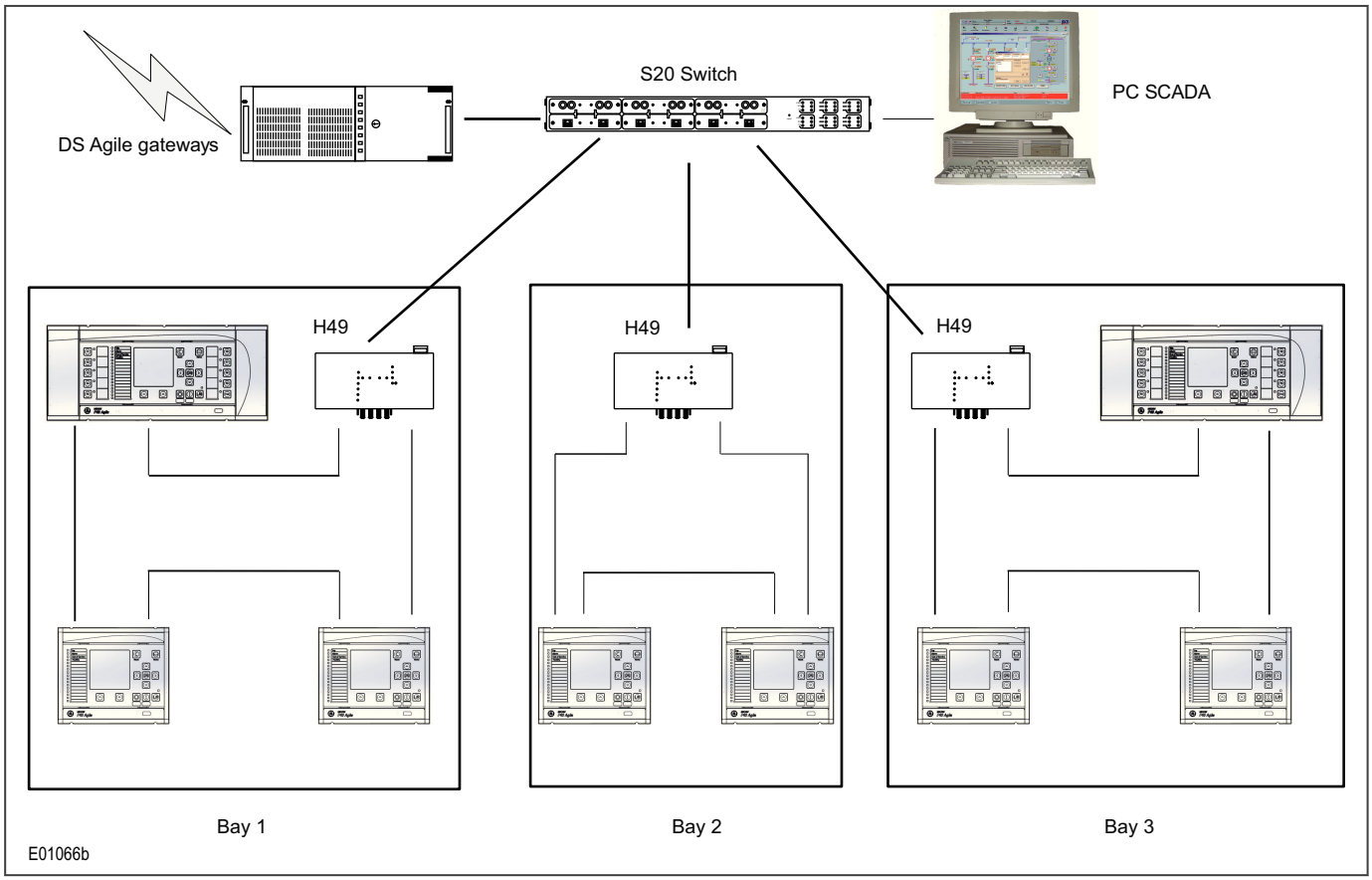


Figure 41: HSR application in the substation

6.5.3 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.

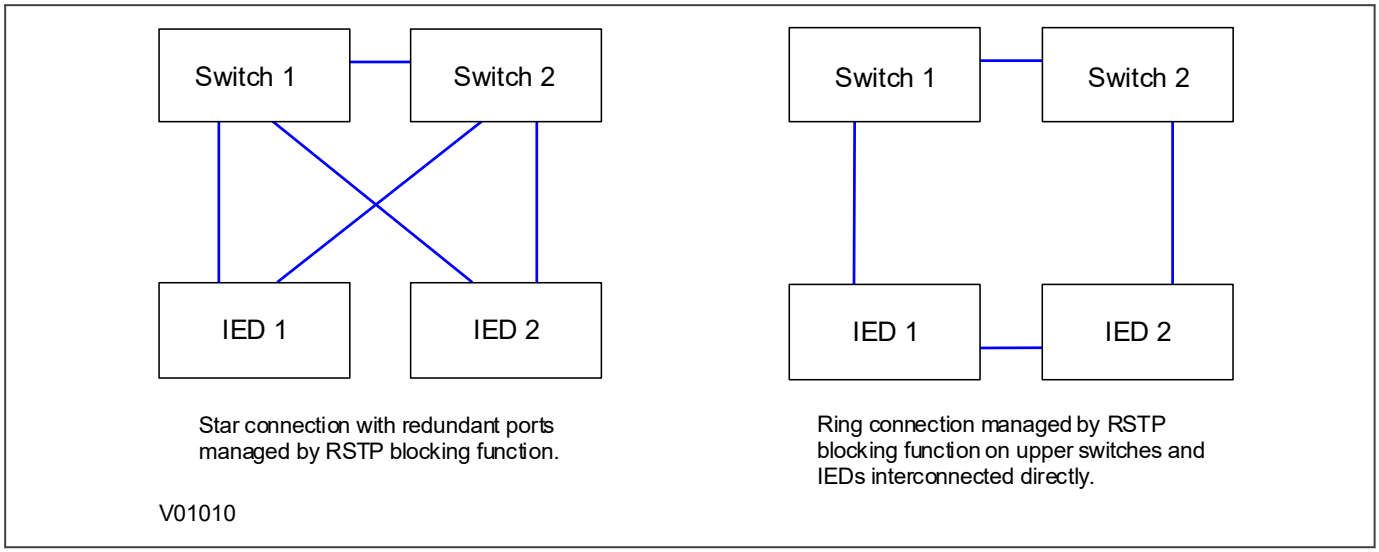


Figure 42: IED attached to redundant Ethernet star or ring circuit

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.

6.5.4 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.

6.6 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.

6.6.1 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 standardized.

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.

6.6.2 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

6.6.3 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						IreConfiguration
							0					IreConfigurationGeneralGroup
								1				IreManufacturerName
								2				IreInterfaceCount
							1					IreConfigurationInterfaceGroup
								0				IreConfigurationInterfaces
									1			IreInterfaceConfigTable
										1		IreInterfaceConfigEntry
											1	IreInterfaceConfigIndex
											2	IreRowStatus
											3	IreNodeType
											4	IreNodeName
											5	IreVersionName
											6	IreMacAddressA

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

6.6.4 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.

6.6.5 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 in order 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 the ***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.

6.7 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 Courier	IEC 61850 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

6.7.1 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.

6.7.1.1 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.*

6.7.1.2 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.

6.7.1.3 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.

6.7.1.4 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.

6.7.1.5 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.

6.7.1.5.1 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.

6.7.1.5.2 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.

6.7.1.6 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.

6.7.1.7 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.

6.7.1.8 TIME SYNCHRONISATION

The time and date can be set using the time synchronization feature of the Courier protocol. The device will correct for the transmission delay. The time synchronization message may be sent as either a global command or to any individual IED address. If the time synchronization 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 synchronization Courier event will be generated/produced whether the time-synchronization message is sent as a global command or to any individual IED address.

If the clock is being synchronized 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 synchronized internal clock.

6.7.1.9 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
```

6.7.2 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:

- Initialization (reset)
- Time synchronization
- Event record extraction
- General interrogation
- Cyclic measurements
- General commands
- Disturbance record extraction
- Private codes

6.7.2.1 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.

6.7.2.2 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.

6.7.2.3 TIME SYNCHRONISATION

The time and date can be set using the time synchronization 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 synchronization message is sent as a send/confirm message then the device will respond with a confirm message. A time synchronization Class 1 event will be generated/produced whether the time-synchronization message is sent as a send confirm or a broadcast (send/no reply) message.

If the clock is being synchronized 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 synchronized internal clock.

6.7.2.4 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.

Setting	Description
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.

6.7.2.5 SPONTANEOUS EVENTS

Events are categorized 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 settting the ***Config Mode*** cell to `Std+UserConfig`, and configuring the DDB masks as required.

6.7.2.6 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.

6.7.2.7 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.

6.7.2.8 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’.

6.7.2.9 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'.

6.7.2.10 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.

6.7.2.11 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

6.7.2.12 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.

6.7.3 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).

6.7.3.1 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.

6.7.3.2 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.

6.7.3.3 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.

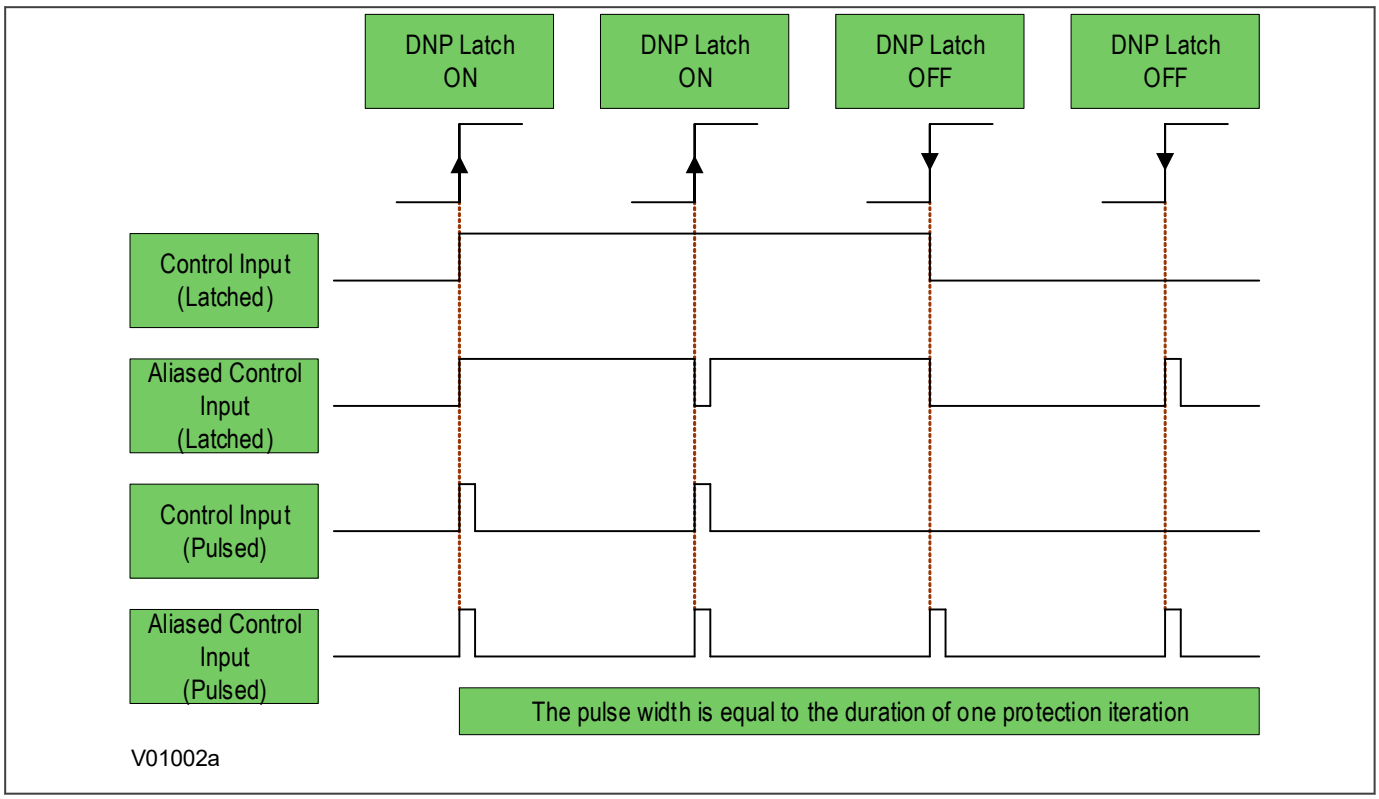


Figure 43: Control input behaviour

Many of the IED's 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 maybe 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

6.7.3.4 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.

6.7.3.5 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 normalized 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 normalized 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).

6.7.3.6 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.

6.7.3.7 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 synchronized 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 synchronized internal clock.

6.7.3.8 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.

6.7.3.8.1 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)
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

DNP 3.0 Device Profile Document	
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
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

6.7.3.8.2 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)				

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	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)				
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)

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)	
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)
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)

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)	
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)				
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)				

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)	
			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.

6.7.3.8.3 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 synchronization 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

Bit	Indication	Description	Supported
6	Reserved	Always returned as zero.	
7	Reserved	Always returned as zero.	

6.7.3.8.4 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 authorized	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.

6.7.3.9 DNP3 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 `DNP3.0`.

```
COMMUNICATIONS
RP1 Protocol
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.

```
COMMUNICATIONS
RP1 Address
1
```

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.

```
COMMUNICATIONS
RP1 Baud rate
9600 bits/s
```

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.

```
COMMUNICATIONS
RP1 Parity
None
```

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. 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.

```
COMMUNICATIONS
RP1 Time Sync
Enabled
```

6.7.3.9.1 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**.

6.7.4 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 so 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.

Software Version 70 onwards provides an IEC 61850 Edition 2 compatible implementation.

From Software Version 91 onwards, it supports Edition 1 and Edition 2 for P442 and P444. Switching between Edition 1 and Edition 2 is described in the Selection of the IEC 61850 Edition section.

An additional section detailing the enhancements in Edition 2 models is documented later in this chapter, if applicable.

6.7.4.1 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 every-day use
- There is a wide range of Ethernet-compatible products that may be used to supplement the LAN installation (hubs, bridges, switches)

6.7.4.2 IEC 61850 INTEROPERABILITY

A major benefit of IEC 61850 is interoperability. IEC 61850 standardizes 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 of the new data. IEC 61850 brings improved substation communications and interoperability to the end user, at a lower cost.

6.7.4.3 THE IEC 61850 DATA MODEL

The data model of any IEC 61850 IED can be viewed as a hierarchy of information, whose nomenclature and categorization is defined and standardized in the IEC 61850 specification.

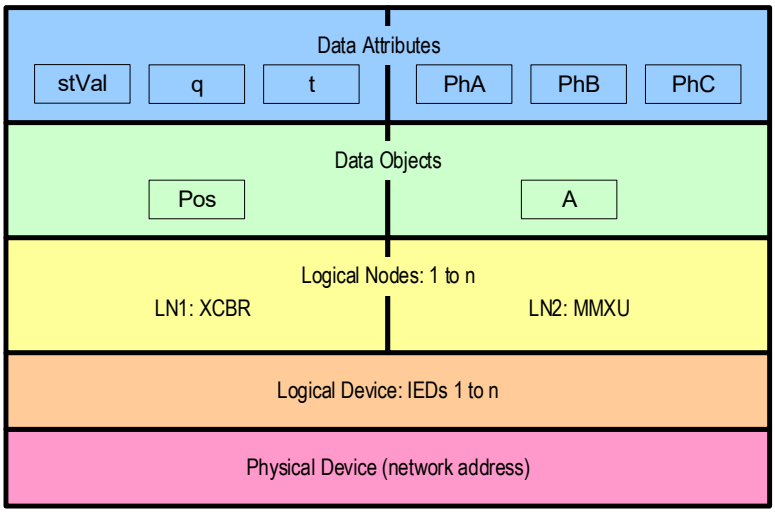


Figure 44: Data model layers in IEC 61850

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) indicating actual position of circuit breaker for Data Object type Pos of Logical Node type XCBR.

6.7.4.4 IEC 61850 IN MICOM IEDS

IEC 61850 is implemented by use of 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 synchronization over an Ethernet link. (This is used to synchronize the IED's 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.

6.7.4.5 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.

6.7.4.6 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.

6.7.4.7 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.

6.7.4.8 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 IEC61850 LGOS logical node.

6.7.4.9 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

6.7.4.9.1 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.

6.7.4.10 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.

6.7.4.11 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, however, you can configure it with the HMI. To configure IEC61850 edition 2 using the HMI, you must first enable the IP From 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.

6.7.4.11.1 IEC 61850 CONFIGURATION BANKS

There are two configuration banks:

- Active Configuration Bank
- Inactive Configuration Bank

Any new configuration sent to the IED is automatically stored in the inactive configuration bank, therefore not immediately affecting the current configuration.

Following an upgrade, the IEC 61850 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.

6.7.4.11.2 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.

6.7.4.12 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.

6.7.4.13 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.

6.7.4.13.1 BACKWARD COMPATIBILITY

IEC61850 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:

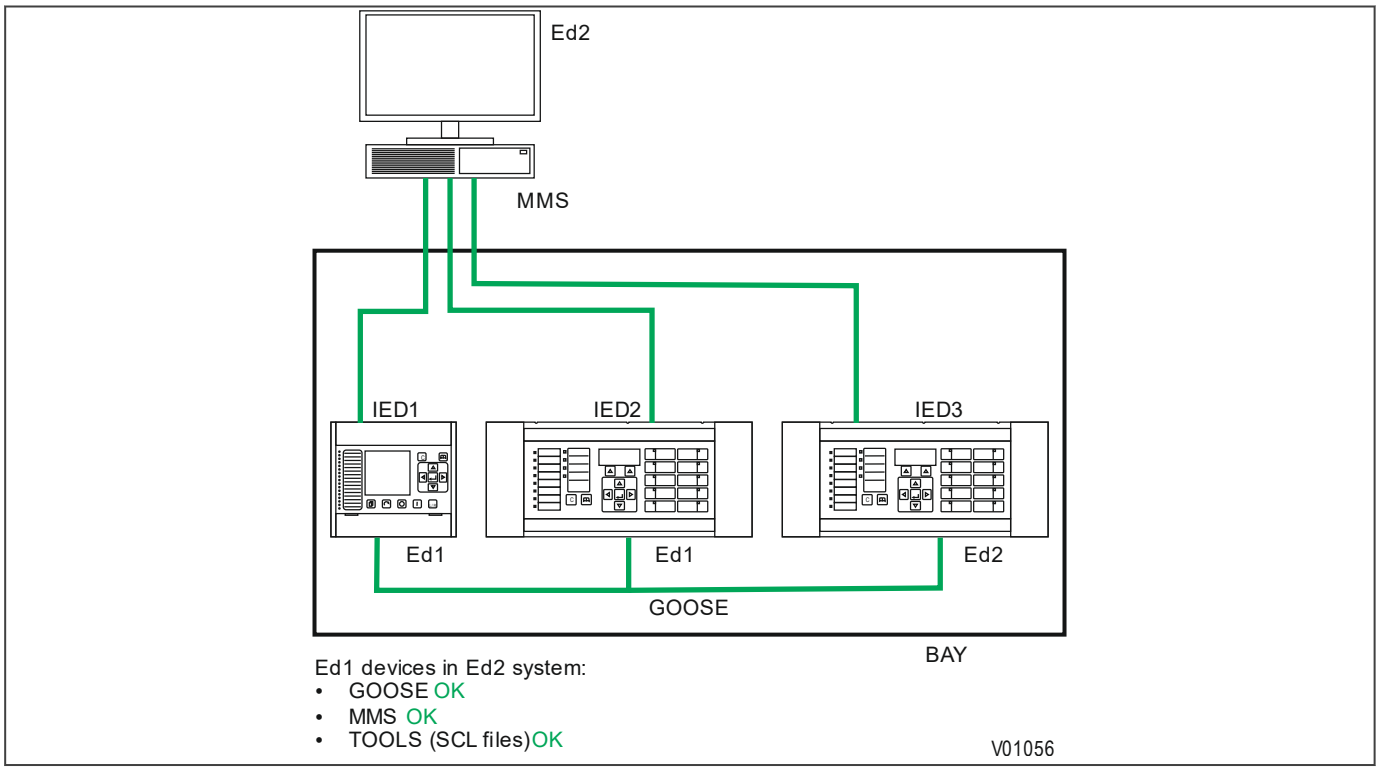


Figure 45: Edition 2 system - backward compatibility

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.

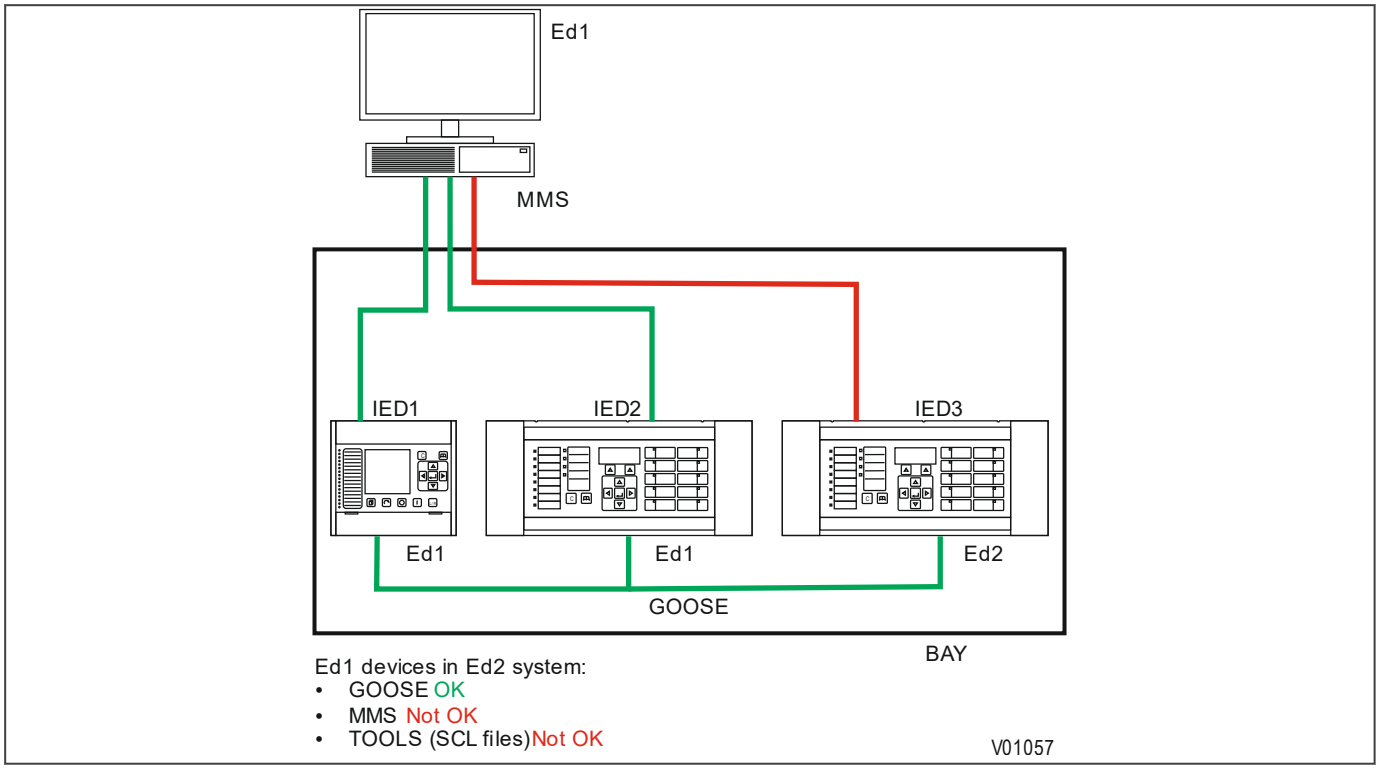


Figure 46: Edition 1 system - forward compatibility issues

6.7.4.13.2 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.

6.7.4.13.3 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.

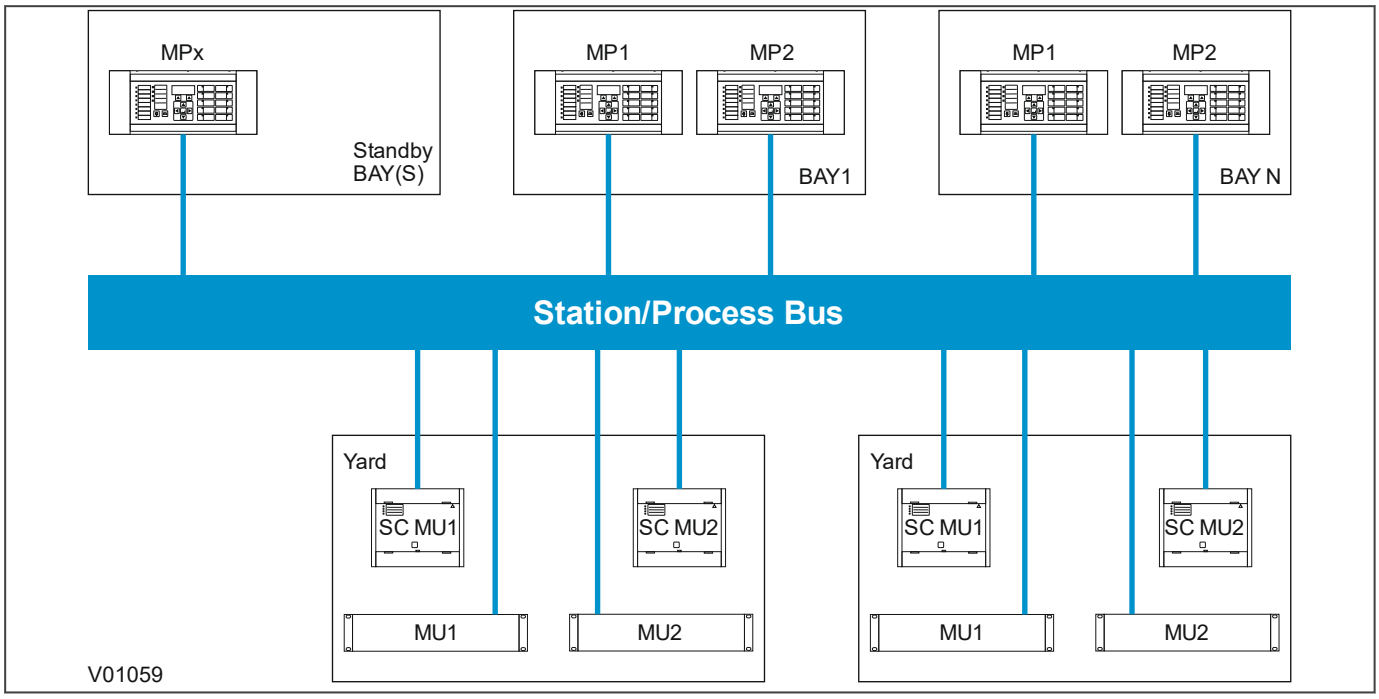


Figure 47: Example of Standby IED

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.

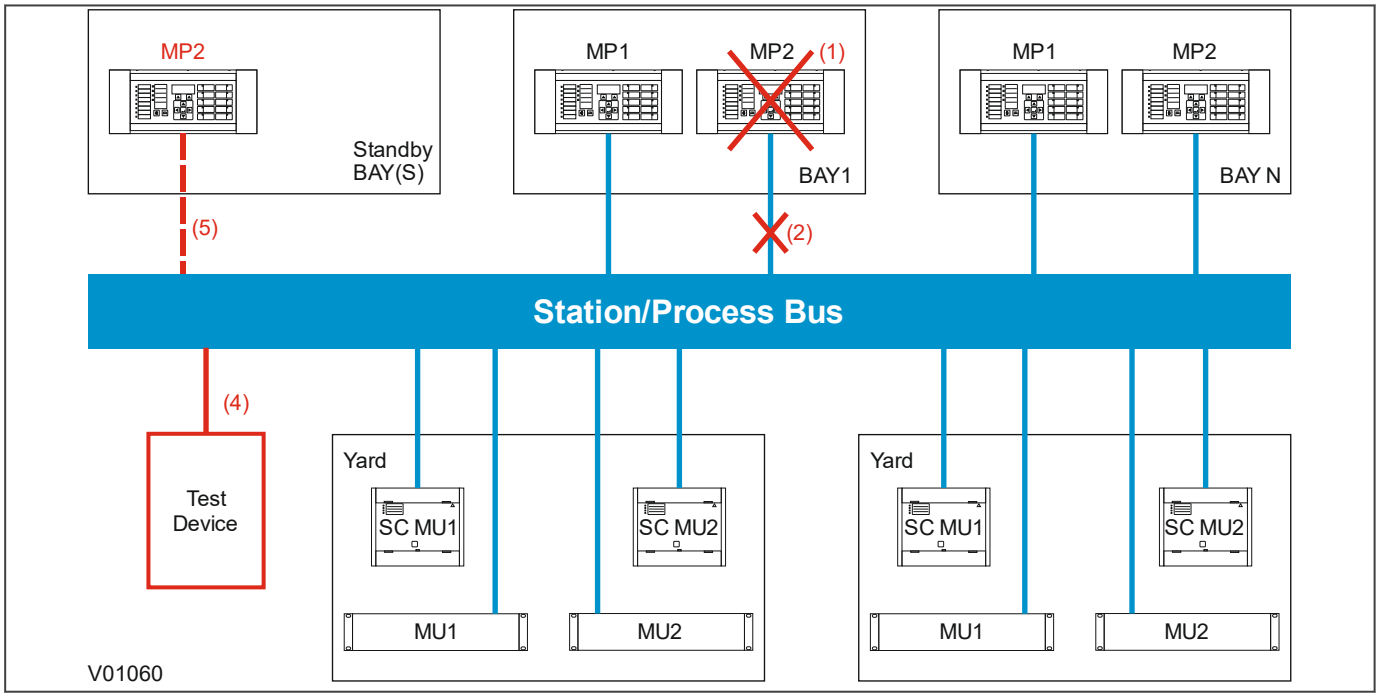


Figure 48: Standby IED Activation Process

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.

6.8 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.

6.8.1 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.

6.8.2 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

6.8.3 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

6.8.4 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)

6.8.5 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.

6.9 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.

6.10 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

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.

6.10.1 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.

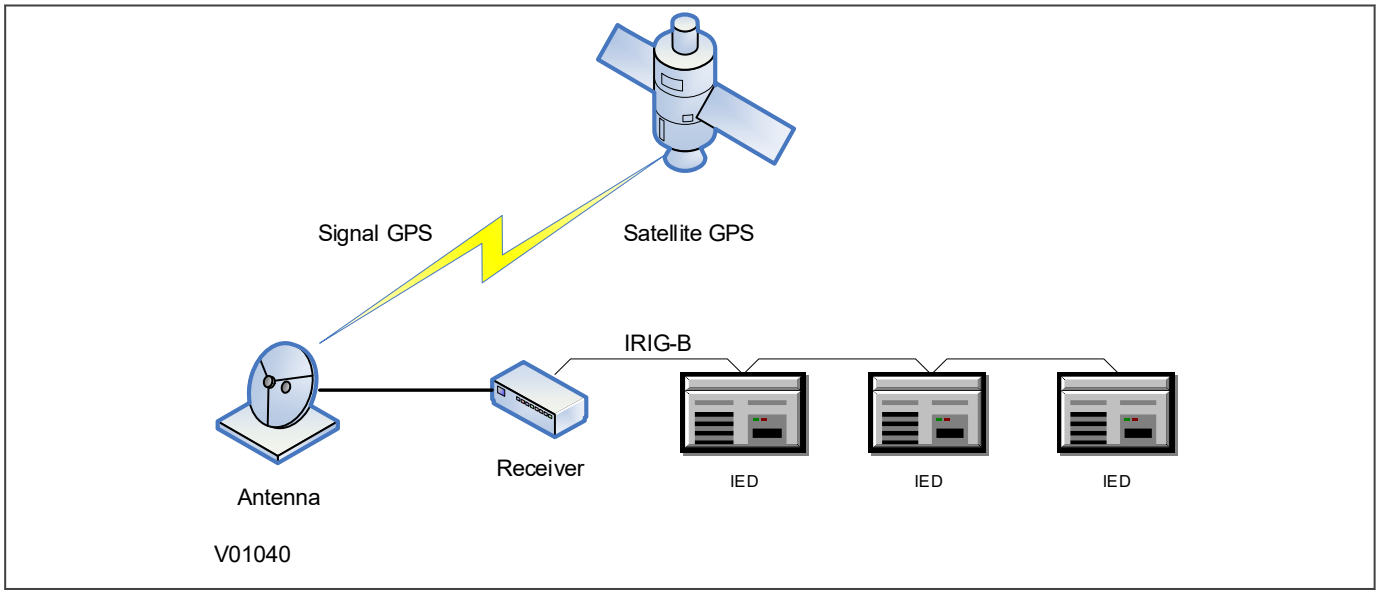


Figure 49: GPS satellite timing signal

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).

6.10.1.1 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 board, 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. The boards support universal IRIG-B, which means they accept demodulated or modulated IRIG-B.

To set the device to use IRIG-B, use the setting ***IRIG-B Sync*** 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.

6.10.2 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.

6.10.2.1 LOSS OF SNTP SERVER SIGNAL ALARM

This function issues an alarm when there is a loss of time synchronization 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.

6.10.3 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 synchronization 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.

6.10.3.1 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.

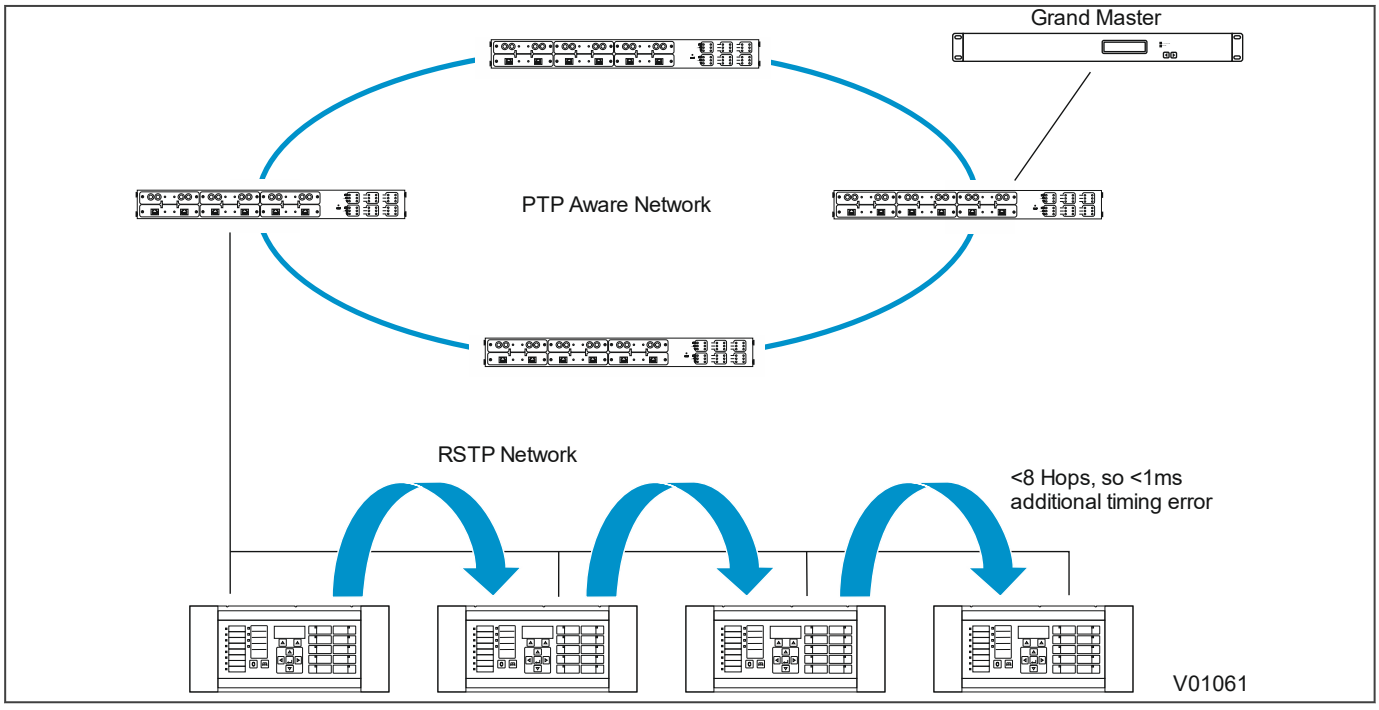


Figure 50: Timing error using ring or line topology

6.10.3.2 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.

