

# MiCOM S1 Agile

## User Guide MiCOM IED Support Software

Software version: 3.0

Publication Reference: P40-MCR-SAS-UG-EN-6





# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>User Interface</b>	<b>4</b>
2.1	Tile Structure	4
2.2	Menu Structure	5
<b>3</b>	<b>Getting Started</b>	<b>6</b>
3.1	Quick System Guide	7
3.2	Download Data Models	7
3.3	Set Up a System	7
3.4	Connect to an IED	7
3.5	Connect to an IED in a System	7
3.6	Send Settings to a Device	7
3.7	Extract Settings From a Device	8
3.8	Compare Settings Files	8
3.9	Extract a DNP3 File From a Device	8
3.10	Extract an Events File From a Device	8
3.11	Extract a Disturbance Record From a Device	8
<b>4</b>	<b>Cyber Security</b>	<b>9</b>
4.1	Overview	9
4.2	The Need for Cyber-Security	9
4.3	Standards	10
4.3.1	NERC Compliance	10
4.3.2	IEEE 1686-2013	12
4.4	Cyber-Security Implementation	13
4.4.1	Initial Setup	13
4.5	Roles and Permissions	14
4.5.1	Roles	14
4.5.2	Permissions	15
4.6	Authentication	17
4.6.1	Authentication Methods	17
4.6.2	Bypass	17
4.6.3	Login	18
4.6.4	User Sessions	19
4.6.5	User Locking Policy	20
4.6.6	Logout	21
4.6.7	Device Users	22
4.6.8	Password Policy	22
4.6.9	Change Password	22
4.6.10	RADIUS	22
4.6.11	Recovery	24
4.6.12	Disabling Physical Ports	26
4.6.13	Disabling Logical Ports	27
4.7	Security Event Management	27
4.7.1	Security Events: Courier	27
4.7.2	Syslog	29
4.7.3	Syslog Client	30
4.7.4	Syslog Functionality	30
<b>5</b>	<b>PSL Editor</b>	<b>33</b>
5.1	Loading Schemes from Files	33
5.2	PSL Editor Toolbar	33
5.2.1	Logic Symbols	33
5.3	Logic Signal Properties	34
5.3.1	Link Properties	35
5.3.2	Opto Signal Properties	35
5.3.3	Input Signal Properties	35
5.3.4	Output Signal Properties	35
5.3.5	GOOSE Input Signal Properties	35

5.3.6	GOOSE Output Signal Properties	36
5.3.7	Control Input Signal Properties	36
5.3.8	InterMiCOM Input Properties	36
5.3.9	InterMiCOM Output Properties	36
5.3.10	Function Key Properties	37
5.3.11	Fault Recorder Trigger Properties	37
5.3.12	LED Signal Properties	37
5.3.13	Contact Signal Properties	37
5.3.14	LED Conditioner Properties	37
5.3.15	Contact Conditioner Properties	38
5.3.16	Counter Properties	38
5.3.17	Timer Properties	38
5.3.18	Gate Properties	39
5.3.19	Off-Page Connector Properties	39
5.3.20	SR Programmable Gate Properties	44
5.4	PSL Converter	45
5.4.1	PSL Converter Prerequisites	45
5.4.2	File Conversion	45
5.5	DDB Monitoring	45
5.5.1	DDB Monitoring Prerequisites	45
5.5.2	Setting the DDB Monitoring Session	46
5.5.3	Saving the DDB Monitoring Session	46
5.5.4	Playing the DDB Monitoring Session	46
5.6	Viewing and Printing PSL Diagrams	46
<b>6</b>	<b>SLD Editor</b>	<b>48</b>
6.1	SLD Editor Implementation	48
6.2	SLD Editor Symbols	48
<b>7</b>	<b>IED Configurator</b>	<b>53</b>
7.1	IED Configurator Tool Features	53
7.2	IEC 61850 Substation Configuration Languages	53
7.3	IEC 61850 Substation Configuration Files	54
7.4	Opening a Preconfigured SCL File	55
7.5	Opening An ICD Template File	55
7.5.1	Template Installed for Required IED Type	56
7.5.2	Template Not Installed for Required IED Type	56
7.6	Opening an Existing MCL Configuration File	56
7.7	Configuring a MiCOM IED	56
7.7.1	Reading or Editing IED Details	57
7.7.2	Communications Setup	58
7.7.3	Editing Communications Settings	59
7.7.4	Ethernet Failover Settings	60
7.7.5	Configuring the IED for SNTP	60
7.7.6	Configuring the SNTP Server	61
7.7.7	Editing Dataset Definitions	62
7.7.8	Configuring Optimised Performance Goose Datasets	63
7.7.9	GOOSE Publishing Configuration	64
7.7.10	GOOSE Subscription Configuration	65
7.7.11	Report Control Block Configuration	67
7.7.12	Controls Configuration	68
7.7.13	Editing Configurable Data Attributes	69
7.7.14	Editing Measurement Configurations	69
7.8	Full Validation of IED Configuration	71
7.9	Validation Summary	71
7.10	Managing SCL Schema Versions	72
7.10.1	Adding and Removing SCL Schemas	72
7.11	Configuration Banks	72
7.12	Transfer of Configurations	73
7.13	Exporting Installed ICD Template files	73

7.14	Exporting Configured SCL Files	73
7.15	Exporting Logical Device and Node Models to a Document	74
7.16	Managing Logical Devices and Nodes	74
7.16.1	Editing Logical Devices and Nodes	74
7.16.2	Configuring Logical Devices	74
7.16.3	Configuring Logical Nodes	75
<b>8</b>	<b>DNP3 Configurator</b>	<b>77</b>
8.1	Preparing Files Offline to Send to an IED	77
8.2	Send Settings to an IED	77
8.3	Extract Settings From an IED	77
8.4	View IED Settings	78
<b>9</b>	<b>Curve Tool</b>	<b>79</b>
9.1	Features	79
9.2	Curve Plot Pane	79
9.2.1	Open a Curve	79
9.2.2	Zooming and Panning	79
9.2.3	Change the Graph to Default Size	80
9.2.4	Change the Graph Grid Lines	80
9.2.5	Change the Graph Scale	80
9.2.6	Change Curve Colours	80
9.2.7	Print a Curve	80
9.2.8	Save a Curve as an Image	80
9.3	Curve Points Details Pane	80
9.3.1	Create a New Curve	81
9.3.2	Entering Values of Q and T into the Table	81
9.3.3	Edit a Curve	81
9.3.4	Interpolating Curve Points	82
9.3.5	Import Curve Points	82
9.3.6	Export Curve Points	82
9.4	Formula Editor	82
9.4.1	Pick-Up Setting and TMS	83
9.5	Curve Templates	83
9.5.1	Select a Curve Template	85
9.6	Connecting to an IED	85
9.6.1	Connecting to a Serial Port	85
9.6.2	Connecting to the Ethernet Port	86
9.7	Send a Curve to an IED	86
9.8	Extract a Curve from an IED	86
<b>10</b>	<b>S&amp;R Courier</b>	<b>87</b>
10.1	Set Up IED Communication	87
10.2	Create a New Communication Setup	87
10.3	Open a Connection	87
10.4	Create a New or Default IED DNP 3.0 File	88
10.5	Extract a Settings File From a Device	88
10.6	Save a Settings File	88
10.7	Send a Settings File to a Device	88
<b>11</b>	<b>Monitoring Module</b>	<b>89</b>
11.1	Offline and Online Monitoring Module	89
11.2	Online Monitoring Module	89
<b>12</b>	<b>GOOSE Editor</b>	<b>91</b>
12.1	Set Up IED Communication	91
12.2	Create a New Communication Setup	91
12.3	Open a Connection	91
12.4	Scan for Available Devices	91
12.5	Extract GOOSE Settings From a Device	92
12.6	Open, Edit and Save a GOOSE File	92
12.7	Send GOOSE Settings to a Device	92

<b>13</b>	<b>GOOSE Configurator</b>	<b>93</b>
13.1	Open an MCL File	93
13.2	Export From An S1 System To GOOSE Configurator	93
13.3	Publish a Message	93
13.4	Show Published Messages	93
13.5	Clone Publishing	94
13.6	Subscribe to a Message	94
13.7	Set A PSL File Path	94
13.8	Open A PSL File Path	94
13.9	Manage GOOSE Connections	94
13.10	Show IED Details	94
13.11	Working with SCL Files	94
13.12	Save Changes	95
13.13	Restore MCL Files	95
13.14	Currently Opened Files	95
13.15	Recently Used Files	95
13.16	Close Files	95
13.17	Application Note	95
13.17.1	Configuring the IED	96
13.17.2	Exporting a Preconfigured System to GOOSE Configurator	98
13.17.3	Adding a New IED to the Goose Configurator	99
13.17.4	Creating a New GOOSE Publication	100
13.17.5	GOOSE Subscription	101
13.17.6	Cloning of a Publisher	103
13.17.7	View Subscriptions	105
<b>14</b>	<b>Phasor Terminal</b>	<b>107</b>
14.1	System Stability	107
14.2	Phasor Measurement Units	107
14.3	IEEE Synchrophasor Standard	107
14.4	Hardware Installation	107
14.5	Using the Main Window	107
14.6	Creating a New Device	108
14.7	Editing an Existing Device Configuration	108
14.8	Manage Device Connections	108
14.9	Using Phasor Terminal	108
14.10	Change a Device Name	109
14.11	Displaying Quantities	109
14.12	Selecting Items to Display	109
14.12.1	Changing Plot Properties	109
14.12.2	Displaying Data in a Relative View	109
14.12.3	Changing Plot Name	110
14.13	View Device Properties	110
14.14	View Point Properties	110
14.15	Connect to a Device	110
14.16	Disconnect From a Device	111
14.17	Control Commands	111
14.18	Capturing Binary Data	111
14.19	Export Data	111
14.20	Modify Data Archive Settings	111
<b>15</b>	<b>Offline Fault Locator</b>	<b>113</b>
15.1	Create a New Network	113
15.2	Define Nodes	113
15.3	Define Lines	114
15.4	Network Design Requirements	115
15.5	Example Networks	115
15.5.1	Example 1	115
15.5.2	Example 2	117

15.6	Locate Faults	119
15.6.1	COMTRADE Requirements	120
15.7	Network Topologies and Restrictions	122
15.8	Looped Networks	122
15.9	Supported Topologies	123
15.9.1	Two Terminal Network	123
15.9.2	Three Terminal One Junction Network	123
15.9.3	Three Terminal Two Junction Network	124
15.9.4	Four Terminal One Junction Network	124
15.9.5	Four Terminal Two Junction Network	125
15.9.6	Four Terminal Three Junction Network	125
15.9.7	Five Terminal One Junction Network	126
15.9.8	Five Terminal Two Junction Network	126
15.9.9	Five Terminal Three Junction Network	127
15.9.10	Five Terminal Four Junction Network	127
15.9.11	Six Terminal One Junction Network	128
15.9.12	Six Terminal Two Junction Network	128
15.9.13	Six Terminal Three Junction Network	129
15.9.14	Six Terminal Four Junction Network	129
<b>16</b>	<b>Redundant Ethernet Configurator</b>	<b>131</b>
16.1	Connecting the IED to a PC	131
16.2	Installing the Configurator	131
16.3	Starting the Configurator	132
16.4	Device Identification	132
16.5	Selecting the Device Mode	132
16.6	Filter by Board Type	132
16.7	Password Configuration	132
16.8	IP Address Configuration	132
16.9	SNTP IP Address Configuration	133
16.10	Check MAC Table for Connected Equipment	133
16.11	PRP Configuration	133
16.12	HSR Configuration	133
16.13	RSTP Configuration	134
16.14	Bridge parameters	134
16.15	Port Parameters	134
16.16	Port States	135
16.17	Failover Configuration	135
16.18	Filtering Database	135
16.19	End of Session	136
<b>17</b>	<b>PRP/HSR Configurator</b>	<b>137</b>
17.1	Connecting the IED to a PC	137
17.2	Starting the Configurator	137
17.3	PRP/HSR Device Identification	138
17.4	Selecting the Device Mode	138
17.5	PRP/HSR IP Address Configuration	138
17.6	SNTP IP Address Configuration	138
17.7	Check for Connected Equipment	138
17.8	PRP Configuration	138
17.9	HSR Configuration	139
17.10	Filtering Database	139
17.11	End of Session	140
<b>18</b>	<b>RSTP Configurator</b>	<b>141</b>
18.1	Connecting the IED to a PC	141
18.2	Starting the Configurator	141
18.3	RSTP Device Identification	142
18.4	RSTP IP Address Configuration	142
18.5	SNTP IP Address Configuration	142

18.6	Check for Connected Equipment	142
18.7	RSTP Configuration	142
18.7.1	Bridge parameters	143
18.7.2	Port Parameters	143
18.7.3	Port States	143
18.8	End of Session	143
<b>19</b>	<b>Switch Manager</b>	<b>144</b>
19.1	Installation	144
19.2	Setup	145
19.3	Network Setup	145
19.4	Bandwidth Used	145
19.5	Reset Counters	145
19.6	Check for Connected Equipment	146
19.7	Mirroring Function	146
19.8	Ports On/Off	146
19.9	VLAN	146
19.10	End of Session	147
<b>20</b>	<b>AE2R</b>	<b>148</b>
20.1	Initialisation File	148
20.2	Common Section	148
20.3	Communications Section	150
20.4	Setting the Password	151
20.5	Running AE2R	151
20.6	Inspecting the Extracted Event Files	151
<b>21</b>	<b>AEDR2</b>	<b>152</b>
21.1	Initialisation File	152
21.1.1	Common Section	152
21.1.2	Courier Section	153
21.1.3	IEC 60870-5-103 Section	154
21.1.4	Example INI File	155
21.2	Connection	155
21.3	Operation	155
21.4	Disturbance Record Files	156
21.5	Log File	156
21.6	Using the Scheduled Tasks Program	156
<b>22</b>	<b>WinAEDR2</b>	<b>158</b>
22.1	Functions	158
<b>23</b>	<b>Wavewin</b>	<b>159</b>
23.1	File Manager Features	159
23.2	Save as Comtrade	159
<b>24</b>	<b>Device (Menu) Text Editor</b>	<b>161</b>
24.1	Open a Connection	161
24.2	Change Connection Password	161
24.3	Open a Menu Text File as a Reference	161
24.4	Edit Text File of Device	161
24.5	Send Edited Text File to Device	161
<b>25</b>	<b>Settings Excel Export</b>	<b>163</b>
25.1	Mapping Files	163
25.1.1	Export Default Mapping	163
25.1.2	Create Custom Mapping	163
25.1.3	Create Custom Mapping from Default Mapping	163
25.1.4	Hide or Show Mapped Settings	163
25.2	Exporting an Excel File	164
25.2.1	Export to XRIO	164
25.2.2	About XRIO	164
25.2.3	Export to CSV	165
25.2.4	Export to CAPE	165



25.3	Importing an Excel File	165
25.4	Hide or Show Read Only Settings	165
25.5	Select Language	166
<b>26</b>	<b>P747 Busbar Commissioning Tool (Remote HMI)</b>	<b>167</b>
26.1	Scheme Editor	167
26.1.1	Connections	167
26.1.2	Scheme Elements	168
26.1.3	Working with Text on the Scheme	168
26.2	Protection Data Monitor	169
26.2.1	Connect to the IED	169
<b>27</b>	<b>Dynamic Synoptic</b>	<b>171</b>
27.1	Synoptic Main Window	171
27.2	Synoptic Main Window	171
27.3	Menu	174
27.3.1	File	174
27.3.2	Device	175
27.4	Tools	175
27.5	View	175
27.5.1	Device Data	176
27.5.2	Logic Values of the CU	176
27.5.3	Logic Values of the PU	176
27.5.4	CU Analogue Values	176
27.5.5	PU Analogue Values	177
27.6	Help	177
<b>28</b>	<b>Remote HMI</b>	<b>178</b>
28.1	Communication Settings	178
28.1.1	Serial Settings	178
28.1.2	Ethernet Settings	179
28.2	Scheme Editor	180
28.2.1	Principle of Operation	180
28.2.2	Constraints	185
28.3	Scheme Design	185
28.3.1	Creating a New Scheme	185
28.3.2	Creating a Busbar	185
28.3.3	Creating a Busbar Link	185
28.3.4	Creating a Tie Group	186
28.3.5	Creating a Feeder Group	186
28.3.6	Association of Zones for Isolators	186
28.3.7	Edit Options	187
28.4	Dynamic Synoptic	188
28.5	Dynamic Synoptic	188
28.5.1	File	188
28.5.2	Edit	189
28.5.3	View	189
28.5.4	Device	189
28.5.5	Mode	190
28.5.6	Language	190



# SETTINGS APPLICATION SOFTWARE



---

## **1 INTRODUCTION**

---

MiCOM S1 Agile enables you to manage MiCOM devices in your system. You can build a list of devices and organise them in the same way as they physically exist in a real-world system. Parameters can be created and uploaded for each device, and they can be supervised directly.

## 2 USER INTERFACE

### 2.1 TILE STRUCTURE



Figure 1: Tile structure

## 2.2 MENU STRUCTURE

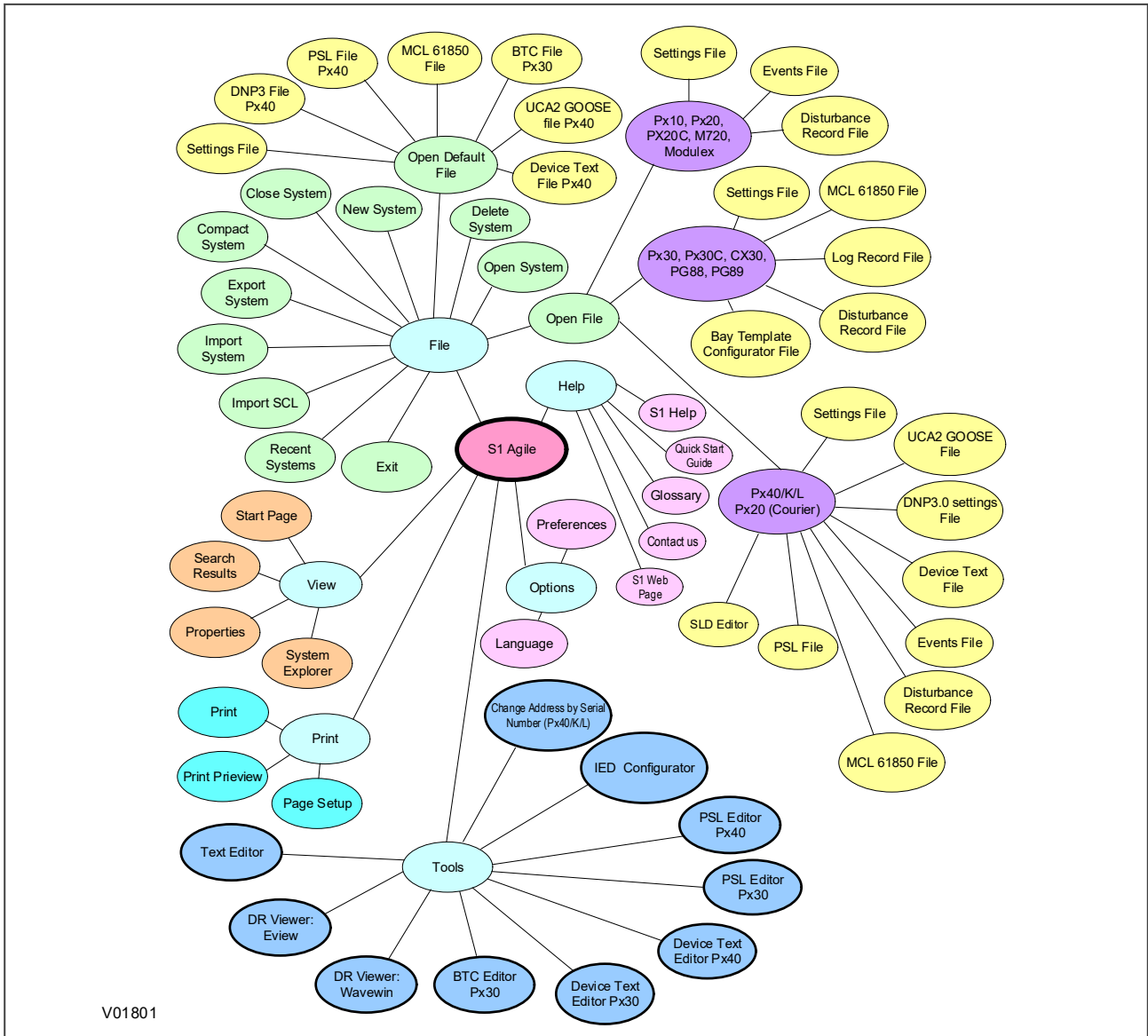


Figure 2: Menu structure

### 3 GETTING STARTED

This Settings Application software allows you to create a model of a power system which simulates a real-world protection system. You can add substations, bays, voltage levels and devices to the system. First you need to download the data models for the devices in the system. Then you can either create a new system or open an existing system. You can connect to an IED either directly through the front port or to an IED in the system model. You can then send or extract settings. You can also extract PSL, Events or Disturbance Record files, as well as certain data protocol files.