6.11 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.

6.12 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

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.

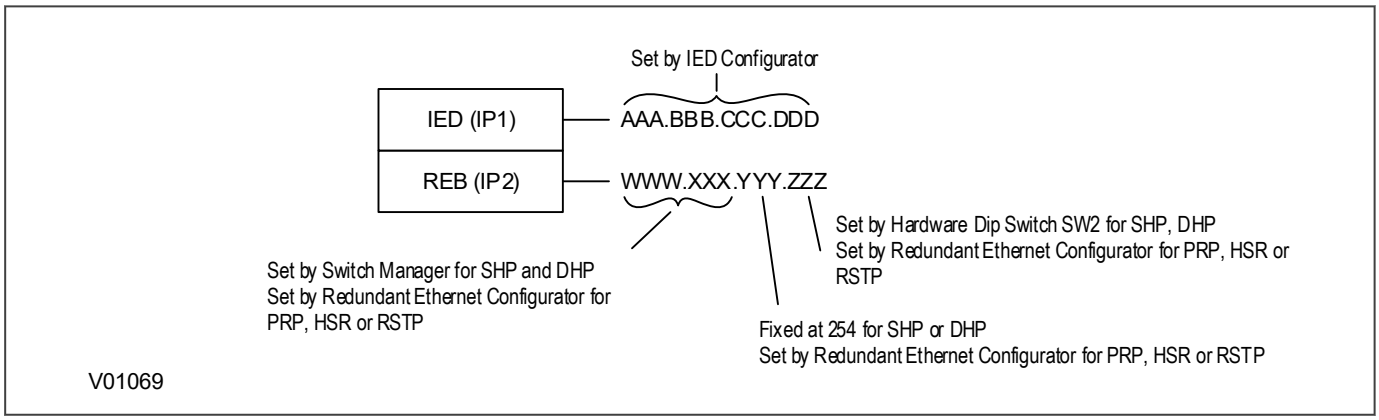


Figure 51: IED and REB IP address configuration

6.12.1 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.

6.12.2 CONFIGURING THE REB IP ADDRESS

The board IP address must be configured before connecting the IED to the network to avoid an IP address conflict.

PRP/HSR/RSTP/Failover

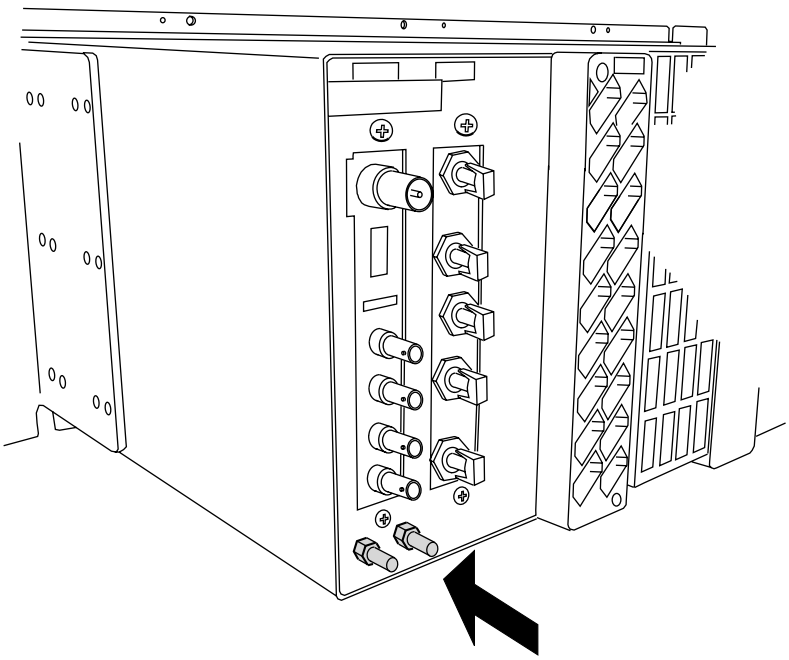
From S1 Agile 2.0.1. onwards cards that support the PRP/HSR/RSTP/Failover protocols in any of the combinations are configured using the Redundant Ethernet Configurator software tool. If you are using a ZN008700X card only this tool supports it.

6.12.2.1 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.

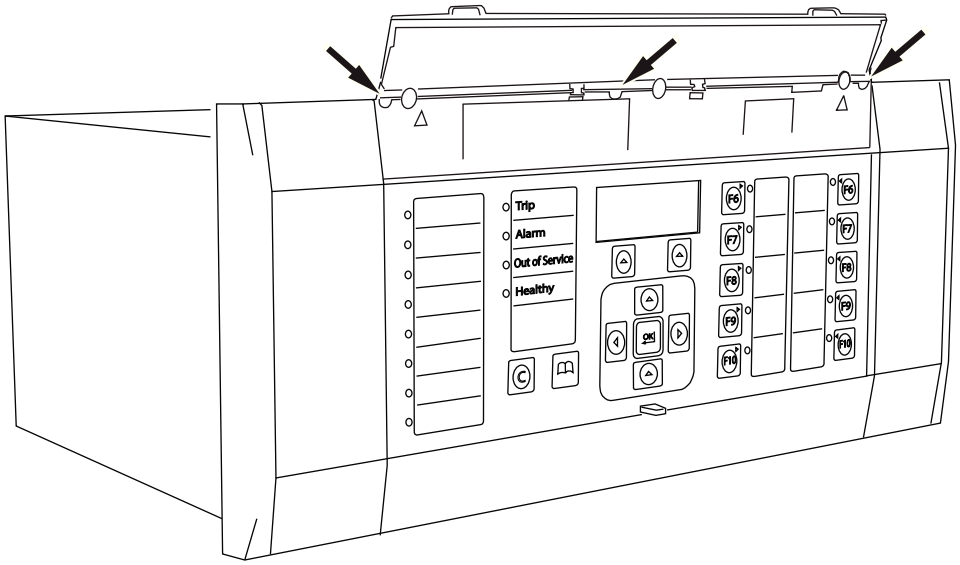
Warning:
Configure the hardware settings before the device is installed.

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.



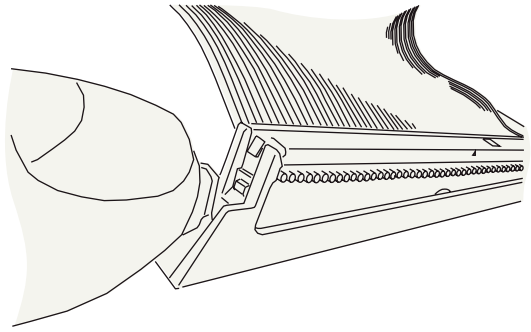
E01019

1. Lift the upper and lower flaps. Remove the six screws securing the front panel and pull the front panel outwards.



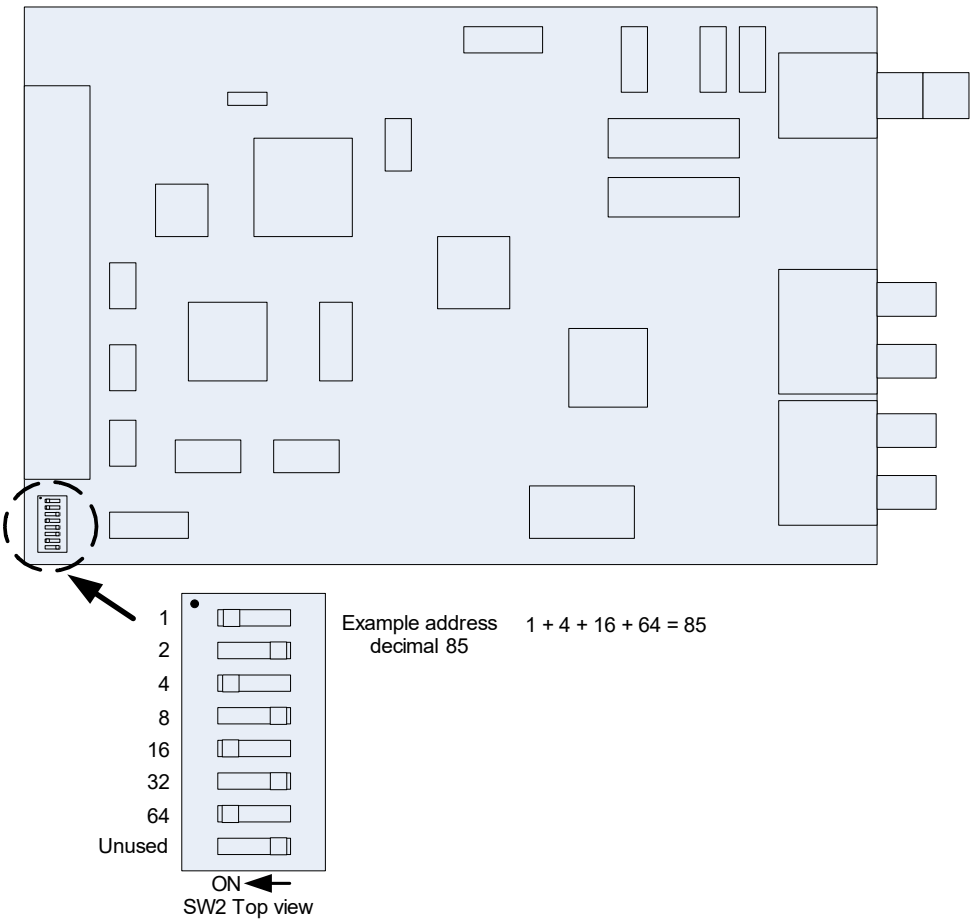
E01020

1. Press the levers either side of the connector to disconnect the ribbon cable from the front panel.



E01021

1. Remove the redundant Ethernet board. Set the last octet of IP address using the DIP switches. The available range is 1 to 127.



1. 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.

6.13 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.

6.13.1 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.

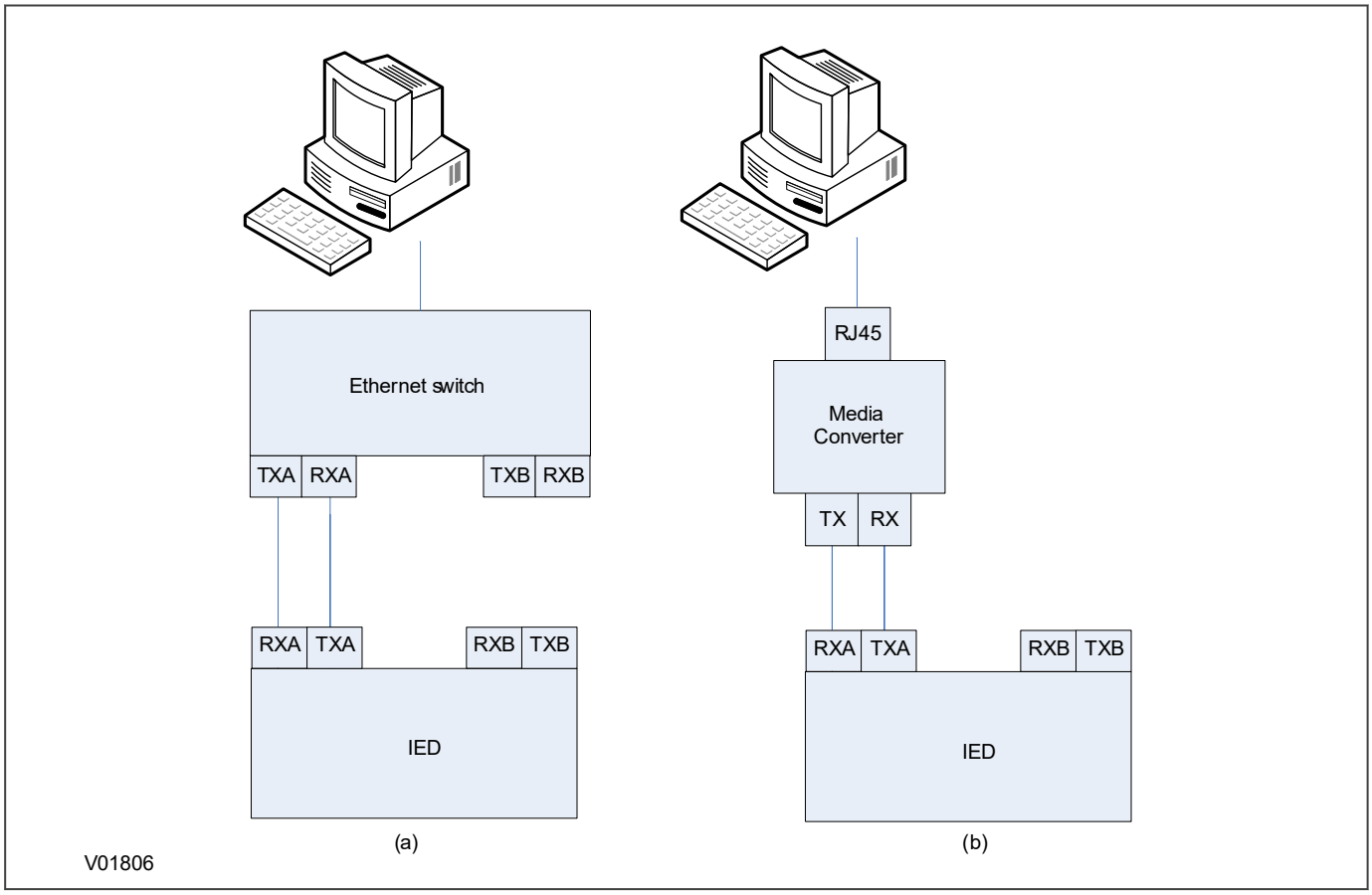


Figure 52: Connection using (a) an Ethernet switch and (b) a media converter

6.13.2 INSTALLING THE CONFIGURATOR

The Redundant Ethernet Configurator is installed as part of S1 Agile 2.0.1 onwards.

6.13.3 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.

6.13.4 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.

6.13.5 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.

6.13.6 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.

6.13.7 PASSWORD CONFGURATION

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 then the password can be recovered by using the **Recover Password** button and following the instructions.

6.13.8 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.

6.13.9 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.

6.13.10 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.

6.13.11 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.

6.13.12 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.

6.13.13 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

6.13.14 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 grayed 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. Also make sure the priority values for all IEDs are higher than that of the switch.

6.13.15 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.

6.13.16 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.

6.13.17 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.

6.13.18 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.

6.13.19 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.

6.14 GENERAL FUNCTIONS FOR REDUNDANT ETHERNET BOARDS

The following functions apply to all redundant Ethernet protocols.

6.14.1 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.

CHAPTER 7

CYBERSECURITY

7.1 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.

7.2 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 151
Overview 152
The Need for Cybersecurity 153
Standards 154
Cyber-Security Implementation 158
Roles and Permissions 159
Authentication 162
Security Event Management 174

7.3 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.

7.4 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

7.4.1 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 Standard	Description
CIP-009-1 Recovery Plans	Define and document Recovery plans for Critical Cyber Assets

7.4.1.1 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

7.4.1.2 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 centralized 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.

7.4.1.3 CIP 004

CIP 004 requires that personnel with authorized cyber access or authorized 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

7.4.1.4 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

7.4.1.5 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

7.4.1.6 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

7.4.1.7 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.

7.4.1.8 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

7.4.2 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.

7.5 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, Authorization, 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).

7.5.1 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.

7.6 ROLES AND PERMISSIONS

7.6.1 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.

7.6.2 PERMISSIONS

Authentication and authorization 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

7.7 AUTHENTICATION

7.7.1 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*.

7.7.2 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.

7.7.3 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

Local Access	Front Port	Rear Port (1/2)	NIC (Ethernet) Port	Supported Auth. Mechanism
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

7.7.3.1 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
```

7.7.3.2 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.

7.7.3.3 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.

7.7.3.4 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.

7.7.4 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.

7.7.5 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.

7.7.6 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.

7.7.6.1 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
```

7.7.6.2 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**.

7.7.7 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.

7.7.8 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.

7.7.9 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.

7.7.10 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.

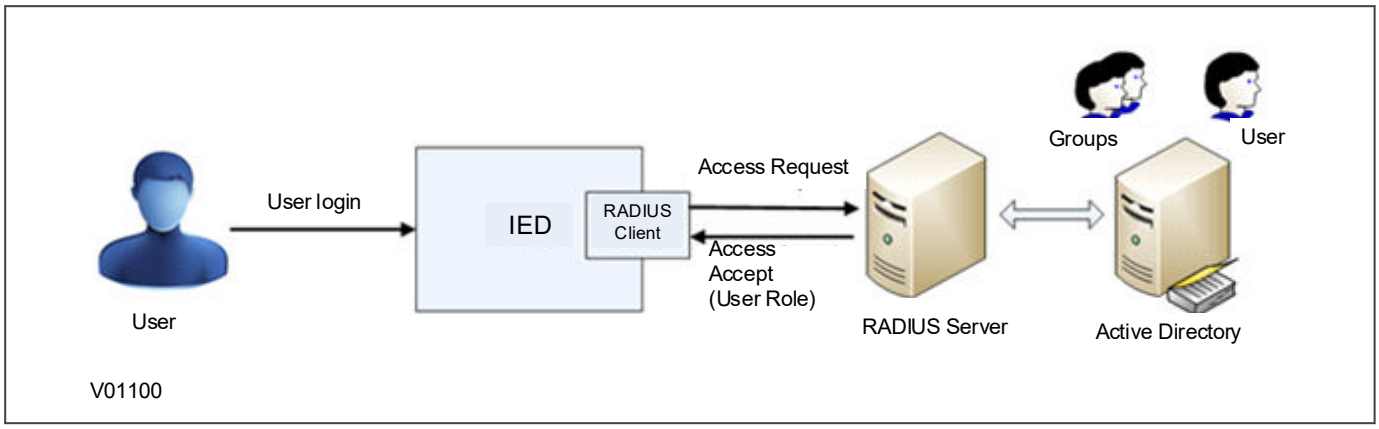


Figure 53: RADIUS server/client communication

7.7.10.1 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).

7.7.10.2 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

7.7.10.3 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*.

7.7.10.4 RADIUS ACCOUNTING

RADIUS accounting is not supported by the IED. The user can achieve accounting through syslog (see the SYSLOG section).

7.7.10.5 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.

7.7.11 RECOVERY

7.7.11.1 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.

7.7.11.2 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 in to 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.

7.7.11.3 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

7.7.12 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.

7.7.13 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.

7.8 SECURITY EVENT MANAGEMENT

To implement NERC-compliant cyber-security, a range of security events are logged in the Security Event file.

7.8.1 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.

7.8.2 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)

7.8.3 SYSLOG CLIENT

The IED supports security event reporting through the Syslog protocol for supporting Security Information Event Management (SIEM) systems for centralized 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

7.8.4 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 8

INSTALLATION

8.1 CHAPTER OVERVIEW

This chapter provides information about installing the product.

This chapter contains the following sections:

Chapter Overview 180
Handling the Goods 181
Mounting the Device 182
Cables and Connectors 184
Case Dimensions 189

8.2 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.

8.2.1 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.

8.2.2 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.

8.2.3 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.

8.2.4 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.

8.3 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.

8.3.1 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.

8.3.2 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.

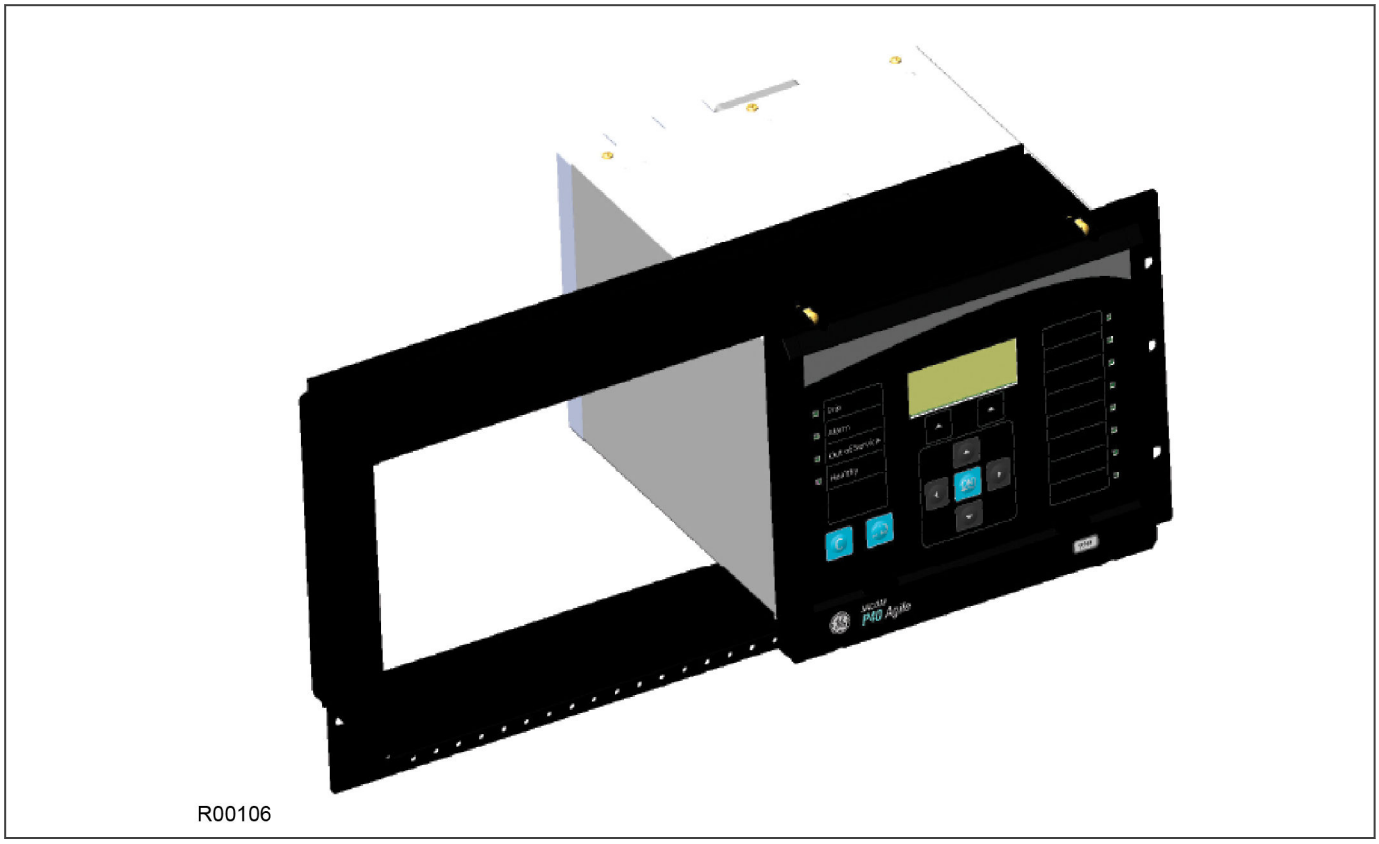


Figure 54: Rack mounting of products

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

8.4 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.

8.4.1 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

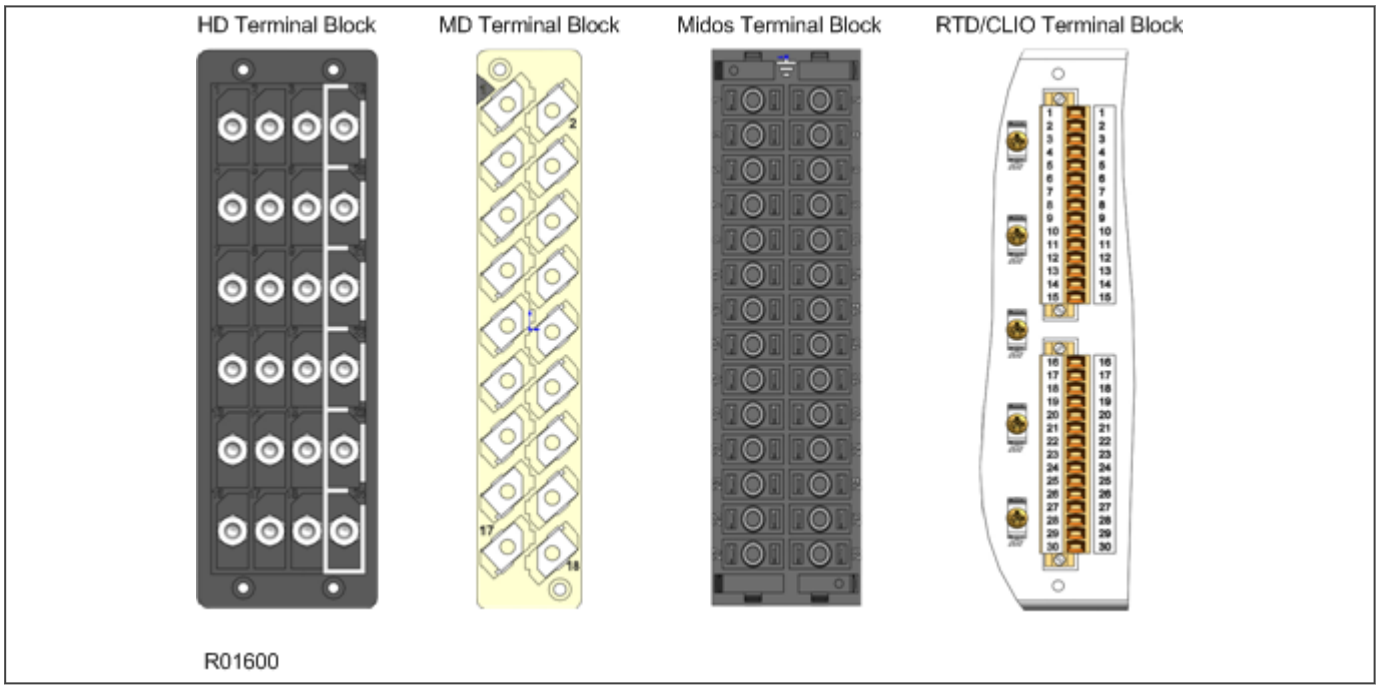


Figure 55: Terminal block types

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 color
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.

8.4.2 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.

8.4.3 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.

8.4.4 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.

8.4.5 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.

8.4.6 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.

8.4.7 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

8.4.8 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.

8.4.9 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.

8.4.10 OUTPUT RELAY CONNECTIONS

These should be wired with 1 mm PVC insulated multi-stranded copper wire terminated with M4 ring terminals.

8.4.11 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

8.4.12 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.

8.4.13 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.

8.4.14 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.

8.4.15 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.

8.5 CASE DIMENSIONS

Not all products are available in all case sizes.

8.5.1 CASE DIMENSIONS 40TE

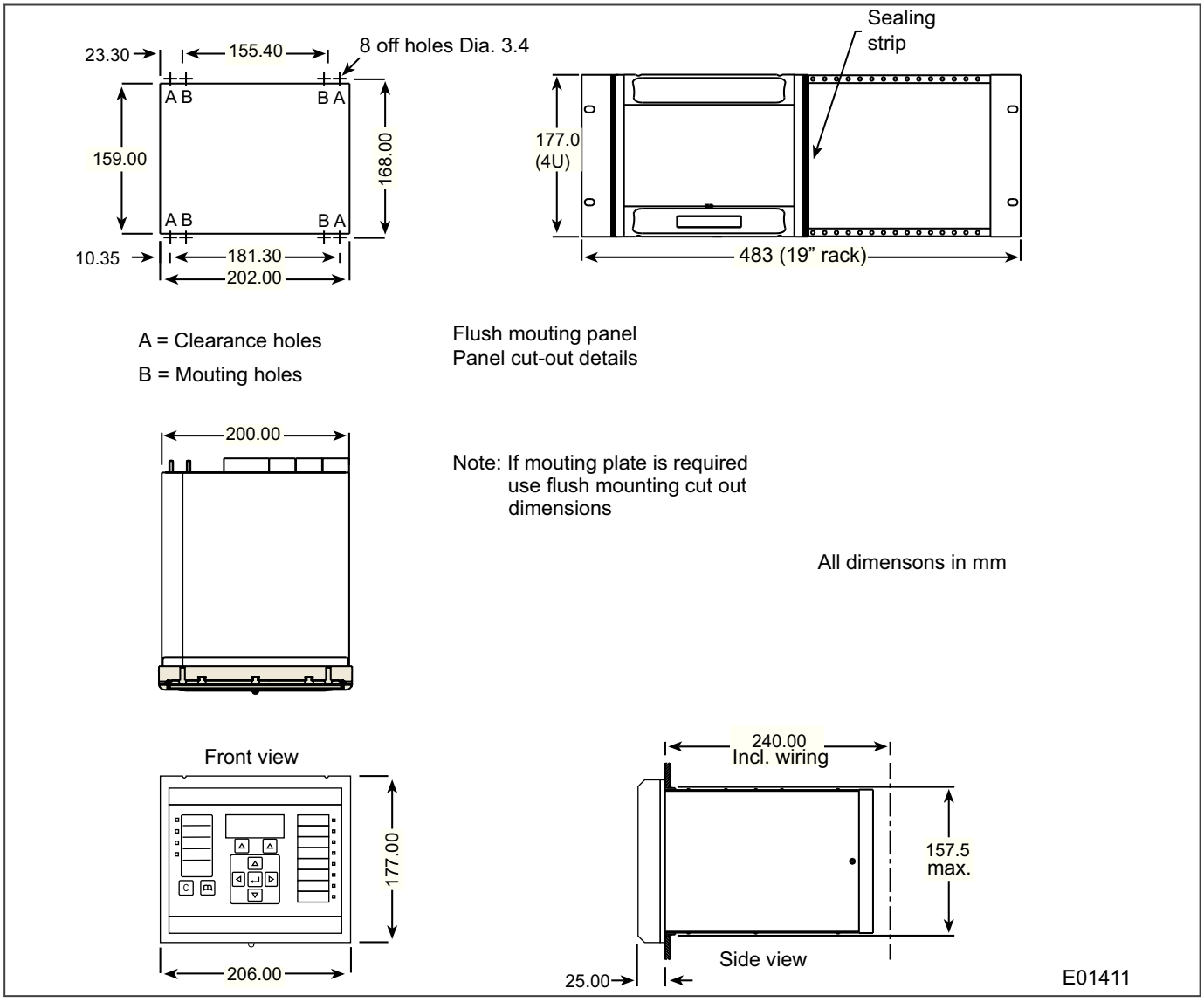


Figure 56: 40TE case dimensions

8.5.2 CASE DIMENSIONS 60TE

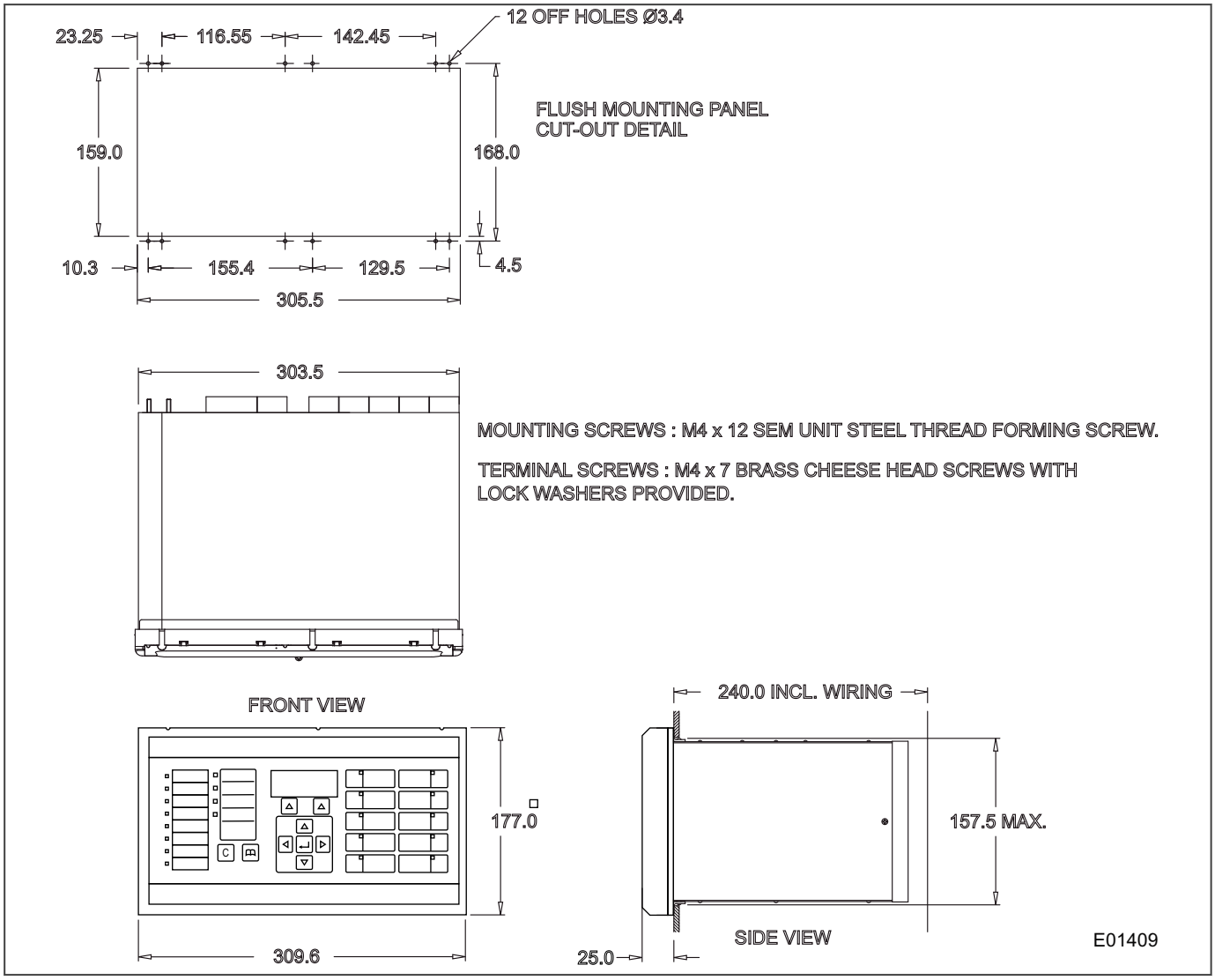


Figure 57: 60TE case dimensions

8.5.3 CASE DIMENSIONS 80TE

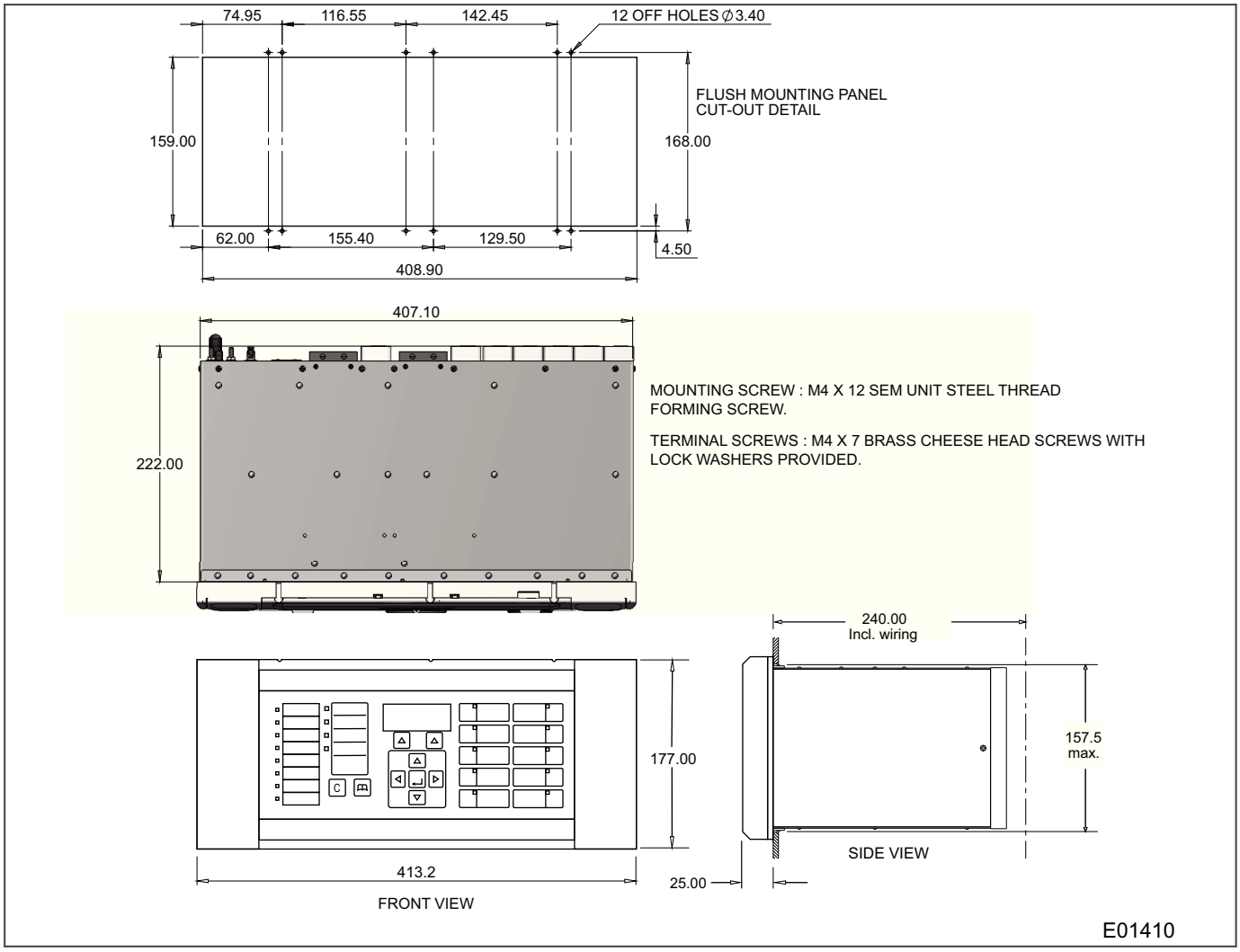


Figure 58: 80TE case dimensions

CHAPTER 9

COMMISSIONING INSTRUCTIONS

9.1 CHAPTER OVERVIEW

This chapter contains the following sections:

Chapter Overview 193
General Guidelines 194
Commissioning Test Menu 195
Commissioning Equipment 198
Product Checks 200
Setting Checks 209
IEC 61850 Edition 2 Testing 211
Correct Distance Function Operation 216
Distance Scheme Test (if Activated in MiCOM S1 Agile) 234
Loss of Guard/Loss of Carrier Test 235
Weak Infeed Mode Test 236
Protection Operation During Fuse Failure 238
Demonstrate Correct Overcurrent Function Operation 239
Check Trip and Auto-reclose Cycle 241
Protection Timing Checks 242
Onload Checks 244
Final Checks 246

9.2 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.

9.3 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.

9.3.1 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.

9.3.2 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 relay 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.*

9.3.3 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).

9.3.4 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.

9.3.5 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.*

9.3.6 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.

9.3.7 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.*

9.3.8 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***.

9.3.9 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 `3 Pole Test` command 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 *3 Pole Test* command.

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.*

9.3.10 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.*

9.4 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.

9.4.1 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

9.4.2 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

9.4.3 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/MODBUS/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 or BFOC (LC) connectors depending on the Ethernet board ordered for testing the fibre-optic RP1 port.

9.5 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.

9.5.1 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.

9.5.1.1 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.

9.5.1.2 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.

9.5.1.3 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.

9.5.1.4 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.

9.5.1.5 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

9.5.1.6 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.

9.5.2 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.

9.5.2.1 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

9.5.2.2 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.

9.5.2.3 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.

9.5.2.4 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.

9.5.2.5 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.

9.5.2.6 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.

9.5.2.7 TEST USER-PROGRAMMABLE LEDS

To test these LEDs, set the Test LEDs cell to `Apply Test`. Check that all user-programmable LEDs illuminate.

9.5.2.8 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.

9.5.2.9 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`.

9.5.2.10 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.

9.5.2.10.1 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:

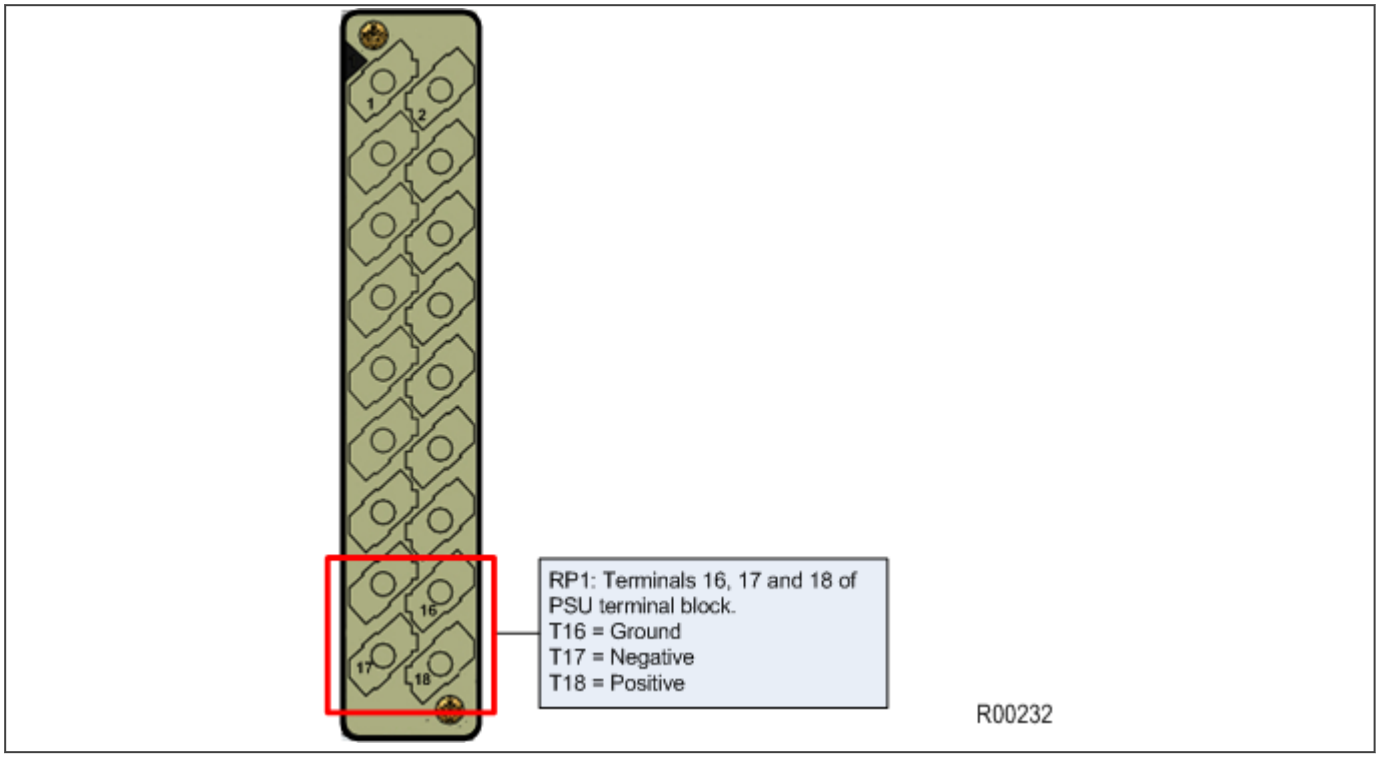


Figure 59: RP1 physical connection

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.

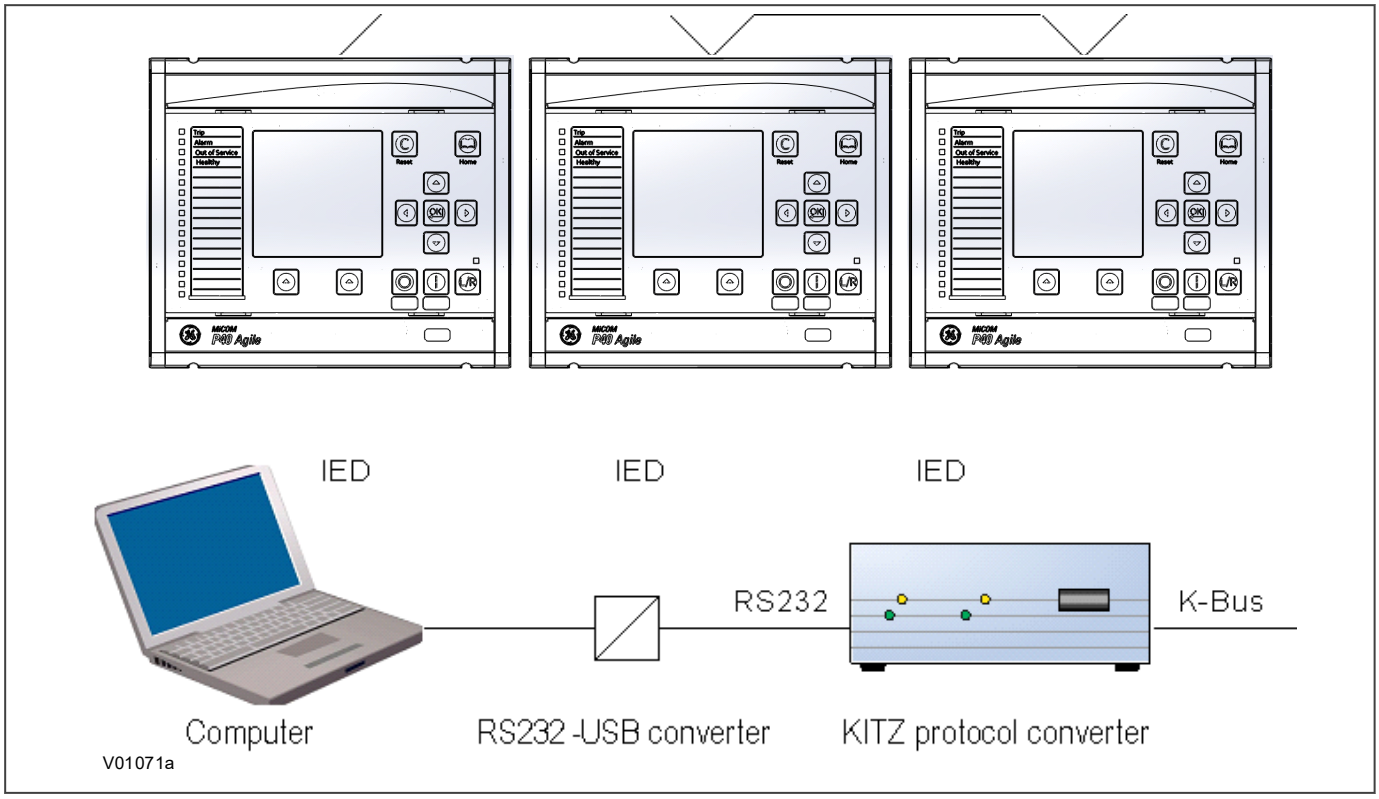


Figure 60: Remote communication using K-bus

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.

9.5.2.10.2 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.

9.5.2.11 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).

9.5.2.12 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).

9.5.3 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.

9.5.3.1 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.

9.5.3.2 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.

9.6 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.*

9.6.1 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

9.6.1.1 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.*

9.6.1.2 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.

9.7 IEC 61850 EDITION 2 TESTING

9.7.1 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.

9.7.1.1 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.

9.7.1.2 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

9.7.2 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:

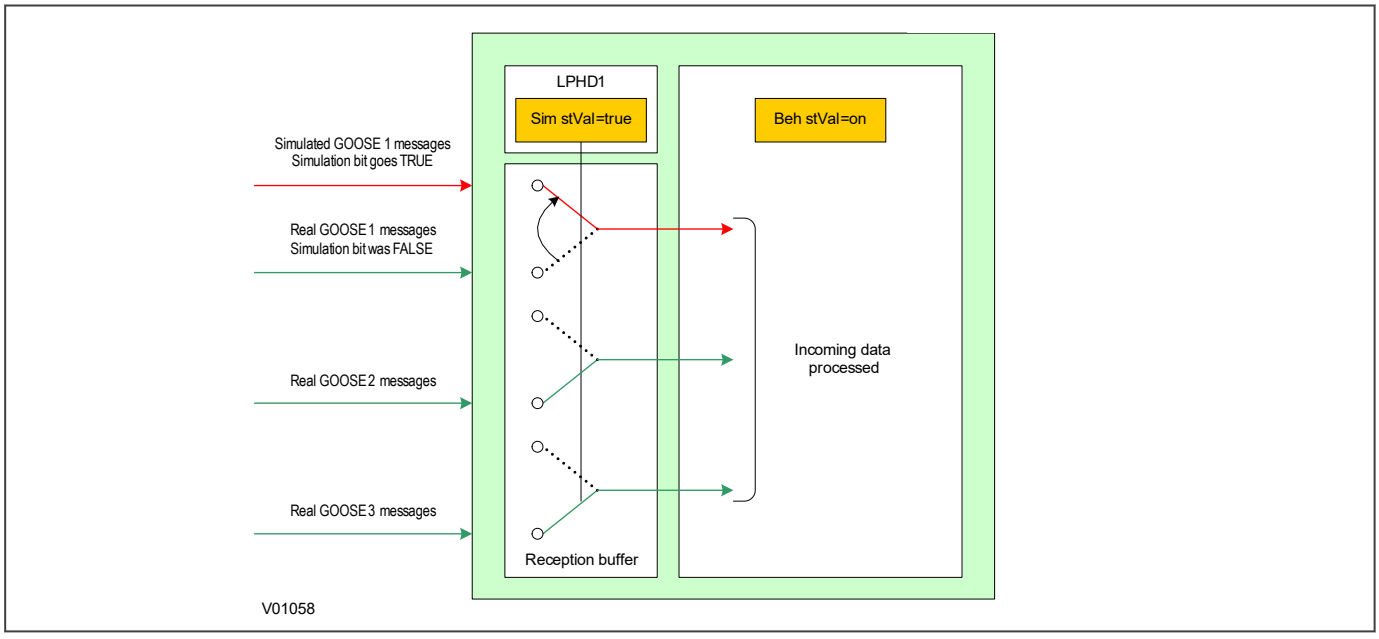


Figure 61: Simulated input behaviour

9.7.3 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.

9.7.3.1 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

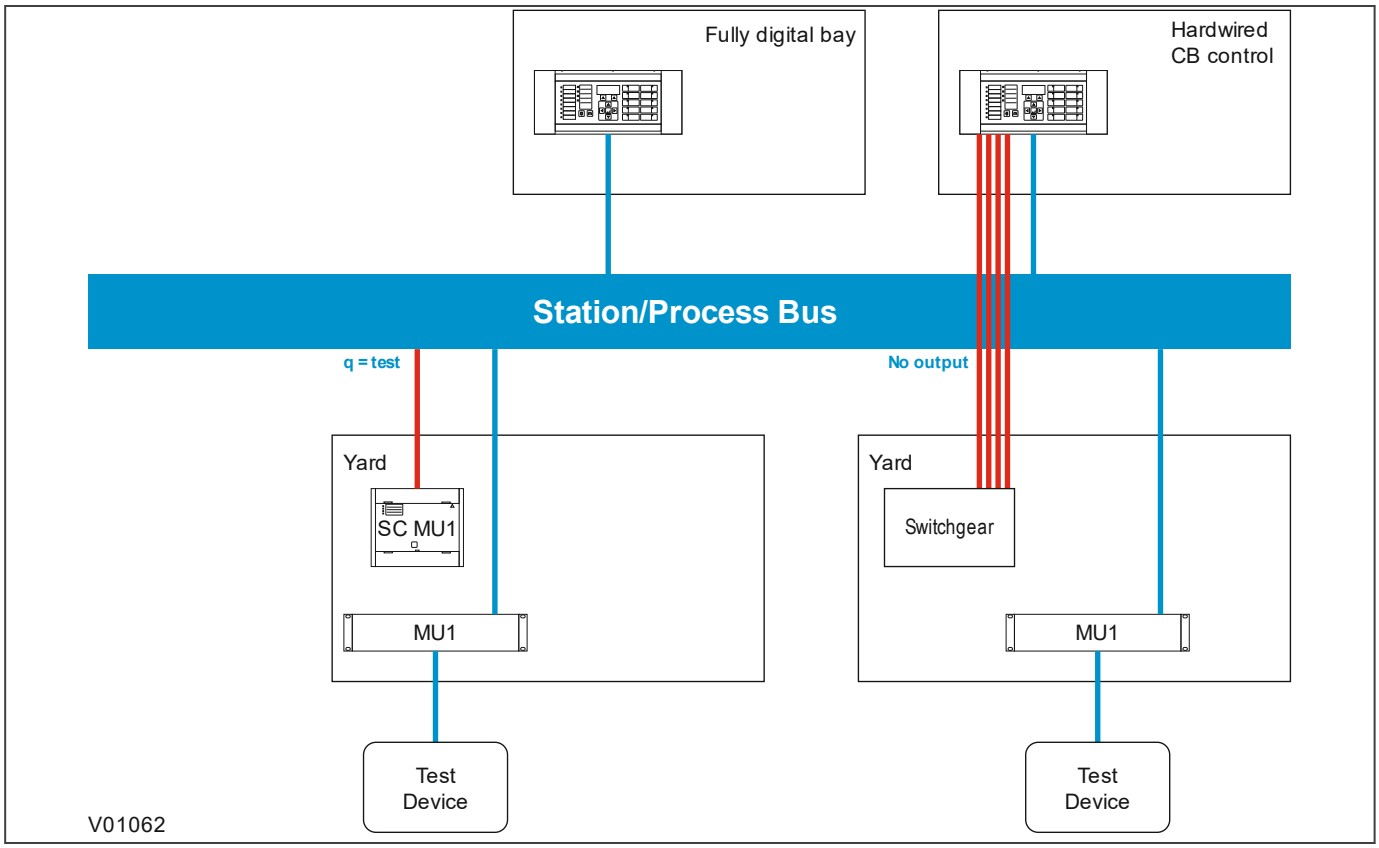


Figure 62: Test example 1

9.7.3.2 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

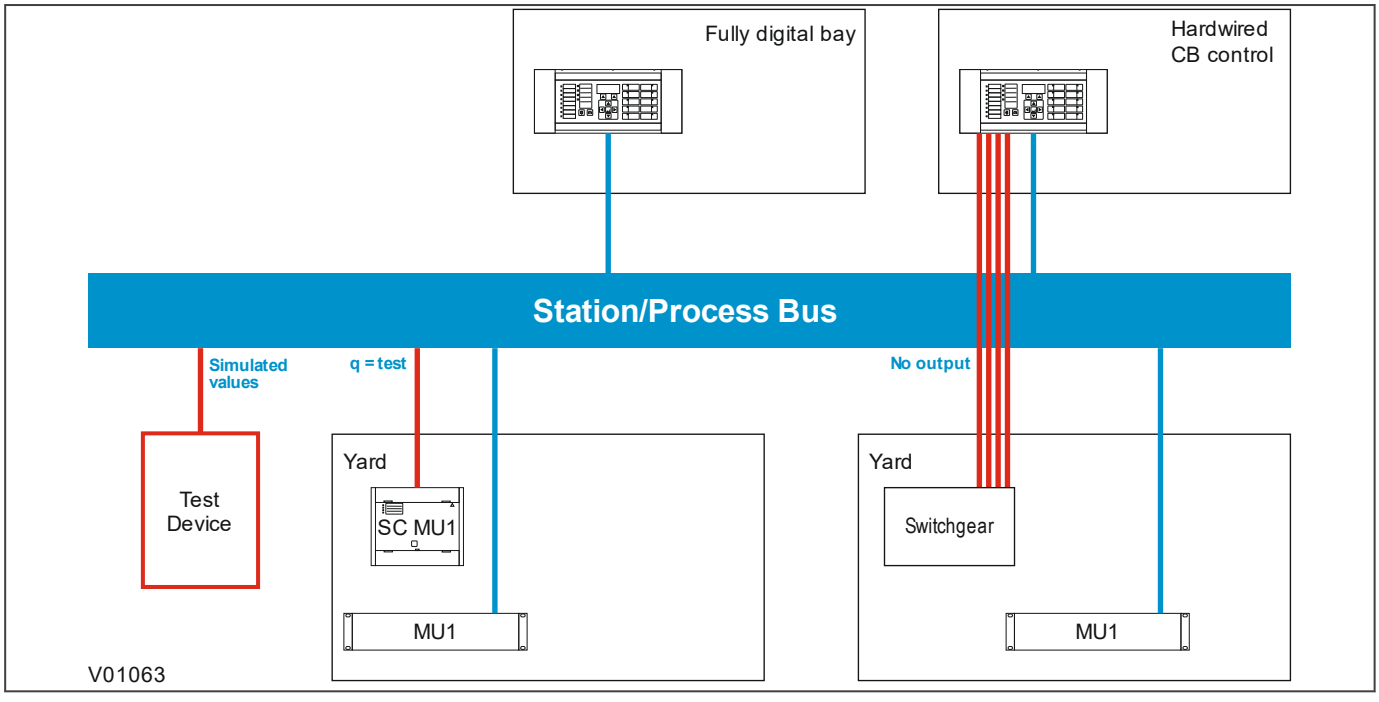


Figure 63: Test example 2

9.7.3.3 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:

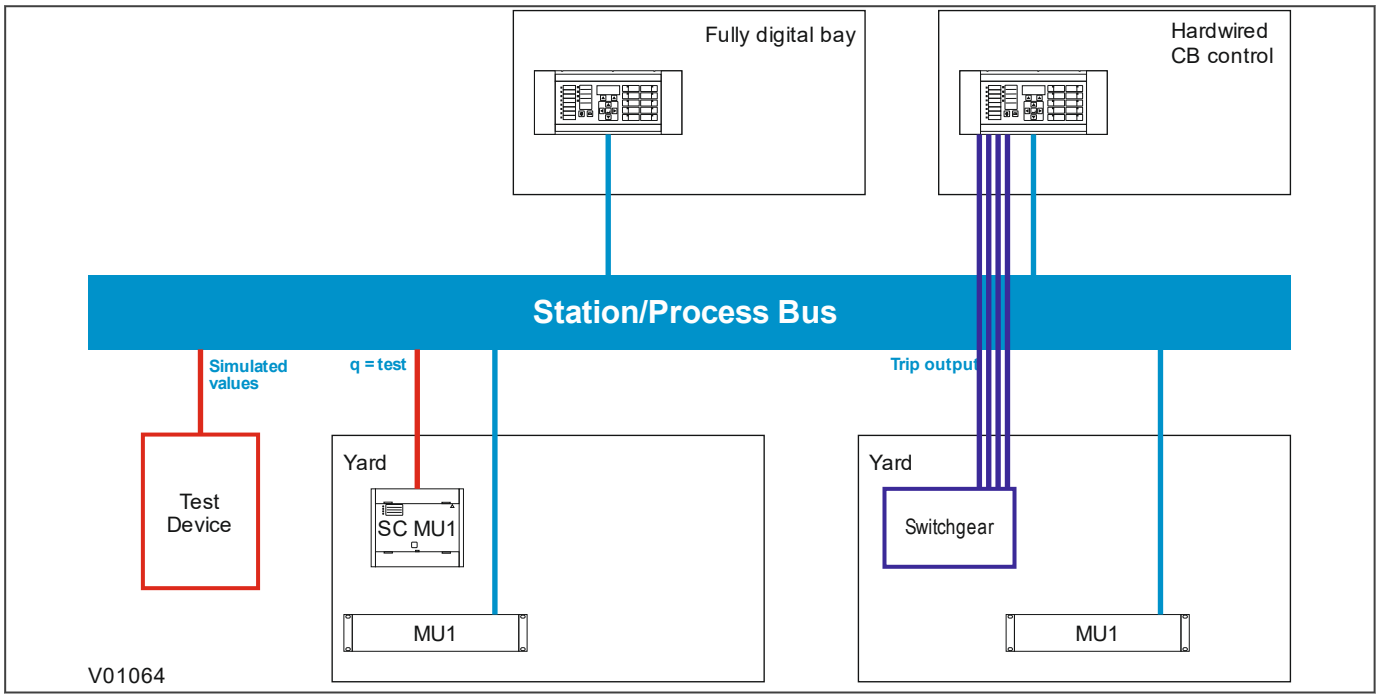


Figure 64: Test example 3

9.7.3.4 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.*

9.8 CORRECT DISTANCE FUNCTION OPERATION

9.8.1 FUNCTIONAL TESTS: START, CONTROL & DISTANCE CHARACTERISTIC LIMITS

Tests can be performed to check that the relay has the right characteristics for the different functions and settings options (protection (with MiCOM S1 Agile/settings & records) and logic schemes (with MiCOM S1 Agile/PSL Editor) settings).

The Distance scheme test (if activated in MiCOM S1 Agile) section, explains how to perform a complete check of all the distance protection functions of the relay (with the factory's settings & PSL: "P&C by default").

In the event of relay or application failure:



Caution:
Return to the basic configuration (settings & PSLI) and then validate the tests following the enclosed description (via the LCD on the front panel (configuration/ restore defaults/all settings+validate))

The default password required to confirm the settings is:

AAAA

Every action performed using a laptop can also be performed using the LCD front panel (only PSL and Text Editor require a computer).

9.8.1.1 MEASUREMENTS CHECK

Before starting the tests, perform the following injections on the secondary side of the relay:

Test 1	Currents	IA	0.2 In	0°
		IB	0.4 In	- 120°
		IC	0.8 In	+ 120°
	Voltages	VAN	30 V	0°
		VBN	40 V	- 120°
		VCN	50 V	+ 120°

- Check the displayed values on the relay's front panel (LCD): "*system/meas1*"
- Secondary values in amplitude and phase
- Or primary values (control of ratios VT & CT) - if selected:

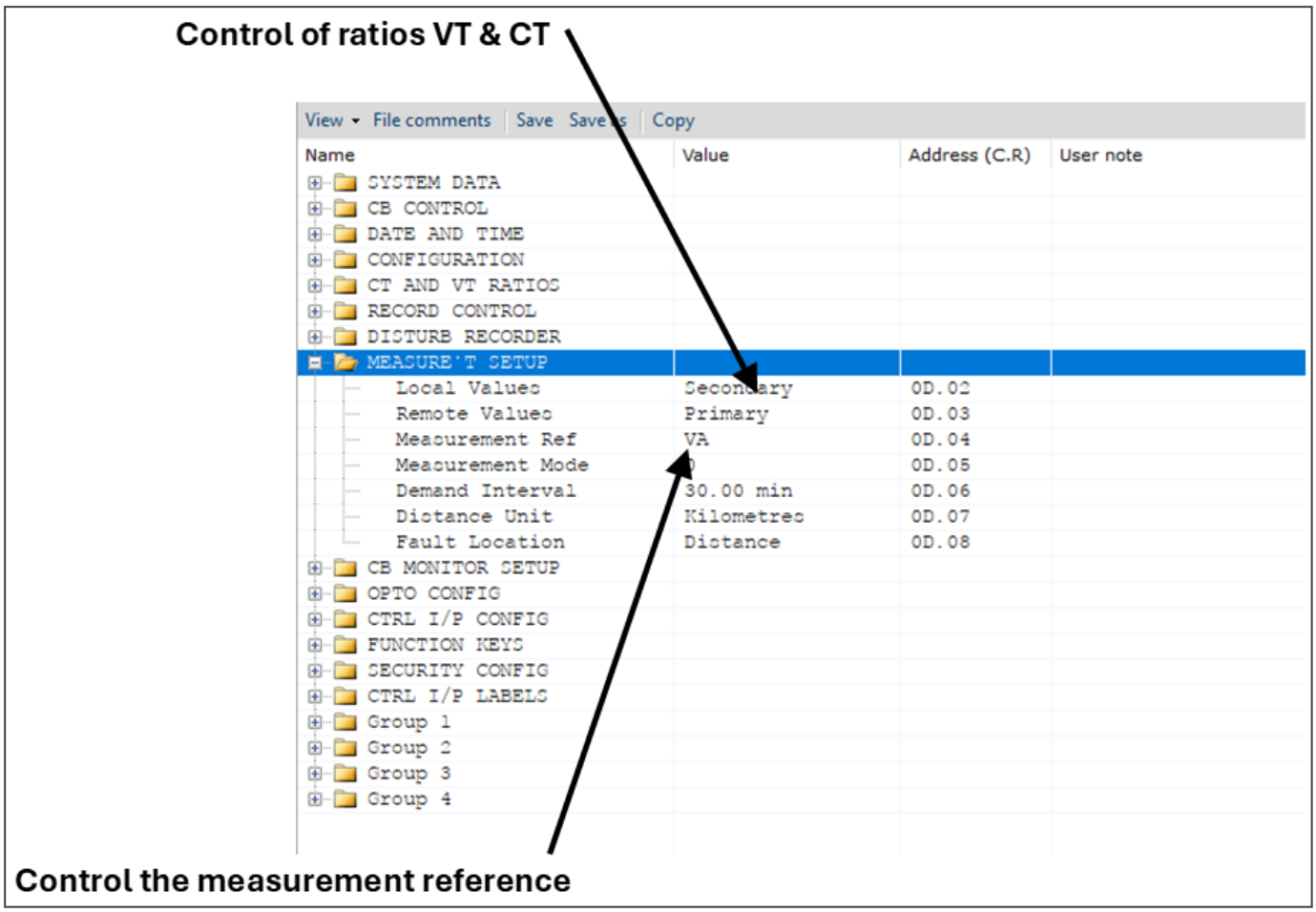


Figure 65: Control of VT & CT ratio's

Note:
1: Check the measurement reference (ref. angle of phase shift) in:
"Measurt set up/Measurement ref." (VA by default).

Monitoring can also be selected to poll the network parameters (I/U/P/Q/f…

Note:
2: In LCD: IN=3I0
After this step, the errors on the phase sequences, ratio's of CT, VT and wiring (analogue input only) will be detected.

Note:
3: See connection drawings.

Note:
4: See LCD structure in test tools.

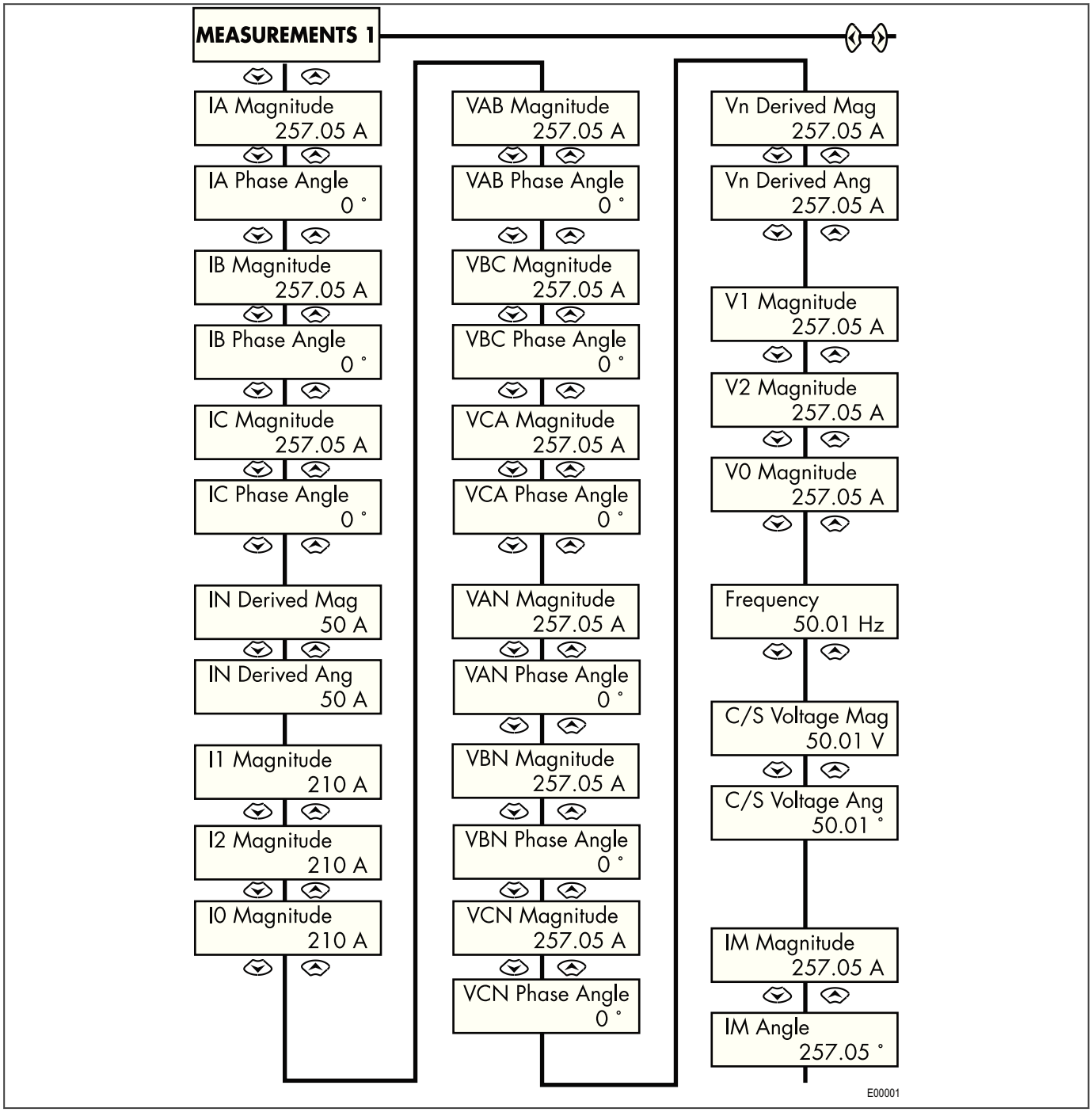


Figure 66: Measurement 1/LCD menu

Check the polarisation of the protection: inject a three-phase symmetrical load according to the following table:

Test 2		IA	IN	20°
	Currents	IB	IN	-100°
		IC	IN	+140°
		VAN	57 V	0°
	Voltages	VBN	57 V	-120°
		VCN	57 V	+120°

- If one phase is missing, the output Fuse Failure alarm will pick up and the LED general alarm on the front panel will light up (see the Fuse Failure description in the Application Notes chapter.
- According to the chosen measurement mode, the following is obtained:
    - MiCOM S1 Agile Measurement setup/Measurement mode):

Measurement Mode	0	1	2	3
P	+	-	+	-
Q	-	-	+	+

Selected in MiCOM S1 Agile by:

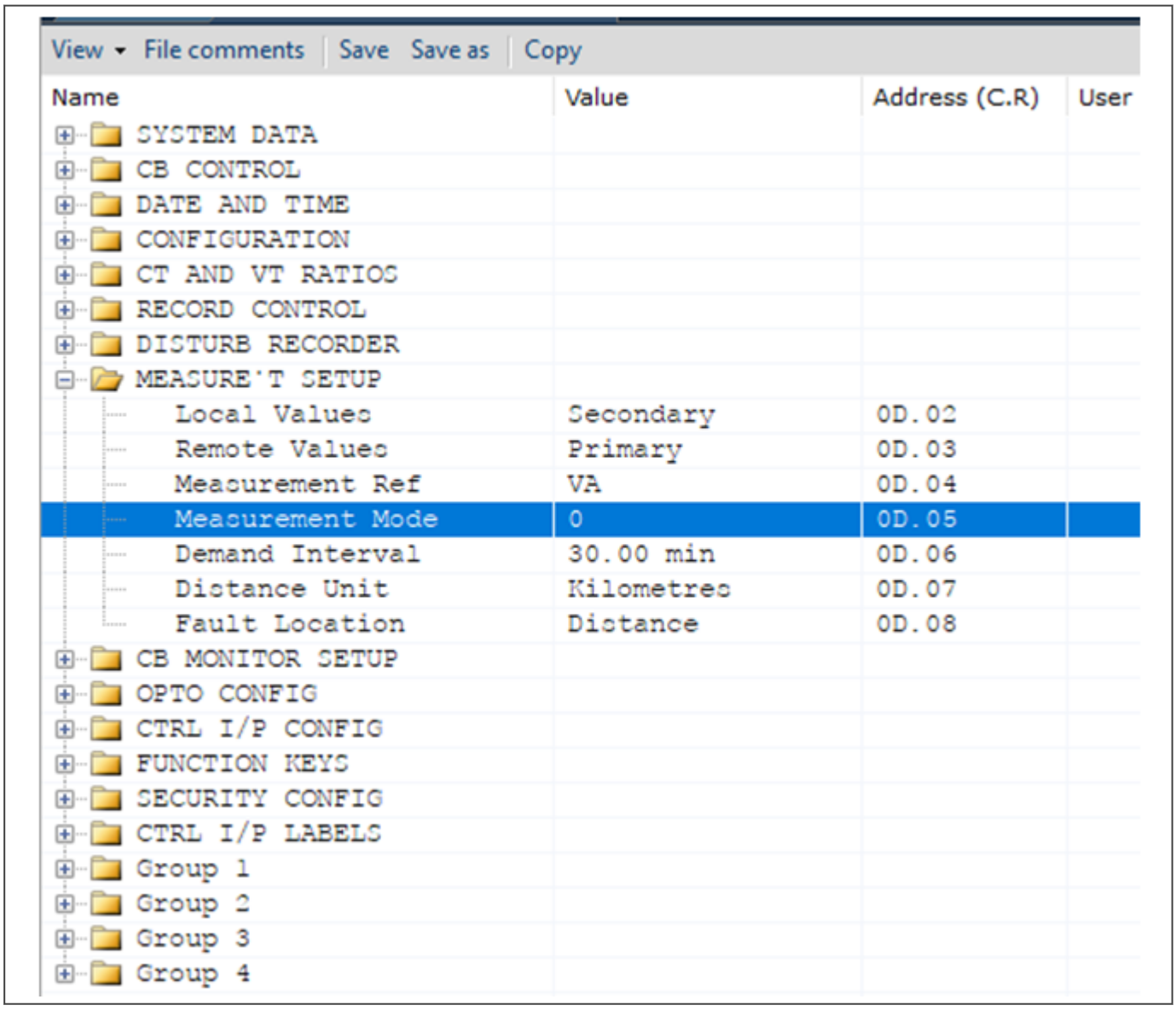
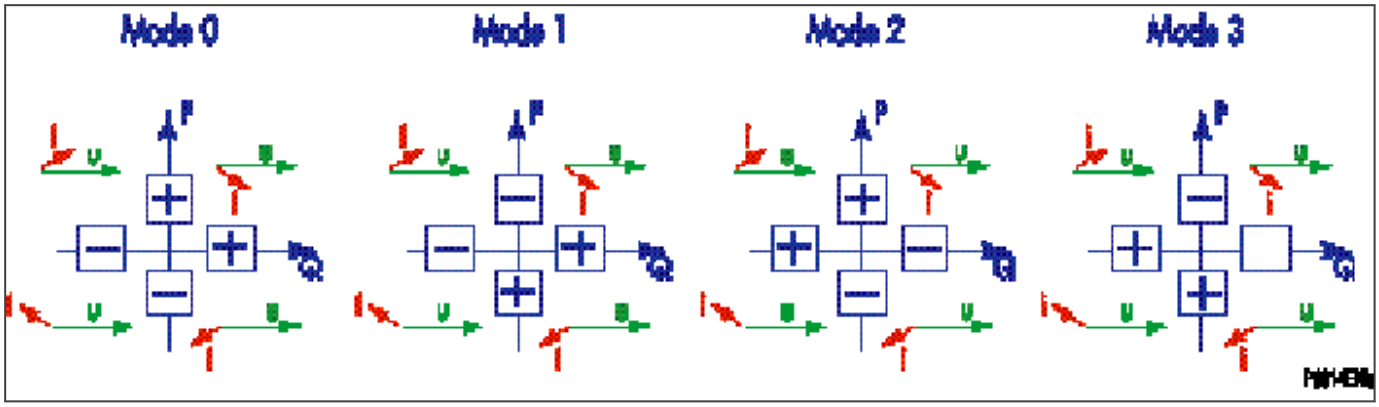


Figure 67:



- Check the signs of values P, Q to LCD ("Measurements 2") - settable with LCD (see the figure above).