If there is no default system, select **Quick Connect** from the menu to automatically create one.

If a system is no longer needed, right-click it and select **Delete** to permanently delete it.

Systems are not opened automatically. To change this, select **Options** then **Preferences** then check the checkbox **Reopen last System at start-up**.

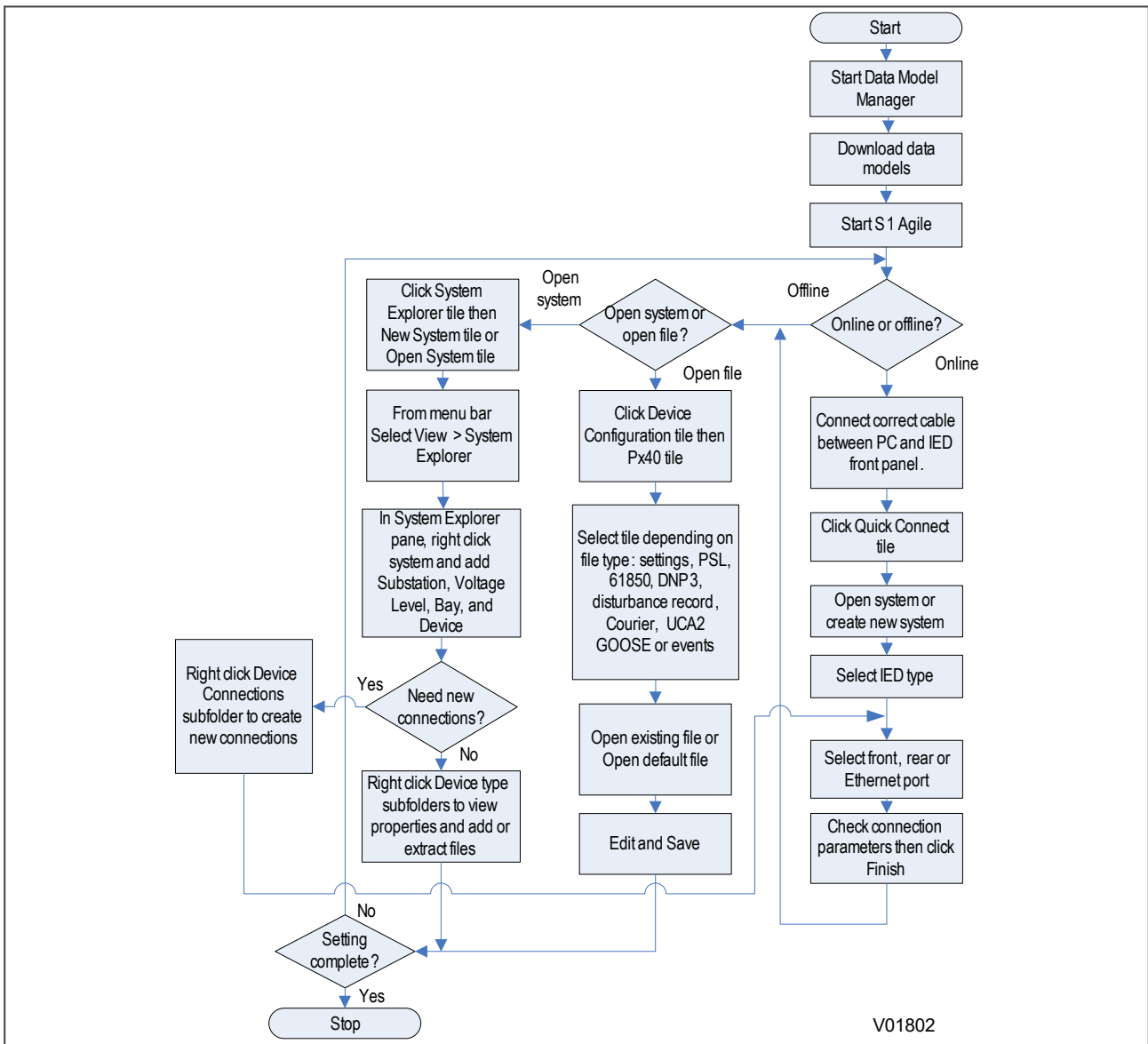


Figure 3: Flowchart showing how S1 Agile can be used to set up and save a protection system offline or online.



---

### 3.1 QUICK SYSTEM GUIDE

S1 Agile allows you to create a model of a protection system which simulates a real-world protection system. You can add substations, bays, voltage levels and devices to the system. First you need to download the data models for the devices in the system. Then you can either create a new system or open an existing system.

You can connect to an IED either directly through the front port or to an IED in the system model. You can then send or extract settings. You can also extract a PSL, DNP3, Events or Disturbance Record file.

If there is no default system, use **Quick Connect** to automatically create one. If a system is no longer needed, right-click it and select **Delete** to permanently delete it.

Systems are not opened automatically. To change this, select **Options** then **Preferences** then check the checkbox **Reopen last System at start-up**.

---

### 3.2 DOWNLOAD DATA MODELS

1. Close S1 Agile and run the Data Model Manager.
2. Follow the on-screen instructions.

---

### 3.3 SET UP A SYSTEM

1. Click the System **Explorer** tile then the **New System** tile or **Open System** tile.
2. From the menu bar select **View** then **System Explorer**.
3. In the System Explorer pane, right click **System** and select **New Substation**, **New Voltage Level**, **New Bay**, and **New Device**.
4. Right-click the **Device** subfolders to view properties and add or extract files.

---

### 3.4 CONNECT TO AN IED

1. Connect the PC and IED as required.
2. From the main screen, click **Quick Connect**.
3. Select the product range.
4. Select connection to the required port.
5. Set the connection parameters and click **Finish**.

---

### 3.5 CONNECT TO AN IED IN A SYSTEM

1. Make sure that the correct physical connection is in place.
2. Find the device in the system explorer and create the appropriate connection. If the connection already exists, right click on it and select the **Test Connection** option.
3. Set the connection parameters and click **Finish**.

---

### 3.6 SEND SETTINGS TO A DEVICE

To send settings to a device there must be at least one setting file in a settings folder for a device.

1. Right-click the device name in System Explorer and select **Send**.
2. In the **Send To** dialog select the setting files and click **Send**.
3. Click **Close** to close the **Send To** dialog.

---

### 3.7 EXTRACT SETTINGS FROM A DEVICE

1. Using System Explorer, find the device.
2. Right-click the device's Settings folder and select **Extract Settings** or **Extract Full Settings**.
3. Once the settings file is retrieved, click **Close**.

---

### 3.8 COMPARE SETTINGS FILES

1. In the System Explorer, find the desired first file to compare.
2. If the two files to be compared are within the same S1 system, right-click the settings file and select **Compare - First File**.
3. Find the second settings file, right-click on it and select **Compare - Second File**.
4. A comparison page will be launched. If the second file was outside of the system, select **Compare with External File** when right clicking on the settings file, then browse for the second file and the same comparison page will be launched.
5. By default, the comparison will show the visible settings that are different between the two files. Any invisible settings due to disabled features will not be compared.
6. At the top left there is a display filter option. Different options are available to select the data presented.
7. Settings can differ in the value or in the user note attached to it.

*Note:*

User Notes can be added to individual cells for MiCOM P40 Agile setting files which can be compared using the setting file comparison. One application example of the User Notes comparison is to add user notes to each setting cell to identify if they should be 'Fixed' or 'Flexible' or are 'Unused'. Then using the setting file comparison these notes can be compared to verify the cells with the User Note 'Fixed' have the same pre-set value and any cell with the User Note 'Flexible' can have different values and any cell with the User Note 'Unused' has a default value. When comparing two setting files with User Notes in each file the columns can be sorted by User Note Name (Ascending or Descending) to make the comparison easier.

---

### 3.9 EXTRACT A DNP3 FILE FROM A DEVICE

1. Using System Explorer, find the device.
2. Right-click the device's **DNP3** folder and select **Extract**.
3. Once the file is retrieved, click **Close**.

---

### 3.10 EXTRACT AN EVENTS FILE FROM A DEVICE

1. Using System Explorer, find the device.
2. Right-click the device's **Events** folder and select **Extract Events**.
3. Once the file is retrieved, click **Close**.

---

### 3.11 EXTRACT A DISTURBANCE RECORD FROM A DEVICE

1. Using System Explorer, find the device.
2. Right-click the device's **Disturbance Records** folder and select **Extract Disturbances**.
3. Select a disturbance record to extract.
4. Choose a COMTRADE format, 1991 or 2001.
5. Click **Extract** or **Save**. Save leaves the record in the device, Extract deletes it.
6. Once the disturbance records file is retrieved, click **Close**.

---

## 4 CYBER SECURITY

---

### 4.1 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.*

---

### 4.2 THE NEED FOR CYBER-SECURITY

Cyber-security 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 cyber-security may be unintentional (e.g. natural disasters, human error), or intentional (e.g. cyber-attacks by hackers).

Good cyber-security 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 cyber-security.

### 4.3 STANDARDS

There are several standards, which apply to substation cyber-security. The standards currently applicable to GE 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 cyber-security 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 cyber-security
CPNI Guidelines (Centre for the Protection of National Infrastructure)	UK	Clear and valuable good practices for Process Control and SCADA security

#### 4.3.1 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 standard	Description
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 Cyber-security Incidents relating to Critical Cyber Assets are identified
CIP-009-1 Recovery Plans	Define and document Recovery plans for Critical Cyber Assets

**4.3.1.1 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'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

**4.3.1.2 CIP 003**

CIP 003 requires the implementation of a cyber-security 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's contribution:
To create a Cyber-security 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.

**4.3.1.3 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's contribution:
To provide appropriate training of its personnel	We can provide cyber-security training

**4.3.1.4 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'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

**4.3.1.5 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'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 cannot provide additional help with this aspect.

**4.3.1.6 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'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

**4.3.1.7 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's contribution:
To provide an incident response team and have appropriate processes in place.	GE cannot provide additional help with this aspect.

**4.3.1.8 CIP 009**

CIP 009 states that a disaster recovery plan should be created and tested with annual drills.

Power utility responsibilities:	GE's contribution:
To implement a recovery plan	To provide guidelines on recovery plans and backup/restore documentation

**4.3.2 IEEE 1686-2013**

IEEE 1686-2013 is an IEEE Standard for substation IEDs' cyber-security 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.

---

## 4.4 CYBER-SECURITY IMPLEMENTATION

General Electric 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).

### 4.4.1 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.

## 4.5 ROLES AND PERMISSIONS

### 4.5.1 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
<b>VIEWER</b>	VIEWER	Level 0
<b>OPERATOR</b>	OPERATOR	Level 1
<b>ENGINEER</b>	ENGINEER	Level 2
<b>ADMINISTRATOR</b>	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
<b>ADMINISTRATOR</b>	ChangeMe1#
<b>ENGINEER</b>	ChangeMe1#
<b>OPERATOR</b>	ChangeMe1#
<b>VIEWER</b>	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.

#### 4.5.2 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
<b>VIEWER</b>	x			x							
<b>OPERATOR</b>	x	x		x				x			
<b>ENGINEER</b>	x	x	x	x		x	x		x		
<b>ADMINISTRATOR</b>	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

## 4.6 AUTHENTICATION

### 4.6.1 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*.

### 4.6.2 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
<i>Disabled</i>				
<i>Local &amp; Remote</i>	X	X	X	X
<i>Local</i>	X	X		
<i>Remote</i>			X	X
<i>HMI-Only</i>	X			

The DDB signal **Security Bypass** is available to indicate that the IED is in **Bypass Auth.** mode.

### 4.6.3 LOGIN

A user can only login through the following methods:

- Front Panel User Interface
- Using MiCOM S1 Agile, connected to either the Front Port, Rear Port 1 or 2, or NIC (Ethernet) interface.

The interfaces/protocols implemented in P40 are listed in the following table.

The product supports both RBAC (with *Server + Device* authentication) and original Access Level. The Courier Interfaces/HMI use the RBAC whilst other protocols such as MODBUS, IEC 60870-5-103, DNP3 use the original Access Level to authenticate.

The following table shows different product variants that supports different protocols on Rear ports and Network port.

Local Access	Front Port	Rear Port (1/2)	NIC (Ethernet) Port	Supported Auth. Mechanism
HMI Courier	Courier	Courier	-	Device
HMI Courier	Courier	Courier	IEC 61850 + SNMP + Courier tunnel	Server and Device
HMI Courier	Courier	MODBUS (no server, device auth only, old access levels)	-	Device Old Access level for MODBUS
HMI Courier	Courier	IEC 60870-5-103 (no server, device auth only, old access levels)	-	Device Old Access level for 103
HMI Courier	Courier	IEC 60870-5-103 (no server, device auth only, old access levels)	IEC 61850 + SNMP + Courier tunnel	Server and Device Old Access level for 103
HMI Courier	Courier	DNP3 (no server, device auth only, old access levels)	-	Device Old Access level for DNP3
HMI Courier	Courier	Courier	DNP3 + SNMP + Courier tunnel	Server and Device Old Access level for DNP3

#### 4.6.3.1 FRONT PANEL LOGIN

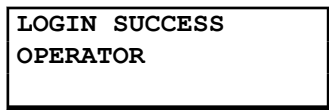
Front panel User Interface supports both Device authentication and Server authentication. The P40 gives the user the option to enter a username in HMI panel.

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:



A rectangular box with a black border containing the text "LOGIN SUCCESS" on the first line and "OPERATOR" on the second line.

#### 4.6.3.2 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.

#### 4.6.3.3 WARNING BANNER

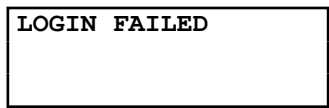
After successful authentication and authorisation to access the IED, MiCOM S1 Agile will display a security warning banner to the user.

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.

#### 4.6.3.4 LOGIN FAILED

When Device authentication fails, a failure message is displayed:



A rectangular box with a black border containing the text "LOGIN FAILED" on the first line.

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.

#### 4.6.4 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 InactivTimer**
- **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.

#### 4.6.5 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
```

Username 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.

#### 4.6.6 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.

##### 4.6.6.1 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
```

##### 4.6.6.2 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**.

#### 4.6.7 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.

#### 4.6.8 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.

#### 4.6.9 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.

#### 4.6.10 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.

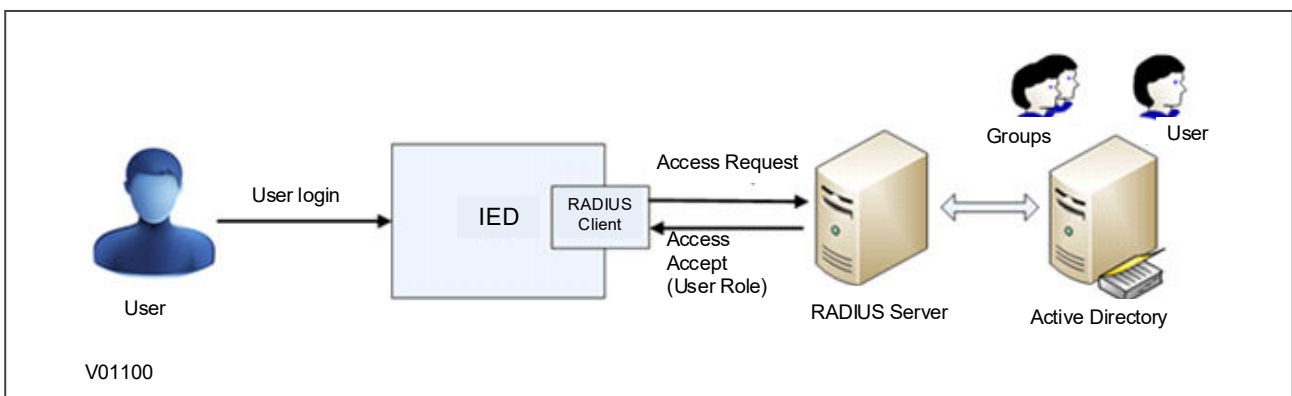


Figure 4: RADIUS server/client communication



#### 4.6.10.1 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).

#### 4.6.10.2 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
<b>P40 Role Values</b>	
Administrator	3
Engineer	2
Operator	1
Viewer	0

#### 4.6.10.3 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

Setting Name	Description	Min	Max	Default	Units	Minimum Permissions
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*.

#### 4.6.10.4 RADIUS ACCOUNTING

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

#### 4.6.10.5 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.

#### 4.6.11 RECOVERY

##### 4.6.11.1 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.

#### 4.6.11.2 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 and the security code. The Contact Centre will use these items to generate a Recovery Password.

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.*

#### 4.6.11.3 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

#### 4.6.12 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.*

#### 4.6.13 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.*

## 4.7 SECURITY EVENT MANAGEMENT

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

### 4.7.1 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}

Event Value	Display
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 CONFIG D/LOAD BY {int}
USER CURVES DOWNLOADED	USER CRV D/LOAD BY {int} GROUP {crv}
PSL CONFIG DOWNLOADED	PSL CONFIG 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 CONFIG UPLOAD BY {int}
USER CURVES UPLOADED	USER CRV UPLOAD BY {int} GROUP {crv}
PSL CONFIG UPLOADED	PSL CONFIG UPLOAD BY {int} GROUP {grp}
SETTINGS UPLOADED	SETTINGS UPLOAD BY {int} GROUP {grp}
EVENTS HAVE BEEN EXTRACTED	EVENTS EXTRACTED BY {int} {nov} EVNTS

Event Value	Display
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.*

#### 4.7.2 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)

### 4.7.3 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

### 4.7.4 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:	<pre>&lt;38&gt;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 &lt;38&gt;1 2018-02-06T11:46:32.074Z Feeder1 userlog - 9999 [timeQuality tzKnown=0][geUserInfo channel=UI loginId=user1] Login - Authentication successful</pre>	

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	04-19-2019 13:36:08 Auth.Info 192.168.1.30 1 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)	04-17-2019 15:29:20 Auth.Info 192.168.1.30 1 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	04-19-2019 13:52:08 Auth.Info 192.168.1.30 1 1994-01-25T20:42:42.782Z 192.168.1.30 userlog - 9999 [timeQuality tzKnown=0][geUserInfo channel=RP1 loginid=ADMINISTRATOR] Logout
RADIUS Unavailable	FP	04-18-2019 12:40:14 Auth.Alert 192.168.1.30 1 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	04-18-2019 12:39:19 Auth.Warning 192.168.1.30 1 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	04-18-2019 11:52:35 Auth.Notice 192.168.1.30 1 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

## 5 PSL EDITOR

The Programmable Scheme Logic (PSL) is a module of programmable logic gates and timers in the IED, which can be used to create customised internal logic. This is done by combining the IED's digital inputs with internally generated digital signals using logic gates and timers, then mapping the resultant signals to the IED's digital outputs and LEDs.