The primary side orientation remains to be achieved (repeat previously points with a primary injection).

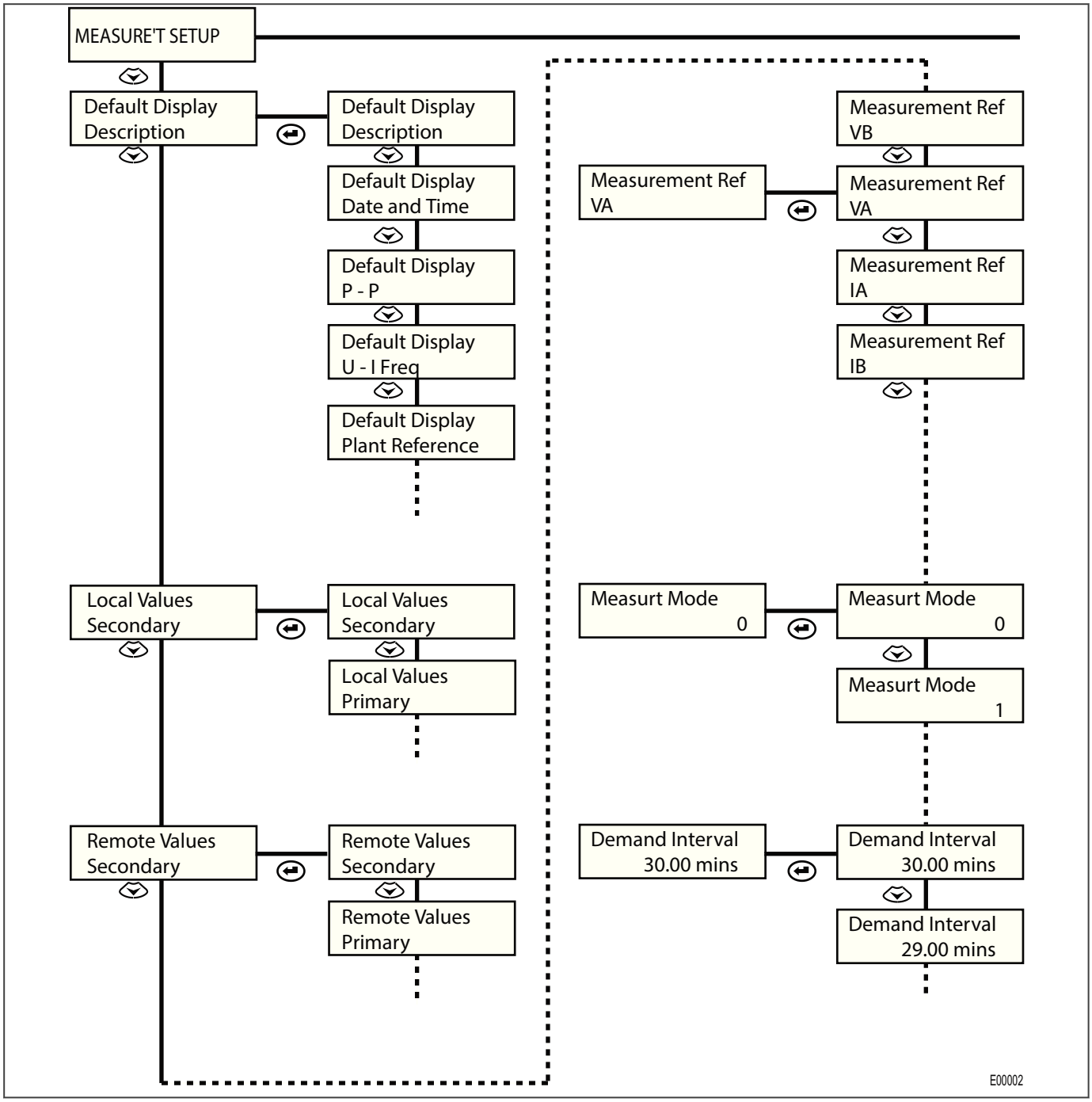


Figure 68: Measurement setup/LCD menu

9.8.1.2 DEFAULT SIMULATION PRINCIPLE

Simulating a single-phase fault

The distance protection detects a single-phase default in E if the impedance and phase of this point place it inside the characteristic. The relation between the impedance and phase and the injected voltage and current is as follows:

- Fault Impedance Z = Vphase/Iphase
- Fault Phase φ = phase-shift (Vphase, Iphase)
- The Vphase voltage has to remain lower than the rated voltage value

Impedance test for zone 1:

I1 = 1A

$\varphi 1$ = line angle = 76°

$V1/I1$ = Zfault = Zd (1 + k0) + Rfault

Rfault = R loop

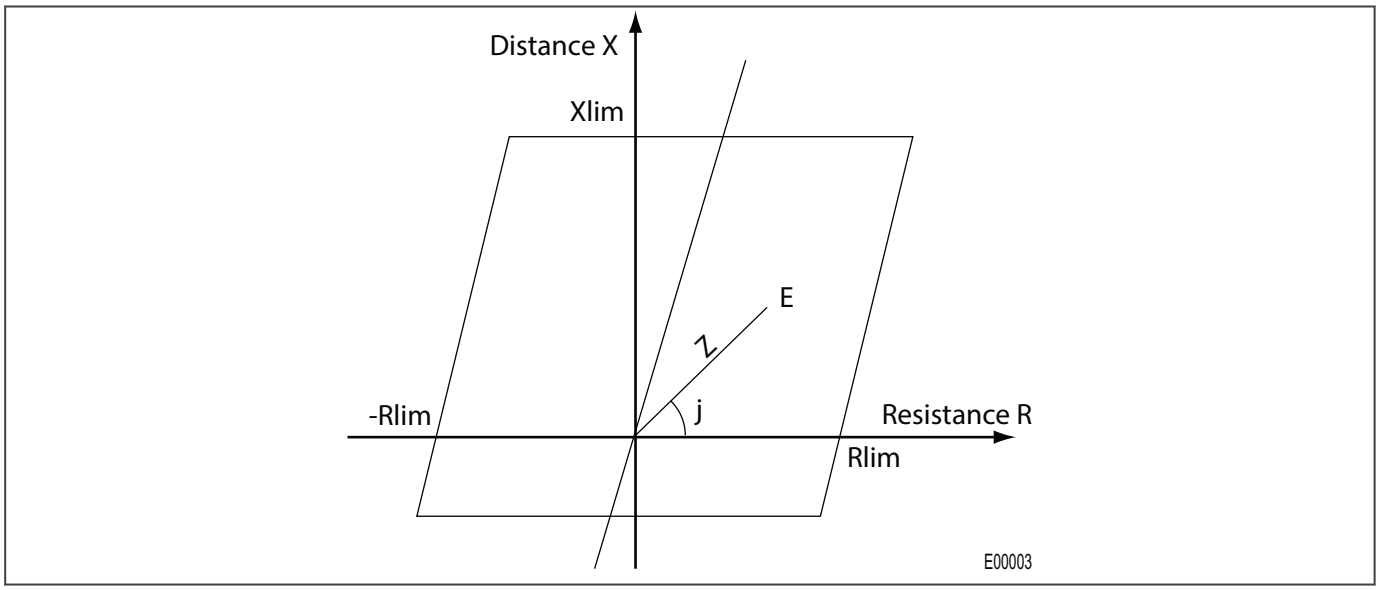


Figure 69: Characteristic point determination (Rlim two-phase & Single-phase can be different)

The characteristic angle is:

- For phase-to-phase: Argument of the positive impedance of the line (Z1)
- For phase-to-earth: Argument of 2Z1+Z0

The relay characteristic can be created and displayed with Z-Graph (MiCOM Z-Graph software is a tool delivered with the protection).

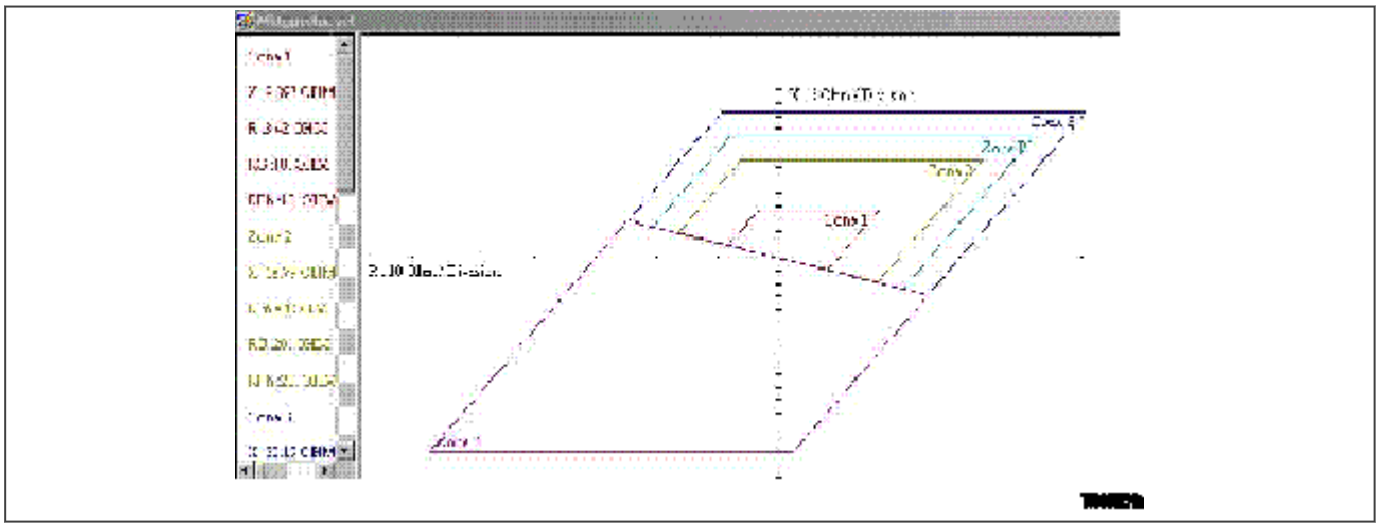


Figure 70: Example of Z-graph screen (Rio format can be created as well)

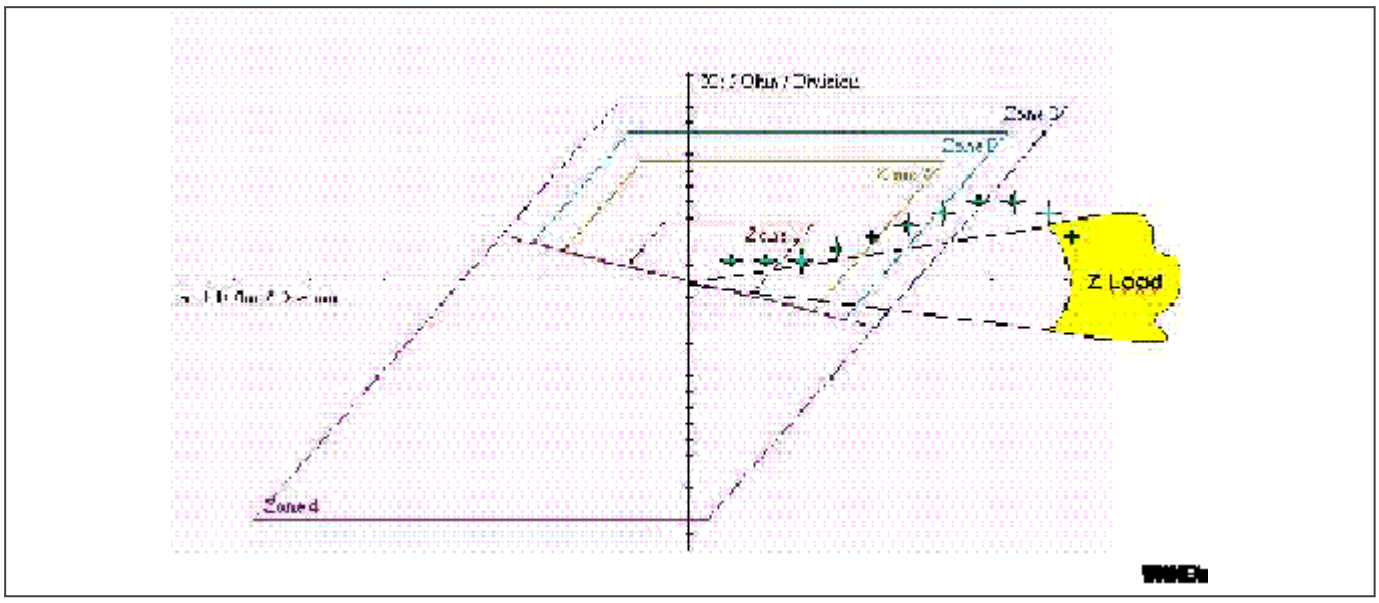


Figure 71: Evolving impedance from the load area to the final fault impedance in Zone1

To simulate a fault in a zone, it is necessary to vary the current progressively to move the point from the load area into the desired zone.

A single-phase starting characteristic with different values of K0 can be created:

$K0x = (Zx0 - Z1)/(3\ Z1)$

(In S1 there are up to four possibilities KZ1 & KZ2, KZp, KZ3/4).

This solution is carried out in case of an underground cable/overhead line section ($KZ1 \neq KZ2 = KZp = KZ3/4$) where the Z01 & Z02 angles can be very different (HV Line at 80° and cable at 45°).

The most common injection devices do not allow several values of K0 to be handled (the same for Z-Graph); so for accurate control of zone limits, it will be necessary to generate several characteristic files (as many Rio files as KZ values).

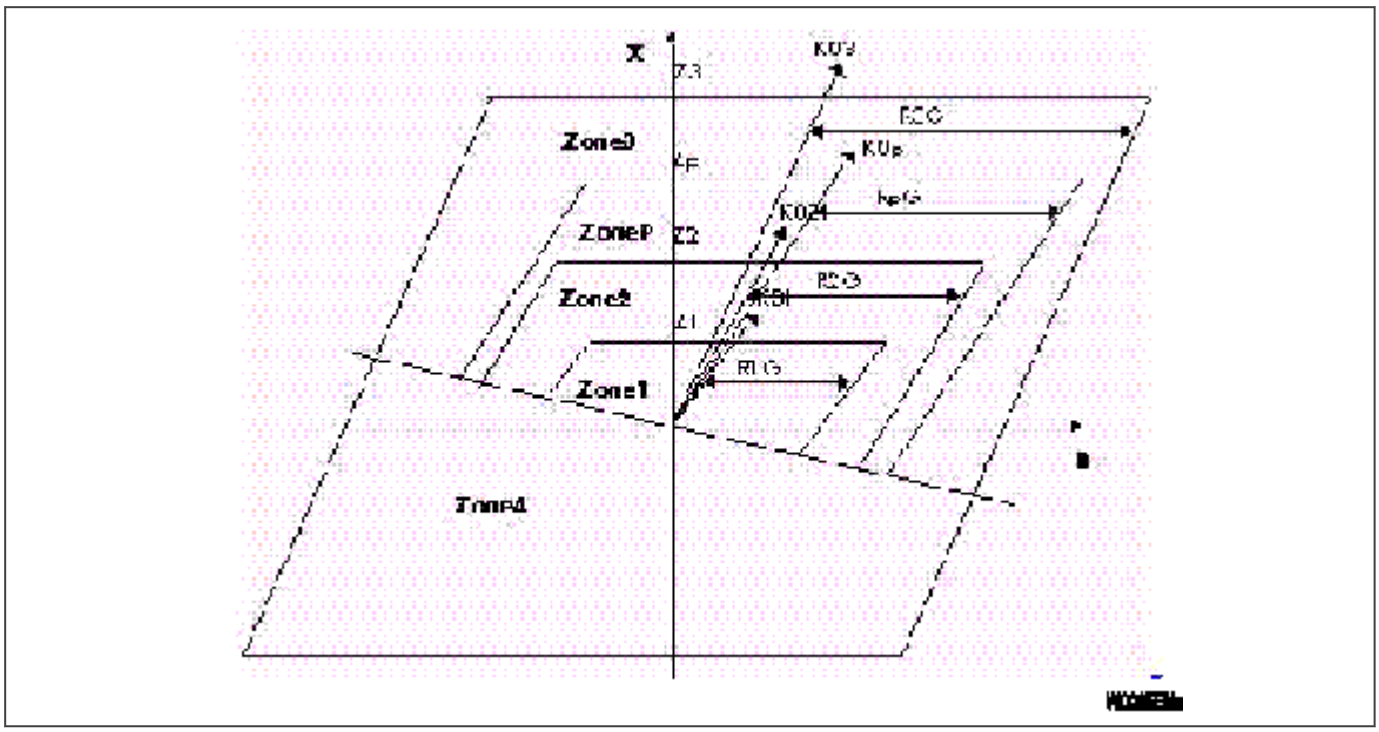


Figure 72: Single characteristic with P forward zone

Z1, Z2, Z3, Zp, Z4 : limits of zone 1, 2, 3, p, 4

R1G, R2G, R3G, RpG : resistance limits of zone 1, 2, 3, p, 4 for single-phase fault

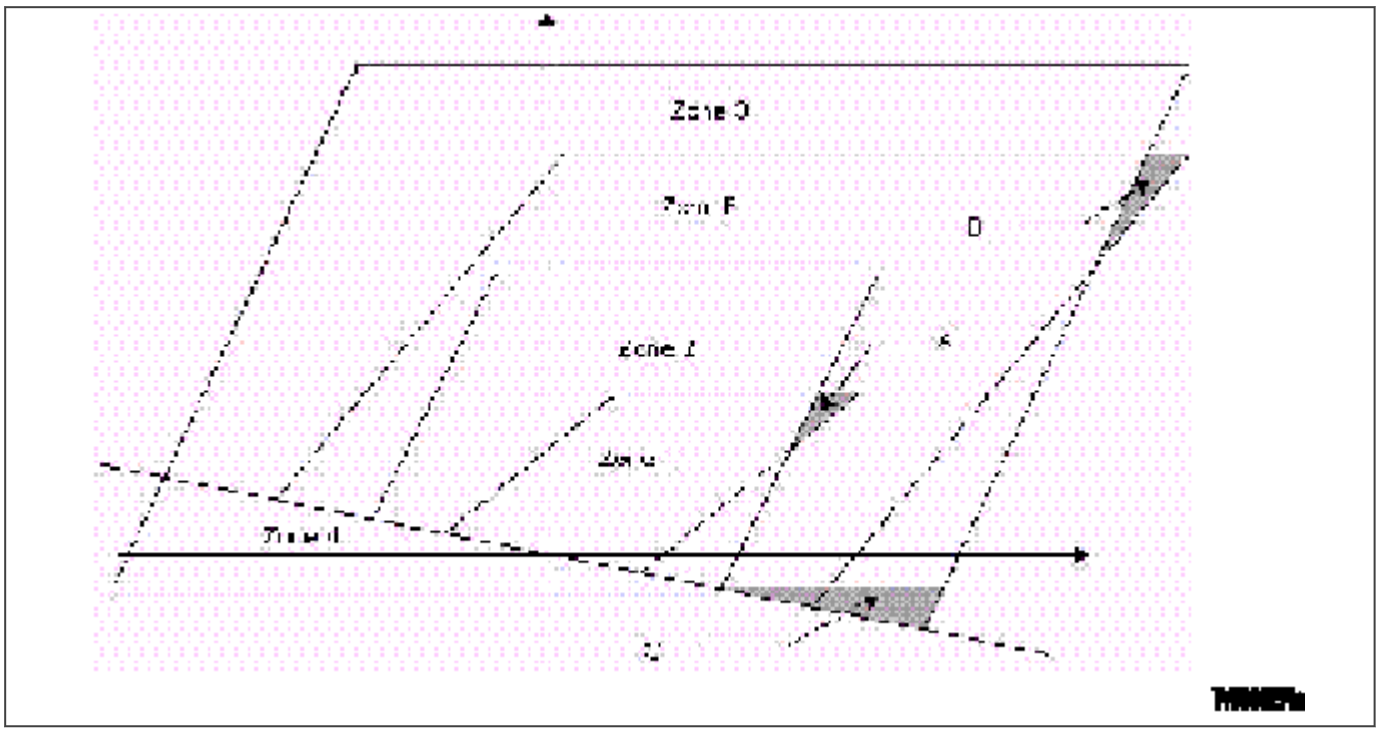
K01, K02, 03, K0p : residual compensation factor of zone 1, 2, 3, p

Zone 1, 2, 3 & P can have different resistance limits and residual factors. Zones 3 and 4 (start zone) have the same resistance sensitivity and residual compensation factor. The residual compensation factor depends on the lines characteristic in each zone.

Line angle: $\varphi pg = Arg\ ((2xZ1 + Zx0)/3)$ where Z*x*0 is the zero sequence impedance for zone x and Z1 is the positive impedance.

Zones coverage

Different line angles for each single-phase characteristic zone can be defined, and depending on the configuration of each zone, some encroachment between zones could occur.



In the characteristic above, the parts marked A, B and C are intersections between several zones.

- Surface A is considered as being in zone 1
- Surface B is not a part of the characteristic (no start element)
- Surface C is not a part of the starting characteristic (up to version A4.0, a new logic is implemented to keep Z1 forward detection in area C (even with a fault negative reactance value higher than the reverse limit X4)).

Plausibility

For a characteristic to be plausible, its various parameters must comply with the following equations: (no blocking plausibility check is provided by the internal logic control of the relay).

- If zone P is set forward:
  - $Z1 < Z1ext < Z2 < Zp < Z3$
  - $tZ1 < tZ2 < tZp < tZ3$
  - $R1G \leq R2G \leq RpG \leq R3G$
  - $R1Ph \leq R2Ph \leq RpPh \leq R3Ph$
- If zone P is set reverse:
  - $Z1 < Z1ext < Z2 < Z3$
  - $Zp < Z4$
  - $tZ1 < tZ2 < tZ3$
  - $tZp < tZ4$
  - $R1G \leq R2G \leq R3G$

- RpG ≤ R4G
- R1Ph ≤ R2Ph ≤ R3Ph
- RpPh ≤ R4Ph

- The Z minimum value measured by the relay is: 60 mohms (Z1min set in S1 is 1ohm with CT 1Amp & 200 mohms with CT 5Amp).
- There is no limit for the R/X ratio because a floating-point processor is used for the R calculation & X calculation (separated dynamic range for each calculation). As a consequence the limit will be given by the angle error of the CT.

For example in PUR with CT accuracy angle at 1° (for IN), this gives an R/X = 5,7 - to keep a 10% error in the X1 measurement.

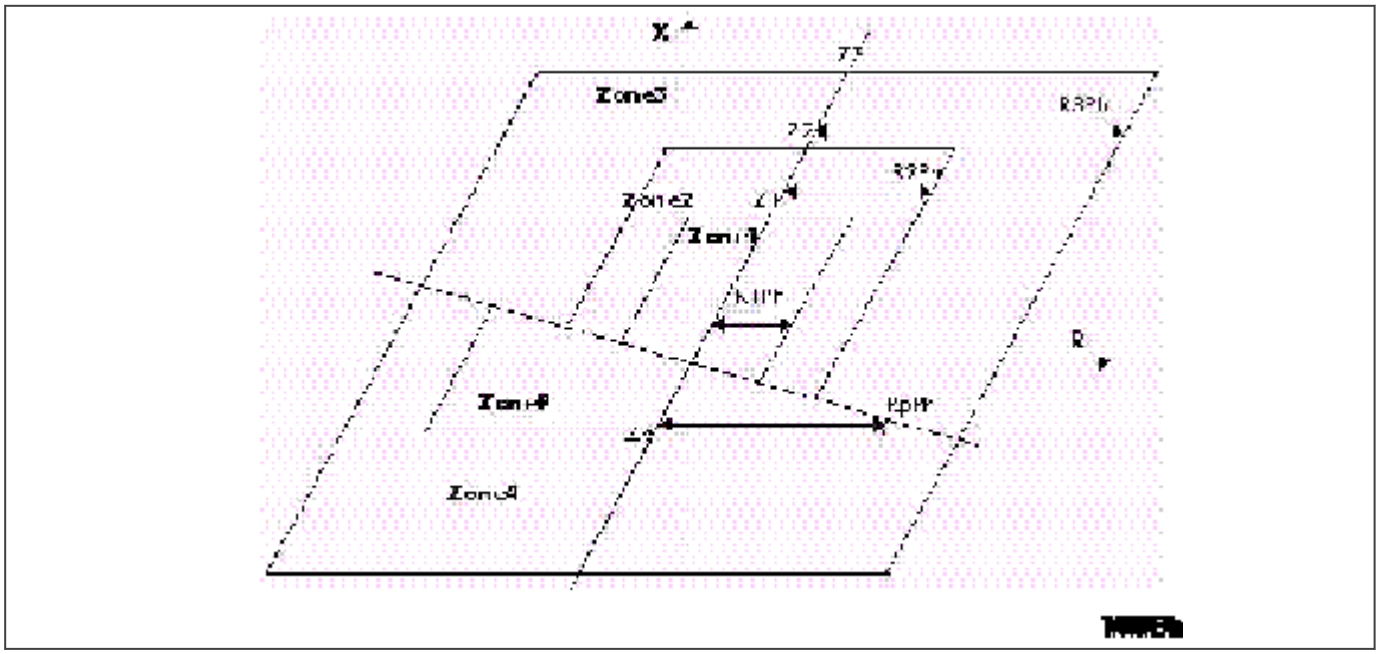
- R limit: min. 0/max. 80 ohms (CT 5Amp) - min. 0/max. 400 ohms (CT 1Amp)
- X limit: min. 0,2/max. 100 ohms (CT 5Amp) - min.1/max. 500 ohms (CT 1Amp)

Simulating a two-phase fault

The two-phase fault simulation principle is the same as the one used to simulate a single-phase fault but:

- The voltage reference is the line to line voltage between phases, Uab for example.
- The reference current is the difference between the phase-currents, Ia - Ib for example.
  - The fault impedance Z = (Uphase-phase/(Iphase1 - Iphase2)).
  - The R1M point (single phase) is replaced by the R1ph point.(Biphase).

Two-phase characteristic with reverse zone P:



Fault simulation = (Uαβ)/I1 = 2 x *Zd + Rfault*

Where:
Uαβ : phase-to-phase fault voltage
I1 : fault current
φ1 : fault angle

Rfault = R loop

For a three-phase fault:

Fault simulation V1/I1 = Zd + (Rfault)/2

Where:
V1 : phase-to-phase fault voltage
I1 : fault current
φ1 : fault angle

Using the Z graph, a Rio format characteristic can be created. This Rio file can be loaded onto a numerical injector that accepts this type of file. The active settings (distance elements) can be modified by Z-graph, and the relay can be upgraded with new distance parameters.

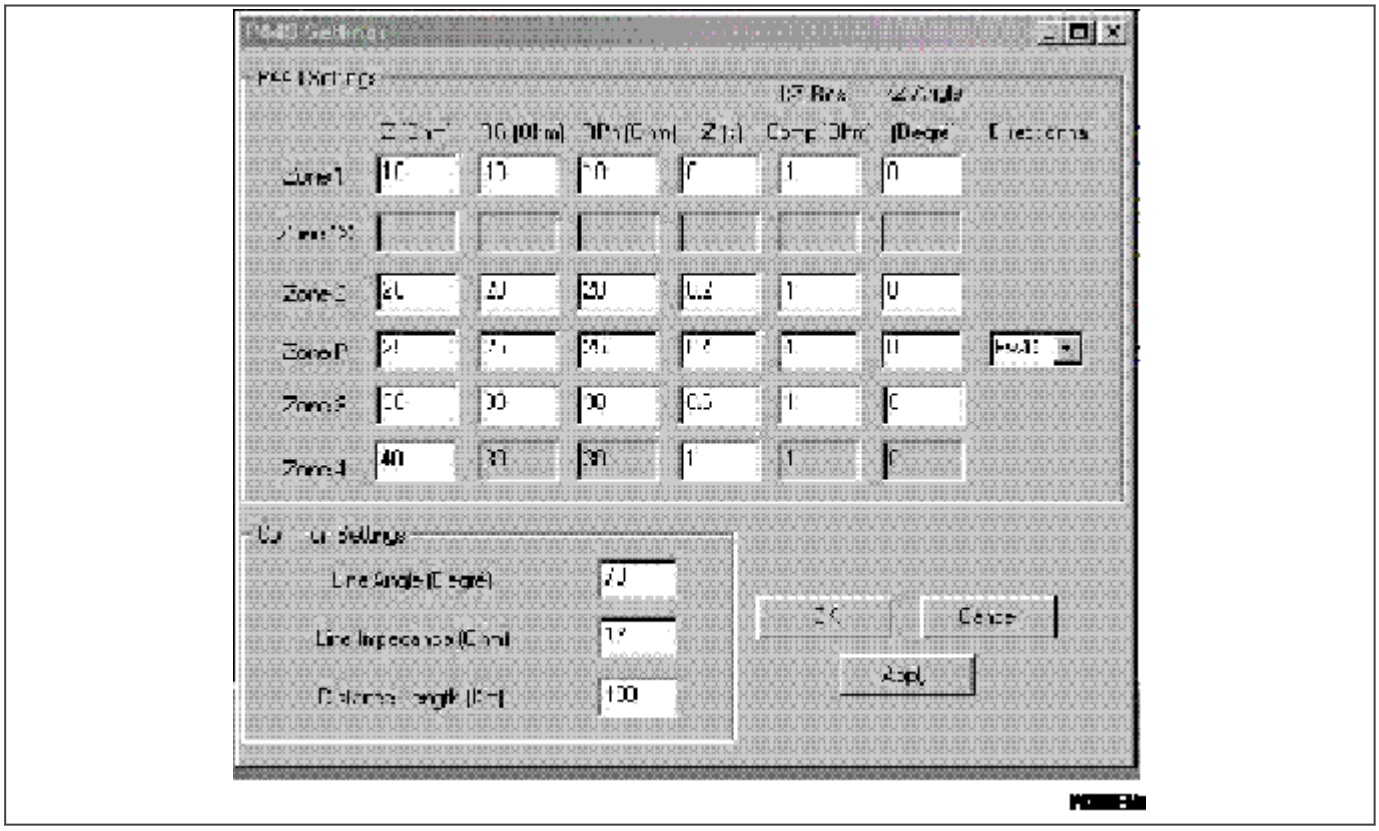
For more detail refer to section: Test tools: "Z graph user"

9.8.1.3 CHECK AND TEST OF THE STARTING CHARACTERISTICS



Caution:
Tests are described using the default parameters.

Open the MiCOM characteristics file if no changes have been made, the following values are obtained (Z-graph screen):



Control of single-phase fault characteristic's

Caution:
If different K0 are used - see the previous section, Default simulation principle.

- Energise MiCOM P44x with a healthy three-phase system (without any unbalanced condition) with a load (during a minimum time of 500 ms). This is to:
  - Enable use of the Delta algorithms
  - Avoid the start of the SOTF logic
- Reduce the current value to obtain a relation between V and I following the appended table (for Rlim - phase-shift at 0°, for Z limit - phase-shift corresponding to Z1 (in multiphase default) or corresponding to 2Z1+Z0 (in single fault).
- Check that the tripping order (DDB: Any trip/Any Trip A/Any Trip B/Any Trip C - see DDB description) is transmitted when the concerned zone time-delay expires (for a distance scheme with transmission and all distance trip logic see the Application Notes chapter.

Note:
The DDB signal any Trip A is an OR gate between:
Ext Trip A
Int Trip A

- See the test report model at the end of this section.
- Check the PSL (programmable scheme logic) trip command addresses (any Trip is linked by default to relay 7).

By default: see the wiring diagram for assignment of inputs/outputs.

Useful tip: to check the logic level of internal datas (DDB cells), all or some of the 8 red LEDs on the front panel could be assigned using the PSL.