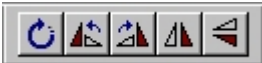
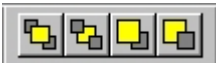

The Programmable Scheme Logic (PSL) Editor allows you to create and edit scheme logic diagrams to suit your own particular application.

### 5.1 LOADING SCHEMES FROM FILES

The product is shipped with default scheme files. These can be used as a starting point for changes to a scheme. To create a new blank scheme, select **File** then **New** then **'Blank scheme...'** to open the default file for the appropriate IED. This deletes the diagram components from the default file to leave an empty diagram but with the correct configuration information loaded.

### 5.2 PSL EDITOR TOOLBAR




There are a number of toolbars available to help with navigating and editing the PSL.




















Toolbar	Description
	Standard tools: For file management and printing.
	Alignment tools: To snap logic elements into horizontally or vertically aligned groupings.
	Drawing tools : To add text comments and other annotations, for easier reading of PSL schemes.
	Nudge tools: To move logic elements.
	Rotation tools: Tools to spin, mirror and flip.
	Structure tools: To change the stacking order of logic components.
	Zoom and pan tools: For scaling the displayed screen size, viewing the entire PSL, or zooming to a selection.

#### 5.2.1 LOGIC SYMBOLS

The logic symbol toolbar provides icons to place each type of logic element into the scheme diagram. Not all elements are available in all devices. Icons are only displayed for elements available in the selected device.



Symbol	Function	Explanation
	Link	Create a link between two logic symbols.
	Opto Signal	Create an opto-input signal.
	Input Signal	Create an input signal.

Symbol	Function	Explanation
	Output Signal	Create an output signal.
	GOOSE In	Create an input signal to logic to receive a GOOSE message transmitted from another IED. Used in either UCA2.0 or IEC 61850 GOOSE applications only.
	GOOSE Out	Create an output signal from logic to transmit a GOOSE message to another IED. Used in either UCA2.0 or IEC 61850 GOOSE applications only.
	Control In	Create an input signal to logic that can be operated from an external command.
	InterMiCOM In	Create an input signal to logic to receive an InterMiCOM command transmitted from another IED.
	InterMiCOM Out	Create an output signal from logic to transmit an InterMiCOM command to another IED.
	Off-page left	Create an output Off-page connector for the off page right connector.
	Off-page right	Create an input Off-page connector to replicate elsewhere in the diagram.
	Function Key	Create a function key input signal.
	Trigger Signal	Create a fault record trigger.
	LED Signal	Create an LED input signal that repeats the status of tri-colour LED.
	Contact Signal	Create a contact signal.
	LED Conditioner	Create an LED conditioner.
	Contact Conditioner	Create a contact conditioner.
	Timer	Create a timer.
	AND Gate	Create an AND Gate.
	OR Gate	Create an OR Gate.
	Programmable Gate	Create a programmable gate.
	Counter	Gate that can add pulses to a configurable threshold.

### 5.3 LOGIC SIGNAL PROPERTIES

1. Use the logic toolbar to select logic signals. This is enabled by default but to hide or show it, select **View** then **Logic Toolbar**.
2. Zoom in or out of a logic diagram using the toolbar icon or select **View** then **Zoom Percent**.
3. Right-click any logic signal and a context-sensitive menu appears.

Certain logic elements show the **Properties** option. If you select this, a **Component Properties** window appears. The contents of this window and the signals listed will vary according to the logic symbol selected. The actual DDB numbers are dependent on the model.

### 5.3.1 LINK PROPERTIES

Links form the logical link between the output of a signal, gate or condition and the input to any element. Any link connected to the input of a gate can be inverted. To do this:

1. Right-click the input
2. Select **Properties...** The Link Properties window appears.
3. Check the box to invert the link. Or uncheck for a non-inverted link

An inverted link is shown with a small circle on the input to a gate. A link must be connected to the input of a gate to be inverted.

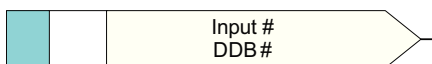
Links can only be started from the output of a signal, gate, or conditioner, and must end at an input to any element.

Signals can only be an input or an output. To follow the convention for gates and conditioners, input signals are connected from the left and output signals to the right. The Editor automatically enforces this convention.

A link is refused for the following reasons:

- There has been an attempt to connect to a signal that is already driven. The reason for the refusal may not be obvious because the signal symbol may appear elsewhere in the diagram. In this case you can right-click the link and select Highlight to find the other signal. Click anywhere on the diagram to disable the highlight.
- An attempt has been made to repeat a link between two symbols. The reason for the refusal may not be obvious because the existing link may be represented elsewhere in the diagram.

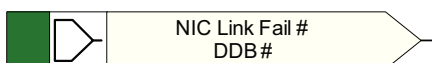
### 5.3.2 OPTO SIGNAL PROPERTIES



E02030

Each opto-input can be selected and used for programming in PSL. Activation of the opto-input drives an associated DDB signal.

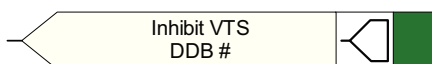
### 5.3.3 INPUT SIGNAL PROPERTIES



E02031

IED logic functions provide logic output signals that can be used for programming in PSL. Depending on the IED functionality, operation of an active IED function drives an associated DDB signal in PSL.

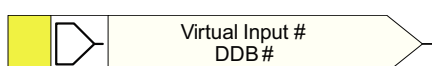
### 5.3.4 OUTPUT SIGNAL PROPERTIES



E02032

Logic functions provide logic input signals that can be used for programming in PSL. Depending on the functionality of the output relay, when the output signal is activated, it drives an associated DDB signal in PSL. This causes an associated response to the function of the output relay.

### 5.3.5 GOOSE INPUT SIGNAL PROPERTIES

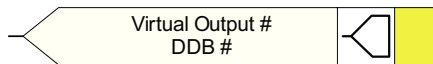


E02033

The Programmable Scheme Logic interfaces with the GOOSE Scheme Logic through 32 Virtual Inputs. The Virtual Inputs can be used in much the same way as the opto-input signals.

The logic that drives each of the Virtual Inputs is contained in the GOOSE Scheme Logic file. You can map any number of bit-pairs from any subscribed device using logic gates onto a Virtual Input.

### 5.3.6 GOOSE OUTPUT SIGNAL PROPERTIES

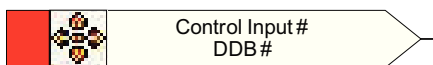


E02034

The Programmable Scheme Logic interfaces with the GOOSE Scheme Logic through 32 Virtual Outputs.

You can map Virtual Outputs to bit-pairs for transmitting to any subscribed devices.

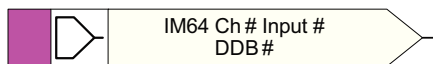
### 5.3.7 CONTROL INPUT SIGNAL PROPERTIES



E02035

There are 32 control inputs which can be activated using the menu, the hotkeys or through courier communications. Depending on the programmed setting that is latched or pulsed, when a control input is operated an associated DDB signal is activated in PSL.

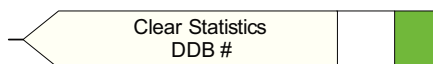
### 5.3.8 INTERMICOM INPUT PROPERTIES



E02036

There are 16 InterMiCOM inputs that can be used for teleprotection and remote commands. **InterMiCOM In** is a signal which is received from the remote end. It can be mapped to a selected output relay or logic input.

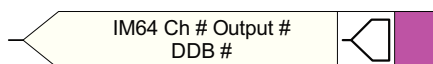
#### IED End B



E02037

At end B, InterMiCOM Input 1 is mapped to the command **Clear Statistics**.

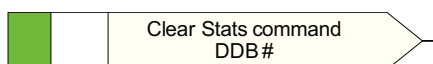
### 5.3.9 INTERMICOM OUTPUT PROPERTIES



E02038

There are 16 InterMiCOM outputs that can be used for teleprotection and remote commands. **InterMiCOM Out** is a send command to a remote end that can be mapped to any logic output or opto-input. This is transmitted to the remote end as a corresponding **InterMiCOM In** command.

#### IED End A



E02039

At end A, InterMiCOM Output 1 is mapped to the command indication **Clear Statistics** issued at end A.

### 5.3.10 FUNCTION KEY PROPERTIES



E02040

Each function key can be selected and used for programming in PSL. Activation of the function key drives an associated DDB signal. The DDB signal remains active according to the programmed setting (toggled or normal). Toggled mode means the DDB signal remains in the new state until the function key is pressed again. In Normal mode, the DDB is only active while the key is pressed.

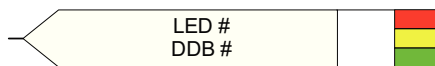
### 5.3.11 FAULT RECORDER TRIGGER PROPERTIES



E02041

The fault recording facility can be activated by driving the fault recorder trigger DDB signal.

### 5.3.12 LED SIGNAL PROPERTIES



E02042

All programmable LEDs drive associated DDB signals when the LED is activated.

### 5.3.13 CONTACT SIGNAL PROPERTIES



E02043

All output relay contacts drive associated DDB signal when the output contact is activated.

### 5.3.14 LED CONDITIONER PROPERTIES

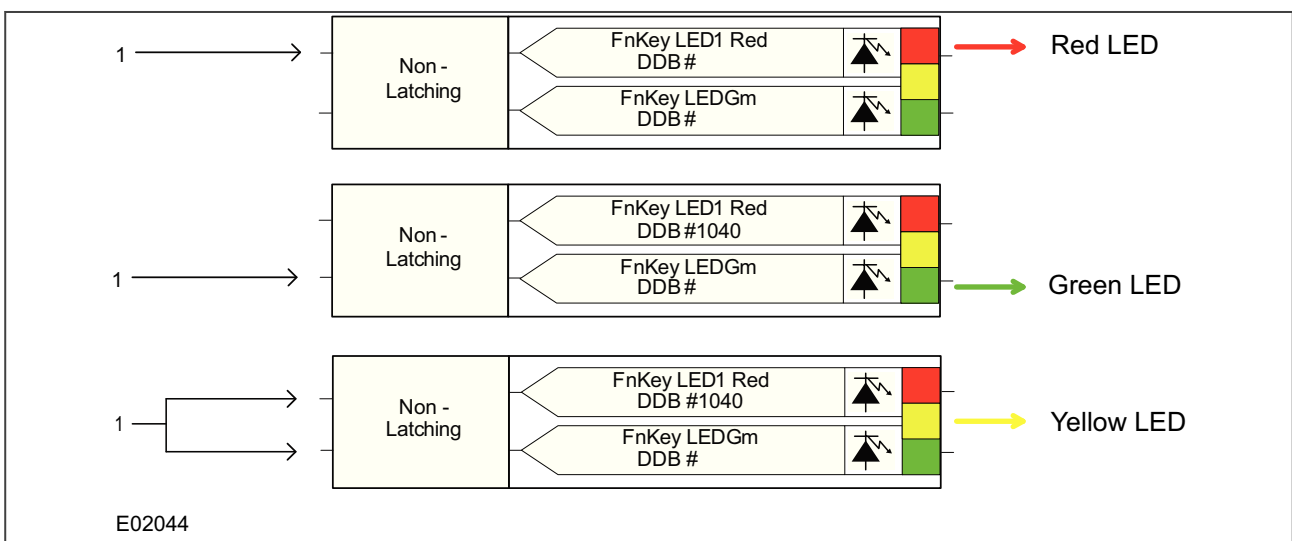


Figure 5: Examples of how to set Red, Green and Yellow LEDs

To set LED conditioner properties,

1. Select the LED name from the list (only shown when inserting a new symbol).
2. Configure the LED output to be Red, Yellow or Green.
3. Configure a Green LED by driving the Green DDB input.
4. Configure a RED LED by driving the RED DDB input.
5. Configure a Yellow LED by driving the RED and GREEN DDB inputs simultaneously.
6. Configure the LED output to be latching or non-latching.

### 5.3.15 CONTACT CONDITIONER PROPERTIES

Each contact can be conditioned with an associated timer that can be selected for pick up, drop off, dwell, pulse, pick-up/drop-off, straight-through, or latching operation.

**Straight-through** means it is not conditioned at all whereas **Latching** is used to create a sealed-in or lockout type function.

To set contact properties,

1. Select the contact name from the **Contact Name** list (only shown when inserting a new symbol).
2. Choose the conditioner type required in the **Mode** tick list.
3. Set the **Pick-up Value** (in milliseconds), if required.
4. Set the **Drop-off Value** (in milliseconds), if required.

### 5.3.16 COUNTER PROPERTIES

Each PSL counter has an increment (+), a decrement (-) and Reset (R) input and a count output (Q) which goes high when the count threshold value is exceeded.

To set counter properties,

1. From the **Trigger Type** tick list, choose either, **Rising edge triggered** or **Falling edge triggered**.
2. Set the **Trigger threshold value**, if required.
3. Set the **Invert output** tick box, if required.
4. From the **Available counters** list, choose the counter required. Note: The counter number will auto-increment when adding counters.
5. Click **OK**.

*Note:*

*The counter threshold can be set in the menu settings, System Config - Counters 1-16 settings if the **CounterSourcePSL** setting = 0000000000000000 for all 16 counters. If the **CounterSourcePSL** setting = 1111111111111111, all 16 counters can be set via the counter properties in the PSL.*

### 5.3.17 TIMER PROPERTIES

Each timer can be selected for pick-up, drop-off, dwell, pulse or pick-up/drop-off operation.

To set timer properties,

1. From the **Timer Mode** tick list, choose the mode.
2. Set the **Pick-up Value** (in milliseconds), if required.
3. Set the **Drop-off Value** (in milliseconds), if required.
4. From the **Available timers** list (not in all products), choose the timer required. Note: The timer number will auto-increment when adding timers.
5. Click **OK**.



### 5.3.18 GATE PROPERTIES

A gate can be an AND, OR, or programmable gate.

- An **AND Gate** requires that all inputs are TRUE for the output to be TRUE.
- An **OR Gate** requires that one or more input is TRUE for the output to be TRUE.
- A **Programmable Gate** requires that the number of inputs that are TRUE is equal to or greater than its **Inputs to Trigger** setting for the output to be TRUE.

To set gate properties,

1. Select the gate type: **AND Gate**, **OR Gate**, or **Programmable Gate**.
2. If you select **Programmable Gate**, set the number of **Inputs to Trigger**.
3. If you want the output of the gate to be inverted, check the **Invert Output** check box. An inverted output appears as a "bubble" on the gate output.
4. Click **OK**.

### 5.3.19 OFF-PAGE CONNECTOR PROPERTIES

The Scheme Logic Editor Off-page connectors, also known as variables, allows the visual scheme logic to be displayed without the links breaking over multiple pages. As a result this makes viewing printed schemes much easier.

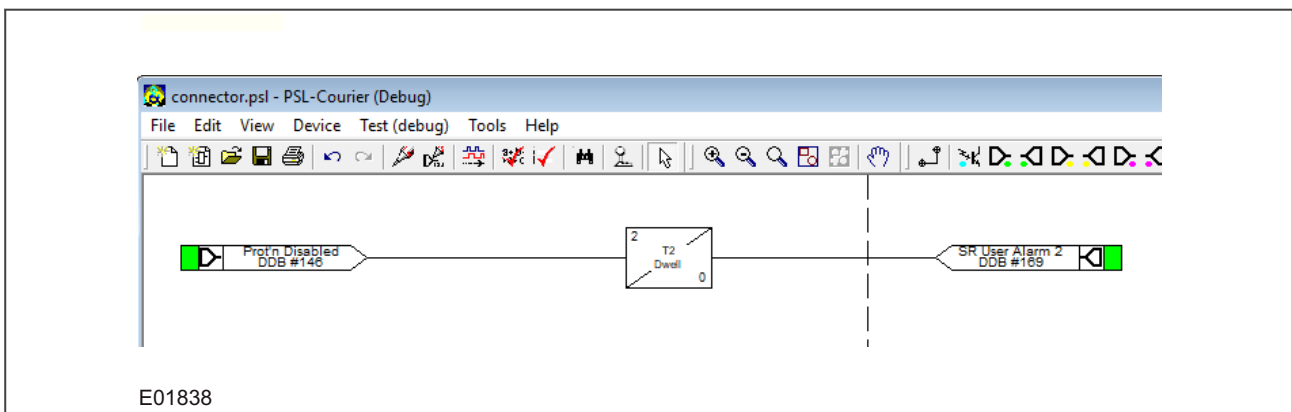


Figure 6: Scheme over 2 pages

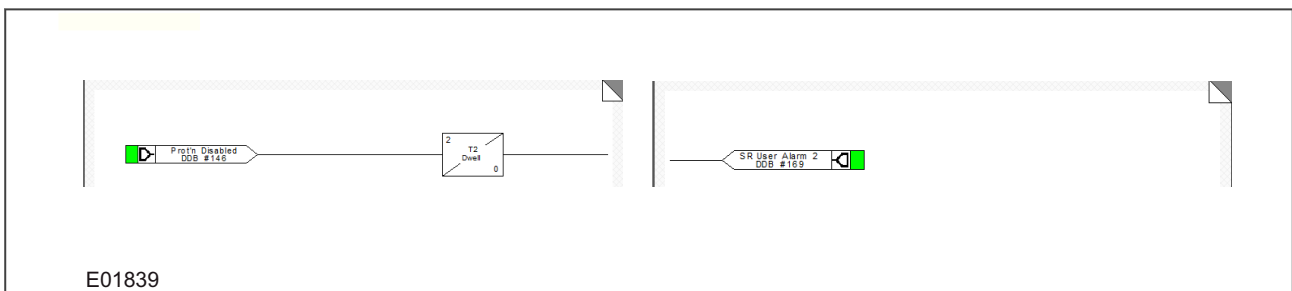


Figure 7: Scheme when printed

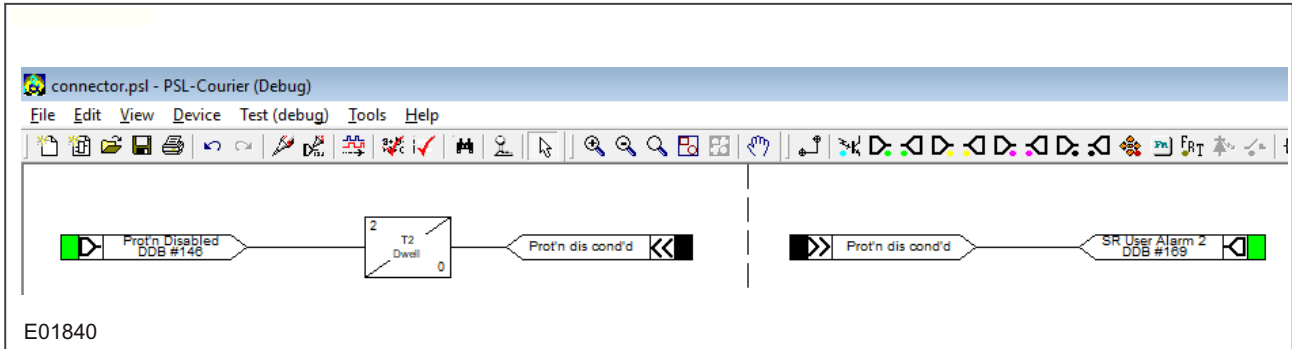


Figure 8: Scheme using Off-page connectors

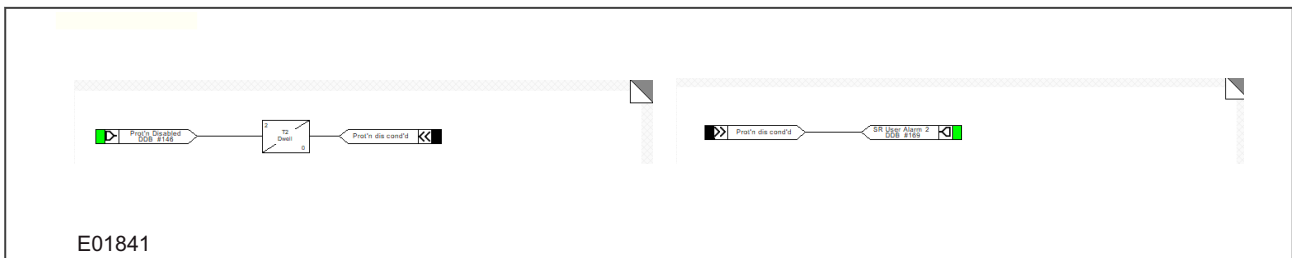


Figure 9: Scheme with Off-page connectors when printed

### 5.3.19.1 USING OFF-PAGE CONNECTORS

From version 2.1 onwards the PSL Editor includes two additional connector buttons on the Logic Toolbar. The Off-Page connector buttons sit in-between the InterMiCOM Out signal and the Control Input signal.

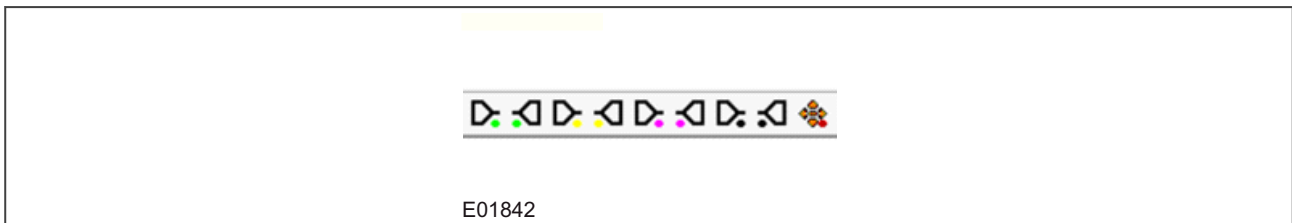


Figure 10: Off-page connector buttons

The input connector to the Scheme typically appears to the left of the page and the output from the Scheme is to the right of the page, as shown in the Scheme using Off-page connectors figure.

To add the connectors:

1. Click on the Off-page button then place the component where it is needed. The Off-page connector properties dialog box will now pop up.
2. The new connector can be assigned from an existing list of Off-page connectors, or given a new name.
3. To add a new name click on the **Add new/rename one...** button. There is no length restriction but longer names will overspill the signal shape.
4. The name will now appear in any further Off-page connector additions. Additionally, it will appear in the Properties dialog when using the Off-page connector menu.

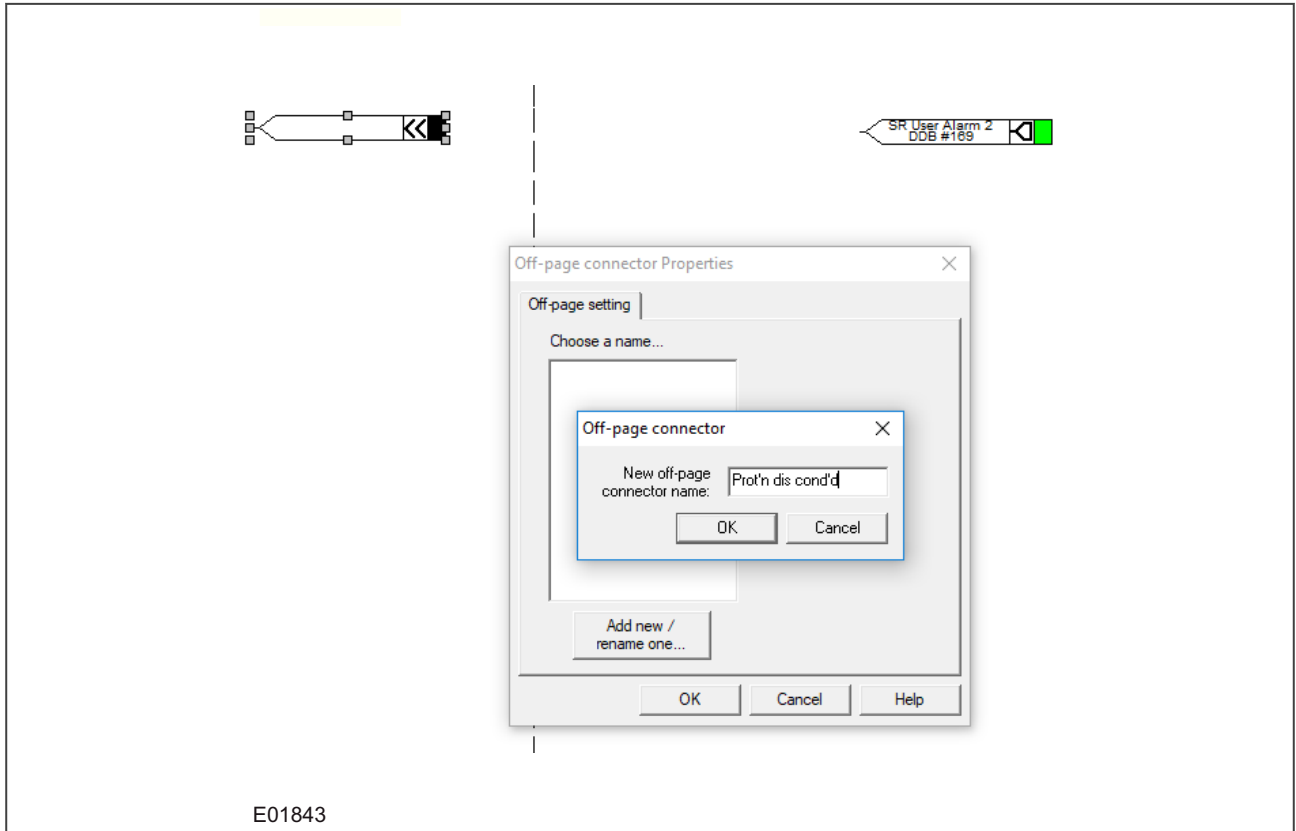


Figure 11: Off-page connector properties

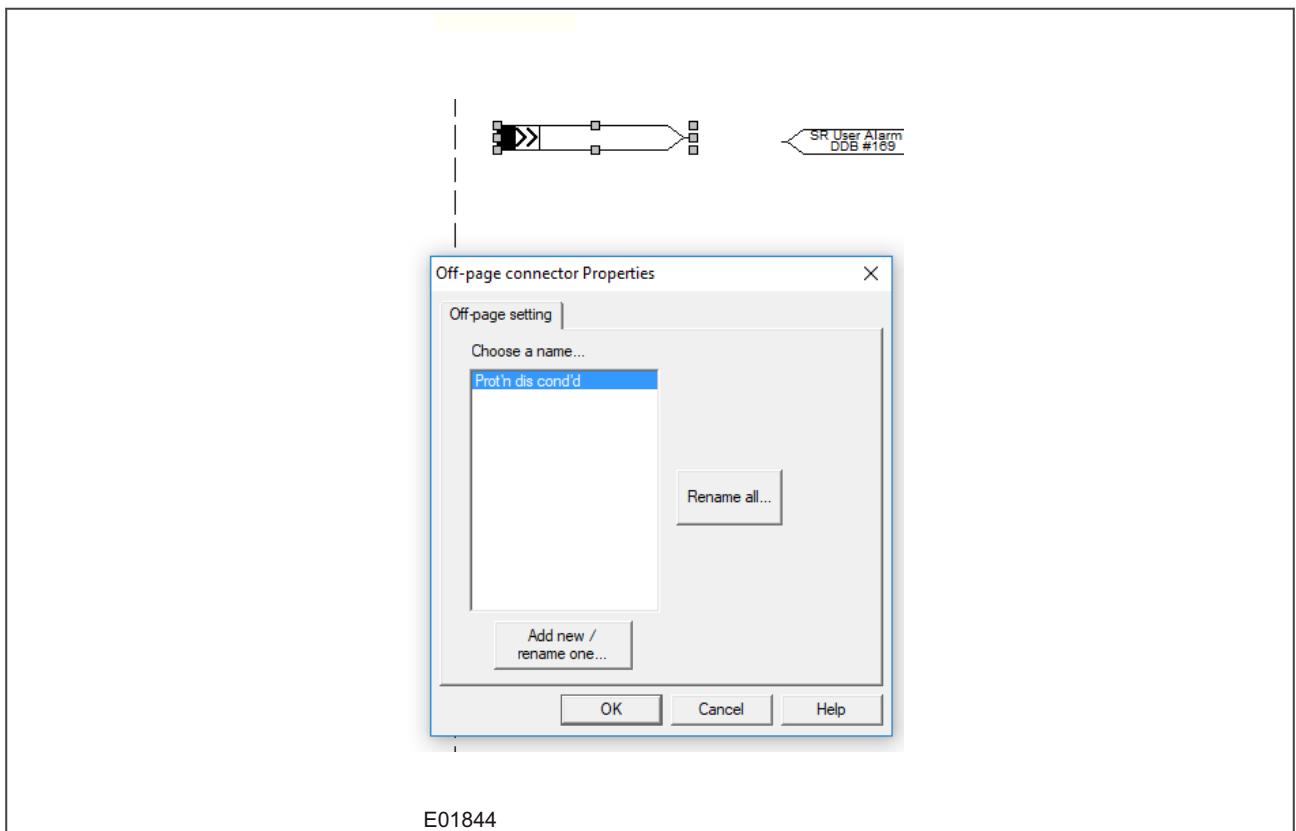


Figure 12: Subsequent OPC addition

### 5.3.19.2 RULES

When it comes to using Off-page connectors in your schemes there are a few rules to note. They are as follows:

1. There is no limit to the number of Off-page connectors that can be placed on the diagram, other than within the constraints of the S1 space within the relay file. The S1 file is stored in the relay flash memory and each Off-page connector occupies only a small amount of space.
2. All OPCs with the same name are logically the same signal so they will be internally 'wired' to each other.
3. A connection can only be made from a logical output signal or input OPC to an output OPC.
4. A connection can only be made from an input OPC to a logical input signal or output OPC.
5. An input OPC can be connected to an output OPC. As shown in the Subsequent OPC addition figure above.
6. When the last OPC with a specific name has been deleted from the Scheme, it will not appear in the OPC Properties list.

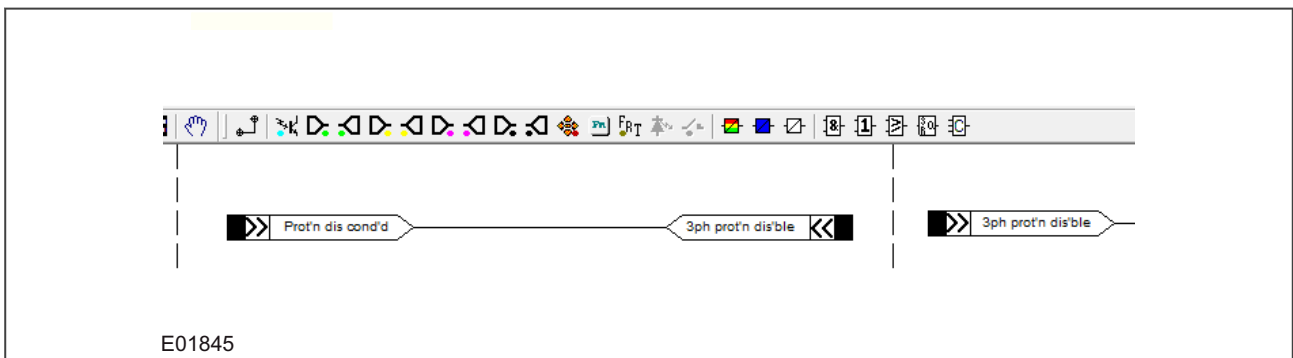


Figure 13: Wiring OPCs together

### 5.3.19.3 EXAMPLES

The following examples show some valid possible uses of the Off-page connectors.

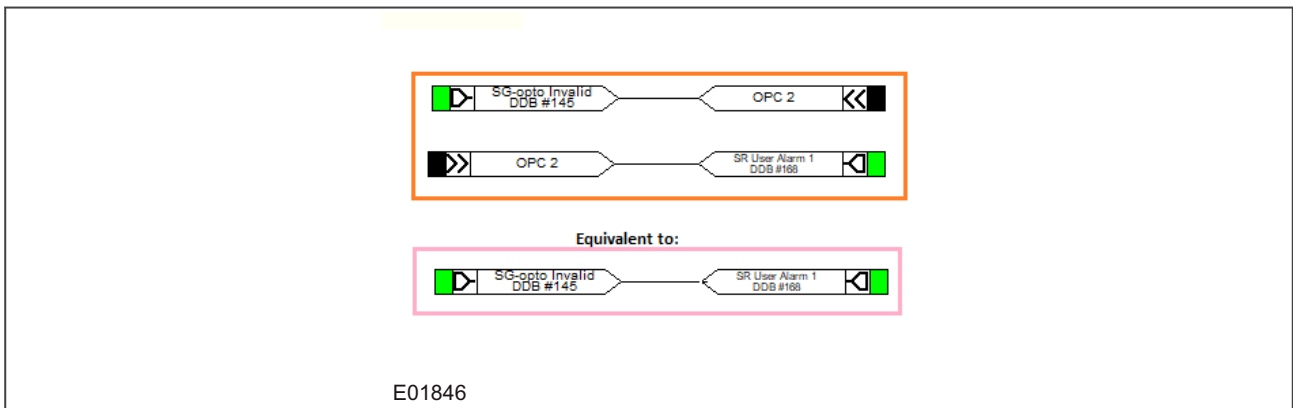


Figure 14: Example 1

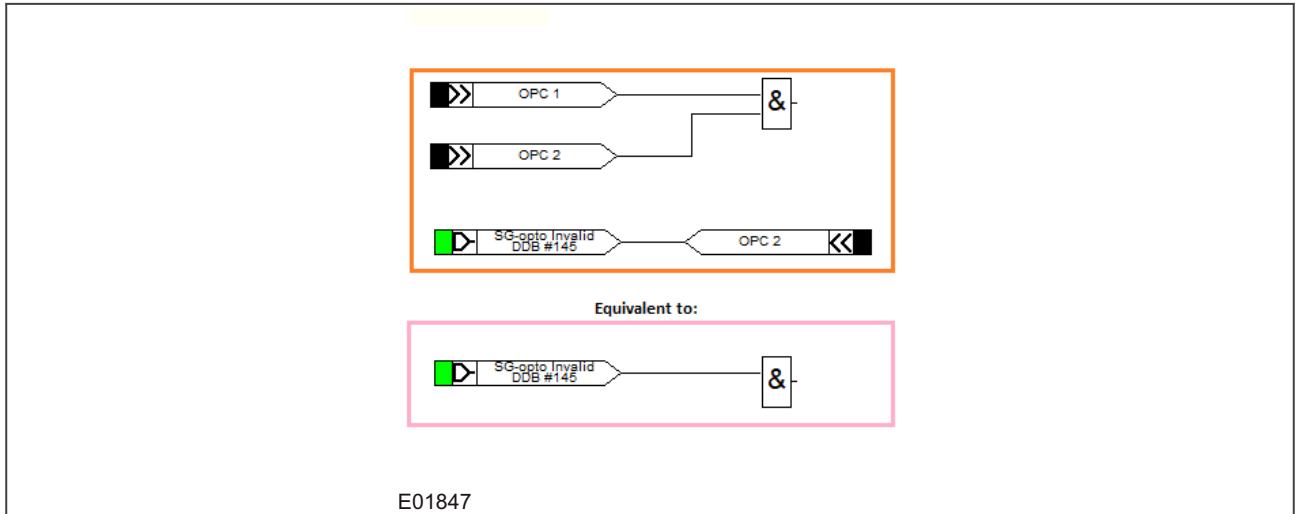


Figure 15: Example 2

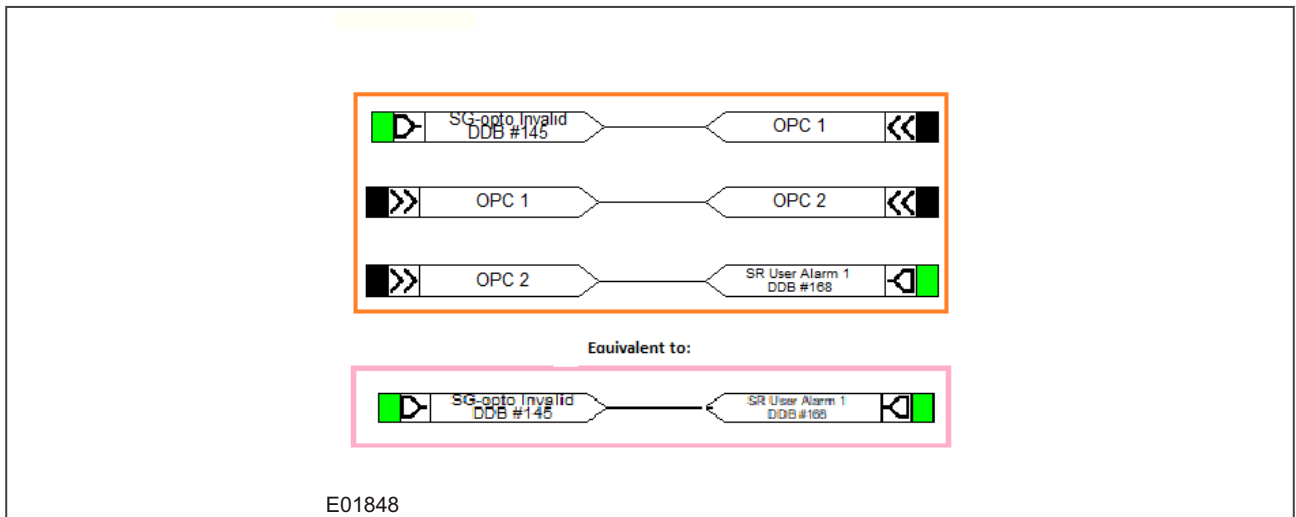


Figure 16: Example 3

The following examples show some invalid ways of connecting the Off-page connectors.