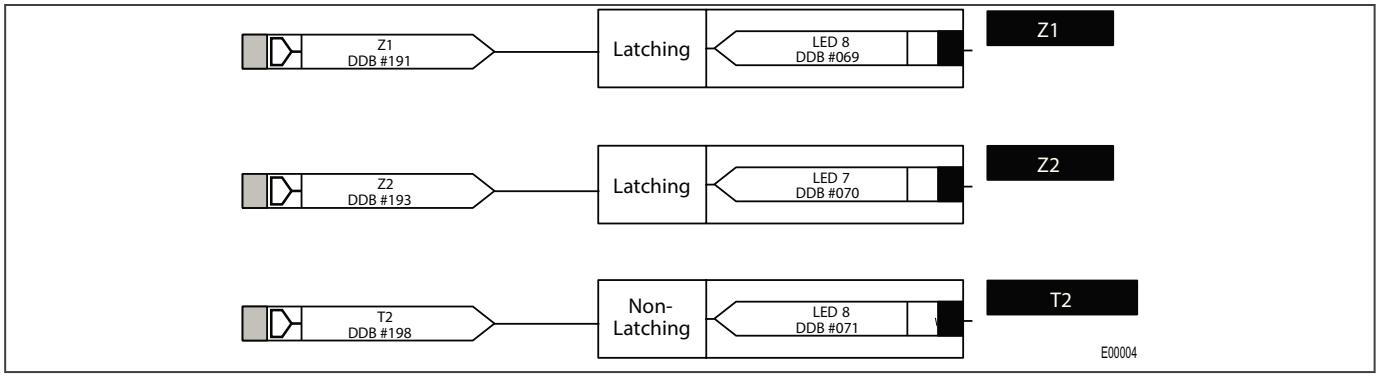
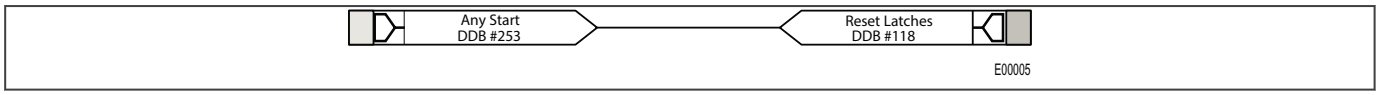


Figure 73:

If the LEDs are latched, the reset latch could be enabled by a dedicated PSL, to avoid needless keypad access during the tests.



Useful tip: to check the logic level of internal data (DDB cells), monitor bit control can be used in "commissioning Test/Opto/Relay/Test port status/Led status/Monitor bit 1 to bit 8". Any cells of the DDB can be assigned and then displayed as 1 of the 8 bits (see User Tools).

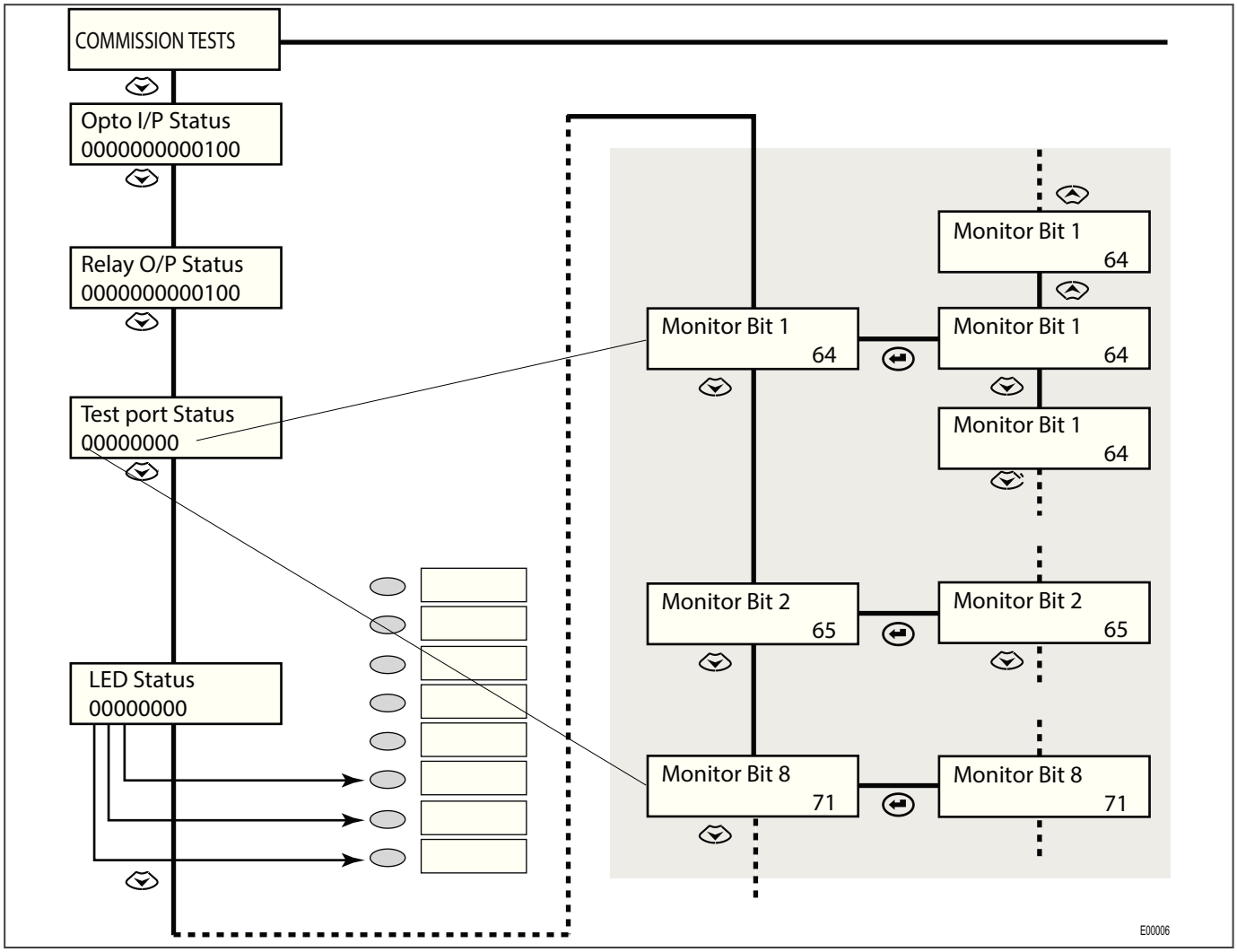


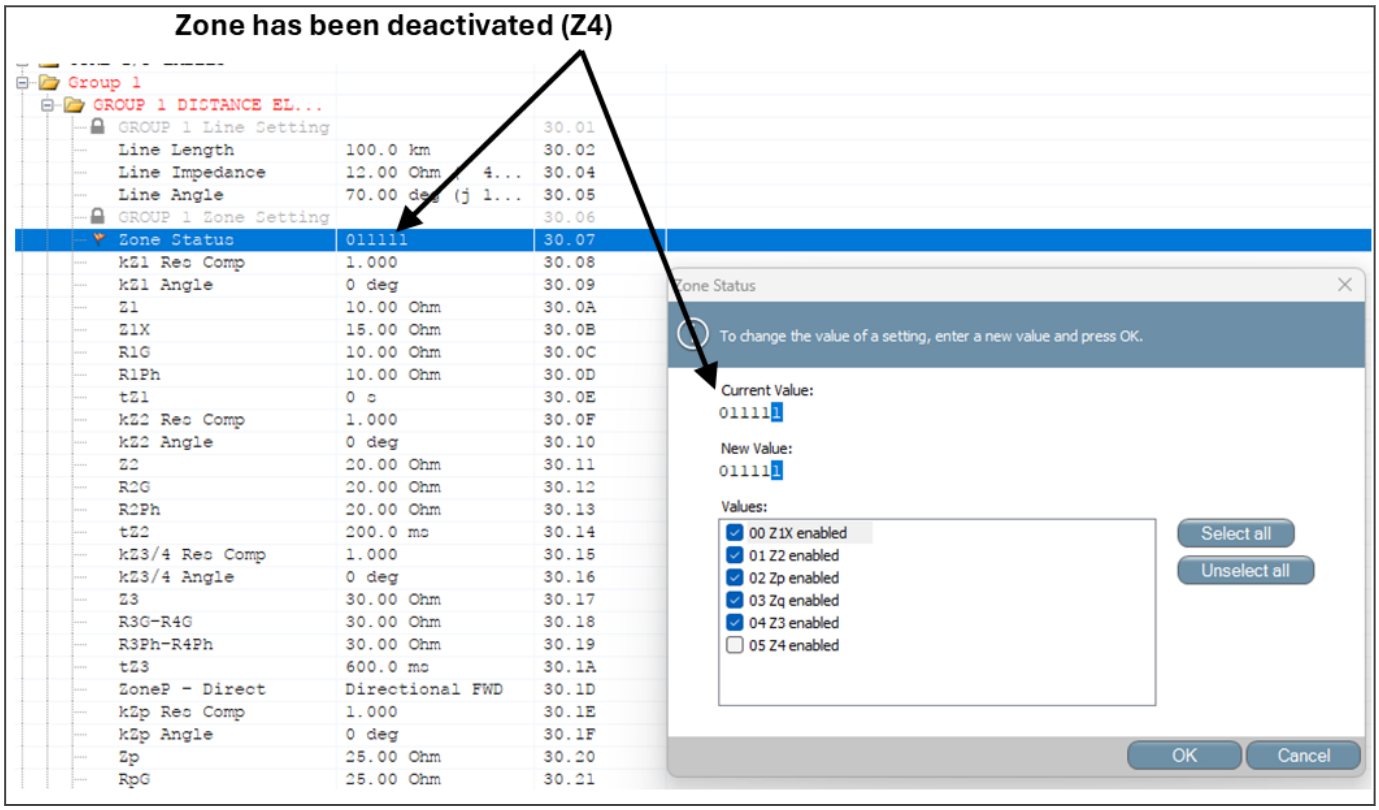
Figure 74: LCD menu for a control of an input/output/monitor bits check

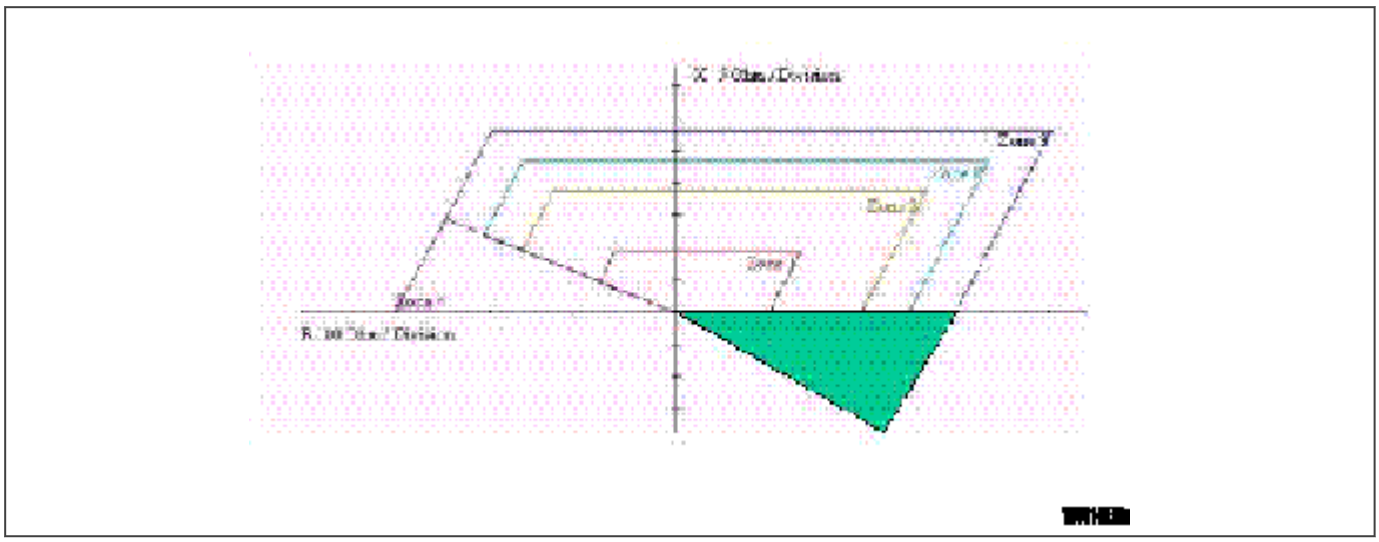
Table 12 - Parameters of zone to test (Zp can be reverse or forward/each zone is enabled or disabled - Z is always enabled)

Test Point B:Bi M:mono	I, V Phase Shift (I is behind V)	Tripping Time
R1 B	0°	T1
R1 M	0°	T1
R2 B	0°	T2
R2 M	0°	T2
Rp B	0°	Tp
Rp M	0°	Tp
R3 B	0°	T3
R3 M	0°	T3
- R Li = -R3	0°	T4
Z1 B	Arg Zd	T1
Z1 M	Arg (2Zd+Z0)	T1

Test Point B:Bi M:mono	I, V Phase Shift (I is behind V)	Tripping Time
Z2 B	Arg Zd	T2
Z2 M	Arg (2Zd+Z0)	T2
Zp B	Arg Zd	Tp
Zp M	Arg (2Zd+Z0)	Tp
Z3 B	Arg Zd	T3
Z3 M	Arg (2Zd+Z0)	T3
Z4 B	Arg Zd	T4

R3 represents the starting limit on the R axis (detection sensitivity of resistive defaults - the starting element for phase/earth can be superior to the phase/phase). If the reverse zone has been disabled (Z4), there is still a no-trip zone (up to version A3.2 & 2.10) in the 4th quadrant below the R axis.





If Z3 is disabled, the resistance limits R3-R4 are no longer visible in MiCOM S1 Agile.

Note:
All other characteristic points can be tested after calculating the impedance and the phase shift between U and I.
All these examples use the default settings.

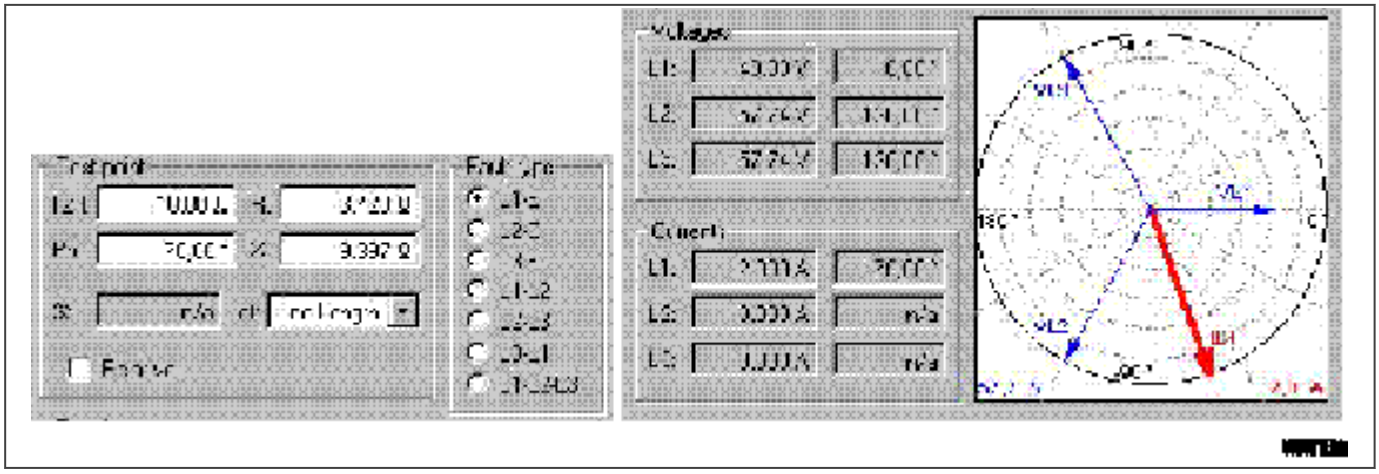


Figure 75: Example: AN - lim Z1

VAN/IA = Zf =Z1(1+K01) 40V/2A (phase shift of -70°) =20 W = Z1(1+1)

Lim Z1=10 W (if KO1=1)

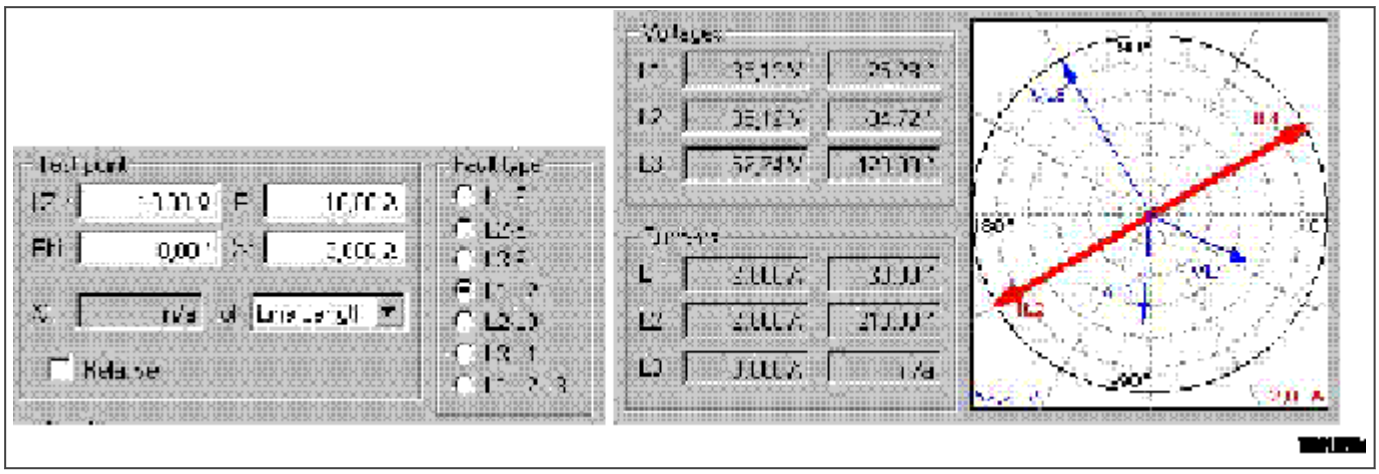


Figure 76: Example: AB - limR2

*VAB = 2 sin 34,72° * 35,12=40 V/IAB=2A*

Uαβ/IA (in phase) =Rf=20 W=LimR2
LimR2 (R2 value in MiCOM S1 Agile in ohms loop).

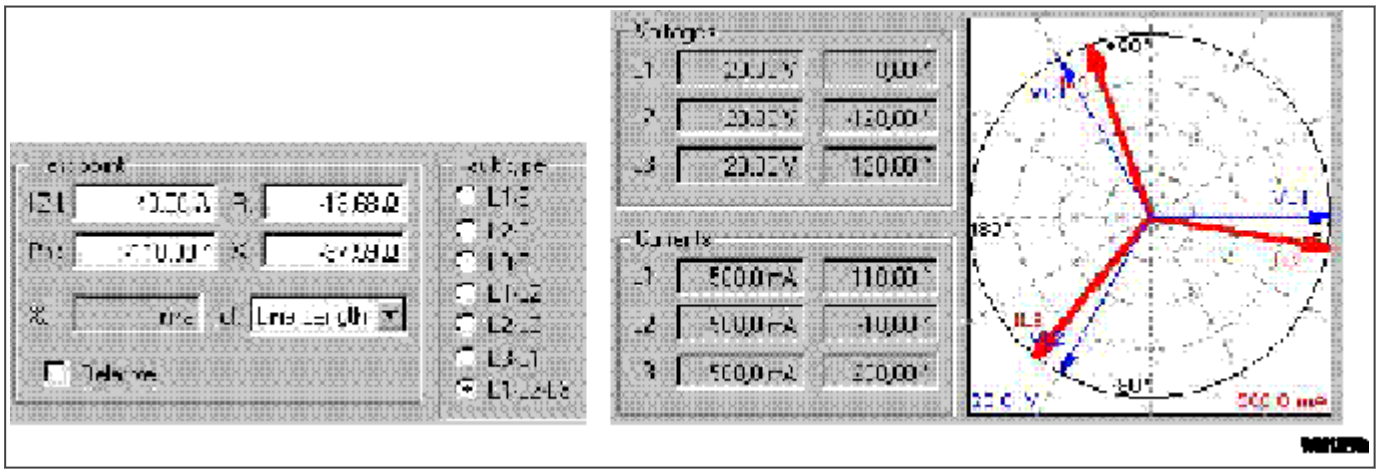


Figure 77: Example: ABC-limZ4 (Reverse)

VAN/IAN = Zf=Rf=20 V/0,500 mA=40 W=Lim Z4 with angle (VAN/IAN)=70°-180°=-110°

Simulator use can generate transients greater than 0.2 In on currents where the generation of a fault condition can induce errors about the directional calculation with "Delta" algorithms. This error is due to the simulator boxes which do not always reflect the real conditions of fault occurrence during the transient condition. To avoid this problem during the starting zones check, we recommend inhibiting the "Delta" algorithms in the characteristics path by setting T1 to 50 ms (beyond 40 ms, algorithms "Delta" are no longer valid). It is the case for numerical injection boxes.

Check in the injection device, whether any possibility of DC component could be chosen to force the start of the faulty current at 0, if not, the model network could be unrealistic.

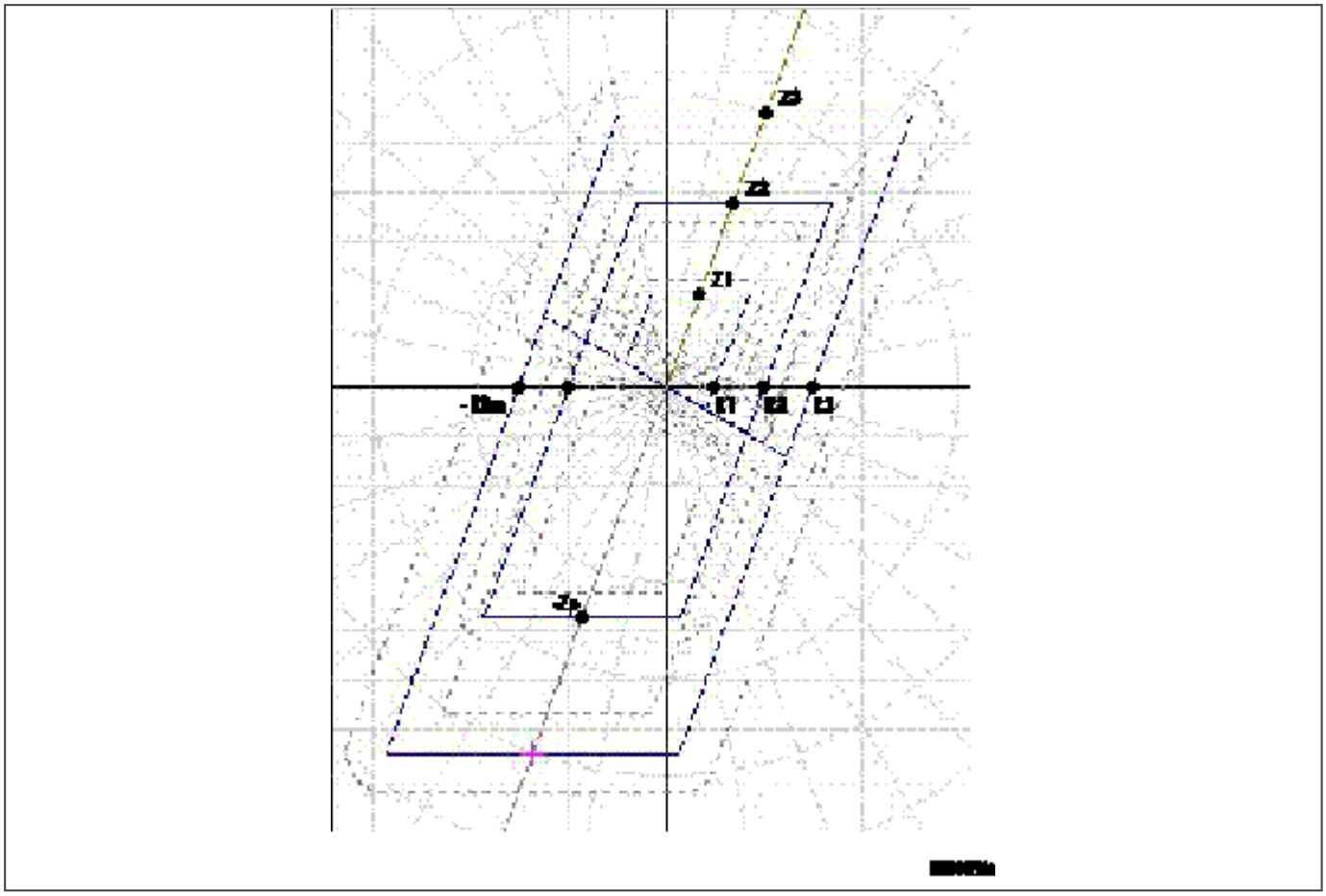


Figure 78: Points limit of the characteristic to be tested (with Zp selected as a reverse zone)

9.9 DISTANCE SCHEME TEST (IF ACTIVATED IN MICOM S1 AGILE)

9.9.1 CONTROL

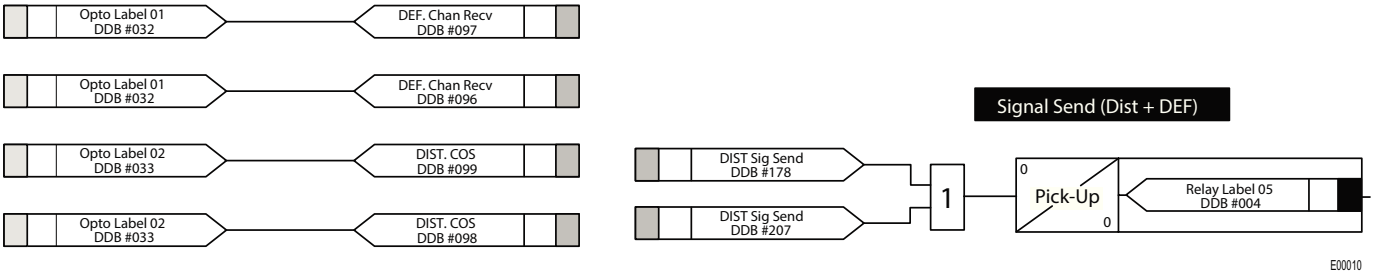
- The type of distance scheme enabled in MiCOM S1 Agile
- The DDB cells assigned for the distance scheme
- Refer to the description feature in the Application Notes chapter "Distance protection schemes":
  - Settings in S1
  - DDB cells
  - Internal logic in A2.10 & A3.2

REMINDER: General equation to the tripping in distance protection since A2.9/A3.1 - from A2.10/A3.2 it can be found in the Application Notes chapter.

Note:
Before testing, check the input presence/output in PSL linked to the selected channel-aided scheme (DDB: DistCR/Dist CS). Also check the I/O condition change on LCD in FAV in "system".

Input: (PSL by default "P&C ") Output: (PSL by default "P&C ")

Caution:
When switching groups via the opto couplers: Optos 1 and 2 must not be assigned in the PSL.



Select a mode.

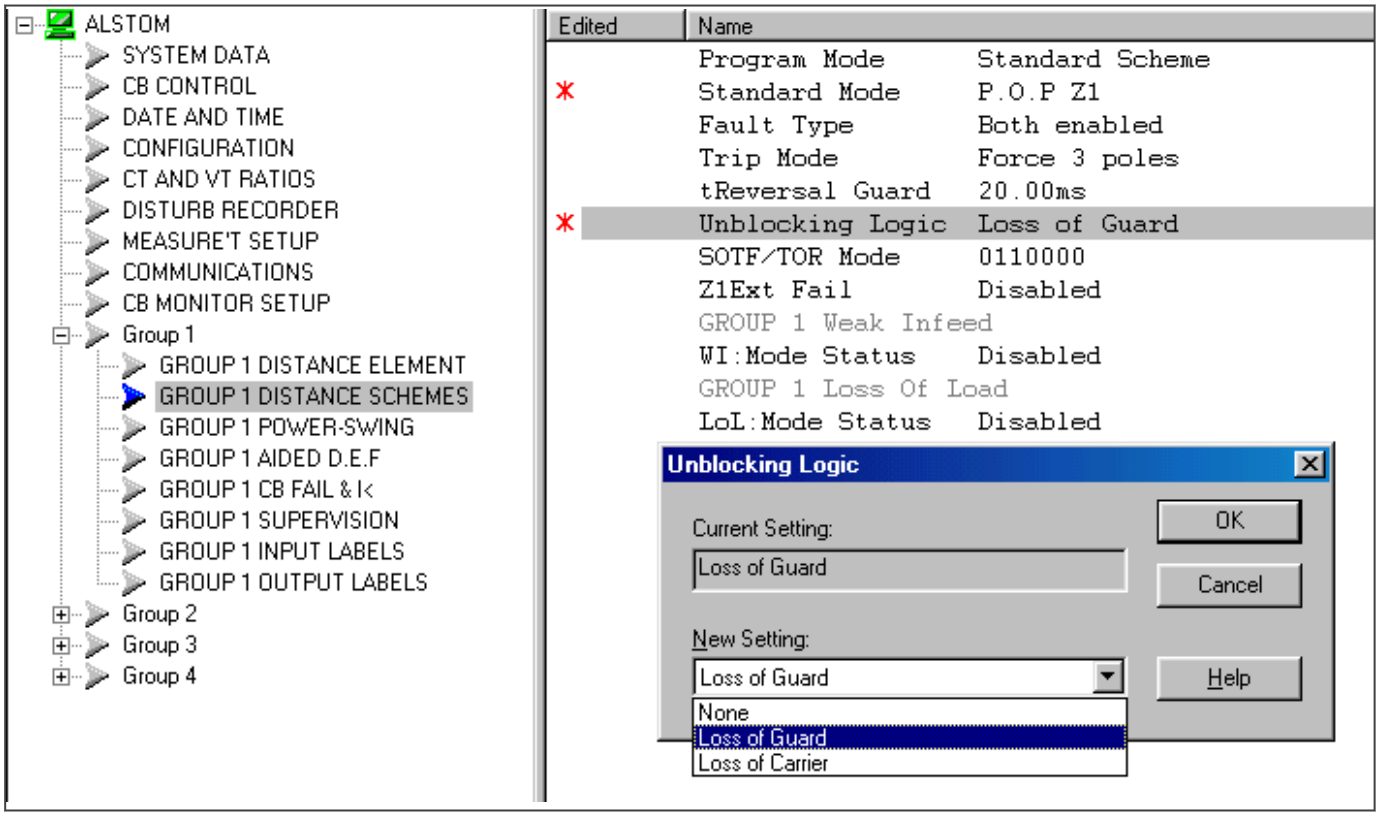
1. Implement the fault indicated in the panel first column, the carrier signal input is enabled, with carrier receive.
2. Check that the trip contact has been energised at the end of the time-delay indicated in the same column, with carrier receive.
3. Repeat step 2 and 3 but without the carrier receive input and checking the indicated time-delay in the panel's 2nd column, without carrier receive.

Repeat step 2 and 4 for the other faulted zones by checking that whatever the carrier receive input state, the time-delays associated with every zone are not modified (according to the 4th column equations).

Note:
Channel-aided schemes can be simulated by inverting the optos.
Channel-aided schemes transmissions can also be checked by generating defaults according to the 3rd column.
To simplify the relay I/O control condition, the assignments of LEDs in the PSL can be modified. It is also possible in MiCOM S1 Agile.

9.10 LOSS OF GUARD/LOSS OF CARRIER TEST

Setting

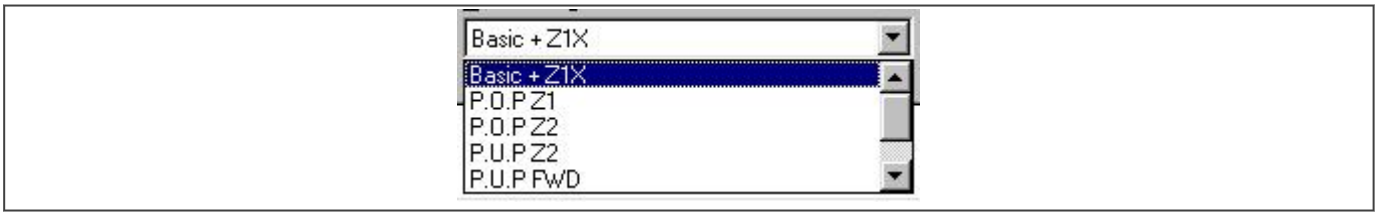


TEST: Follow the truth table in the Application Notes chapter.

Note:
In case of channel-aided loss, the scheme Z1X (out fail) will be applied if selected in MiCOM S1 Agile.

9.11 WEAK INFEED MODE TEST

From MiCOM S1 Agile
(If Permissive schemes are enabled in MiCOM S1 Agile: 4 possible choices): fig winf1



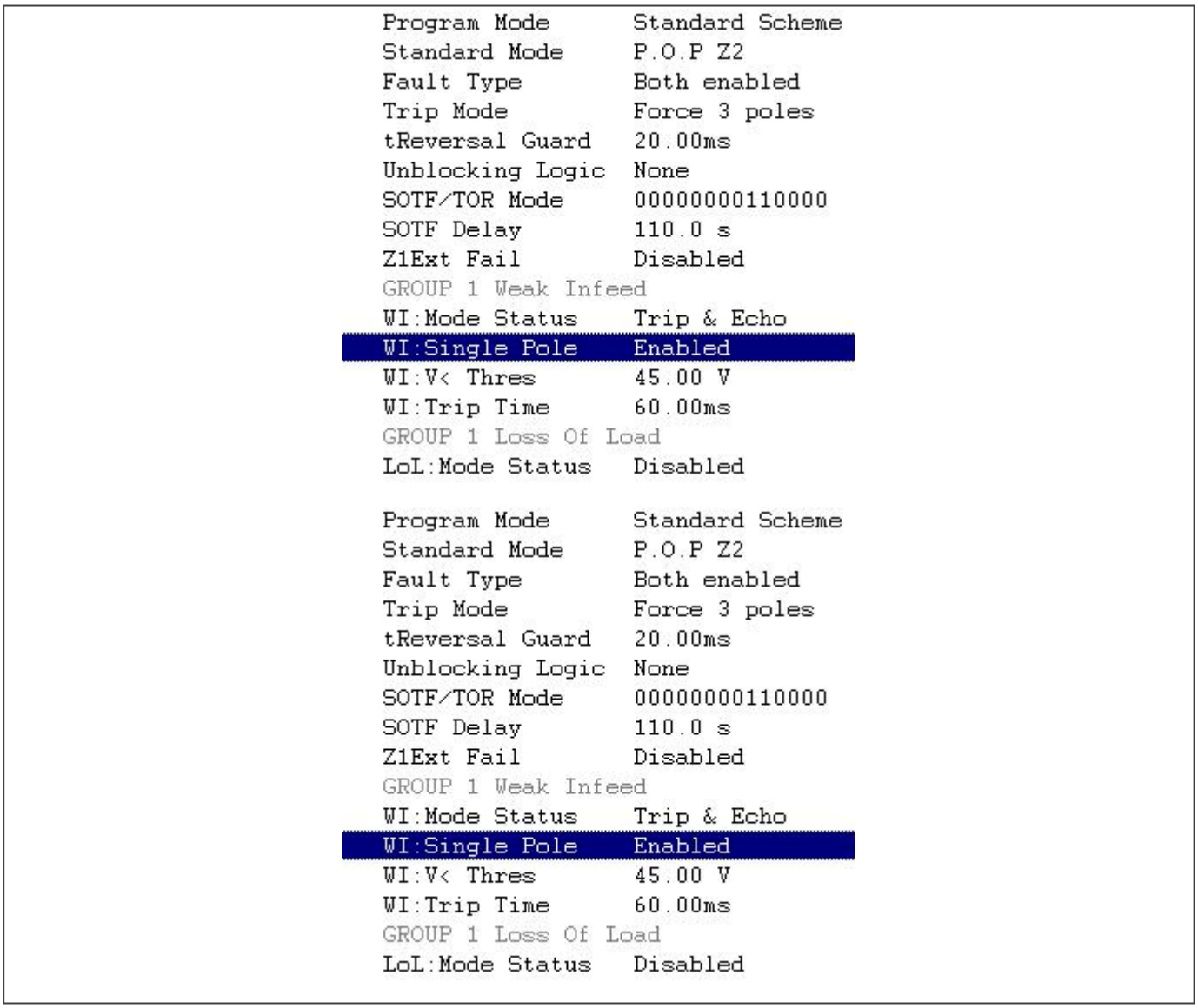


Figure 79: Winf2

Put into service the weak infeed mode (single-pole possible):

- Inhibit tripping authorisation and phase selection
- Enable the carrier receive input
- Check that:
  - The channel-aided scheme transmission signal is enabled
  - The trip contact is not enabled
  - From MiCOM S1 Agile enable the three-phase authorisation.