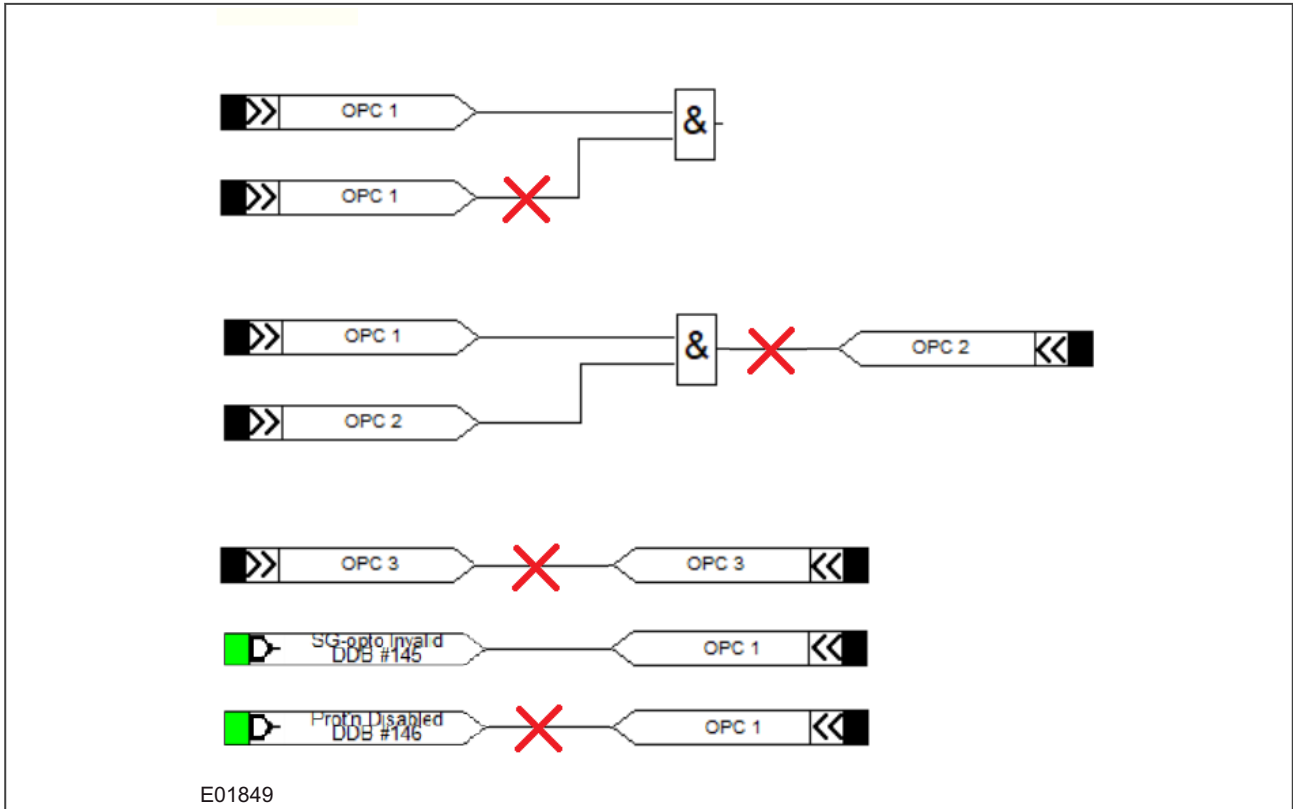


Figure 17: Example 4

### 5.3.20 SR PROGRAMMABLE GATE PROPERTIES

A Programmable SR gate can be selected to operate with the following three latch properties:

Set	Reset	Q0 (Previous Output State)	Q1 Set Dominant	Q1 Reset Dominant	Q1 No Dominance
0	0	0	0	0	0
0	0	1	1	1	1
0	1	1	0	0	0
0	1	0	0	0	0
1	1	0	1	0	0
1	1	1	1	0	1
1	0	1	1	1	1
1	0	0	1	1	1

Q0 is the previous output state of the latch before the inputs change. Q1 is the output of the latch after the inputs change.

The Set dominant latch ignores the Reset if the Set is on.

The Reset Dominant latch ignores the Set if the Reset is on.

When both Set and Reset are on, the output of the non-dominant latch depends on its previous output Q0. Therefore if Set and Reset are energised simultaneously, the output state does not change.

*Note:*  
Use a set or reset dominant latch. Do not use a non-dominant latch unless this type of operation is required.

## SR latch properties

In the Component Properties dialog, you can select S-R latches as **Standard (no input dominant)**, **Set input dominant** or **Reset input dominant**.

If you want the output to be inverted, check the **Invert Output** check box. An inverted output appears as a "bubble" on the gate output.

---

## 5.4 PSL CONVERTER

The PSL Converter allows you to import PSL files from products with very slightly different CORTECs such as protocol support or case size.

### 5.4.1 PSL CONVERTER PREREQUISITES

The PSL Converter performs the following checks to ensure compatibility between the PSL file to be converted and the default PSL file of the destination IED.

- The first four characters of the IED number must match.
- The default file of the destination IED must exist.
- Only the configuration of the destination IED's default file is used.
- The maximum configured number of optos, contacts and LEDs must match.
- Each DDB used in the scheme must be of the same type and source as the default. The actual DDB names are ignored, so the destination model's default file can be in any language.
- The number of DDBs in the source and destination files must be the same.

### 5.4.2 FILE CONVERSION

To convert a PSL file:

1. From the PSL Editor, press Ctrl + Alt + Z simultaneously to launch the PSL Conversion wizard. Keep in mind the restrictions on PSL conversion.
2. Follow the instructions in the model conversion wizard.

---

## 5.5 DDB MONITORING

The status of the DDB signals can be monitored live by using the DDB Monitor Signals feature. This allows the user to visually confirm the status of all the logic elements during transitions using the diagram as reference, making it easier and faster to confirm that the designed logic acts as expected.

### 5.5.1 DDB MONITORING PREREQUISITES

The PSL Editor needs to connect to the IED before monitoring is available. This is an online only feature.

1. First go to **Device** and select **Comms Setup**. The program can take up to one minute to display the next window.
2. Select the correct connection option. If using the P40U converter the COM port should be offered, the **Scheme** section will be empty, and the communication parameters will be correct in the landing page, press **OK** if that is the case. If connecting using any other means, choose the right option in the **Scheme** section. We recommend changing in **Transaction Values** the **Reset Response Time** to 1000 ms.
3. Make sure the PSL file that corresponds to what the relay has, is opened. The best way to ensure this is by sending the file just before testing. On a live relay the preferred option is to use the original PSL file sent, over a recovered PSL file. Before any monitoring is done make sure there is a match in the CRC calculation in the relay (found in the *PSL DATA* menu on the HMI) and the file (located in **Tools** then **Calculate CRC**)

### 5.5.2 SETTING THE DDB MONITORING SESSION

To start the DDB monitoring session:

1. From the PSL Editor, select **Tools** then **Monitor DDB Signals**.
2. When prompted select the option for **Real** values. The Demo option is used for tool R&D purposes only and has no significance for an end user.
3. To begin the first recording session, select the time interval desired for each sample. The lowest value is 0.1 second and this is the fastest speed at which the tool can poll the values of the DDBs. Once chosen select **Start Monitoring**.
4. When the monitoring is activated, DDB signals and links with a value of 1 (ON) are shown in red colour. DDB signals with a value of 0 (OFF) are shown in blue colour. The values of the DDBs will be updated every selected sample interval.

*Note:*

*The relay will still update the PSL file internally at the same speed, the actual PSL file is calculated a lot faster 0.1 seconds but it is not possible to record this in the monitoring as it would affect the relay's performance.*

### 5.5.3 SAVING THE DDB MONITORING SESSION

In most applications, the live monitoring will suffice to verify the integrity of the design of the PSL. However it is possible to save the recording session and rewatch it for slower analysis or for sharing with someone that wasn't present at capture time. To save the monitoring session:

1. Stop the monitoring session if it is still running.
2. On the bottom right corner of the **Monitor DDB Signals** section select the **Save as...** button in the DDB monitor file section.
3. Select a location to store the recording file.

### 5.5.4 PLAYING THE DDB MONITORING SESSION

To play back a recorded DDB Monitoring session:

1. Open the PSL file that corresponds to the recorded session.
2. From the PSL Editor, select **Tools** then **Monitor DDB Signals**.
3. On the bottom right corner of the **Monitor DDB Signals** section select the **Load** button in the DDB monitor file section and locate the recording file.
4. In the **Playback** section, select the playback interval.

*Note:*

*A PSL can be recorded at a fast speed and played back at a slower speed to allow time for the user to see what changes happened between samples.*

## 5.6 VIEWING AND PRINTING PSL DIAGRAMS

You can view and print the PSL diagrams for the device. Typically these diagrams allow you to see the following mappings:

- Opto Input Mappings
- Output Relay Mappings



- LED Mappings
- Start Indications
- Phase Trip Mappings
- System Check Mapping

To download the default PSL diagrams for the device and print them:

1. Close the Settings Application Software.
2. Start the **Data Model Manager**.
3. Click **Add** then **Next**.
4. Click **Internet** then **Next**.
5. Select your language then click **Next**.
6. From the tree view, select the model and software version.
7. Click **Install**. When complete click **OK**.
8. Close the Data Model Manager and start the Settings Application Software.
9. Select **Tools** then **PSL Editor (Px40)**.
10. In the PSL Editor select **File** then **New** then **Default Scheme**.
11. Select the IED type
12. Use the advance button to select the software, then select the model number.
13. Highlight the required PSL diagram and select **File** then **Print**.



**Caution:**  
Read the notes in the default PSL diagrams, as these provide critical information

---

## 6 SLD EDITOR

---

The SLD Configurator enables users to create customized Single Line Diagrams (SLD) for the front panel display. The SLDs must be configured from the SLD Editor accessible through S1 Agile. It allows the user to have breakers, switches, metering, and status items on the Single Line Diagrams. The Single Line Diagram can be viewed from the relay's front panel. The Single Line Diagram page can have a combination of active and passive objects. Status, metering, and control objects are active while static images for bus, generator, motor, transformer and ground, etc. are objects. Active objects are the objects which are constantly refreshing with new values. This includes control, metering and status objects.

---

### 6.1 SLD EDITOR IMPLEMENTATION

To start working on an SLD file, download the Data Model of the relay desired which will make the file available for adding into the S1 system under the relay's SLD folder. Also, all default SLD files are installed in the Data Model storage location in the PC when S1 Agile is first installed. SLD files can also be obtained by navigating to the Data Model location and inspecting the SLD folder under the Courier folder. Once the file has been sent to the relay it can also be recovered using the extract option in the SLD folder of the relay.

The default file is created with the most common application in mind. However, the SLD Editor can be used for a full reconfiguration of the SLD diagram to accommodate the user's needs. The user can redraw the topology to describe a different application or use it for breaker/switch specific CT/VT placement, metering and status display.

The SLD page is saved as an XML file with .8sld extension. Once the configurable SLD is programmed, it is saved within the settings file of the relay.

---

### 6.2 SLD EDITOR SYMBOLS

The SLD Editor utilises elements and functions on the toolbar. The buttons are:

**Select:** The select button is used to return to the select pointer regardless of what object is currently selected to be added to the diagram. Some objects allow users to return to the select tool just by right clicking.

**Line:** The Line button is used to draw a line in the diagram. In most cases this will be either a horizontal line describing a section of busbar, or a vertical line connecting two elements. SLDs are normally designed top to bottom.

**VT (GE):** Is used to add a VT object with GE visuals to the diagram. Each VT added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the VT the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is allowed for this object that changes the connection from a vertical position to a horizontal position. Right clicking shows a menu where you can Copy or Delete the element.

**VT (IEC):** Is used to add a VT object with IEC visuals to the diagram. Each VT added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the VT the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is allowed for this object that changes the connection from a vertical position to a horizontal position. Right clicking shows a menu where you can Copy or Delete the element.

**CT (GE):** Is used to add a CT object with GE visuals to the diagram. Each CT added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the CT the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. Right clicking shows a menu where you can Copy or Delete the element.

**CT (IEC):** Is used to add a CT object with IEC visuals to the diagram. Each CT added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on CT the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can rotate the object, you can perform 90-degree rotations from 0 to 270 degrees. Right clicking shows a menu where you can Copy or Delete the element.

**Metering Object:** Is used to add a Metering value to the diagram. By double clicking on the metered value the Properties menu is shown, or it can be opened by a right click and selecting Properties. The Parameter section

provides a drop-down menu with all the possible metered values that can be displayed. The label section is used to rename the metered value to a more friendly name. Text colour, background colour and font size are used to change the look and feel of the metered value on the screen. Right clicking shows a menu where you can Copy or Delete the element.

**Status Object:** Is used to add a Status Object to the diagram, the status object is composed of two elements, a text element and a graphical element. By double clicking on the status object's text element or the graphical element the Properties menu is shown, or it can be opened by a right click and selecting Properties. The Parameter section provides a drop-down menu with all the possible status objects supported. The label section is used to rename the status object to a more friendly name. Text colour, background colour and font size are used to change the look and feel of the status object in the screen. The colour of the graphical element is not editable. Right clicking either shows a menu where you can Copy or Delete the element. The position of both elements is independent.

**Text Object:** Is used to add a Text Object to the diagram, it is simple text not tied to any specific functionality. By double clicking on the text object the Properties menu is shown, or it can be opened by a right click and selecting Properties. The label section is used to rename the Text Object to a more friendly name. Text colour, background colour and font size are used to change the look and feel of the Text Object on the screen. Right clicking shows a menu where you can Copy or Delete the element.

**Control Objects:** The control objects consist of selectable breakers and disconnect switches. The table shows the different symbols in GE's Standard style and IEC style. If the switching element is tagged, blocked, or bypassed, indicators with letters "T", "B", and "By" appear on the lower right corner of the element. Additionally, the breaker/switch name is displayed at the top of the object.

Component		Symbols	
		GE	IEC
Breaker	BKR Open		
	BKR Closed		
	BKR Bad Status		
	BKR Tagged (T) /Blocked (B) /Bypassed (By)		
	SW Open		
Disconnect Switch	SW Closed		
	SW Unknown Status		
	SW Intermediate		
	SW Tagged (T) /Blocked (B) /Bypassed (By)		

**Breaker (GE):** Is used to add a breaker with GE visuals to the diagram. Each breaker added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the breaker or the text of the

breaker the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is used for this object that changes the connection from a vertical position to a horizontal position. The Selected Breaker drop down menu is used to reassign the breaker in the diagram from the breakers supported by the relay. The name of the breaker is not editable. The **Color scheme** setting is used to change from the green colour to the red colour. This setting is globally shared by all breakers and switches. Right clicking shows a menu where you can Copy or Delete the element.

**Breaker (IEC):** Is used to add a Breaker with IEC visuals to the diagram. Each breaker added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the Breaker or the text of the breaker the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is used for this object that changes the connection from a vertical position to a horizontal position. The Selected Breaker drop down menu is used to reassign the breaker in the diagram from the breakers supported by the relay. The name of the Breaker is not editable. The **Color scheme** setting is used to change from the green colour to the red colour. This setting is globally shared by all breakers and switches. Right clicking shows a menu where you can Copy or Delete the element.

**Disconnect Switch (GE):** Is used to add a disconnect switch with GE visuals to the diagram. Each disconnect switch added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the switch or the text of the switch the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. The Selected Disconnect Switch drop down menu is used to reassign the switch in the diagram from the switches supported by the relay. The name of the switch is not editable. The **Color scheme** setting to change from the green colour to red colour. This setting is globally shared by all breakers and switches. Right clicking shows a menu where you can Copy or Delete the element.

**Disconnect Switch (IEC):** Is used to add a Disconnect Switch with IEC visuals to the diagram. Each disconnect switch added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the switch or the text of the switch the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. The **Selected Disconnect Switch** drop down menu is used to reassign the switch in the diagram from the switches supported by the relay. The name of the switch is not editable. This setting is globally shared by all breakers and switches. Right clicking shows a menu where you can Copy or Delete the element.

**Transformer 2W (GE):** Is used to add a transformer with two windings with GE visuals to the diagram. Each transformer with two windings added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the transformer the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is used for this object that changes the connection from a vertical position to a horizontal position. Right clicking shows a menu where you can Copy or Delete the element.

**Transformer 3W (GE):** Is used to add a transformer with three windings with GE visuals to the diagram. Each transformer with three windings added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the transformer the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. Right clicking shows a menu where you can Copy or Delete the element.

**Transformer 2W (IEC):** Is used to add a transformer with two windings with IEC visuals to the diagram. Each transformer with two windings added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the transformer the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is used for this object that changes the connection from a vertical position to a horizontal position. Right clicking shows a menu where you can Copy or Delete the element.

**Transformer 3W (IEC):** Is used to add a transformer with three windings with IEC visuals to the diagram. Each transformer with two windings added counts towards the maximum, independent of the visuals chosen for each one. By double clicking on the transformer the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. Right clicking shows a menu where you can Copy or Delete the element.

**Generator:** Is used to add a Generator element to the diagram. This element is cosmetic and aims to help visualisation of the SLD.

**Motor:** Is used to add a Motor element to the diagram. This element is cosmetic and aims to help visualisation of the SLD.

**Reactor (for grounding):** Is used to add a reactor for grounding to the diagram. By double clicking on the reactor the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is used for this object that changes the connection from a vertical position to a horizontal position. Right clicking shows a menu where you can Copy or Delete the element.

**Resistor (for grounding):** Is used to add a resistor for grounding to the diagram. By double clicking on the resistor the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is used for this object that changes the connection from a vertical position to a horizontal position. Right clicking shows a menu where you can Copy or Delete the element.

**Capacitor (polarity):** Is used to add a capacitor with polarity to the diagram. By double clicking on the capacitor the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. Right clicking shows a menu where you can Copy or Delete the element.

**Capacitor (non-polarity):** Is used to add a capacitor with no polarity to the diagram. By double clicking on the capacitor the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu a 90-degree rotation is used for this object that changes the connection from a vertical position to a horizontal position. Right clicking shows a menu where you can Copy or Delete the element.

**Ground:** Is used to add a ground element to the diagram. By double clicking on the ground element the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. Right clicking shows a menu where you can Copy or Delete the element.

**Load:** Is used to add a load element to the diagram. By double clicking on the load element the Properties menu is shown, or it can be opened by a right click and selecting Properties. In this menu you can perform 90-degree rotations from 0 to 270 degrees. Right clicking shows a menu where you can Copy or Delete the element.

## Navigation


The Single Line Diagram can be accessed from the front panel of the relay. In the main menu of the relay, navigate to the Single Line Diagram Menu to enter the Single Line Diagram selection screen. The available Single Line Diagram will be shown. Select the Single Line Diagram to visualize it. Navigation can be restricted in different ways depending on the cybersecurity access level granted to the user.

## Control Operations

Opening/Starting and Closing/Stopping operations can be carried out by pressing the Open/Start and Close/Stop pushbuttons on the relay's front panel. Other operations such as tagging, blocking and bypassing can be carried out by pressing the control pushbuttons that appear after the control object selection.

Once the selected breaker or switch is tagged, a letter "T" appears below the associated element. Similarly, for blocking, letter "B" appears and for bypassing, letters "By" appear below the associated breaker or switch as shown in the last column of the following table. The blocking and bypassing letters also appear if the breakers/switches are blocked or bypassed remotely. A remotely blocked breaker can be unblocked locally and vice versa. These are linked to their respective breaker/switch in the SLD Configurator window so that when that breaker/switch is deleted, the letters also get deleted.

Permitted breaker/switch operations are described in the following table below when various letter indications are present under the control element.

Breaker/Switch Position	Letter Indication	Operation	Sample Indication
Open	B	Closing is blocked.	
Closed	B	Opening is blocked.	
Open	B By	Closing is blocked but bypassing is allowed. Closing is permitted.	
Closed	B By	Opening is blocked but bypassing is allowed. Opening is permitted.	
Open or Closed	T	Tagged by operator. No operation allowed.	
Open or Closed	T By	Tagged by operator. No operation allowed.	
Open or Closed	T B By	Tagged by operator. No operation allowed.	

---

## 7 IED CONFIGURATOR

---

IEC 61850 is a substation communications standard. It standardizes the way data is transferred to and from IEC 61850 compliant IEDs, making the communication independent of the manufacturer. This makes it easier to connect different manufacturers' products together and simplifies wiring and network changes.

The IED Configurator tool is used to configure the IEC 61850 settings of MiCOM IEDs, not the protection settings. It also allows you to extract a configuration file so you can view, check and modify the IEC 61850 settings during precommissioning.

---

### 7.1 IED CONFIGURATOR TOOL FEATURES

The IED configurator allows you to:

- Select and check IEC 61850 Edition 1 or Edition 2.
- Configure basic IEC 61850 communication parameters of the IED.
- Configure IED time synchronisation using SNTP.
- Edit Logical Devices and Logical Nodes.
- Define datasets for inclusion in report and GOOSE control blocks.
- Configure GOOSE control blocks for publishing (outgoing) messages.
- Configure virtual inputs, mapping them onto subscribed (incoming) GOOSE messages.
- Configure report control blocks.
- Configure the operation of control objects (circuit breaker trip and close):
  - The control mode (such as Direct, Select Before Operate)
  - Uniqueness of control (to ensure only one control in the system can operate at any one time).
- Configure measurements:
  - Scaling (multiplier unit such as kA, MV).
  - Range (minimum and maximum measurement values).
  - Deadband (percentage change of measurement range for reporting).
- Transfer IEC 61850 configuration information to and from an IED.
- Import SCL files for any IEC 61850 device (including devices from other manufacturers) to simplify configuration of GOOSE messaging between IEDs.
- Generate SCL files to provide IED configuration data to other manufacturers' tools, allowing them to use published GOOSE Messages and reports.

---

### 7.2 IEC 61850 SUBSTATION CONFIGURATION LANGUAGES

The following languages are used.

#### MiCOM Configuration Language (MCL)

This is a proprietary language file which contains a MiCOM device's IEC 61850 configuration information. This file is used for transferring data to or from a MiCOM IED.

#### Substation Configuration Language (SCL)

This is an XML-based standard language used to configure IEC 61850 IEDs in substations. It allows common substation files to be exchanged between all devices and between different manufacturers' toolsets. This helps to reduce inconsistencies in system configurations. Users can specify and provide their own SCL files to ensure that IEDs are configured according to their requirements.

SCL also allows IEC 61850 applications to be configured off-line without needing a network connection to the IED. Off-line system development tools can be used to generate the files needed for IED configuration automatically.

from the power system design. This significantly reduces the cost of IED configuration by eliminating most of the manual configuration tasks.

SCL specifies a hierarchy of configuration files, which enable the various levels of the system to be described: SSD, SCD, ICD, CID and IID files.

---

## 7.3 IEC 61850 SUBSTATION CONFIGURATION FILES

These files all use the standard Substation Configuration Language (SCL). They have the same construction but differ depending on the application.

### System Specification Description (SSD)

This contains the complete specification of a substation automation system including a single line diagram for the substation and its functionalities, or logical nodes. The SSD contains SCD and ICD files.

### Substation Configuration Description (SCD)

This contains information about the substation, all IEDs, data types and communications configuration. When engineering a system from the top down, an SCD file is produced and imported into the IED Configurator. To ensure consistency with the configuration of other IEDs in the system, this SCD file normally should not be edited. If there is no SCD file available, and you need to manually configure a MiCOM IED for precommissioning tests, you can open an ICD file and edit this to suit the IED application. The ICD file can be preinstalled as a template in the IED Configurator and opened directly, or it can be provided separately.

### IED Capability Description file (ICD)

This describes the IED's capabilities, including information on its data model (Logical Devices or Logical Node instances) and GOOSE support. The IEC 61850 Configurator can be used before commissioning an IED to create a blank configuration ICD file. The IEC 61850 Configurator can also extract an ICD file for viewing or modification and error checking a MiCOM IED.

### Configured IED Description File (CID) or Instantiated IED Description File (IID)

This describes a single IED in the system, including communications parameters.



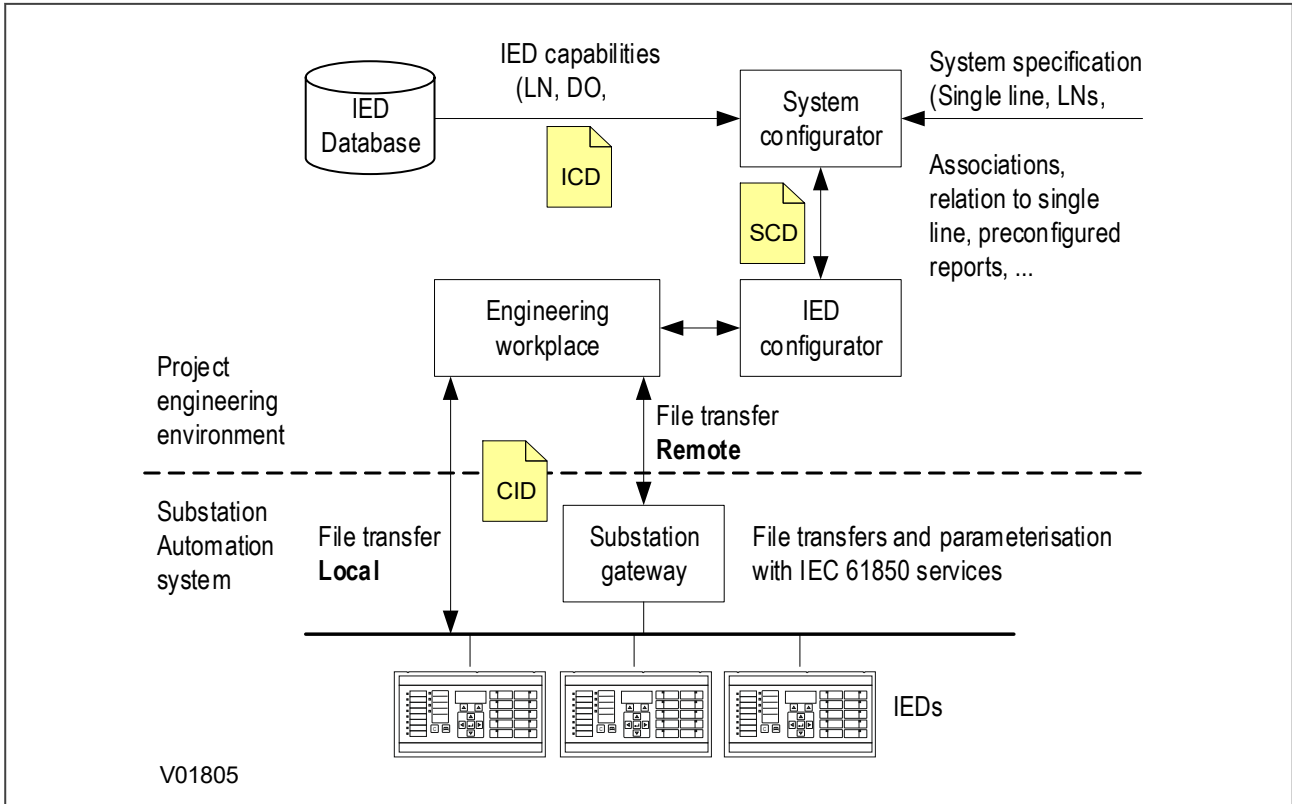


Figure 18: IEC 61850 project configuration

## 7.4 OPENING A PRECONFIGURED SCL FILE

An SCL configuration file contains the information for the MiCOM IED that is to be configured. To open an SCL configuration file for the system

1. Select **File** then **Import SCL**. A search dialog box appears.
2. Select the required SCL file and click **Open**.
3. The SCL Explorer window appears, showing an icon for each IED present in the SCL file.

IEDs which can be configured using the IEC 61850 Configurator are shown in a bold typeface and an icon with a green tick.

IEDs which cannot be configured using the IEC 61850 Configurator are shown with greyed text and an icon with a red X.

The left hand side of the window shows information on the SCL file and any selected IED tasks that can be performed on the selected IED(s). Alternatively right-click an IED to list tasks that can be performed on that particular IED.

## 7.5 OPENING AN ICD TEMPLATE FILE

If there is no SCD configuration file available, open an ICD template file for the MiCOM IED type that is to be configured. Once the ICD template is successfully loaded you can then look for all the IEDs that are connected.

1. Select **File** then **New**. The **Select Template** window appears.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.

### 7.5.1 TEMPLATE INSTALLED FOR REQUIRED IED TYPE

The ICD files for IED types whose data model has been downloaded using Data Model Manager will be available. Highlight the desired one and click the **Select** button. The configuration opens in manual editing mode so it can be customised for the application.

### 7.5.2 TEMPLATE NOT INSTALLED FOR REQUIRED IED TYPE

1. If there is no installed ICD file for the IED type that is to be configured, but there is one available from your supplier, click **Browse for External**.
2. A search dialog box appears. When you have found the required ICD file, click **Open**.
3. If the selected ICD Template file is already available as an installed template, a message appears and a new IED Configuration is created from the installed file.
4. If the selected ICD Template file has additional supported model numbers, a message appears asking if the additional model numbers should be merged into the installed template.
5. Select **Yes** to merge the new model numbers into the installed ICD Template file. This makes it available the next time the Template window appears.
6. If the selected ICD Template file is not installed, a message asks if it should be added to the application template library.
7. Select **Yes** to copy the selected ICD template file into the application library. This makes it available the next time the Template window appears.

---

## 7.6 OPENING AN EXISTING MCL CONFIGURATION FILE

1. Select **File** then **Open**. A search dialog box appears.
2. Select the required MCL file and click **Open**.
3. The tool tries to automatically match the MCL data to an installed ICD Template file and then display the configuration data in a read-only mode.
4. If it cannot automatically match the MCL data to an ICD Template file, the Template window appears. This allows you to manually assign the MCL data to an ICD Template file. If there is no suitable template available, click **Cancel**.
5. A message asks if the configuration is to be opened with Restricted Editing. Select **Yes** to display the configuration data in a read-only mode.

---

## 7.7 CONFIGURING A MICOM IED

Working offline:

1. Select **File** then **New**.  
The **Select Template** window appears. This allows you to create a new IED configuration from an installed ICD file.
2. Enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type and click **Next**.
3. Select the IED address and click **Next**. The IEC 61850 Configurator tool reads information from the IED and shows them in the **Summary** view.

**Note:**

This option is disabled by default in the tool, but can be made available in the main S1 window by removing the / nocommunication argument found in the Editors menu under **Options > Preferences** in the tool bar

Then:

Double click **TEMPLATE** in the left-hand pane to expand the tree structure.

The aspects of a MiCOM IED that can be configured come from its ICD Template file. These are shown in the main area of the IED Configurator tool, in the left hand side of the Editor window. The right hand side of the Editor window shows the configuration page of the selected category.

Each configurable item of the MiCOM IED is categorised into one of the following groups in the Editor window.

**IED Details** Displays general configuration and data about the IED and the selected ICD template file.

**Communications** Displays configuration of the communications Subnetwork.

**SNTP** Displays configuration of the client/server SNTP time synchronisation.

**Dataset Definitions** Displays dataset definitions used by the IED's GOOSE and report control blocks.

**GOOSE Publishing** Displays configuration for the GOOSE control blocks and associated messages to be published.

**GOOSE Subscribing** Displays configuration of virtual inputs that are subscribed to published GOOSE messages.

**Report Control Blocks** Displays configuration for the report control blocks in the IED data model.

**Controls** Displays configuration of control objects and uniqueness of control parameters (for larger control systems).

**Measurements** Displays configuration of measurement objects in the IED data model.

**Configurable Data Attributes** Displays parameter values for the configurable data attributes in the IED data model.

Each configurable item is either read-only or editable in manual mode. If it is read-only it is always non-editable. If it is editable in manual mode, some items may not be configurable if opened from a configured SCL file.

If a configured SCL file or MCL file was opened, and it is necessary to edit the configuration, select **View** then **Enter Manual Editing Mode** or click the toolbar icon. If an ICD file is opened, these items are automatically displayed in manual editing mode.

### 7.7.1 READING OR EDITING IED DETAILS

Working offline:

Select **File** then **New**. The **Select Template** window appears.

To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.

If you can find the IED type or ICD template, click **Select**.

If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **IED Details** item to show more information and edit the settings.

The following IED details can be viewed/edited.

**SCL File ID** The identification name, taken from the header section of an SCL file. Editable in Manual Editing Mode.

**SCL File Version** The version number, taken from the header section of an SCL file. Editable in Manual Editing Mode.

**Name** The IED name, taken from the IED section of an SCL file. This should be unique for all IEDs on the IEC 61850 network and is an Object Reference type so can be up to 65 characters long. However, we recommend that you restrict IED names to 8 characters or less. Editable in Manual Editing Mode.

**ICD Template** The ICD Template filename associated with the device's IEC 61850 configuration (MCL data). Read-only.

**SCL Schema Version** The SCL Schema version number. Read-only.

**IEC 61850 Edition** The IEC 61850 Edition number, indicates whether the device supports IEC 61850 Edition 1 or Edition 2. Read-only.

**Description** A basic description of the MiCOM IED type. It is taken from the IED section of the ICD template file and is not stored in MCL data or sent to the MiCOM IED. Read-only.

**Type** The MiCOM IED type. It is taken from the IED section of the ICD template file and is not stored in MCL data or sent to the MiCOM IED. Read-only.

**Configuration Revision** The software version of the target MiCOM IED. It is taken from the IED section of the ICD template file and is not stored in MCL data or sent to the MiCOM IED. Read-only.

**Supported Models** The specific MiCOM IED models supported by the ICD template file. If an ICD file is opened, these models are supported directly. If a configured SCL file is opened, these models are derived from the ICD file which is used to create a configured SCL file. It is not stored in MCL data nor sent to the MiCOM IED. Read-only.

**Functional Naming** allows the user to rename certain Logical Nodes and the new name would be visible to any IEC 61850 external party. This feature is only supported on IEC 61850 Edition 2 Px4x Modular relays. The name chosen for each Logical Node overwrites the default name given to it by the manufacturer. If using Functional Naming, all Logical Node name fields need to be filled before the change can be implemented. Logical Nodes that need no change need to have the default name written in the section provided. Functional Naming does not change the Logical Node name in the IED Configurator view, the change is only for external tools.

## 7.7.2 COMMUNICATIONS SETUP

Before the IED Configurator tool can manage an IED's configuration, you must first configure the communication parameters.

Select **Tools** then **Options**, then select the tab according to the protocol used.

**IEC 870-5-103 Communications** tab. Communication is through a serial connection from a COM port of the PC to the front port of the IED. If supported by the IED, you can also use the rear port. The Ethernet connection is not used, because the MiCOM IED does not have an IP address until it has been configured. This is also used for Px30 products.

**Courier Communications** tab. Communication is through a serial connection from a COM port of the PC to the front port of the IED. If supported by the IED, you can also use the rear port. The Ethernet connection is not used, because the MiCOM IED does not have an IP address until it has been configured. This is typically used for Px40 products.

1. In the **Default Configurations** field, if using the front port, select **MiCOM P\*40 Front Port (COM \*)**, if using the rear port, select **Courier (COM \*)**.
2. Set the **Connection Values** and **Transaction Parameters** as required or leave them at the default values.
3. Click **OK**.

**FTP communications** tab. Communication is over Ethernet to the FTP server of a MiCOM IED. The IP Address settings for both the PC and MiCOM IED must be for the same SubNetwork, especially if a direct connection is used with a cross-over network lead. If there is no valid or active IEC 61850 configuration in the IED, configure a default IP Address for the IED. This is also used for Mx70 products.

### 7.7.3 EDITING COMMUNICATIONS SETTINGS

Working offline:

1. Select **File** then **New**. The **Select Template** window appears.
2. Enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the Summary view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **Communications** item to read and edit the settings.

The following communications settings can be edited.

**Connected Subnetwork** This is the subnetwork name to which the IED is connected. It is particularly important for subscribing to GOOSE messages because an IED can only subscribe to publishers that are connected to the same subnetwork. The subnetwork name is taken from the Communications section of an SCL file. Normally editable in Manual Editing Mode, except if opened from a configured SCL file.

**Access Point** The Access Point (physical port) name for the MiCOM IED. This is taken from the IED Access Point section of the ICD template file. It is not stored in MCL data or sent to the MiCOM IED. Read-only.

**IP Address** Used to configure the unique network IP address of the MiCOM IED. It is taken from the ConnectedAP Address section of the configured SCL file. Editable in Manual Editing Mode.

**SubNet Mask** Used to configure the IP subnet mask for the network to which the MiCOM IED will be connected. It is taken from the ConnectedAP Address section of the configured SCL file. Editable in Manual Editing Mode.

**Gateway Address** Used to configure the IP address of any gateway (proxy) device, to which the MiCOM IED is connected. It is taken from the ConnectedAP Address section of the configured SCL file.

If there is no gateway (proxy) in the system, leave this at its default unconfigured value of 0.0.0.0. Editable in Manual Editing Mode.

**Ethernet Failover** This setting only applies to Single Ethernet Cards with 6/A/B in the Hardware Options section of the Cortec. The setting allows you to define how long the main connection needs to be down before the backup link is activated. The minimum value is 2 seconds. For cards with R/S/T in the Hardware Options section of the Cortec the Failover setting is performed in the Redundant Ethernet Configurator. This is explained in the Redundant Ethernet Board Manual.

**Media** This defines the default interface used to communicate between clients and peers, and the MiCOM IED. The value is taken from the ConnectedAP/PhysConn section of the configured SCL file and is editable in Manual Editing Mode. The single Ethernet board has one fibre and one copper interface, and it is normally identified with digits 6/A/B in the Hardware Options section of the Cortec. If you are using fibre, select **Single Fibre**. If you are using copper, select **Single Copper** or **Redundant (Fibre or Copper)**. If you are using a Redundant Ethernet board, normally identified with digits G/H/J/K/L/M/N/P/R/S/T in the Hardware Options section of the Cortec, select **Single Copper** or **Redundant (Fibre or Copper)**.

**TCP Keepalive** Used to set the frequency at which the MiCOM IED sends a TCP Keepalive message to keep open an association with a connected client. This setting is not taken from SCL. It is specific to MCL with a setting range of 1 to 20 seconds. Editable in Manual Editing Mode.

**Database Lock Timeout** Used to set how long the MiCOM IED waits without receiving any messages on the active link before it reverts to its default state. This includes resetting any password access that was enabled. It is taken

from the IED/AccessPoint/Server section of the configured SCL file and has a valid setting range of 60 to 1800 seconds (1 to 30 minutes). Only applicable to MiCOM IEDs that support setting changes over IEC 61850. Editable in Manual Editing Mode.

#### 7.7.4 ETHERNET FAILOVER SETTINGS

Working offline:

1. Select **File** then **New**.  
The **Select Template** window appears. This allows you to create a new IED configuration from an installed ICD file.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number and click **Next**.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the Summary view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **Communications** item to read and edit the settings.
3. The **Media** setting defines the default interface used to communicate between clients and peers, and the MiCOM IED. The value is taken from the ConnectedAP/PhysConn section of the configured SCL file and is editable in Manual Editing Mode.  
The single Ethernet board has one fibre and one copper interface:  
If you are using fibre, select **Single Fibre**.  
If you are using copper, select **Single Copper or Redundant (Fibre or Copper)**.  
If you are using a Redundant Ethernet board, select **Single Copper or Redundant (Fibre or Copper)**.
4. Set the **Ethernet Failover** to **Enable** and adjust the **Failover Timeout** as required. This does not appear if the product does not have Ethernet Failover.
5. Select **File** then **Save**.

#### 7.7.5 CONFIGURING THE IED FOR SNTP

These settings allow you to configure a MiCOM IED for SNTP.