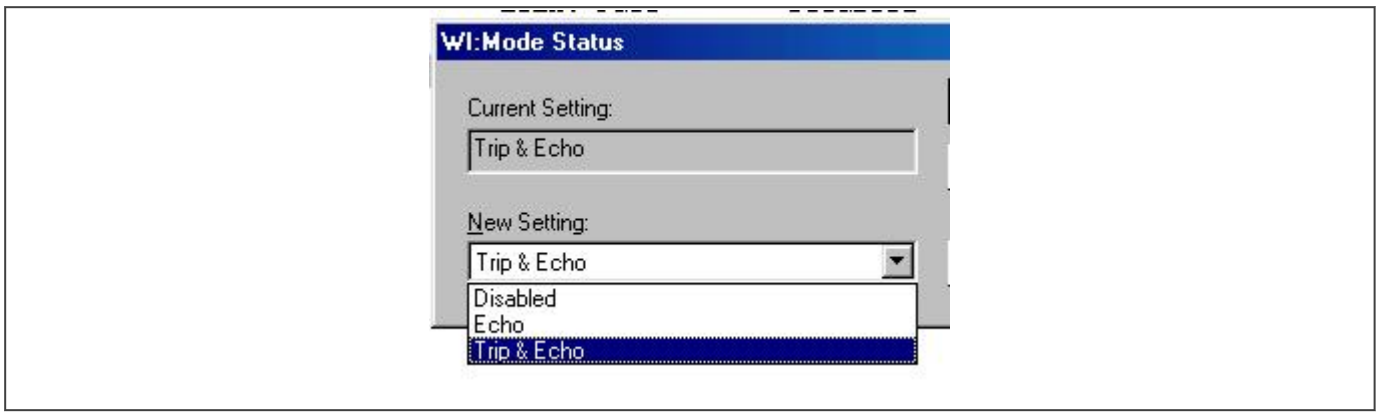


Figure 80:

- Enable the carrier receive input
- Check that:
  - The channel-aided scheme signal is enabled
  - The trip contacts closing

From MiCOM S1 Agile, enable the minimum voltage phase selection, set the undervoltage threshold to 0.4 Vn, make VB = –VC = Vn, enable the single-phase tripping authorisation.

- Enable the carrier receive input
- Check that:
  - The channel-aided scheme transmission signal is enabled
  - The protection trips phase A.

9.12 PROTECTION OPERATION DURING FUSE FAILURE

See the internal logic description in the Application Notes chapter - "Voltage Transformer Supervision" section.

Relay blocking (loss of 1 or 2 phases)

- Supply MiCOM P44x with a "healthy" system with load
- Remove the phase A supply ((V0) & (/I0) creation)
- Check that:
  - The fuse failure signal is activated at the end of the signal time-delay sign
  - The protection start and trip signal are not activated

Relay unblocking

- Keep the phase A supply cut-off and generate a fault (1- or 3-phase) which fault current (IR>3I0) is higher than the set threshold (I2 or I0)
- Check that the trip contact is activated

Relay locking (3 phases loss)

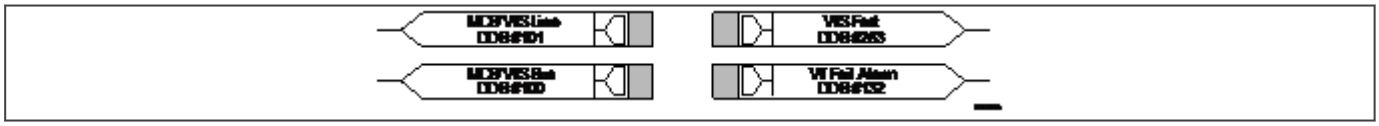
- Repeat step 1 and then open the 3 voltage channels without creating a delta I. Check as in step 3.

Outside sign

Polarise the input and check that the outputs change state.

Signal repercussions

The signal (VT fail alarm) drops off if:



Fuse_Failure = 0

and

INP_FFUS_Line = 0

and

(All Poles Dead Or healthy system)

All poles dead

No current AND no voltage on the line or open circuit-breaker.

Healthy system

Rated voltage on the line AND

- No zero sequence voltage and current AND
- No starting AND
- No power swing

9.13 DEMONSTRATE CORRECT OVERCURRENT FUNCTION OPERATION

This test, performed in stage 1 of the overcurrent protection function in setting group 1, demonstrates that the relay is operating correctly at the application-specific settings.

It is not considered necessary to check the boundaries of operation where cell ***[3502: GROUP 1 OVERCURRENT, I>1 Direction]*** is set to '`Directional Fwd`' or '`Directional Rev`' as the test detailed test already confirms the correct functionality between current and voltage inputs, processor and outputs and earlier checks confirmed that the measurement accuracy lies within the stated tolerance.

9.13.1 CONNECT THE TEST CIRCUIT

Determine which output relay has been selected to operate when an I>1 trip occurs by viewing the relay's programmable scheme logic.

The programmable scheme logic can only be changed using the appropriate software. If the software is unavailable the default output relay allocations will still be applicable.

If the trip outputs are phase-segregated, i.e. a different output relay allocated for each phase, the relay assigned for tripping on 'A' phase faults should be used.

If stage 1 is not mapped directly to an output relay in the programmable scheme logic, output relay 3 should be used for the test as it operates for any trip condition.

The associated terminal numbers can be found either in the external connection diagram in the Installation chapter or in Table 5.

Connect the output relay so that its operation will trip the test set and stop the timer.



Caution:
Connect the current output of the test set to the 'A' phase current transformer input of the relay, terminals C3 and C2 where 1A current transformers are being used, and terminals C1 and C2 for 5A current transformers.

If ***[3502: GROUP 1 OVERCURRENT, I>1 Direction]*** is set to '`Directional Fwd`', the current should flow out of terminal C2 but into C2 if set to '`Directional Rev`'.

If cell ***[351D: GROUP 1 OVERCURRENT, VCO Status]*** is set to '`Enabled`', overcurrent function configured for voltage controlled overcurrent operation or ***[3502: GROUP 1 OVERCURRENT, I>1 Direction]*** has been set to '`Directional Fwd`' or '`Directional Rev`' then rated voltage should be applied to terminals C19 and C22.

Ensure that the timer will start when the current is applied to the relay.

Note:
If the timer does not start when the current is applied and stage 1 has been set for directional operation, the connections may be incorrect for the set direction of operation set. Try again with the current connections reversed.

9.13.2 PERFORM THE TEST

Ensure that the timer is reset.

Apply a current of twice the setting in cell ***[3504: GROUP 1 OVERCURRENT, I>1 Current Set]*** to the relay and note the time displayed when the timer stops.

9.13.3 CHECK THE OPERATING TIME

Check that the operating time recorded by the timer is within the range shown in Table 13.

Note:
Except for the definite time characteristic, the operating times given in Table 13 are for a time multiplier or time dial setting of 1. Therefore, to obtain the operating time at other time multiplier or time dial settings, the time given in Table 13 must be multiplied by the setting of cell ***[3507: GROUP 1 OVERCURRENT, I>1 TMS]*** *for IEC and UK characteristics or cell* ***[3508: GROUP 1 OVERCURRENT, Time Dial]*** *for IEEE and US characteristics.*
In addition, for definite time and inverse characteristics there is an additional delay of up to 0.02 seconds and 0.08 seconds respectively that may need to be added to the relay's acceptable range of operating times.
For all characteristics, allowance must be made for the accuracy of the test equipment being used.

Table 13 - Characteristic operating times for I>1

Characteristic	Operating Time at Twice Current Setting and Time Multiplier/ Time Dial Setting of 1.0	
	Nominal (Seconds)	Range (Seconds)
DT	***[3505: 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	0.64	0.61 - 0.67
IEEE V Inverse	1.42	1.35 - 1.50
IEEE E Inverse	1.46	1.39 - 1.54
US Inverse	0.46	0.44 - 0.49

9.14 CHECK TRIP AND AUTO-RECLOSE CYCLE

If the autoreclose function is being used, the circuit breaker trip and autoreclose cycle can be tested automatically at the application-specific settings.

To test the first autoreclose cycle, set cell ***[0F13: COMMISSIONING TESTS, Autoreclose Test]*** to "*3 Pole Test*". The relay will perform a trip/reclose cycle. Repeat this operation to test the subsequent autoreclose cycles.

Check that all output relays used for circuit breaker tripping and closing, blocking other devices, etc. operate at the correct times during the trip/close cycle.

9.15 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.

9.15.1 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.

9.15.2 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.*

9.15.3 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.

9.15.4 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.

9.16 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.

9.16.1 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.

9.16.2 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.

9.16.3 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.

9.17 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 10

MAINTENANCE AND TROUBLESHOOTING

10.1 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 Authorization (RMA) form.

This chapter contains the following sections:

Chapter Overview 248
Maintenance 249
Troubleshooting 257

10.2 MAINTENANCE

10.2.1 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.

10.2.1.1 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.

10.2.1.2 OPTO-ISOLATORS

Check the opto-inputs by repeating the commissioning test detailed in the Commissioning chapter.

10.2.1.3 OUTPUT RELAYS

Check the output relays by repeating the commissioning test detailed in the Commissioning chapter.

10.2.1.4 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.

10.2.2 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.

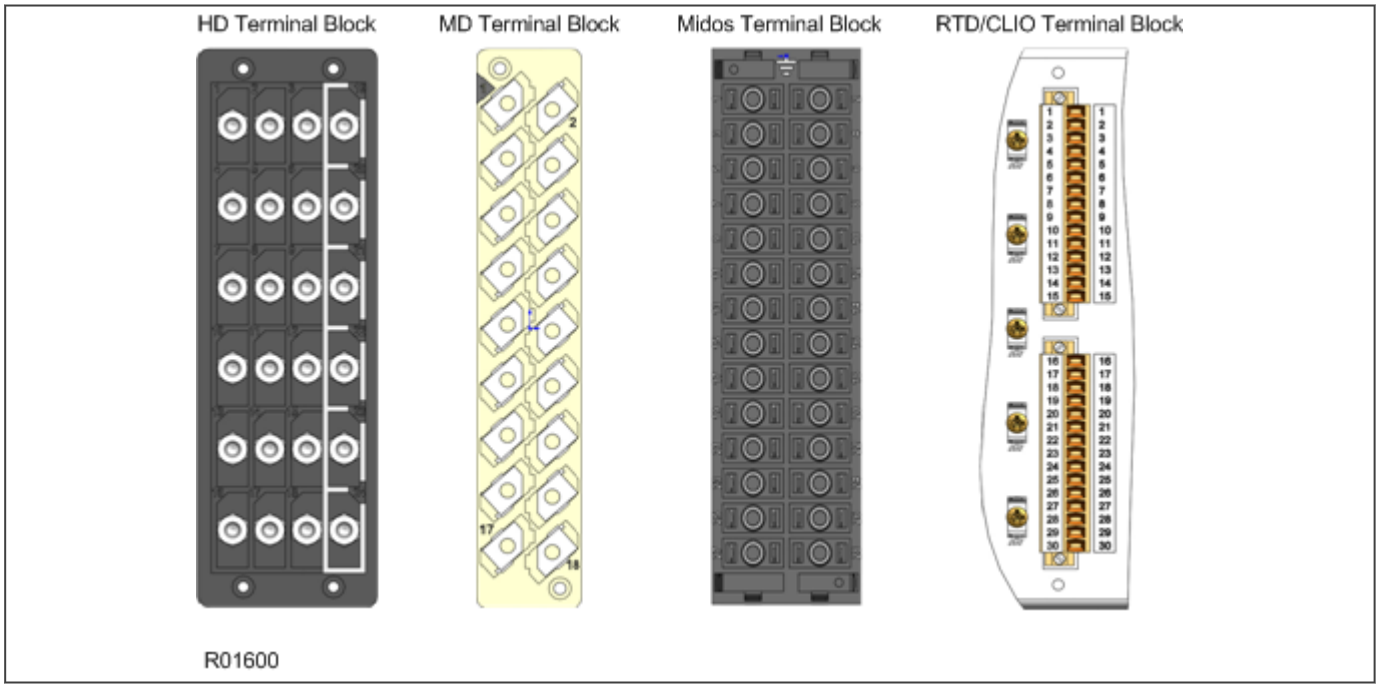


Figure 81: Possible terminal block types

10.2.3 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 authorization 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.

10.2.4 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 relay 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.

10.2.5 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.

10.2.5.1 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.

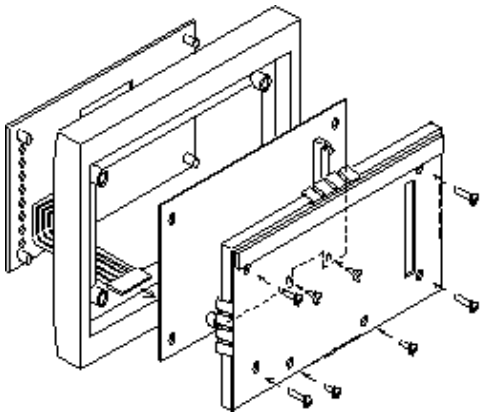


Figure 82: Front panel assembly

10.2.5.2 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 relay 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.

10.2.5.3 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.

10.2.5.4 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.

10.2.5.5 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.

10.2.6 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.

10.2.7 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.

10.2.8 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.

10.3 TROUBLESHOOTING

10.3.1 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.

10.3.2 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.

10.3.3 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.

10.3.4 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

Test	Check	Action	
		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)

10.3.5 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.

10.3.6 MAL-OPERATION DURING TESTING

10.3.6.1 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 energized. 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 relay 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 relay to check the relay output contacts operate.	If the output relay operates, the problem must be in the external wiring to the relay. If the output relay does not operate the output relay contacts may have failed (the self-tests verify that the relay coil is being energized). Ensure the closed resistance is not too high for the continuity tester to detect.

10.3.6.2 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.

10.3.6.3 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.

10.3.7 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

10.3.7.1 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

10.3.7.2 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.

10.3.8 REPAIR AND MODIFICATION PROCEDURE

Please follow these steps to return an Automation product to us:

1. Get the Repair and Modification Return Authorization (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 11

TECHNICAL SPECIFICATIONS

11.1 CHAPTER OVERVIEW

This chapter describes the technical specifications of the product.

This chapter contains the following sections:

Chapter Overview 263
Technical Data 264
Interfaces 265
Measurements and Recording 269
Ratings 270
Mechanical Specifications 272
Type Tests 273
Environmental Conditions 274
Electromagnetic Compatibility 275
Regulatory Compliance 278

11.2 TECHNICAL DATA

11.2.1 INPUT/OUTPUT (I/O)

Input/Output (I/O)	
P442 (with or without Check Synchronism):	16I/21O
	18I/18O (4 high break)
	16I/21O (3 or 6 Fast Trip)
P444 (with or without Check Synchronism):	24I/32O
	24I/46O
	24I/34O (12 high break)

Note:
If the number of output contacts energised at one time is greater than 32, there may be delayed operation for some of the contacts.

11.3 INTERFACES

11.3.1 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

11.3.2 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

11.3.3 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

11.3.4 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

11.3.5 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

11.3.6 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

11.3.7 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

11.3.8 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

11.3.9 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

11.3.9.1 100 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 Center	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

11.3.9.2 100 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

11.3.10 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

11.3.10.1 100 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 Center	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

11.3.10.2 100 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.

Conditions: TA = 0°C to 70°C

11.4 MEASUREMENTS AND RECORDING

11.4.1 GENERAL

General Measurement Accuracy	
General measurement accuracy	Typically +/- 1%, but +/- 0.5% between 0.2 - 2 In/Vn
Phase	0° to 360° +/- 0.5%
Current (0.05 to 3 In)	+/- 1.0% of reading, or 4mA (1A input), or 20mA (5A input)
Voltage (0.1 to 2 Vn)	+/- 1.0% of reading
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)	+/- 5.0% 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

11.4.2 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)

11.4.3 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

11.4.4 FAULT LOCATOR

Accuracy	
Fault Location	+/- 5% of line length Reference conditions: solid fault applied on line

11.5 RATINGS

11.5.1 AC MEASURING INPUTS

AC Measuring Inputs	
Nominal frequency	50 Hz or 60 Hz (settable)
Operating range	45 to 65 Hz

11.5.2 CURRENT TRANSFORMER INPUTS

AC Current Inputs	
Nominal current (In)	1A and 5A dual rated (separate terminals are provided for the 1A and 5A windings, with the neutral input of each winding sharing one terminal)
Nominal burden per phase 1A	<0.04 VA at rated current
Impedance per phase 1A	<40 mΩ over 0 - 30 In
Nominal burden per phase 5A	<0.15 VA at rated current
Impedance per phase 5A	<8 mΩ over 0 - 30 In
AC current thermal withstand	4 In (continuous operation) 30 In (for 10 s) 100 In (for 1 s)
Linearity	Standard: Linear up to 64 × In (non-offset AC current)

11.5.3 VOLTAGE TRANSFORMER INPUTS

AC Voltage Inputs	
Version	100 V to 120 V (ph-ph)
Nominal burden per VT input *1	< 0.02 VA @ Vn
Linearity for each VT input	Linear up to 200 Vac rms
Continuous rating for each VT input	2 Vn
10 seconds rating for each VT input	2.6 Vn

Note:
*Reference Conditions: *1 = Overfrequency operating range 50/60 Hz and over temperature range 20° +/- 5° C.*

11.5.4 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

11.5.5 SUPERCAPACITOR

Discharge time	>14 days

11.6 MECHANICAL SPECIFICATIONS

11.6.1 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.*

11.6.2 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

11.6.3 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

11.6.4 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

11.7 TYPE TESTS

11.7.1 INSULATION

Compliance	IEC 60255-27: 2013
Insulation resistance	> 100 M ohm at 500 V DC (Using only electronic/brushless insulation tester)

11.7.2 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

11.7.3 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

11.7.4 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.

11.8 ENVIRONMENTAL CONDITIONS

11.8.1 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)

11.8.2 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)

11.8.3 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

11.8.4 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

11.9 ELECTROMAGNETIC COMPATIBILITY

11.9.1 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

11.9.2 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

11.9.3 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

11.9.4 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)

11.9.5 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

11.9.6 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

11.9.7 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

11.9.8 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%

11.9.9 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

11.9.10 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

11.9.11 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

11.9.12 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)

11.9.13 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

11.9.14 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.

11.10 REGULATORY COMPLIANCE

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

CE

11.10.1 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.

11.10.2 LVD COMPLIANCE: 2014/35/EU

The product specific Declaration of Conformity (DoC) lists the relevant harmonized 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.

11.10.3 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

	Variants Order No.									
Distance Protection **P442**	P442							**		
Nominal Auxiliary Voltage										
24-54 Vdc	7									
48-125 Vdc (40-100 Vac)	8									
110-250 Vdc (100-240 Vac)	9									
In/Vn Rating										
Dual rated CT (1 & 5A : 100 - 120V)		1								
Module Sum (∑1A/PXDB)		5								
Redundant Ethernet PRP/Failover, 2 multi-mode fibre ports, IEC 61850-9-2 LE Sampled Analogue Values - Process Bus Model		C								
Hardware Options										
Standard version			1							
IRIG-B Only (Modulated)			2							
IRIG-B input and Fibre optic converter (Courier, Modbus, IEC 60870-5-103 or DNP3) (Note: converts RS485 port to fibre optic; NOT extra port)			4							
Ethernet 10Mbit/s			5							
Single Ethernet 100Mbit/s			6							
Second Rear Comms + InterMiCOM			7							
IRIG-B (Modulated) + Second Rear Comms + InterMiCOM			8							
Single Ethernet (100Mbit/s) plus IRIG-B (Modulated) Software version '31' and later (Suffix J)			A							
Single Ethernet (100Mbit/s) plus IRIG-B (Un-modulated) Software version '31' and later (Suffix J)			B							
InterMiCOM + Courier Rear Port + IRIG-B modulated *			F							
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Modulated IRIG-B			J							
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Un-modulated IRIG-B			K							
Redundant Ethernet PRP/HSR, 2 fibre ports + Modulated IRIG-B			N							
Redundant Ethernet PRP/HSR, 2 fibre ports + Unmodulated IRIG-B			P							
Single Ethernet 1 LC Duplex port + Universal IRIG-B + 1588			U							
Redundant Ethernet PRP/HSR/RSTP/Failover 2 RJ45 + Universal IRIG-B + 1588			W							
Redundant Ethernet PRP/HSR/RSTP/Failover 2 LC Duplex ports + Universal IRIG-B + 1588			Y							
Software Options										
16 Logic Inputs & 21 Relay Outputs				B						
16 Logic Inputs & 21 Relay Outputs (3 Fast trip)				D						
16 Logic Inputs & 21 Relay Outputs (6 Fast trip)				E						
16 Logic Inputs & 18 Relay Outputs (4 High Break) *				C						
* NB: Option C is only available with Design Suffix K & Software version 40 or later										
Protocol Options										
K-Bus					1					
Modbus					2					
VDEW (IEC 60870-5-103)					3					
DNP3.0					4					
UCA2 + Courier via rear RS485 port (Ethernet hardware options [i.e. 6] only)					5					
IEC 61850 + Courier via rear RS485 port *					6					
IEC 61850 + IEC 60870-5-103 via rear RS485 port *					7					
DNP3 over Ethernet with Courier rear port K-Bus/RS485 protocol					8					
* NB: IEC 61850 Edition 2 available with '82' Software										
Mounting										
Flush/Panel Mounting with Harsh Env. Coating, with USB Port, Black and Silver Front Panel						S				
Language										
English, French, German, Spanish							0			
English, French, German, Italian							4			
Software Version										
Date and application dependant								**		
Customer Specific Options										
Standard version									0	
Customer engineered version: ENEL									1	
Customer engineered version: TERNA									2	
Customer engineered version: RTE									4	
Customer engineered version: general									A	
Hardware Version										
Model and hardware version dependant										*

	Variants Order No.									
Distance Protection **P444** P444							**			
Nominal Auxiliary Voltage										
24-54 Vdc	7									
48-125 Vdc (40-100 Vac)	8									
110-250 Vdc (100-240 Vac)	9									
In/Vn Rating										
Dual rated CT (1 & 5A : 100 - 120V)		1								
Module Sum (∑1A/PXDB)		5								
Redundant Ethernet PRP/Failover, 2 multi-mode fibre ports, IEC 61850-9-2 LE Sampled Analogue Values - Process Bus Model		C								
Hardware Options										
Standard version			1							
IRIG-B input			2							
IRIG-B input and Fibre optic converter (IEC 60870-5-103)			4							
Ethernet 10Mbits			5							
Single Ethernet 100Mbit/s			6							
Rear Comms + InterMiCOM			7							
Rear Comms + IRIB-B + InterMiCOM			8							
Single Ethernet (100Mbit/s) plus IRIG-B (Modulated) Software version '31' and later (Suffix J)			A							
Single Ethernet (100Mbit/s) plus IRIG-B (Un-modulated) Software version '31' and later (Suffix J)			B							
InterMiCOM + Courier Rear Port + IRIG-B modulated *			F							
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Modulated IRIG-B			J							
Redundant Ethernet RSTP, 2 multi-mode fibre ports + Un-modulated IRIG-B			K							
Redundant Ethernet PRP/HSR, 2 fibre ports + Modulated IRIG-B			N							
Redundant Ethernet PRP/HSR, 2 fibre ports + Unmodulated IRIG-B			P							
Single Ethernet 1 LC Duplex port + Universal IRIG-B + 1588			U							
Redundant Ethernet PRP/HSR/RSTP/Failover 2 RJ45 + Universal IRIG-B + 1588			W							
Redundant Ethernet PRP/HSR/RSTP/Failover 2 LC Duplex ports + Universal IRIG-B + 1588			Y							
** For HSR - contact GE Vernova for details										
Models										
1 & 3 Pole tripping/reclosing with 24 inputs & 32 outputs				B						
1 & 3 Pole tripping/reclosing with 24 inputs & 34 ouputs (12 high break)				C						
1 & 3 Pole tripping/reclosing with 24 inputs & 32 outputs (4 fast output contacts)				D						
1 & 3 Pole tripping/reclosing with 24 inputs & 32 outputs (8 fast output contacts)				E						
1 & 3 Pole tripping/reclosing with 24 inputs & 46 outputs				J						
1 & 3 Pole tripping/reclosing with 24 inputs & 46 outputs (4 fast output contacts)				K						
1 & 3 Pole tripping/reclosing with 24 inputs & 46 outputs (8 fast output contacts)				L						
1 & 3 Pole tripping/reclosing with 20 inputs & 50 outputs				M						
1 & 3 Pole tripping/reclosing with 20 inputs & 50 outputs (4 fast output contacts)				N						
1 & 3 Pole tripping/reclosing with 20 inputs & 50 outputs (8 fast output contacts)				P						
1 phase tripping and 1 phase auto reclose: 8 inputs and 8 outputs Mounting Option ‘R’				R						
Protocol Options										
K-Bus					1					
Modbus					2					
VDEW (IEC 60870-5-103) (RS485 or Fibre Optic)					3					
DNP3.0					4					
IEC 61850 + Courier via rear RS485 port *					6					
IEC 61850 + IEC 60870-5-103 via rear RS485 port *					7					
DNP3 over Ethernet with Courier rear port K-Bus/RS485 protocol					8					
* NB: IEC 61850 Edition 2 available with '82' Software										
Mounting										
19" Rack Mounting with Harsh Env. Coating, with USB Port, Black and Silver Front Panel						T				
40TE Case (9-2LE models only) Flush/Panel Mounting with Harsh Env. Coating, with USB Port, Black and Silver Front Panel						U				
Language										
English, French, German, Spanish							0			
English, French, German, Italian							4			
Software Version										
Date and application dependant										
Customer Specific Options										
Standard version								0		
Customer engineered version: ENEL								1		
Customer engineered version: TERNA								2		
Customer engineered version: RTE								4		
Customer engineered version: General								A		
Hardware Version										
Model and hardware version dependant									*	

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.

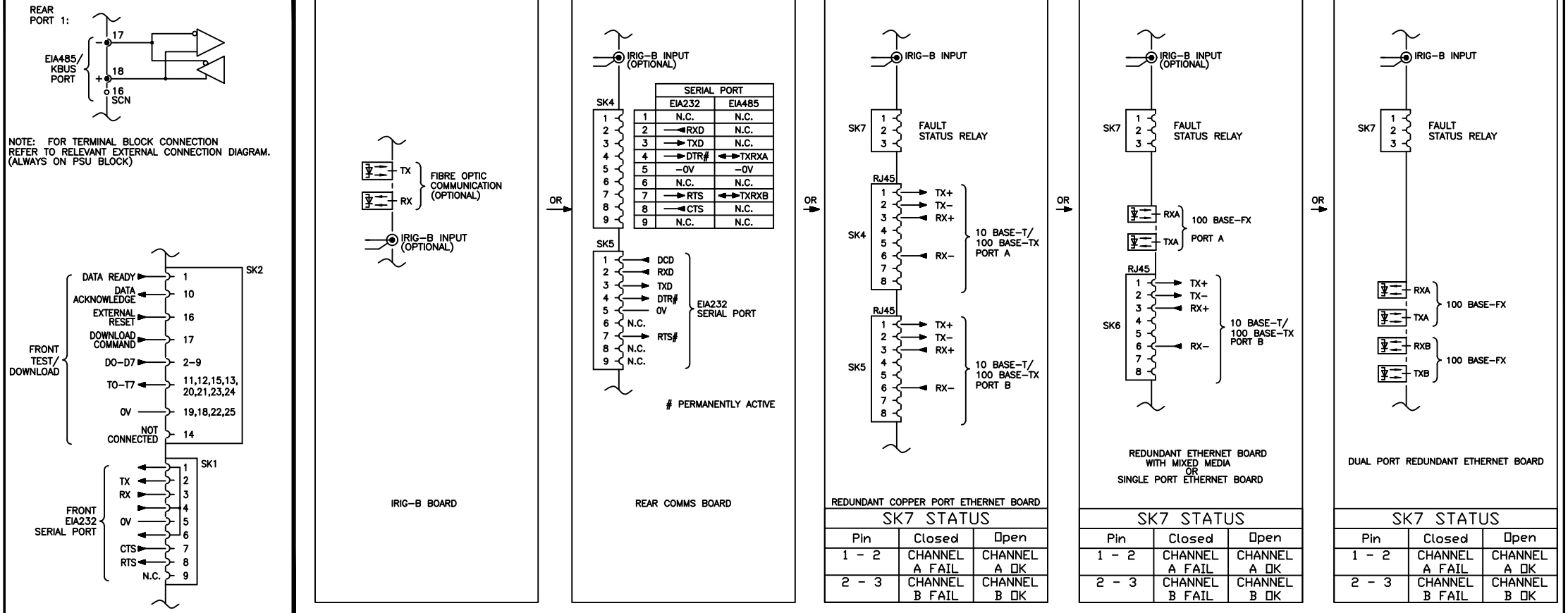
Settings and Signals

APPENDIX C

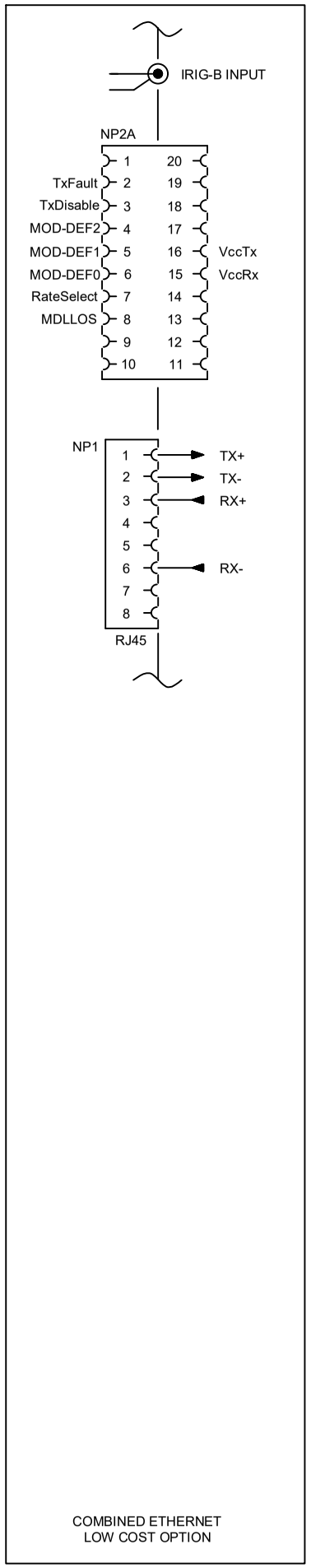
WIRING DIAGRAMS

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
P442	I/O Option D I/O Option E	16 Logic Inputs & 21 Relay Outputs (3 Fast Trip) (60TE) 16 Logic Inputs & 21 Relay Outputs (6 Fast trip) (60TE)	10P44201-1 10P44201-2	Q F
	I/O Option B	16 Logic Inputs & 21 Relay Outputs (60TE)	10P44202-1	F
	I/O Option C	16 Logic Inputs & 18 Relay Outputs (4 High Break) (60TE)	10P44203-1 10P44203-2	F E
	I/O Option E	Distance Protection with NCIT 16 Inputs, 21 Outputs (6 Optional Fast Trip) (60TE)	10P44204-1	E
	I/O Option C	Distance Protection with NCIT 16 Inputs, 14 Outputs & 4 High Break Relays (60TE)	10P44205-1	E
P444	I/O Option D	1 & 3 Pole Tripping/Reclosing with 24 Inputs, 32 Outputs (4 Fast Output Contacts) (80TE)	10P44401-1	H
	I/O Option E	1 & 3 Pole Tripping/Reclosing with 24 Inputs, 32 Outputs (8 Fast Output Contacts) (80TE)		
	I/O Option K	1 & 3 Pole Tripping/Reclosing with 24 Inputs, 46 Outputs (4 Fast Output Contacts) (80TE)		
	I/O Option L	1 & 3 Pole Tripping/Reclosing with 24 Inputs, 46 Outputs (8 Fast Output Contacts) (80TE)		
	I/O Option B I/O Option J	1 & 3 Pole Tripping/Reclosing with 24 Inputs, 32 Outputs (80TE) 1 & 3 Pole Tripping/Reclosing with 24 Inputs, 46 Outputs (80TE)	10P44402-1	F
	I/O Option C	1 & 3 Pole Tripping/Reclosing with 24 Inputs, 34 Outputs (12 High Break) (80TE)	10P44403-1 10P44403-2	F E
			10P44406-1	F
	I/O Option J	1 & 3 Pole Tripping/Reclosing with 24 Inputs, 46 Outputs (80TE)	10P44405-1	E
	I/O Option M	1 & 3 Pole Tripping/Reclosing with 20 Inputs, 50 Outputs (80TE)	10P44408-1	B
	I/O Option N	1 & 3 Pole Tripping/Reclosing with 20 Inputs, 50 Outputs (4 Fast Output Contacts) (80TE)		
	I/O Option P	1 & 3 Pole Tripping/Reclosing with 20 Inputs, 50 Outputs (8 Fast Output Contacts) (80TE)		

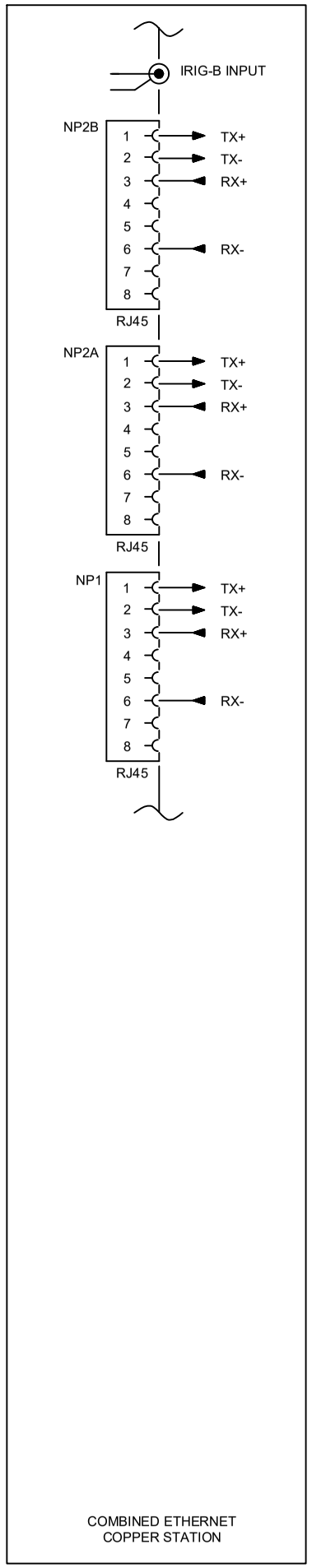
* When selecting the applicable wiring diagram(s), refer to the appropriate model CORTEC.