Working offline:

1. Select **File** then **New**. The **Select Template** window appears.
2. Enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the Summary view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **SNTP** item, expand it and select **General Config** (configuring the IED for SNTP).

The following settings can be edited.

**Poll Rate** Use this to configure the interval at which the MiCOM IED requests time synchronisation from the selected SNTP server(s). This setting is not taken from SCL. It is specific to MCL with a setting range of 64 to 1024 seconds and is editable in Manual Editing Mode.

**Accepted Stratum level** SNTP uses a hierarchical system of clock sources. Each level is known as a stratum and is assigned a layer number starting with zero at the top, which is the reference time signal. The Accepted Stratum level setting specifies the stratum range for all configured SNTP servers. It defines the range MiCOM IEDs need to be able to accept time synchronisation responses. Any server response outside the specified range is discarded. You cannot edit this setting.

**Time server** This configures whether or not the IED acts as a time server in the system. If this option is enabled, other devices can synchronise their clocks to this IED. The value for this setting is taken from the IED/AccessPoint section of the configured SCL file. This setting is editable in Manual Editing Mode.

### 7.7.6 CONFIGURING THE SNTP SERVER

These settings allow you to configure external SNTP time servers with which the IED tries to synchronize its clock and connect.

Working offline:

1. Select **File** then **New**. The **Select Template** window appears.
2. Enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **SNTP** item, expand it and select **External Server** (configuring external SNTP time servers to which the IED connects).

The following details can be edited.

**Server Name** If opened from a configured SCL file, this shows the name of the device with which the MiCOM IED attempts to synchronise its clock. If you need to change the device, click the drop-down list to see all time-server devices in the configured SCL file. This is Read-only, is not stored in MCL data and is not sent to the MiCOM IED.

**Access Point** If opened from a configured SCL file, this shows the connected Access Point of the device with which the MiCOM IED attempts to synchronise its clock. This is Read-only, is not stored in MCL data and is not sent to the MiCOM IED.

**Sub Network Name** If opened from a configured SCL file, this shows the Sub Network name with which the device is connected. This is Read-only, is not stored in MCL data and is not sent to the MiCOM IED.

**IP Address** This is the IP Address of the device that provides SNTP Time synchronisation services. Devices are assigned to SNTP servers based on the contents of a configured SCL file. The IED/Access Point section of the SCL file lists devices supporting SNTP time synchronisation. This setting is editable in Manual Editing Mode.



**Use Anycast button** This button automatically sets the SNTP Server IP address to the broadcast address of the Sub Network to which the MiCOM IED is connected. Using the SubNet broadcast address forces the IED to use the Anycast SNTP Mode of operation. This button is only enabled when the IED has a valid IP Address and SubNet Mask. This setting is editable in Manual Editing Mode.

### 7.7.7 EDITING DATASET DEFINITIONS

To edit a dataset definition, working offline:

1. Select **File** then **New**. The **Select Template** window appears.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **Dataset Definitions** item.

If supported by the IED, datasets can be dynamically defined.

1. Right-click the **Dataset Definitions** item and select **Add New Dataset**.  
or on the **Dataset Definitions Summary** page, in the **Task** pane, click **Add Dataset**.
2. Find the dataset to be specified and click **Set**. A dataset can be created in any logical node of the IED's data model.
3. The **Dataset Definition** appears listing **Name**, **Location**, **Contents** and **GOOSE Capacity**.

The following settings can be edited.

**Name** The name of the dataset. This value is derived from the Dataset section of the selected logical node location in the configured SCL file. The initial character must be an alphabetic character (a-z, A-Z) while the remainder of the name can be either alphanumeric or the underscore symbol. The dataset name must be unique in the logical node where it is contained. Editable in Manual Editing Mode.

**Location** The location of the dataset in the IED data model. The location is always read-only. To change the read-only status, click **>>**. Specify a new location for the dataset. Editable in Manual Editing Mode.

**Contents** This shows the Functionally Constrained Data Attributes (FCDA) contained in the dataset. The ordering of these FCDA items in this list shows how values are seen over MMS communications.

Using the following icons on the toolbar, FCDA items can be moved around, deleted or added.

Toolbar Icon	Definition
Up & down arrows icon	These toolbar buttons move the selected FCDA up and down in the dataset definition.
Plus symbol	This toolbar button launches a dialog that allows you to select multiple FCDA items which can be added to the dataset definition. Items that can be selected have an outline tick symbol. Items that have been selected have a green tick symbol and are shown in the selection summary at the bottom of the dialog.
Minus symbol	This toolbar button removes the selected FCDA items from the dataset definition.
Square dot icon	For convenience a dataset can be defined from a supported Functional Constraint. This toolbar button expands the selected Functional Constraint into a list of Data Objects it contains. A dataset cannot contain both Data Objects and a Functional Constraint.



Toolbar Icon	Definition
Rotating arrows icon	<p>If the dataset is assigned to one or more control blocks (GOOSE), clicking this toolbar button automatically increments each control block's Configuration Revision. The Configuration Revision is used to identify changes to data, therefore this toolbar button is only enabled when the dataset definition is modified.</p> <p>If you change the selected configuration page and this toolbar button is enabled, you are asked if associated Configuration Revisions should be updated. Editable in Manual Editing Mode.</p>

**GOOSE Capacity.** The size (in bytes) of a GOOSE message has an upper restriction. It can not be any larger than the maximum allowable size of an Ethernet frame. This restriction limits the maximum number of items that can be included in a dataset.

The GOOSE Capacity gauge shows how large a dataset definition is with respect to GOOSE. If a dataset that is too large for transmission in a GOOSE message is assigned to a GOOSE Control Block, a validation warning appears. Read-only.

To delete Dataset definitions,

1. Right-click the dataset definition icon.
2. Select **Delete Dataset**.

or

1. In the **Dataset Definitions Summary** page, select a dataset.
2. In the task pane, click **Delete Dataset**.

To delete every dataset definition in the configuration data, click **Delete All Datasets**.

Any references in GOOSE or Reporting Control Blocks to the deleted dataset remain unchanged. However, a validation warning appears stating that the dataset definition does not exist.

### 7.7.8 CONFIGURING OPTIMISED PERFORMANCE GOOSE DATASETS

If supported by the IED, an Optimised Performance GOOSE (OPGoose) dataset can be created. OPGoose is a special datasets whose elements are prioritised for processing by the IED. The information contained in this dataset is for use in high speed GOOSE applications such as tripping or blocking signals between IEDs.

To configure an Optimised Performance Goose dataset:

1. Right-click the **Dataset Definitions** icon and select **Add New OPGoose Dataset** or on the **Dataset Definitions Summary** page, in the Task pane, click **Add New OPGoose Dataset**. The dataset will automatically be populated with all default elements supported for prioritised processing.
2. To add or remove an element from the dataset, select the **+** and **-** buttons, or right-click anywhere in the element list contents window and select **Add new FCDA item(s)** or **Delete FCDA item(s)**. When adding elements, only the OPGoose-related Data Attributes will be listed and shown within the selection table.
3. In the **Dataset FCDA Object Selector** window, the list of items to add may be viewed as a flat list or Hierarchical list by selecting the required **Flat view** or **Hierarchy view radio button**.
4. To move elements up and down the dataset list, select the **↑** and **↓** buttons

*Note:*  
Only one OPGoose dataset may be created per supporting device.

### 7.7.9 GOOSE PUBLISHING CONFIGURATION

Working offline:

1. Select **File** then **New**. The **Select Template** window appears.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**, then select the IED type device number.
2. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **GOOSE Publishing** item. Then select a GOOSE Control Block (GoCB).

The following details can be edited.

**Multicast MAC Address** Configures the multicast MAC address to that which the GoCB publishes GOOSE messages. The first four octets (01 - 0C - CD - 01) are defined by the IEC 61850 standard; leave these at their default values. The multicast MAC address is taken from the ConnectedAP/GSE section of the configured SCL file. Editable in Manual Editing Mode.

**Application ID** Configures the AppID to that which the GoCB publishes GOOSE messages. The AppID is specified as a hexadecimal value with a setting range of 0 to 3FFF and is taken from the ConnectedAP/GSE section of the configured SCL file. Editable in Manual Editing Mode.

**VLAN Identifier** Configures the VLAN (Virtual LAN) on to which the GOOSE messages are published. The VLAN Identifier has a setting range of 0 to 4095 and is taken from the ConnectedAP/GSE section of the configured SCL file. If no VLAN is used, leave this setting at its default value. Editable in Manual Editing Mode.

**VLAN Priority** Configures the VLAN Priority of published GOOSE messages on the VLAN. The VLAN priority has a setting range of 0 to 7 and is taken from the ConnectedAP/GSE section of the configured SCL file. If no VLAN is used, leave this setting at its default value. Editable in Manual Editing Mode.

**Minimum Cycle Time** Configures the Minimum Cycle Time between the first change-driven message being transmitted and its first repeat retransmission. The Minimum Cycle Time has a setting range of 1 to 50 milliseconds and is taken from the ConnectedAP/GSE/MinTime section of the configured SCL file. Editable in Manual Editing Mode.

**Maximum Cycle Time** Configures the Maximum Cycle Time between repeat message transmissions under a quiescent 'no change' state. The Maximum Cycle Time has a setting range of 1 to 60 seconds and is taken from the ConnectedAP/GSE/MaxTime section of the configured SCL file. Editable in Manual Editing Mode.

**Increment** Determines the rate at which the repeat message transmission intervals step up from the Minimum Cycle Time to the Maximum Cycle Time. The higher the number, the fewer the repeat messages (and therefore time) it takes to reach the Maximum Cycle Time. This setting is not taken from SCL. It is specific to MCL with a setting range of 0 to 999 and has no units. Editable in Manual Editing Mode.

**GOOSE Identifier** Configures the 64 character GOOSE Identifier (GoID) of the published GOOSE message that is configured in the SCL file. The initial character must be alphabetic (a to z or A to Z) while the rest of the name can be either alphanumeric or the underscore symbol. The GOOSE Identifier must be unique for the entire system. This setting is taken from the LN0/GSEControl section of the configured SCL file. Editable in Manual Editing Mode.

**Dataset Reference** Configures the dataset which is to be included in the GoCB's published messages. Only datasets that belong to the same logical node as the GoCB can be selected for inclusion in the GOOSE messages. If the dataset definition does not exist or is too large for publishing in a GOOSE message, a warning appears.

This setting is taken from the LN0/GSEControl section of the configured SCL file. Right-click the Dataset Reference control to perform the following operations:

- Create and assign a new dataset definition. Only if the current dataset assignment is empty.
- Delete the current dataset assignment. Only if there is an assigned dataset.
- Edit the currently assigned datasets definition. Only if there is an assigned dataset.

Editable in Manual Editing Mode.

**Configuration Revision** Displays the Configuration Revision of the published GOOSE message. If the dataset reference or dataset contents are changed, the Configuration Revision must be incremented to allow other peers listening to the published GOOSE messages to identify the change in configuration. This setting has a range of 0 to 4294967295 and is taken from the LN0/GSEControl section of the configured SCL file. Editable in Manual Editing Mode.

Any other IED in the system that needs to subscribe to the published GOOSE messages of the MiCOM IEDs must use the same value in its GOOSE subscription configuration.

### 7.7.10 GOOSE SUBSCRIPTION CONFIGURATION

Working offline:

1. Select **File** then **New**.  
The **Select Template** window appears.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **GOOSE Subscribing** item.

Configuration of the GOOSE Subscription depends on whether the IED configuration has been compiled from a configured SCL file, from an MCL file or manually created.

GOOSE Subscription is also based on two concepts.

**Mapped Inputs** Applicable in all instances. A Mapped Input is an External Binding between two IEDs that is assigned to a valid Data Attribute in the IED data model (the internal Data Attribute supports binding to an external value).

For example, on a MiCOM Px40 device, a Mapped Input is an External Binding that has been assigned to a Virtual Input for use in Programmable Scheme Logic.

**Multicast MAC Address** Configures the multicast MAC address to that which the GoCB publishes GOOSE messages. The first four octets (01 – 0C – CD – 01) are defined by the IEC 61850 standard; leave these at their default values. The multicast MAC address is taken from the ConnectedAP/GSE section of the configured SCL file. Editable in Manual Editing Mode.

**Application ID** Configures the AppID to that which the GoCB publishes GOOSE messages. The AppID is specified as a hexadecimal value with a setting range of 0 to 3FFF and is taken from the ConnectedAP/GSE section of the configured SCL file. Editable in Manual Editing Mode.

**Source Path** The source path shows where the value taken from the incoming GOOSE message originates in the publishing IEDs Data model (For example: P145\System\GosGGIO2\Ind1.stVal).

**GoCB Source Reference** This value is derived from the Inputs/ExtRef section of the selected Virtual Inputs Logical Node definition in the configured SCL file.

**GOOSE Identifier** Configures the 64 character GOOSE Identifier (GoID) of the published GOOSE message that is configured in the SCL file. The initial character must be alphabetic (a to z or A to Z) while the rest of the name can be either alphanumeric or the underscore symbol. The GOOSE Identifier must be unique for the entire system. This setting is taken from the LN0/GSEControl section of the configured SCL file. Editable in Manual Editing Mode.

**Dataset Reference** Configures the dataset which is to be included in the GoCB's published messages. Only datasets that belong to the same logical node as the GoCB can be selected for inclusion in the GOOSE messages. If the dataset definition does not exist or is too large for publishing in a GOOSE message, a warning appears.

This setting is taken from the LN0/GSEControl section of the configured SCL file. Right-click the Dataset Reference control to perform the following operations:

- Create and assign a new dataset definition. Only if the current dataset assignment is empty.
- Delete the current dataset assignment. Only if there is an assigned dataset.
- Edit the currently assigned datasets definition. Only if there is an assigned dataset.

**Configuration Revision** Displays the Configuration Revision of the published GOOSE message. If the dataset reference or dataset contents are changed, the Configuration Revision must be incremented to allow other peers listening to the published GOOSE messages to identify the change in configuration. This setting has a range of 0 to 4294967295 and is taken from the LN0/GSEControl section of the configured SCL file. Editable in Manual Editing Mode.

Any other IED in the system that needs to subscribe to the published GOOSE messages of the MiCOM IEDs must use the same value in its GOOSE subscription configuration.

**Data Obj Index** This configures the index of the Data Object within the published GOOSE messages dataset that is to be decoded and processed for assignment to the selected Virtual Input. The setting range is dependent on the contents of the dataset and is derived from its definition in the configured SCL file.

**Data Obj Type** This configures the data type of the Data Object within the published GOOSE messages dataset that is to be decoded and processed for assignment to the selected Virtual Input. The data type of the selected Data Object is taken from the DataType Templates section of the configured SCL file and must match to one of the pre-defined supported data types

**Quality Obj Index** This configures the index of an associated Quality Object within the published GOOSE messages dataset that is to be cross checked and processed as part of the Data Object assignment to the selected Virtual Input. It is not required to assign a quality object but if the selected Data Objects data type is a complex class (i.e. SPS etc) that includes a quality attribute the assignment will be automatic. The setting range is dependent upon the contents of the dataset and is derived from its definition in the configured SCL file.

**Browse buttons** These buttons present a dialog to allow for the quick and easy selection/configuration of a Data Object from a published GOOSE message.

**Unmap button** This button is only applicable if the Source Path parameter has been specified (i.e. non-blank). Clicking this button will remove the External Binding assignment from the selected Virtual Input. The External Binding will now be located within the Unmapped Inputs section where it can then be (re)assigned to another Virtual Input.

**Evaluation Expression** This configures the evaluation expression executed on the decoded Data Object value prior to assigning to the selected Virtual Input. The available expressions are predefined:

- **Equal To:** The decoded value is compared against the configured value to see if they are equal. The result of the comparison is converted to a BOOLEAN value for assignment to the Virtual Input; True = Values are equal, False = Values are not equal.
- **Not Equal To:** The decoded value is compared against the configured value to see if they are not equal. The result of the comparison is converted to a BOOLEAN value for assignment to the Virtual Input; True = Values are not equal, False = Values are not equal.
- **Greater Than:** The decoded value is compared against the configured value to see if it is the greater of the two values. The result of the comparison is converted to a BOOLEAN value for assignment to the Virtual Input; True = Decoded values is greater than the configured value, False = Decoded value is less than (or equal to) the configured value.
- **Less Than:** The decoded value is compared against the configured value to see if it is the lesser of the two values. The result of the comparison is converted to a BOOLEAN value for assignment to the Virtual Input; True = Decoded values is less than the configured value, False = Decoded value is greater than (or equal to) the configured value.
- **Pass Through:** The decoded value is directly passed on to the Virtual Input.

This setting is not taken from SCL. It is specific to MCL.

**Default Input Value** This configures the default value the Virtual Input should take when it is not receiving messages from the configured GOOSE publisher. The default value would normally be considered as a "System safe" default value. The available default value options are selectable from a predefined list:

- **FALSE:** The Virtual input is held at a FALSE value while it is not receiving messages from the GOOSE publisher.
- **TRUE:** The Virtual Input is held at a TRUE value while it is not receiving messages from the GOOSE publisher.
- **Last Known Value:** The Virtual Input remains at the value in the last received GOOSE message.
- **Double Point:** This option has four different values viz., Intermediate (00), Off (01), On (10) and Bad State (11).

This setting is not taken from SCL. It is specific to MCL.

**Invalidity Quality Bits** If a Quality Object has been assigned to the Virtual Input, this configures the quality bits that are to be regarded as invalid/questionable. If any one of the selected quality identifiers is set in the decoded Quality Object value, then the overall validity of the Virtual Input shall be invalid/questionable. The standard quality bits are directly presented for selection and the additional Quality Detail information hidden. If invalidity is to be set for a specific Quality Detail bit, this is displayed in a popup dialog by clicking the ">>" button:

**Unmapped Inputs** Primarily applicable to configured SCL files. An Unmapped Input is similar to the Mapped Input. It is an External Binding between two IEDs but the binding has not yet been assigned to a supporting Data Attribute in the IED data model.

For example, on a MiCOM Px40 device, an Unmapped Input is an External Binding that has been identified as necessary for the IED configuration but has not yet been assigned to a Virtual Input for use in Programmable Scheme Logic.

### 7.7.11 REPORT CONTROL BLOCK CONFIGURATION

Working offline:

1. Select **File** then **New**.  
The **Select Template** window appears.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **Report Control Blocks** item. Then select a Report Control Block (RCB).

The following details can be edited.

**Report Type** Displays the type of the selected RCB. Read-only.

**Report ID** Configures the default Report ID of the RCB. Any clients wanting to use the RCB can override this default value if required. The initial character of the Report ID must be alphabetic (a to z or A to Z) while the rest of the name can be either alphanumeric or the underscore symbol. This setting is taken from the LN(0)/ReportControl section of the required RCB in the configured SCL file. Editable in Manual Editing Mode.

**Dataset Reference** Configures the dataset which is to be included in the generated reports from the RCB. Only datasets that belong to the same logical node as the RCB can be included in the reports. This setting is taken from the LN(0)/ReportControl section of the required RCB in the configured SCL file. Editable in Manual Editing Mode.

**Configuration Revision** Displays the Configuration Revision of the RCB. If there are any changes to dataset reference or dataset contents, the Configuration Revision must be incremented to allow clients receiving the reports to identify the change in configuration. This setting is taken from the LN(0)/ReportControl section of the required RCB in the configured SCL file. Editable in Manual Editing Mode.

### 7.7.12 CONTROLS CONFIGURATION

Working offline:

1. Select **File** then **New**.  
The **Select Template** window appears.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.

Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **Controls** item.

The following details can be edited.