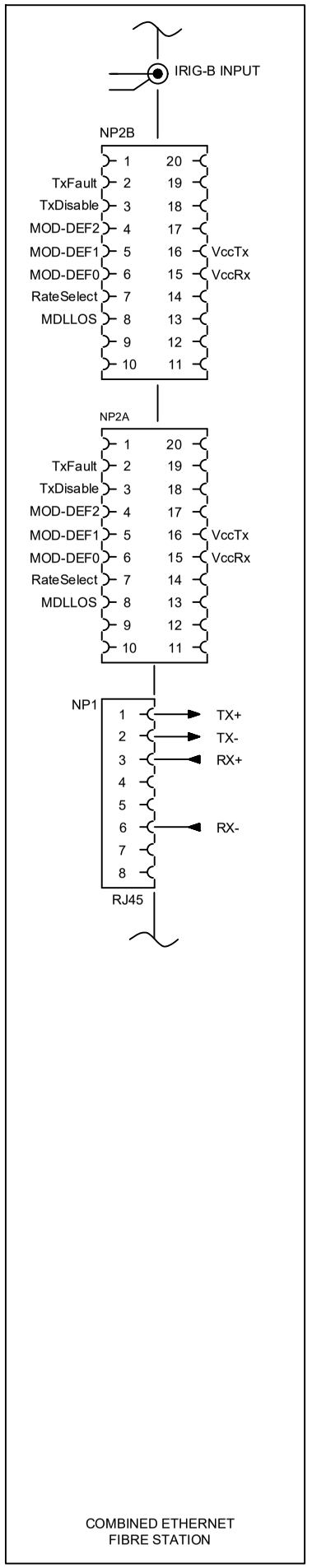
Issue: N	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM: COMMS OPTIONS MICOM Px40 PLATFORM		
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information 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 / Next Sht: 2
Date:	Chkd:				GE VERNOVA



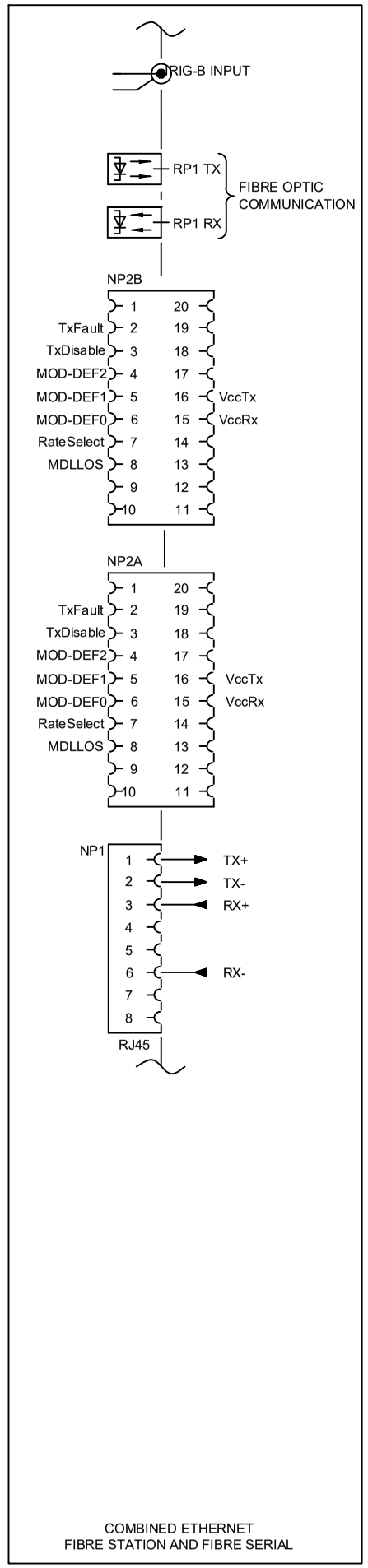
COMBINED ETHERNET
LOW COST OPTION



COMBINED ETHERNET
COPPER STATION

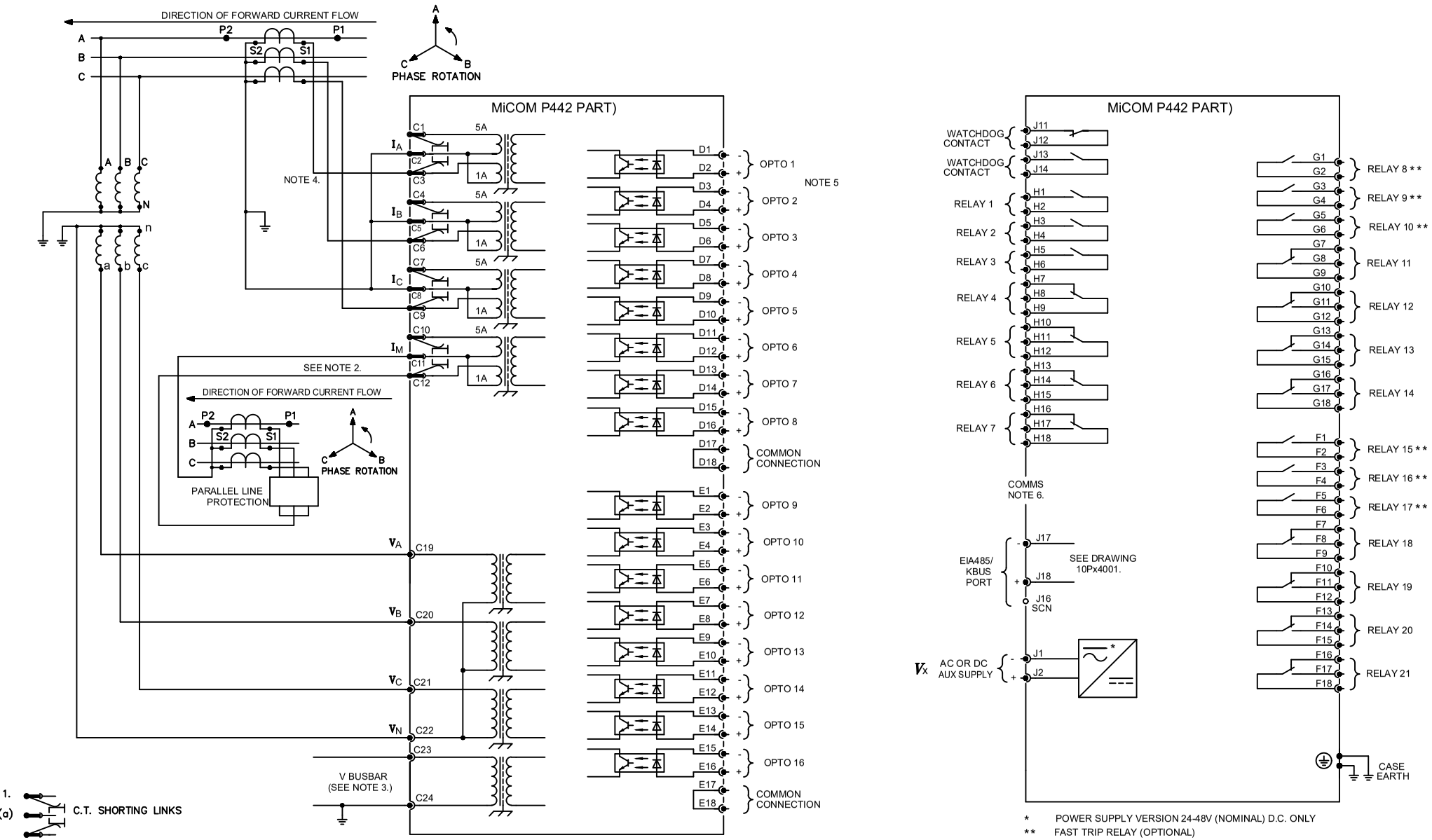


COMBINED ETHERNET
FIBRE STATION



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:					



NOTES 1.

(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

2. I_M INPUT IS FOR OPTIONAL MUTUAL COMPENSATION OF FAULT LOCATOR.

3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.

4. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.

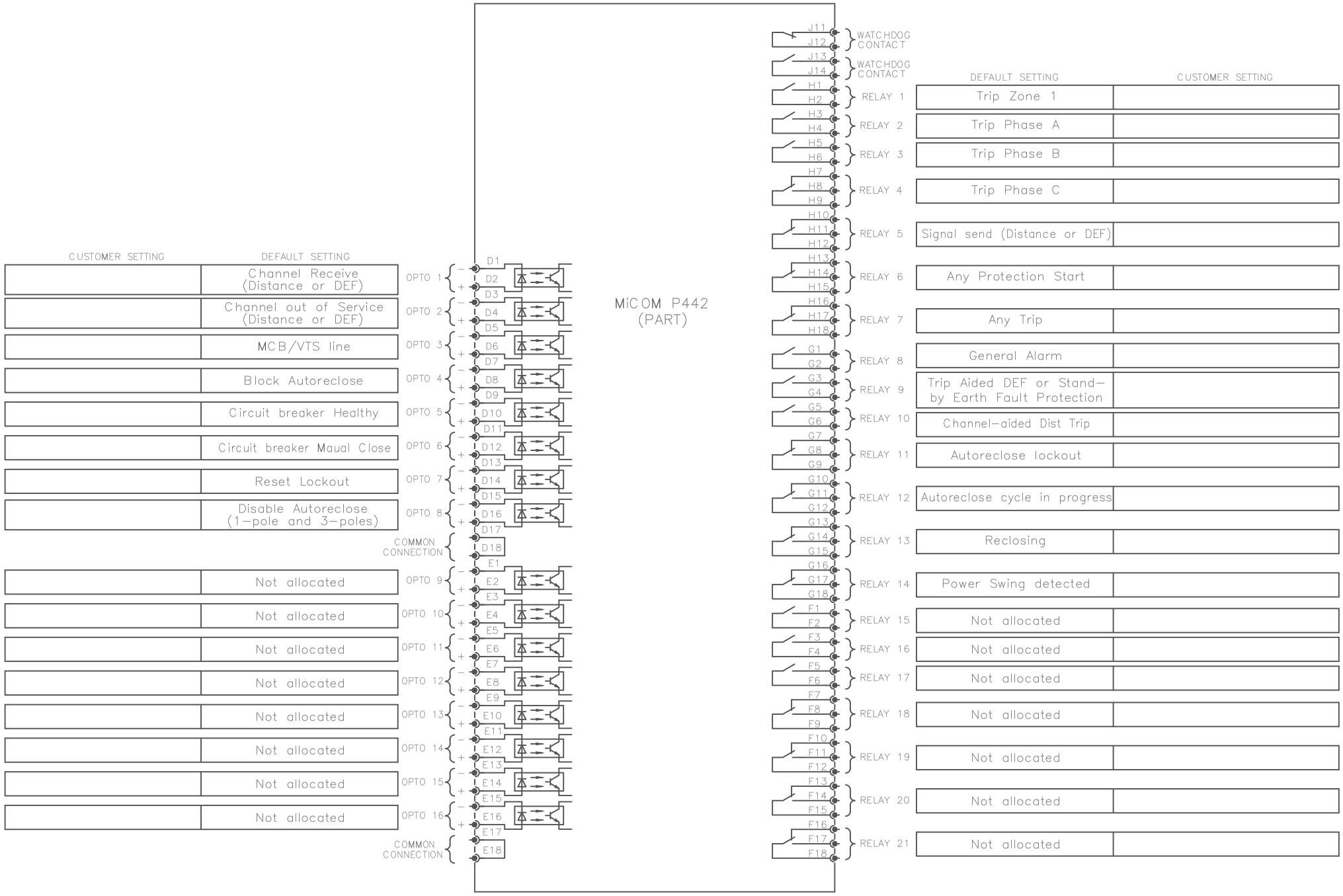
5. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.

6. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

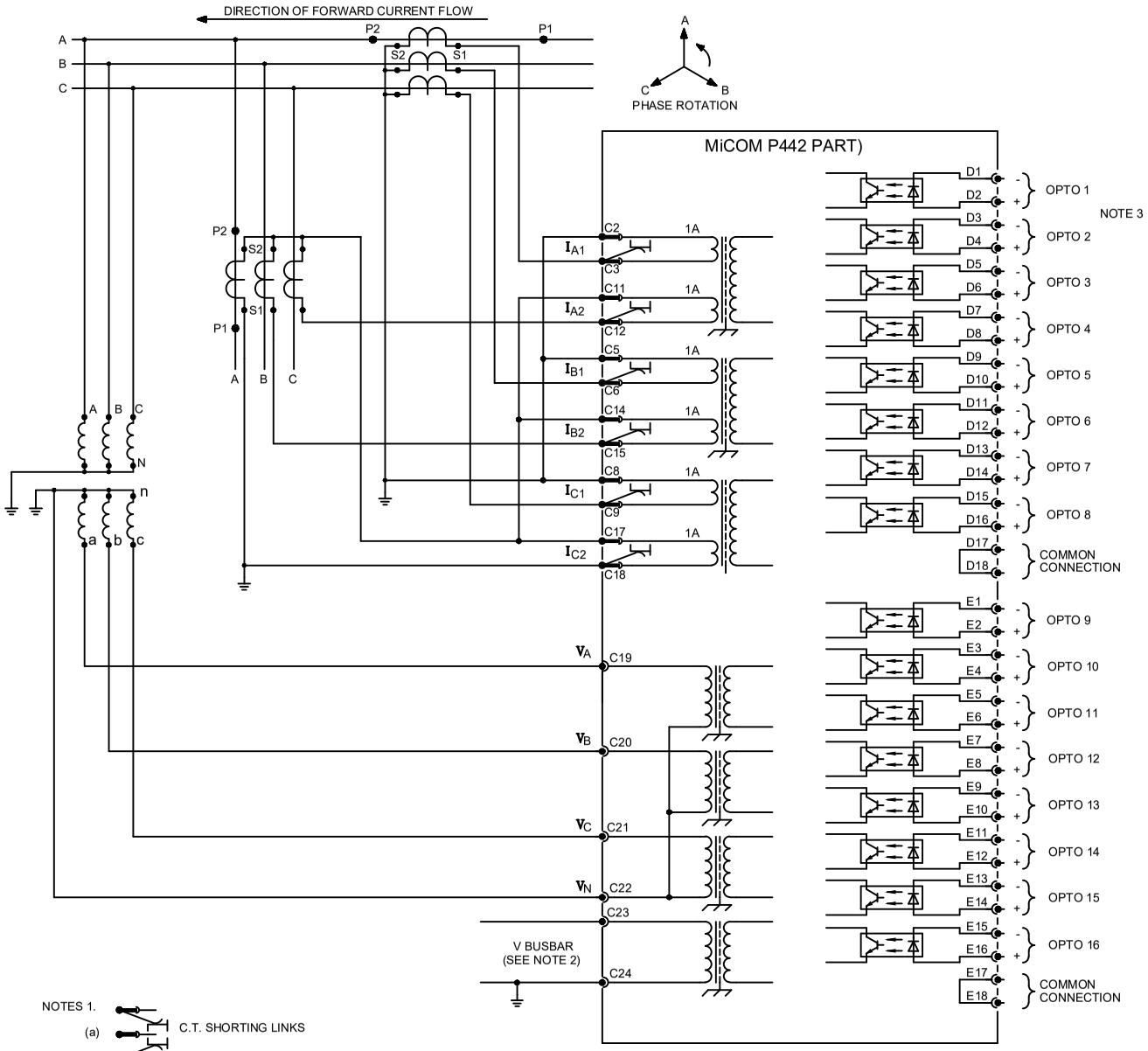
* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

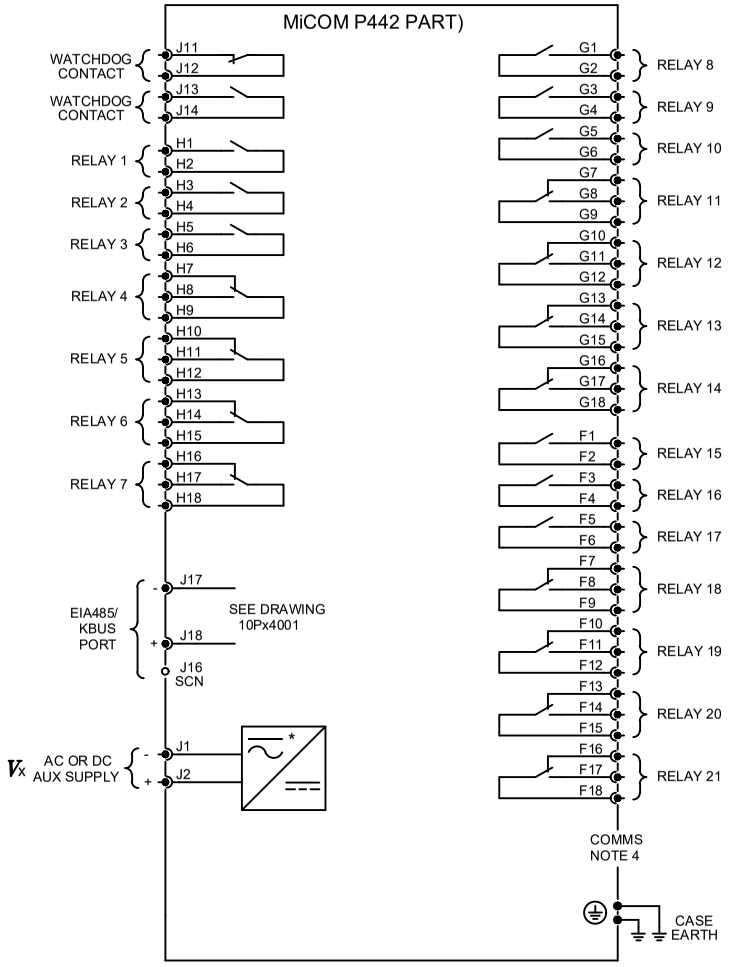
** FAST TRIP RELAY (OPTIONAL)

Issue: Q	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM P442 DISTANCE PROTECTION			
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: **10P44201**	PLM No: A20057271	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	



Issue: F	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXT CONN DIAG: DISTANCE PROT RELAY (60TE) 1 OR 3 POLE TRIPPING DIRECTIONAL PHASE O/C AND E/F AUTO-RECLOSE +I/O (IRIG-B OPTION)				
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: **10P44201**	PLM No: A20057289	Sht: 2	GE VERNOVA
Date:	Chkd:				Next Sht: -		





NOTES 1.

(a) C.T. SHORTING LINKS

(b) PIN TERMINAL (P.C.B. TYPE)

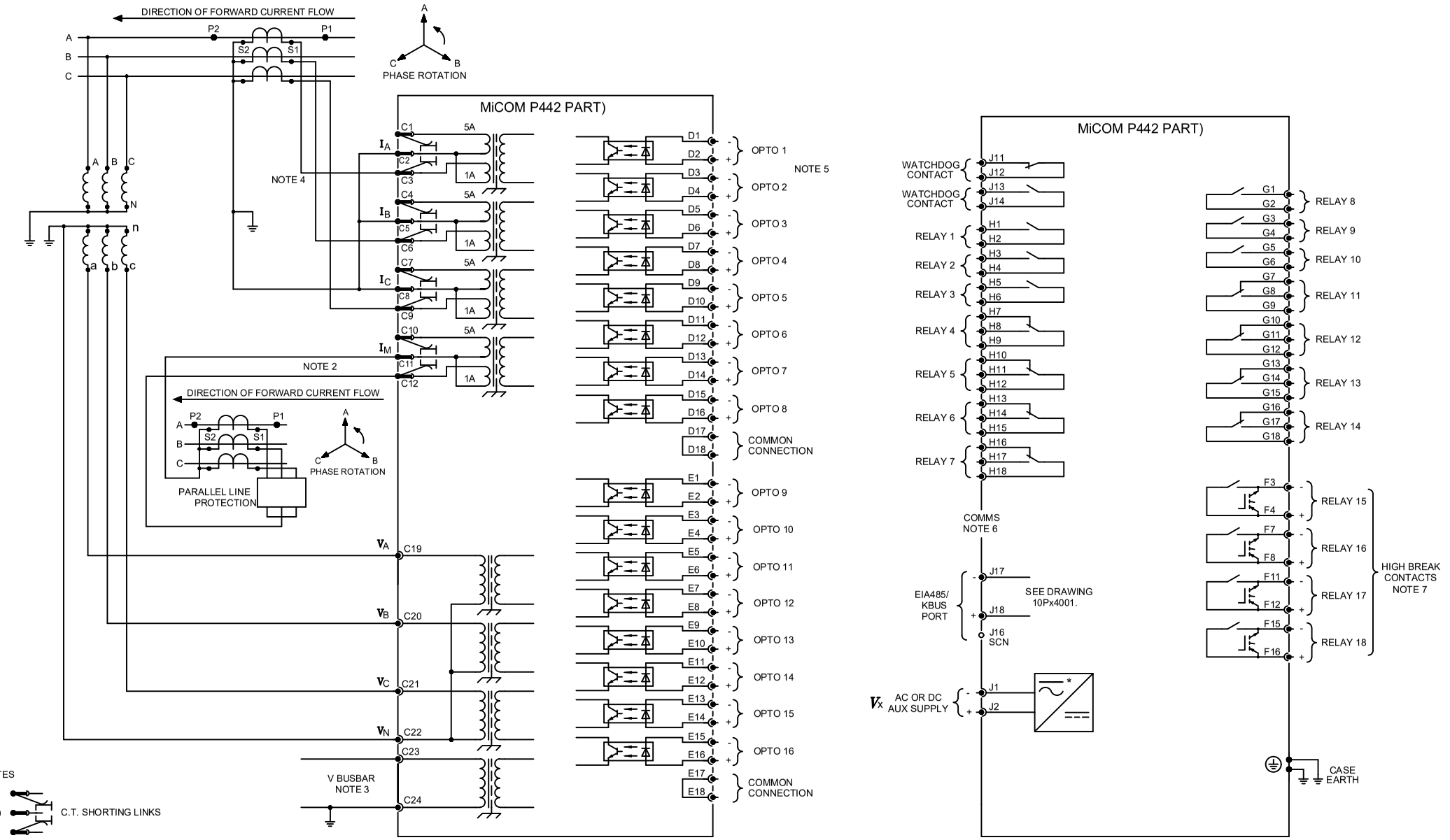
2. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.

3. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.

4. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

Issue: F	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXT. CONNECTION DIAGRAM: P442 DISTANCE PROTECTION FOR RTE (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: **10P44202**	PLM No: A20058054	Sht: 1
Date:	Chkd:			Next Sht: -	GE VERNOVA

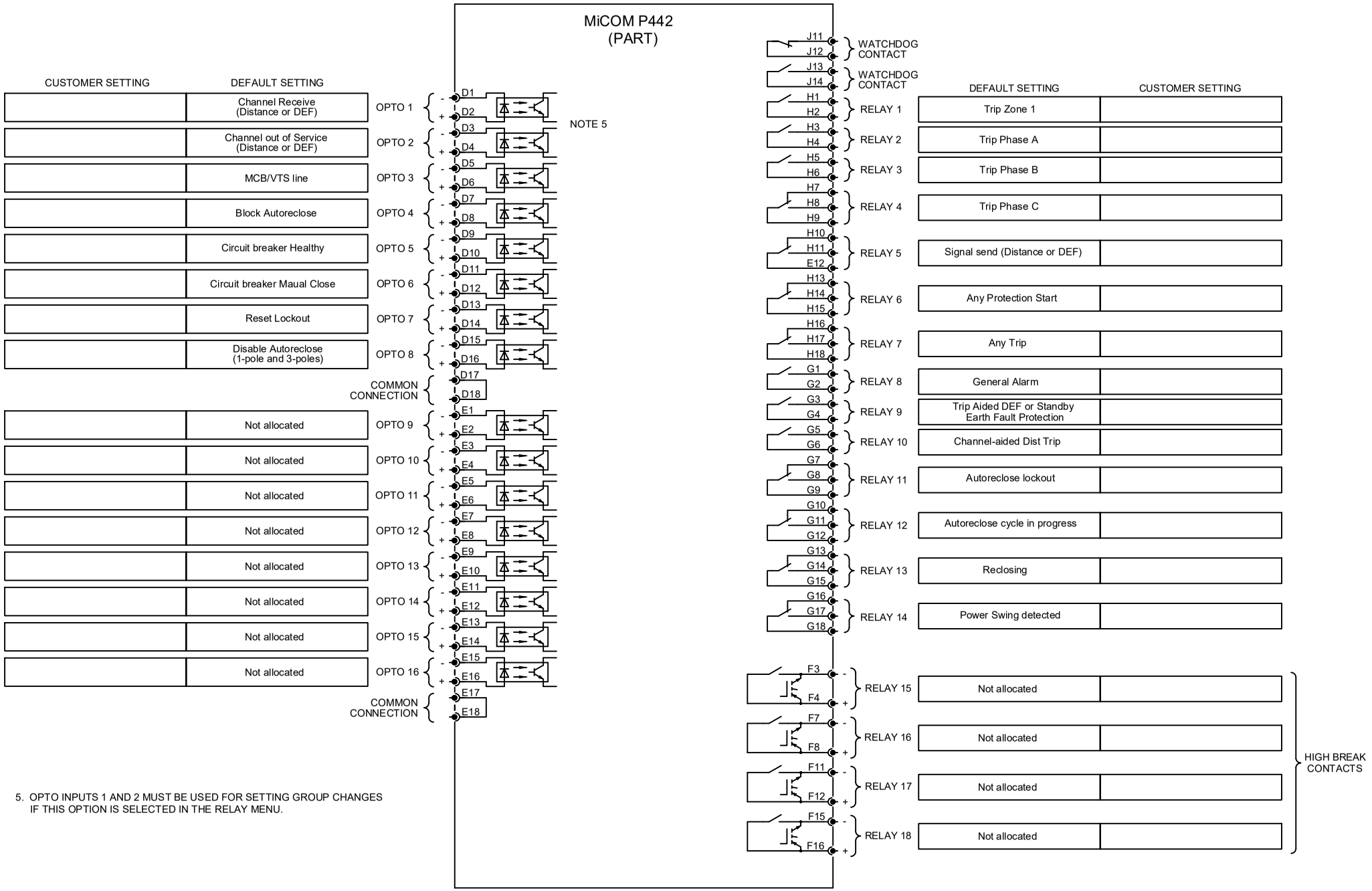


NOTES

1. (a) C.T. SHORTING LINKS
   (b) PIN TERMINAL (P.C.B. TYPE)
2. I_M INPUT IS FOR OPTIONAL MUTUAL COMPENSATION OF FAULT LOCATOR.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
5. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.
6. FOR COMMS OPTIONS SEE DRAWING 10Px4001.
7. TO OBTAIN HIGH BREAK DUTY, CONTACTS MUST BE CONNECTED WITH THE CORRECT POLARITY.

* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

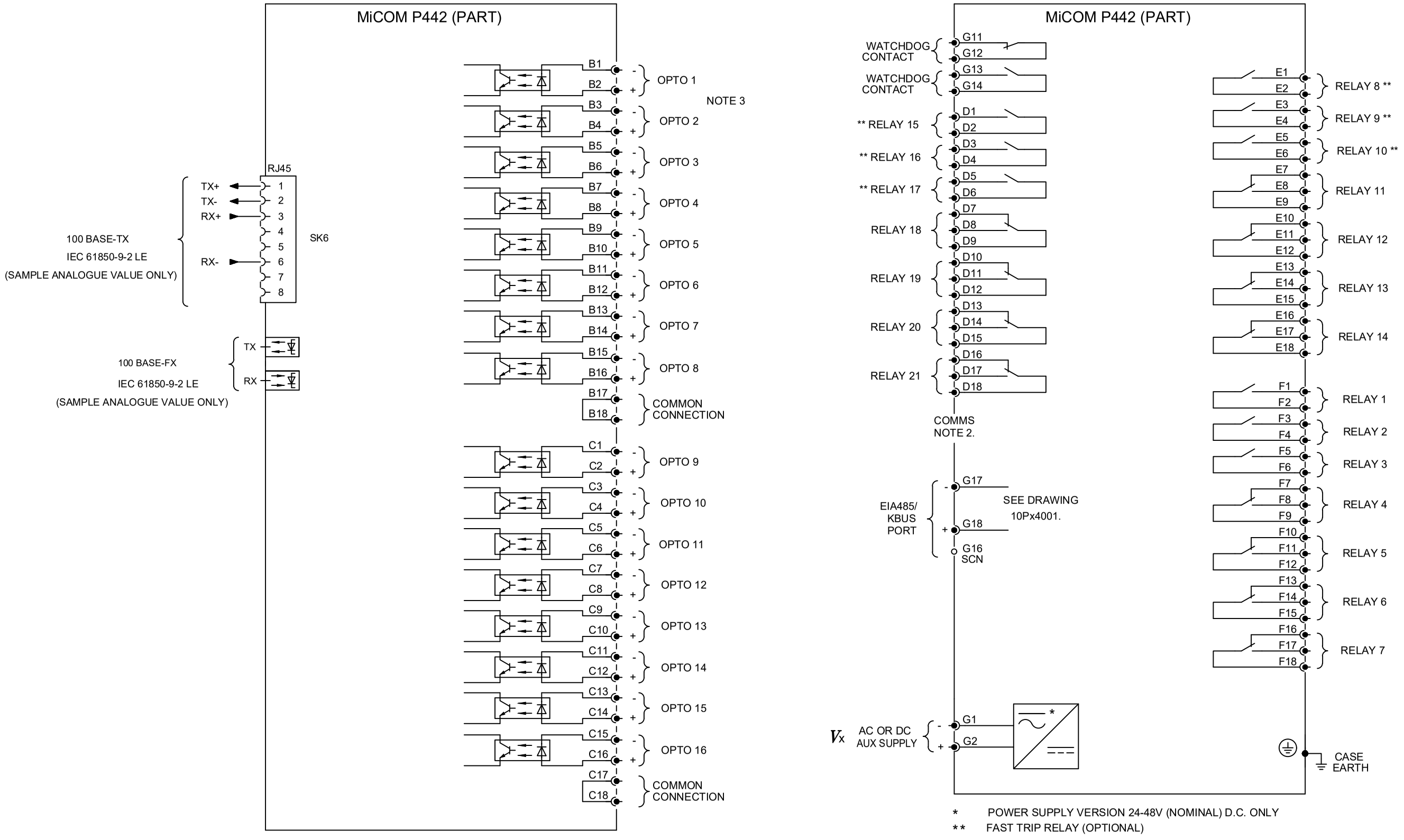
Issue: F	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAG: P442 DISTANCE PROTECTION (60TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information 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: **10P44203**	PLM No: A20064689	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	



5. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAG: P442 DISTANCE PROTECTION (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: **10P44203**	PLM No: A20064602	Sht: 2
Date:	Chkd:				Next Sht: -

GE VERNOVA



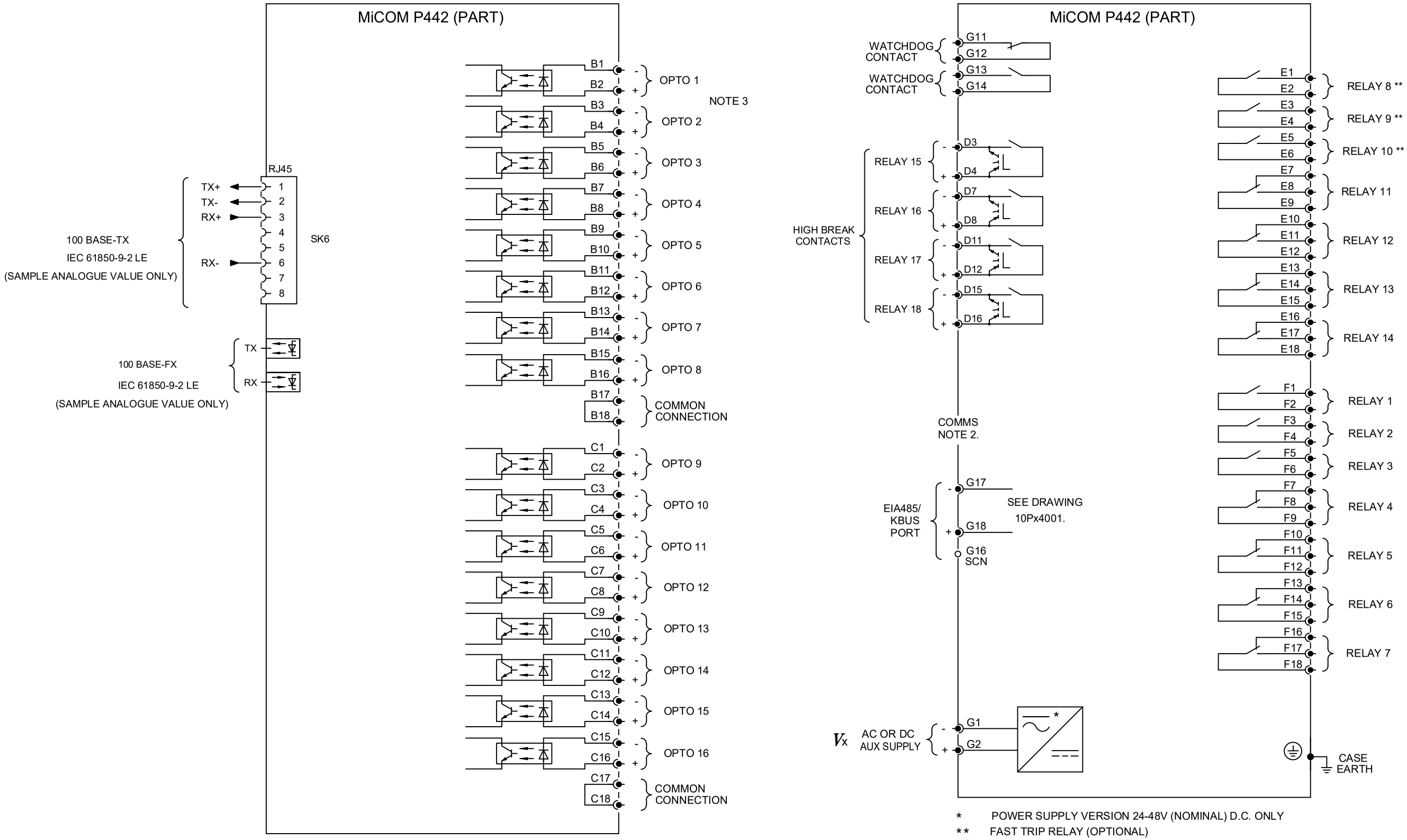
* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

** FAST TRIP RELAY (OPTIONAL)

NOTES .

1. ⊣●⊢ PIN TERMINAL (P.C.B. TYPE)
2. FOR COMMS OPTIONS SEE DRAWING 10Px4001
3. OPTO INPUTS 1 & 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.

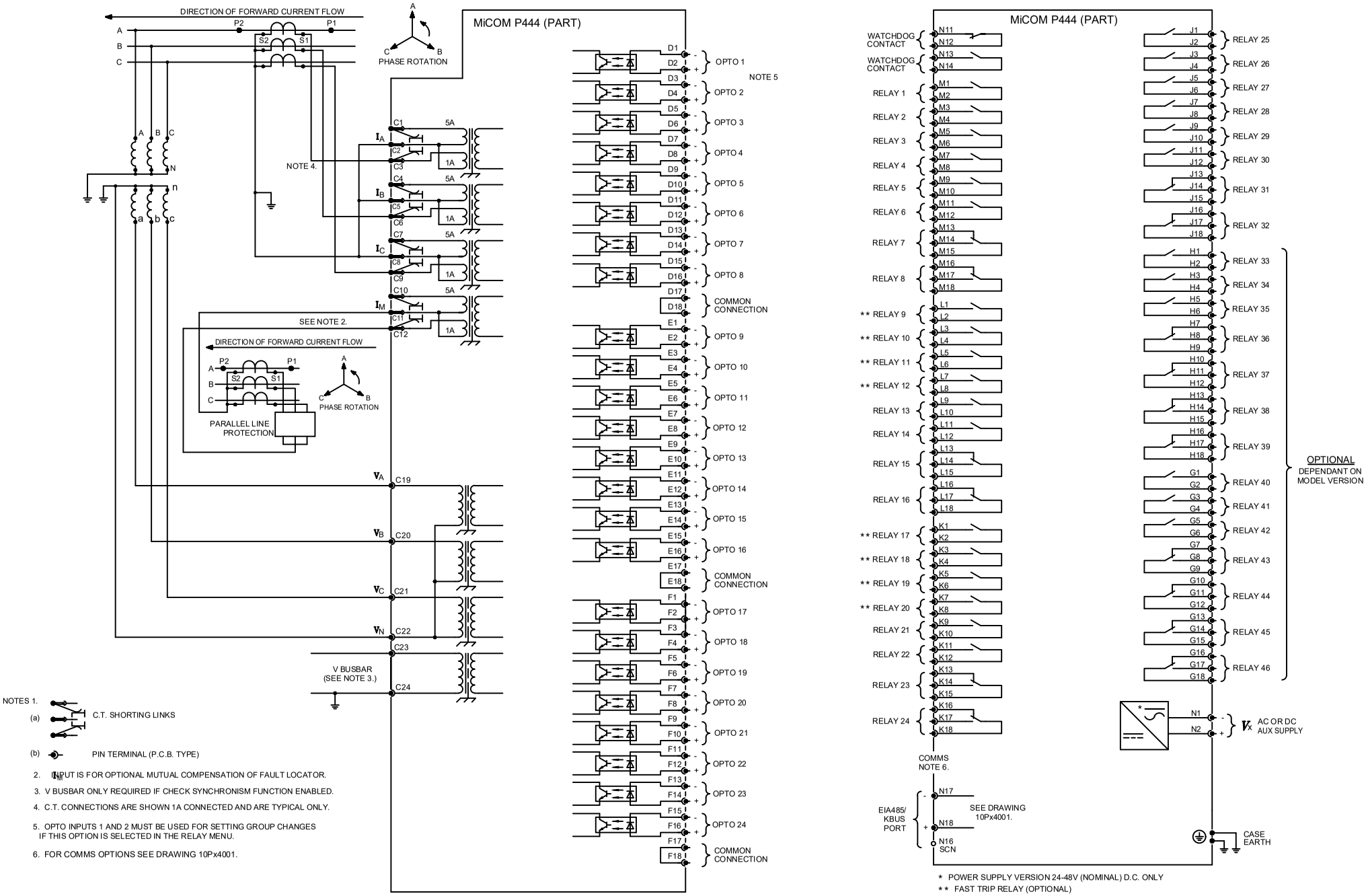
Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAG DIST. PROT'N 60TE WITH NCIT 16 INPUTS, 21 STANDARD RELAYS (6 OPTIONAL FAST TRIP)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE 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: **10P44204**	PLM No: A20065497	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: -	



NOTES .

1. ⊸ PIN TERMINAL (P.C.B. TYPE)
2. FOR COMMS OPTIONS SEE DRAWING 10Px4001
3. OPTO INPUTS 1 & 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAG. DIST.PROT'N 60TE WITH NCIT 16 INPUTS, 14 STANDARD RELAYS & 4 HIGH BREAK RELAYS			
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: **10P44205**	PLM No: A20072032	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: -	



NOTES 1.

(a) C.T. SHORTING LINKS

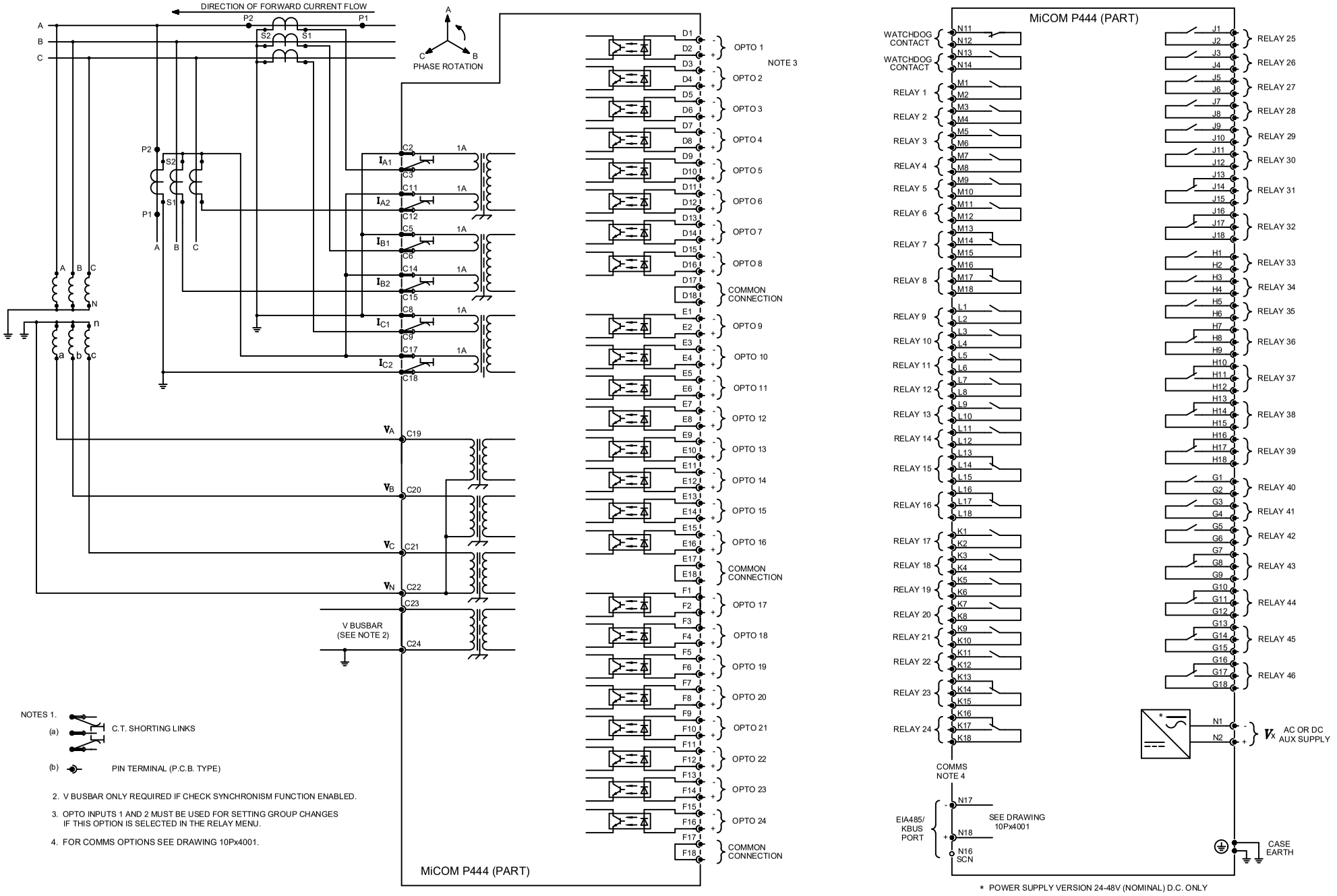
(b) PIN TERMINAL (P.C.B. TYPE)

2. I_N INPUT IS FOR OPTIONAL MUTUAL COMPENSATION OF FAULT LOCATOR.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
5. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.
6. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

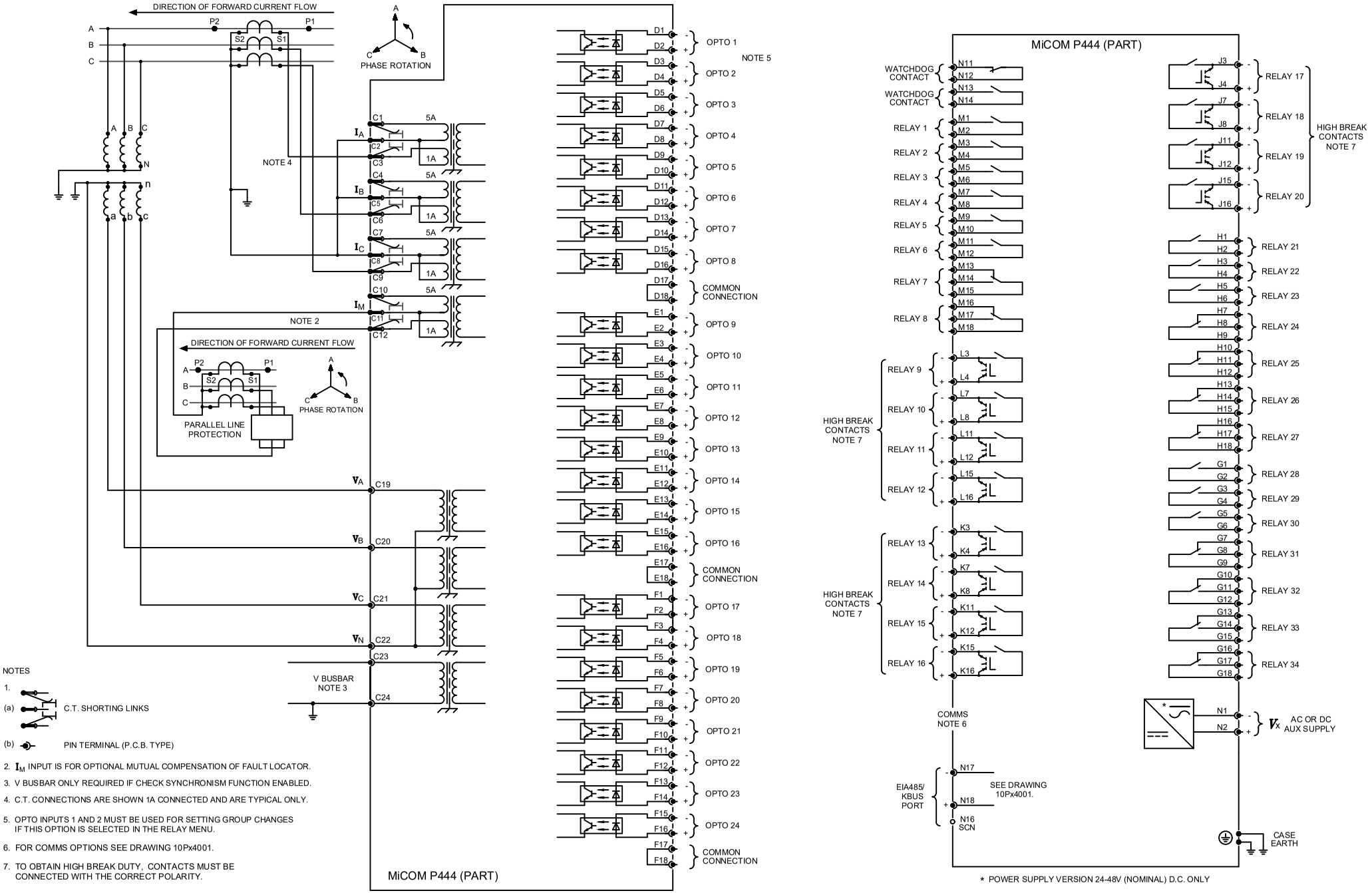
* POWER SUPPLY VERSION 24-48V (NOMINAL) D.C. ONLY

** FAST TRIP RELAY (OPTIONAL)

Issue: H	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM P444		
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: **10P44401**	PLM No: A20057217	Sht: 1
Date:	Chkd:			Next Sht: -	GE VERNOVA



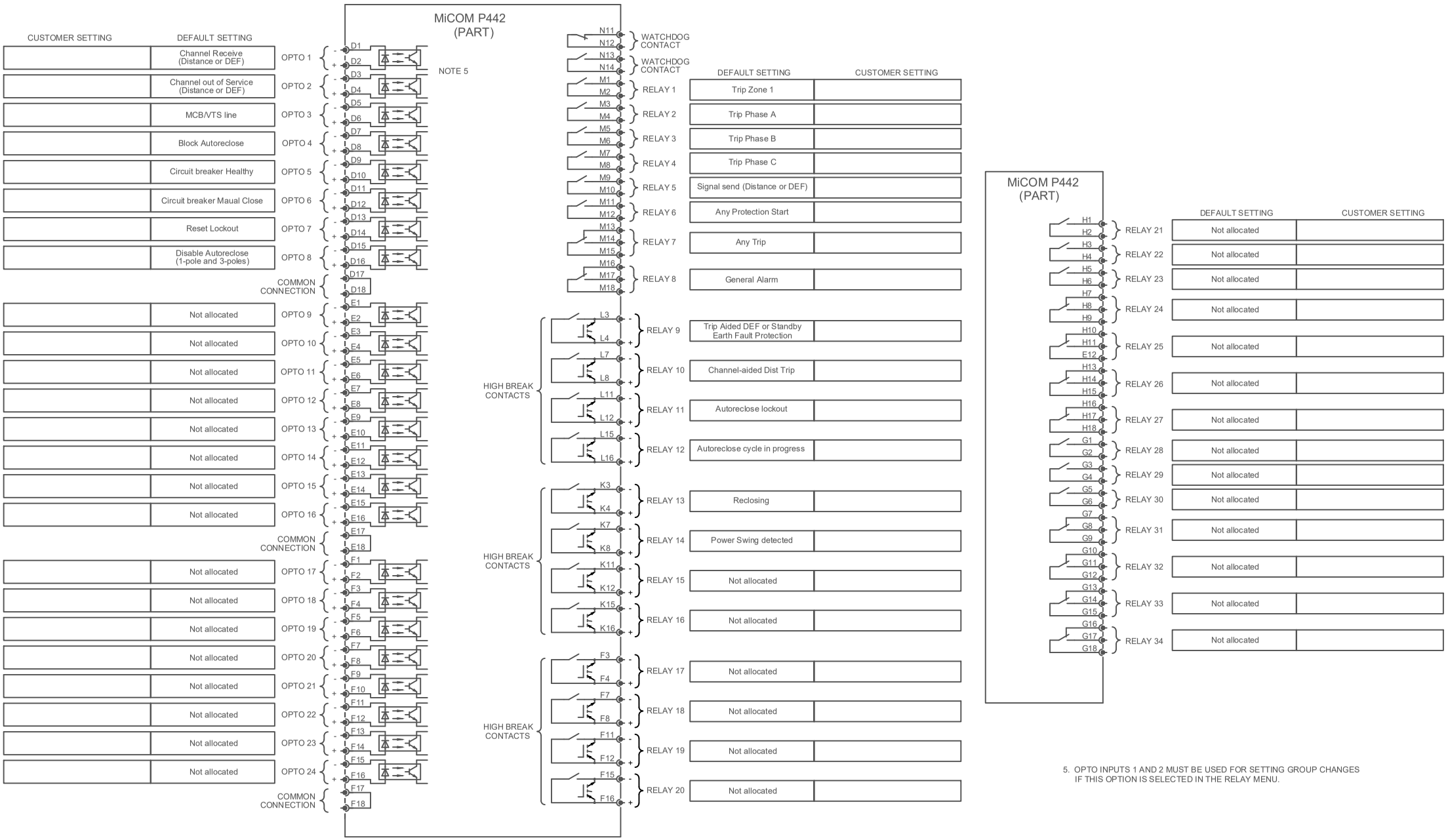
Issue: F	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXT. CONN. DIA: P444 DISTANCE PROTECTION FOR RTE (80TE)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and contains proprietary information 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: **10P44402**	PLM No: A20058235	Sht: 1 Next Sht: -	GE VERNOVA
Date:	Chkd:					



NOTES

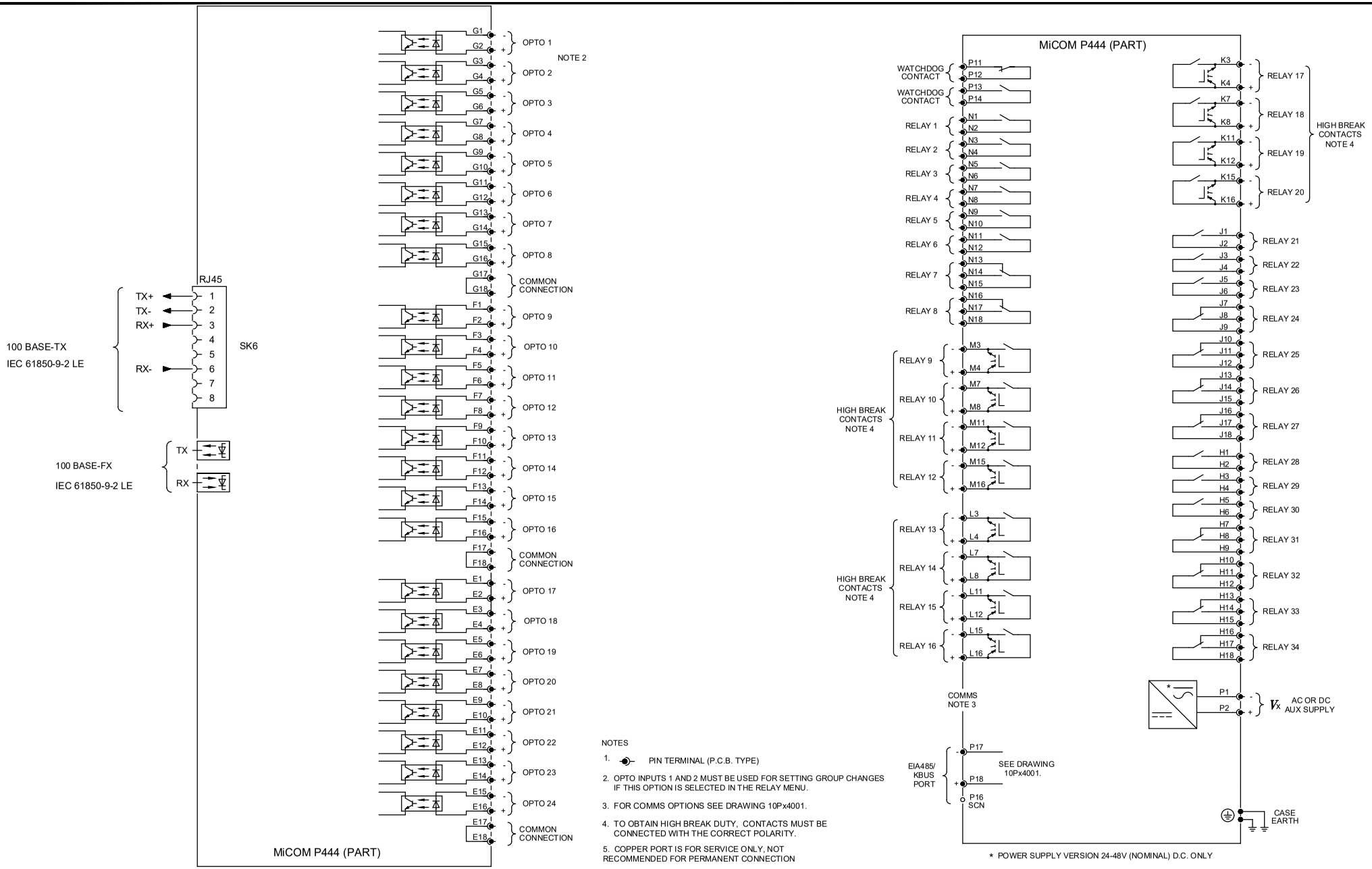
1. (a) C.T. SHORTING LINKS
   (b) PIN TERMINAL (P.C.B. TYPE)
2. I_M INPUT IS FOR OPTIONAL MUTUAL COMPENSATION OF FAULT LOCATOR.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
5. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.
6. FOR COMMS OPTIONS SEE DRAWING 10Px4001.
7. TO OBTAIN HIGH BREAK DUTY, CONTACTS MUST BE CONNECTED WITH THE CORRECT POLARITY.

Issue: F	Status: Approved	Revision Notes: CID008567 - Outline update only	Title: EXT. CONNECTION DIAG: P444 DISTANCE PROTECTION (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: 10P44403	PLM No: A20064639	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: 2	

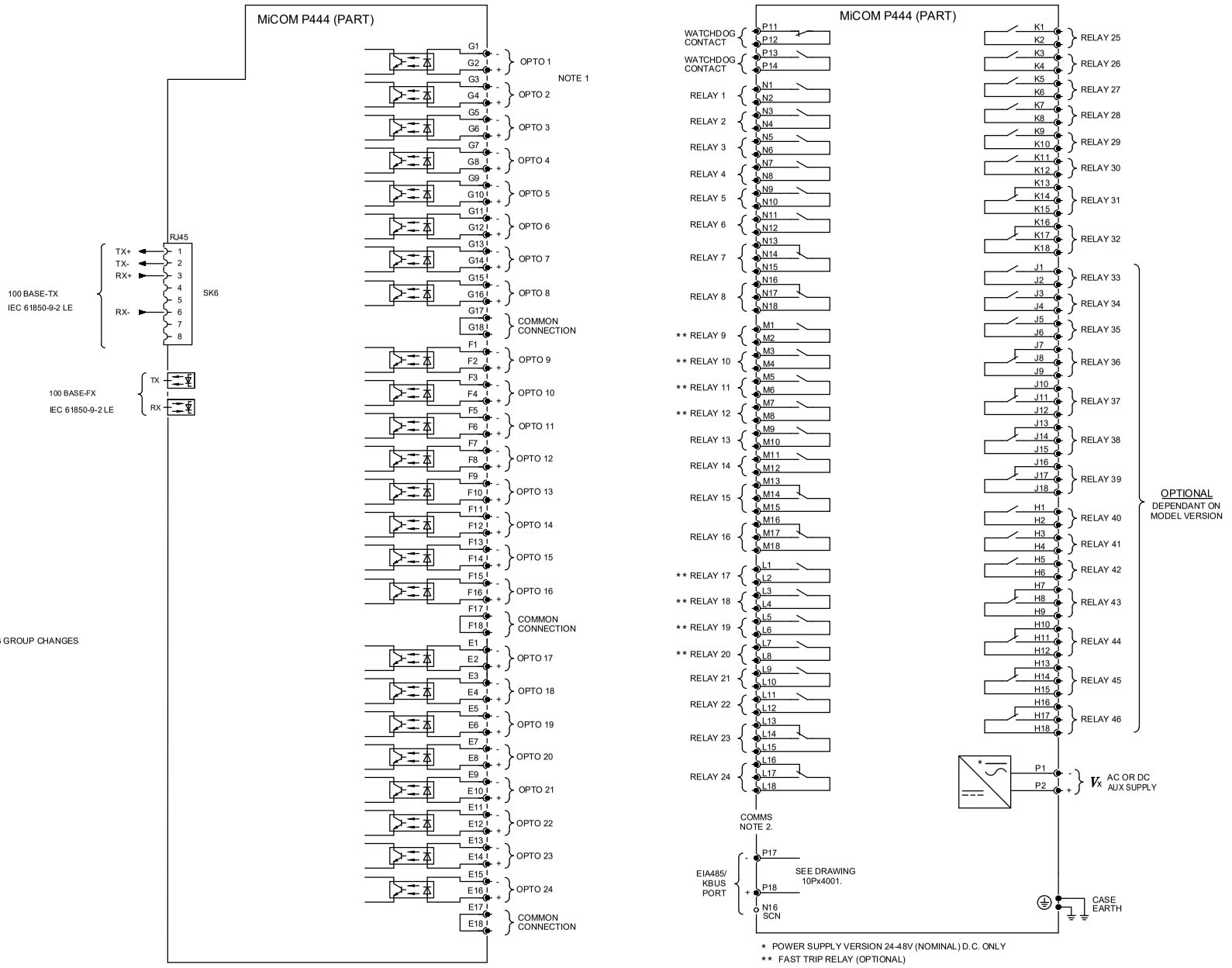


5. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXT. CONNECTION DIAG: P444 DISTANCE PROTECTION (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: **10P44403** / PLM No: A20064686 / Sht: 2 / Next Sht: - / GE VERNOVA
Date:	Chkd:		



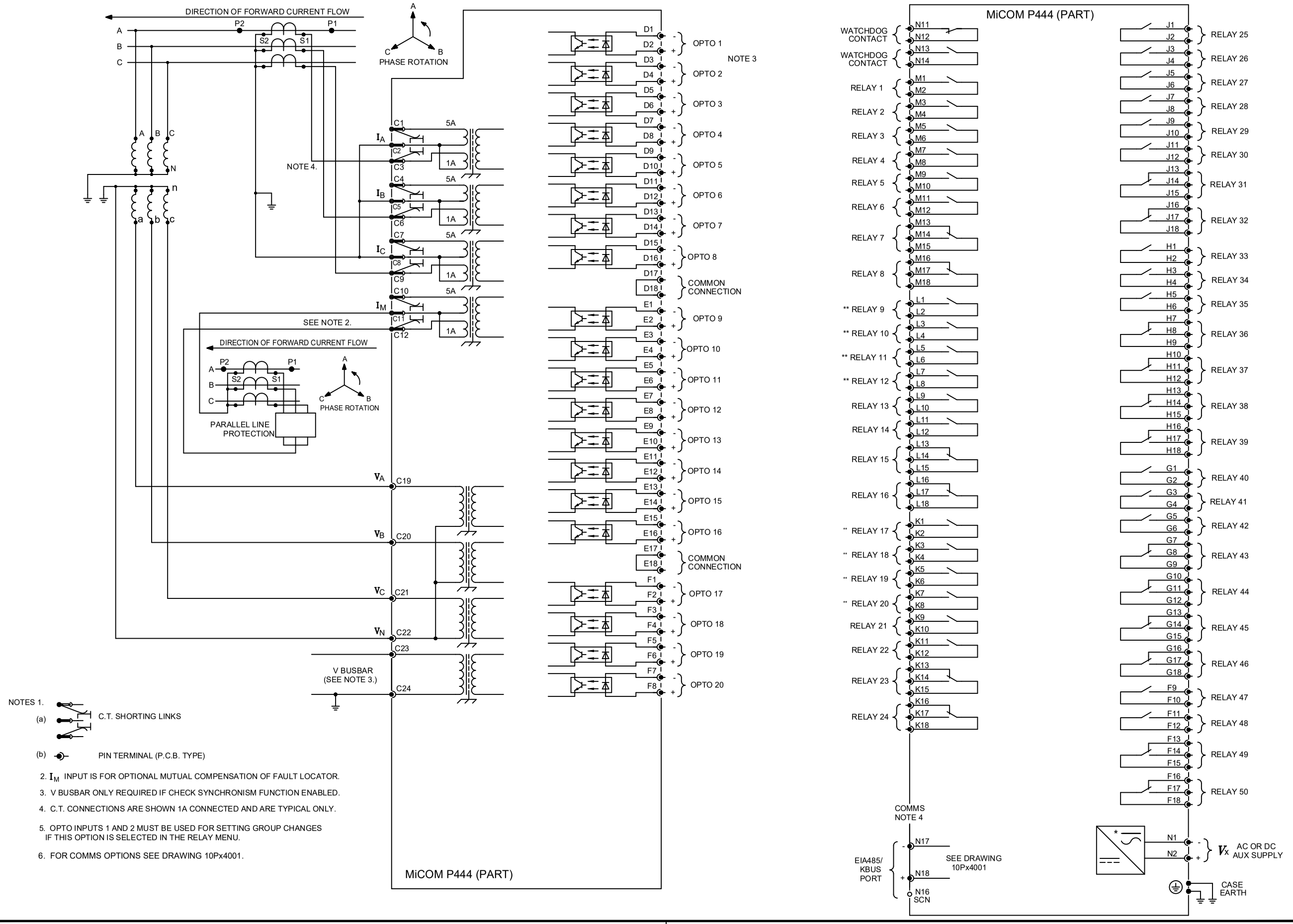
Issue: F	Status: **In Work**	Revision Notes: CID008567 - Outline update only	Title: EXT. CONNECTION DIAGRAM P444 DISTANCE WITH NCIT 80TE 24 OPTOS 34 RELAYS (12 HIGH BREAK)			
Date: 10/10/2024	Name: S Burton	PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of GE Vernova (GEV) and 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: **10P44406**	PLM No: A20065216	Sht: 1 Next Sht: -	GE VERNOVA
Date:	Chkd:					



NOTES

1. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.
2. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

Issue: E	Status: **Approved**	Revision Notes: CID008567 - Outline update only	Title: EXTERNAL CONNECTION DIAGRAM : COMMS OPTION P444 MICOM PX40 PLATFORM NCIT			
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: **10P44405**	PLM No: A20065182	Sht: 1	GE VERNOVA
Date:	Chkd:				Next Sht: -	



NOTES 1.

(a) C.T. SHORTING LINKS

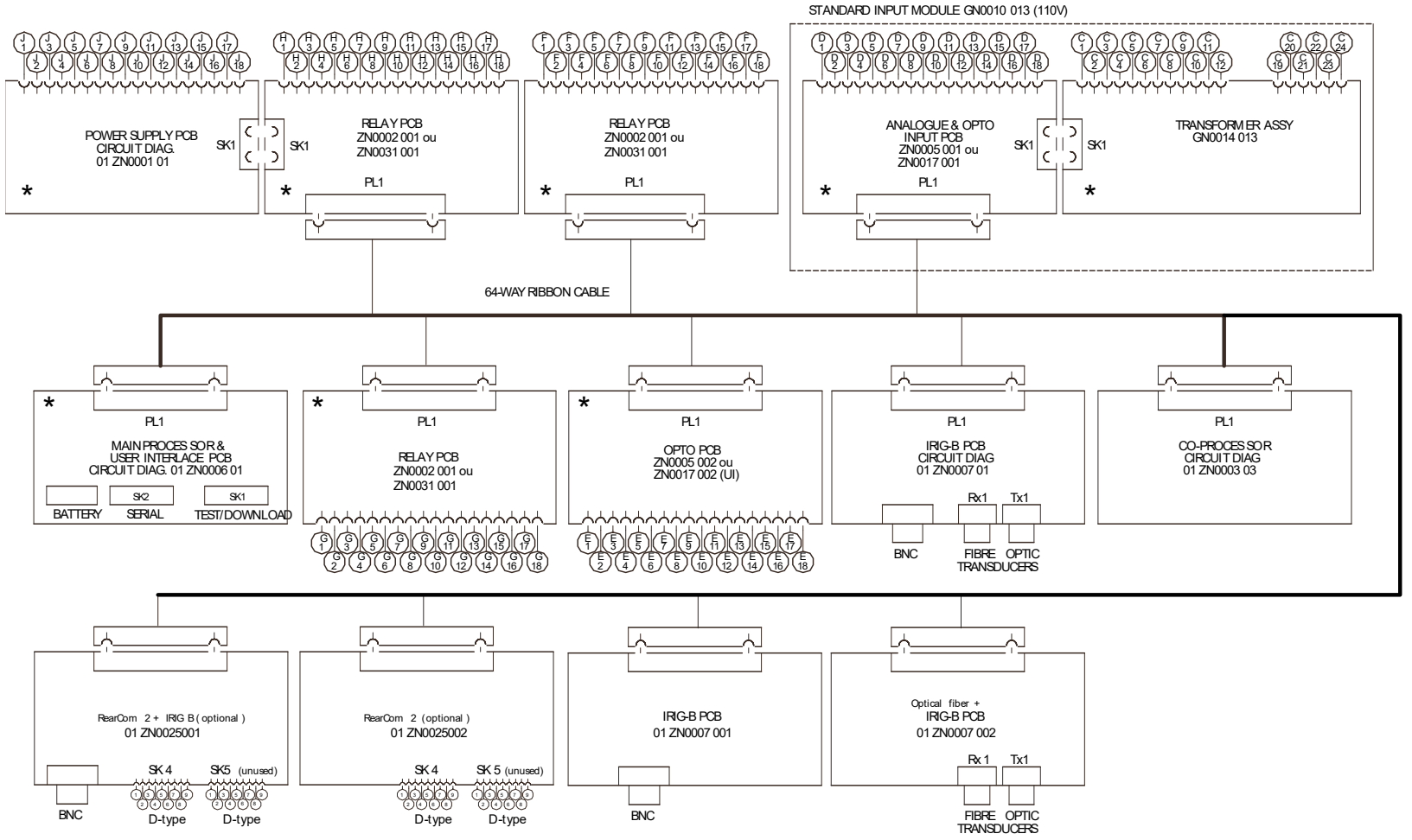
(b) PIN TERMINAL (P.C.B. TYPE)

2. I_M INPUT IS FOR OPTIONAL MUTUAL COMPENSATION OF FAULT LOCATOR.
3. V BUSBAR ONLY REQUIRED IF CHECK SYNCHRONISM FUNCTION ENABLED.
4. C.T. CONNECTIONS ARE SHOWN 1A CONNECTED AND ARE TYPICAL ONLY.
5. OPTO INPUTS 1 AND 2 MUST BE USED FOR SETTING GROUP CHANGES IF THIS OPTION IS SELECTED IN THE RELAY MENU.
6. FOR COMMS OPTIONS SEE DRAWING 10Px4001.

Issue: B	Revision: CID008504. RELAYS 49 AND 50 CONNECTIONS MODIFIED		Title: EXTERNAL CONNECTION DIAGRAM - P444 DISTANCE (20I / 50O) 80TE	
Date: 21/08/2024	Name: S WOOTTON	GE PROPRIETARY AND CONFIDENTIAL INFORMATION This document is the property of General Electric Company ("GE") and contains proprietary information of GE. 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 GE, and that the information shall be used by the recipient only as approved expressly by GE. This document shall be returned to GE upon its request. This document may be subject to certain restrictions under U.S. export control laws and regulations.© General Electric Company, GE CONFIDENTIAL UNPUBLISHED WORK.	Drg No: 10P44408	Sht: 1
Date:	Chkd:			Next Sht: -

GE VERNOVA

P442 BOARD

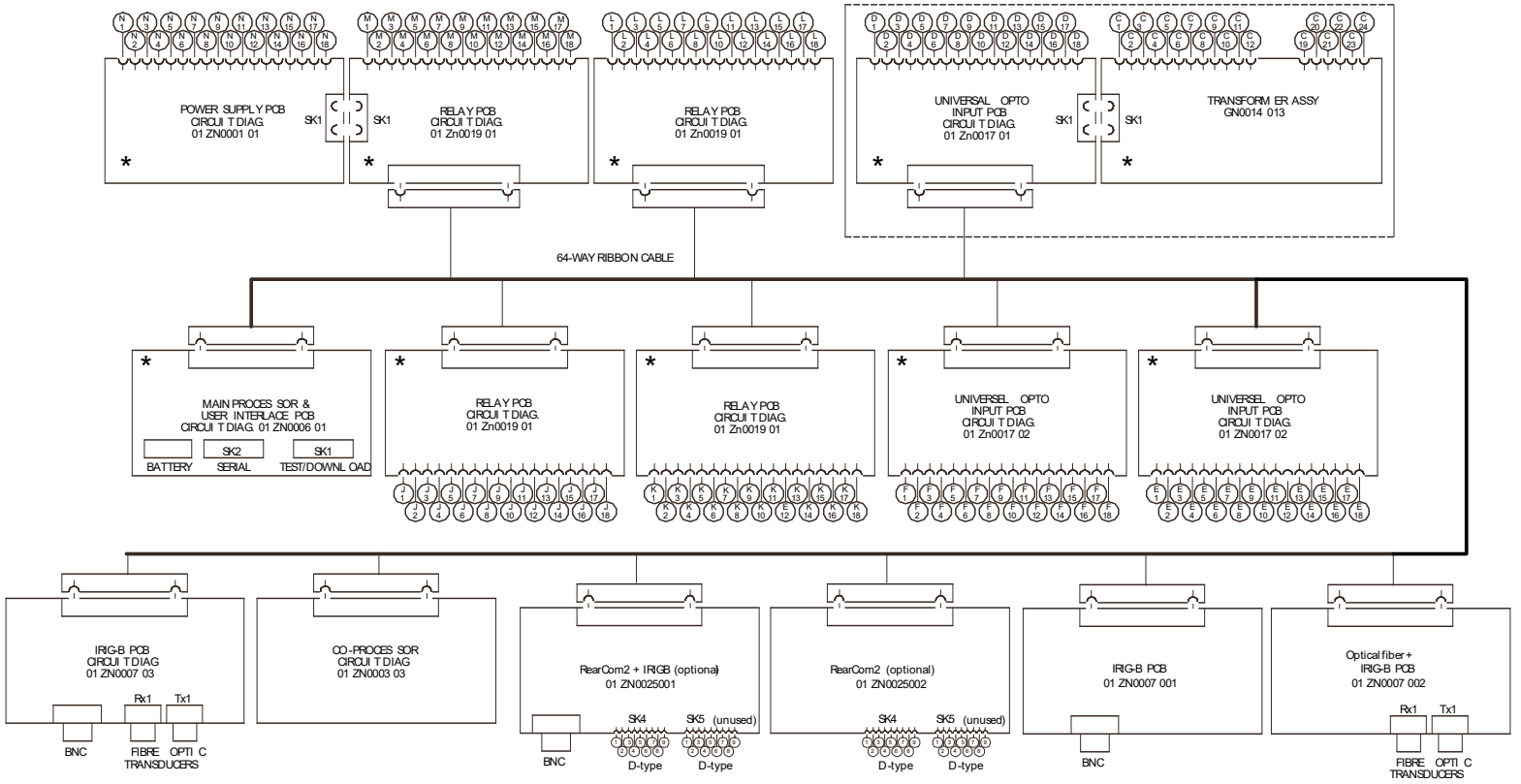


P442

* BOARD CONTAINS SALETY CRITICAL COMPONENTS.

P3911ENa

P444 BOARD



P444

BOARD CONTAINS SALETY CRITICAL COMPONENTS.

EXAMPLE FOR P444114A3A????A

P3912ENa



GE VERNOVA

© 2026 GE Vernova. All rights reserved. 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. Reproduction, use or disclosure to third parties, without express written authority, is strictly prohibited.