- **Control Objects** is the configuration of each Control Object (Circuit Breaker Trip/Close control) in the IED's data model, for example its Control Model Direct Operate, Select Before Operate. This breaks down into:
  - **ctlModel** This configures the control model (ctlModel) of the Control Object to one of the following predefined options and is taken from the LN(0)/DOI/DAI/Val section of the ctlModel in the configured SCL file. Editable in Manual Editing Mode.
    - Status Only**
    - DOns** (Direct Operate - Normal Security)
    - SBOns** (Select-Before-Operate - Normal Security)
    - DOes** (Direct Operate - Enhanced Security)
    - SBOes** (Select-Before-Operate - Enhanced Security)
  - **sboTimeout** If supported by the Control Object, this configures the Select Before Operate timeout. A client has the configured number of milliseconds to operate the control following the select command. If the Control Object is not operated in this time period, it is reset back to an unselected state. This setting is taken from the LN(0)/DOI/DAI/Val section of sboTimeout in the configured SCL file. Editable in Manual Editing Mode.
- **Uniqueness of Control** This adds a layer of security onto control operations by allowing only one Control Object to operate at any time in the whole system. Uniqueness of Control checks are performed using GOOSE, making it simple and reliable without any server redundancy.

### 7.7.13 EDITING CONFIGURABLE DATA ATTRIBUTES

1. Select **Device** then **Manage IED**.
2. Select the IED type.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.
4. Click the **Configurable Data Attributes** tab.
5. Select a Data Attribute.

The following details can be edited.

**Data Type** This shows the SCL Data type of the Data Attribute. The data type influences the type of control used to represent the Data Attributes value.

- Integer based types use a numeric up-down control to specify the value.
- Enumerated types use a combo box to specify the available setting values.
- String types use a text box to allow text entry.

Read-only.

**Value** This is the value to assign to the Data Attribute and is taken from the LN(0)/DOI/DAI/Val section of the required Data Attribute in the configured SCL file. Editable in Manual Editing Mode.

### 7.7.14 EDITING MEASUREMENT CONFIGURATIONS

Working offline:

1. Select **File** then **New**. The **Select Template** window appears.
2. To select the template, enter the IED model number or select the product group. The lower pane shows information about the IED's associated ICD template file, the SCL header details and the IEC 61850 features supported by the IED.
3. If you can find the IED type or ICD template, click **Select**.  
If there is no installed ICD file for the IED but there is one from your supplier, click **Browse for External**.



Or working online:

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads information from the IED and shows them in the **Summary** view.

Then:

1. Double click **TEMPLATE** in the left-hand pane to expand the tree structure.
2. Click the **Measurements** item. Then Select a measurement object.

The following details can be edited.

**Unit multiplier** If supported by the IED, this configures how the measurement value will be scaled when read by or reported to a client. The multiplier is shown in the following table.

Value	Multiplier	Name	Symbol
-24	$10^{-24}$	Yocto	y
-21	$10^{-21}$	Zepto	z
-18	$10^{-18}$	Atto	a
-15	$10^{-15}$	Femto	f
-12	$10^{-12}$	Pico	p
-9	$10^{-9}$	Nano	n
-6	$10^{-6}$	Micro	?
-3	$10^{-3}$	Milli	m
-2	$10^{-2}$	Centi	c
-1	$10^{-1}$	Deci	d
0	1		
1	10	Deca	da
2	$10^2$	Hecto	h
3	$10^3$	Kilo	k
6	$10^6$	Mega	M
9	$10^9$	Giga	G
12	$10^{12}$	Tera	T
15	$10^{15}$	Petra	P
18	$10^{18}$	Exa	E
21	$10^{21}$	Zetta	Z
24	$10^{24}$	Yotta	Y

For example, if the phase A current is 1250 amps and the multiplier is kilo (k), the relay measures 1.250 (kA). Editable in Manual Editing Mode.

**Scaled Measurement Range Min/Max** If supported by the IED, this configures the minimum and maximum values of a measurement object. The min and max values are used with the deadband value to calculate how much a measurement must change to be updated or reported to a client. Editable in Manual Editing Mode.

**Deadband** This configures the deadband, which is a percentage change based on the measurements range in units of 0.001% (giving a range of 0 to 100000). A deadband of 0 means the measurement is updated instantaneously. To simplify the calculation process, click the >> button. Specify the deadband as a percentage change (such as 5%) or as an absolute change (such as 0.1 Hz). Editable in Manual Editing Mode. The deadband



can be specified at any level in the Measurements tab. The range, including the multiplier, can only be specified at a level where all measurement objects are of the same type. For example, all phase current measurements.

---

## 7.8 FULL VALIDATION OF IED CONFIGURATION

The IED Configurator can be used to validate configured SCL files against the SCL schema when they are opened. It can also validate an IED's MCL configuration at any time.

1. In the SCL Explorer workspace, right-click a MiCOM IED and click **Validate**.
2. The selected MiCOM IED is validated and the results appear in a Validation Log window. The log shows three levels of classification:
  - Information. No actions required.
  - Warning. Some consideration may be required.
  - Error. IED may not function as expected with current configuration.
3. Double-click a warning or error item. The configuration page that generated the log entry appears. Double clicking information entries has no effect.

---

## 7.9 VALIDATION SUMMARY

1. Select **Device** then **Manage IED**.
2. Select the IED type device number.
3. Select the IED address and click **Next**. The IED Configurator tool reads details from the IED and shows them in the **Summary** view.
4. Select a category tab. A summary of each the configuration appears in the Summary pane. Double-click an item and a list of log entries appears in the Validation Report pane.

The following log entries can be edited.

**SNTP Summary.** This shows all the server sources available for configuration in the IED. If a server source is configured, it is shown in bold. Also the IP address of the external time synchronisation server is shown. If a server source is unconfigured, it is shown greyed.

**Dataset Definitions Summary.** This shows all the datasets defined throughout the IED's data model. For each defined dataset, its number of Functionally Constrained Data Attributes is also shown. The summary page includes a common set of tasks to manage the dataset definitions.

**GOOSE Publishing Summary.** This shows all of the GOOSE Control Blocks (GoCB) available in the IED. If a GoCB is fully configured, it is shown in bold. A partially configured GoCB is shown in normal typeface. If a GoCB is unconfigured, it is shown greyed.

**GOOSE Subscribing Summary.** This shows all of the Virtual Inputs available in the IED. If a Virtual Input is fully configured, it is shown in bold. A partially configured Virtual Input is shown in normal typeface. If a Virtual Input is unconfigured, it is shown greyed. Any unmapped inputs are listed in an additional summary.

**Report Control Block Summary.** This shows all of the Report Control Blocks (RCB) available in the IED. If an RCB is fully configured, it is shown in bold. A partially configured RCB is shown using in normal typeface. If an RCB is unconfigured, it is shown greyed.

**Control Objects Summary.** This shows all of the Control Objects available in the IED's data model, and what their configured control model is (Direct Operate, Select Before Operate).

**Uniqueness of Control Summary.** This shows all of the Virtual Inputs available in the IED. If a Virtual Input is fully configured, it is shown in bold. A partially configured Virtual Input is shown in normal typeface. If a Virtual Input is unconfigured, it is shown greyed. Any unmapped inputs are listed in an additional summary.

**Measurements Summary.** The Measurements summary shows all of the Measurement Objects available in the IED's data model, plus their configured range and deadband.

**Configurable Data Attributes Summary.** The Configurable Data Attribute summary shows all of the Configurable Data Attributes available in the IED's data model, plus their data type and configured value.

---

## 7.10 MANAGING SCL SCHEMA VERSIONS

The IED Configurator supports several versions of the SCL schema. This improves its reliability and correctly validates any version of SCL file. The schema files are not available and are encoded into a proprietary binary format that allows basic version control management by the IED Configurator tool.

Existing schema versions can be removed or new versions added.

1. Select **Tools** then **Options**.
2. Click the **General** tab.
3. Click the **Manage Schemas** button. New schema versions are provided in a binary distribution file.
4. Click a schema and its details are shown in the left-hand pane.

To add a new SCL Schema:

1. In the left-hand pane, click **Add New SCL Schema** then search for the binary schema distribution file.
2. Click **Open** to import the file. The IED Configurator merges all schema versions in the distribution file into the application repository. If a schema version is already available in the application repository it is skipped.

To remove an SCL Schema:

1. In the right-hand pane, right-click a schema and select **Remove Schema File**. This removes the selected SCL schema from the application repository. The operation cannot be undone.

### 7.10.1 ADDING AND REMOVING SCL SCHEMAS

To add a new SCL Schema:

1. Select **Tools** then **Options**.
2. Click the **General** tab.
3. Click the **Manage Schemas** button.
4. In the left-hand pane, click **Add New SCL Schema** then search for the binary schema distribution file.
5. Click **Open** to import the file. The IED Configurator merges all schema versions in the distribution file into the application repository. If a schema version is already available in the application repository it is skipped.

To remove an SCL Schema:

1. Select **Tools** then **Options**.
2. Click the **General** tab.
3. Click the **Manage Schemas** button.
4. In the right-hand pane, right-click a schema and select **Remove Schema File**. This removes the selected SCL schema from the application repository. The operation cannot be undone.

---

## 7.11 CONFIGURATION BANKS

In the MiCOM IED there are two configuration banks for IEC 61850 configuration. The configuration bank concept is similar to that of setting groups for protection settings, promoting version management and helping to minimise IED down-time during system upgrades and maintenance.

To view an IED's configuration bank details:

1. Establish a connection to the MiCOM IED.
2. Select **Device** then **Manage IED**.
3. If the connection to the MiCOM IED is successful, the Manage IED window appears showing the details of the Active and Inactive configuration banks.

The following configuration banks can be edited.

**Switch banks button.** This toggles the IED's configuration banks so the Active Bank becomes inactive and the Inactive Bank becomes active. The switching technique used ensures the system down-time is minimised to the start-up time of the new configuration.

**Refresh banks button.** This forces the IED Configurator tool to refresh the details displayed for the Active and Inactive configuration banks. It is especially useful if, for example, configuration banks have been toggled directly on the IED.

**Extract ICD file button.** This button is only enabled for IEDs that hold their own local copy of their ICD template file. Press this button to define where the ICD template file that is contained in the IED should be saved. After the ICD template is extracted, it can be made available as an Installed template.

**Extract configuration buttons.** These buttons extract the appropriate configuration bank and open it for viewing or editing in a new window.

---

## 7.12 TRANSFER OF CONFIGURATIONS

The IED Configurator tool can be used to transfer configurations to and from any supporting MiCOM IED.

If you send a configuration to a supporting MiCOM IED, it is automatically stored in the Inactive configuration bank. It therefore does not immediately affect the current Active configuration.

To send a configuration to a MiCOM IED:

1. Establish a connection to the MiCOM IED.
2. Select **Device** then **Send Configuration**.
3. The IED Configurator tool checks the compatibility of the IED model number. It then transfers the configuration to the IED.

---

## 7.13 EXPORTING INSTALLED ICD TEMPLATE FILES

Any installed ICD template file can be exported by the IED Configurator tool to a user-defined location.

1. Select **Tools** then **Export Installed ICD File**. The Template dialog appears.
2. Select the MiCOM IED type for which the template file is to be exported.
3. Click the **Select** button. Specify the location and filename of the ICD template file being exported.

---

## 7.14 EXPORTING CONFIGURED SCL FILES

Any IED configuration in an Editor window can be exported to a configured SCL file, if it has not been opened for restricted editing. To export a configured SCL file, the IED Configurator tool needs the IED's ICD template file.

1. In an Editor window, select **Tools** then **Export Configuration to SCL**.
2. Select the MCL configuration file which is to be exported.
3. Specify the destination file name for the configured SCL file.

Configuration items that are specific to MCL are not exported. This is because the information is not supported by the SCL schema. It is therefore important to save the configuration in an MCL file.

The main reason for exporting configured SCL files is to allow configuration information to be shared between multiple tools. This is for the configuration of, for example, GOOSE message exchange.

**Note:**

*For IEC 61850 Edition 2 products, two different types of SCL schema can be exported:*

*Schema v3.1 for complete Edition 2 systems.*

*Schema v2.1 for mixed Edition 1 and Edition 2 systems. This is the backwards compatible version.*

## 7.15 EXPORTING LOGICAL DEVICE AND NODE MODELS TO A DOCUMENT

A document containing logical node and device model lists may be exported as a Microsoft Word file (\*.doc or \*.docx), or an Adobe Reader Portable Document Format (PDF) file to a user defined location.

1. Select **Tools** then **Export Logical Devices to Doc**. The **Save As** dialog appears.
2. Choose a suitable location and file name.
3. Select the **Save as type**: Word Document (\*.docx), Word 97-2003 (\*.doc) or PDF Document (\*.pdf)
4. Select **Save**.

A document will be created that identifies the modified logical nodes and devices. Use this in combination with the device PIXIT for the complete IEC 61850 modelling documentation.

## 7.16 MANAGING LOGICAL DEVICES AND NODES

The **Manage Logical Devices** option allows users to customise the IEC 61850 modelling structure. Information can be presented in a standardised manner between different IEDs.

This option is currently only available for devices that support IEC 61850 Edition 2

The following restrictions apply when editing logical devices and nodes:

- Logical Devices can be freely renamed or and all can be deleted except for SYSTEM
- Logical Nodes can be both freely renamed or deleted, except for LLNO and LPHD
- Only Logical Nodes can be moved between different Logical Devices
- Only new Logical Devices can be created

*Note:*

*If using test mode features, logical nodes should not be moved from their default locations. This is because if a logical node is moved, its test mode behaviour will no longer be consistent between parent and child.*

### 7.16.1 EDITING LOGICAL DEVICES AND NODES

To edit logical devices and nodes, select **Tools** then **Manage Logical Devices**. The configuration view is selected by the **Hierarchy view** and **Flat view** radio buttons.

#### Configuration Views

- Flat view, is the standard view for devices with IEC 61850 Edition 1. All logical devices are at the same level, and there is no hierarchy shown between the logical devices.
- Hierarchy, presents logical devices grouped as parents and children. This is used to model nested functions and sub-functions, for example **CB Control** contains the sub-function **CB Fail** in the hierarchy view, whereas in the flat view both of these logical devices are presented at the same level.

### 7.16.2 CONFIGURING LOGICAL DEVICES

To create a logical device:

1. In the **Manage Logical Devices** window, select **Add LD**, and assign a name using the **Inst** field.
2. Select **Save**.

*Note:*

*A new logical device is indicated with a green icon.*

To delete a logical device:

1. Select the tick box next to the logical device.
2. Select **Remove**.

*Note:*  
*Multiple selections can be made when deleting.*

To rename a logical device:

1. In the **Manage Logical Devices** window, select the required logical device then **Edit** and modify the **Inst** (instance) field as necessary.
2. Select **Save**.

To restore a logical device to its default setting:

1. Select **Compare with default**.
2. In the **Default Configuration** window, select the tick box next to the logical device.
3. Select **Restore**

*Note:*  
*Multiple selections can be made when restoring.*

To finalise configuration changes:

1. Select **Apply Configuration**. The new logical device structure will then be in effect.

### 7.16.3 CONFIGURING LOGICAL NODES

To move a logical node:

1. Click on the logical node then drag and drop it onto the newly created logical device.

*Note:*  
*Logical nodes cannot be moved to a default logical device, they can only be moved to user created logical devices.*

To rename a logical node:

1. In the **Manage Logical Devices** window, select the logical node then **Edit** and modify the **Prefix** and **Inst** fields as necessary. The **LN class** field is restricted and cannot be renamed.
2. Select **Save**.

To delete a logical node:

1. Select the tick box next to the logical node.
2. Select **Remove**.

*Note:*  
*Multiple selections can be made when deleting.*

To restore a logical node to its default setting:

1. Select **Compare with default**.
2. In the **Default Configuration** window, select the tick box next to the logical node.
3. Select **Restore**.

*Note:*

*Multiple selections can be made when restoring.*

To finalise configuration changes:

1. Select **Apply Configuration**. The new logical node structure will then be in effect.

---

## 8 DNP3 CONFIGURATOR

---

DNP3 (Distributed Network Protocol) is a master/slave protocol developed for reliable communications between various types of data acquisition and control equipment. It allows interoperability between various SCADA components in substations. It was designed to function with adverse electrical conditions such as electromagnetic distortion, aging components and poor transmission media.

The DNP3 Configurator allows you to retrieve and edit its settings and send the modified file back to a MiCOM IED.

---

### 8.1 PREPARING FILES OFFLINE TO SEND TO AN IED

To prepare files, it is not necessary to connect to an IED.

1. Select the IED type.
2. Click the **DNP3 Settings File** tile.
3. Click **Open Default File**.
4. Select the IED from the list and click **Next**.
5. Type or select a model number and click **Finish**. The **Default DNP3 Settings** screen appears.

Or

1. From the main screen, select **File** then **Open File** then **Px40** then **DNP3 Settings File**.
2. Select the IED file from the list and click **Open**.

Then

1. Expand the Explorer view and double click an item.
2. The left-hand column shows a list of available Master Points. Using the buttons, add or remove items from the left-hand column to list of Configured Points in the right-hand column.
3. Right-click any Configured Point in the right-hand column for further settings.
4. Click **OK**.

---

### 8.2 SEND SETTINGS TO AN IED

To send settings to a device, connect the PC to the IED and select the communication port. See [Getting Started](#). There must be at least one setting file in a settings folder for a device.

1. From the main screen, select **View** then **System Explorer**.
2. Expand the view to see the required device.
3. Right-click the device name and select **Send**.
4. In the **Send to...** dialog, select the setting files and click **Send**.
5. Click **Close**.

---

### 8.3 EXTRACT SETTINGS FROM AN IED

1. From the main screen, select **View** then **System Explorer**.
2. Expand the view to see the required device.
3. Right-click the device name and select **Extract Settings**. To extract all settings select **Extract Full Settings** then **Yes**.
4. Click **Close**.

---

## 8.4 VIEW IED SETTINGS

1. In the right-hand pane, expand the system to show the device.
2. Double click the device to show the DNP3 file.
3. Double click the DNP3 file to open it, or right click to select New File.
4. The left-hand pane shows the DNP3 settings. Expand to see all settings.



---

## 9 CURVE TOOL

---

The User Programmable Curve Tool (UPCT) allows you to create user-defined curves and to download and upload these curves to and from the IED. You can use this tool to create programmable operate and reset curves. You can also create and visualize curves either by entering formulae or data points.

---

### 9.1 FEATURES

The Curve Tool allows you to:

- Create, edit and save new curves or edit existing curve files
- Enter a defined number of curve points or a user-defined formula
- Create, edit and save multiple formulae
- Use templates to provide all the data needed to create new curves
- Interpolate between curve points using a template
- Create a curve from a fixed or user defined formula
- Save curve formulae in XML format and configure curve points in CSV format, enabling easy data exchange
- Save configured curve data in CRV format, suitable for download into the IED
- Easily upload the curve data from an IED
- Input constants with user-defined values
- Graphically display curves with zoom, pan, and point-on-curve facilities
- Multiple curves can be drawn and visualized simultaneously
- Curves can be drawn with different colors for better visualization and easy comparison
- Print curves or save curves in a range of standard image formats

---

### 9.2 CURVE PLOT PANE

The Curve Plot pane displays the curves showing time on the y-axis and Q (multiples of nominal current) on the x-axis. This is the standard method of defining protection IED configuration curves.

Right-click anywhere in the Curve Plot pane to carry out a range of flexible operations on the curves from the context-sensitive menu. Operations include copying the image, zooming, panning and printing. Images can be saved as PNG, GIF, JPEG, TIFF or BMP.

Right-click any point on the plot and select **Show Point Values** to show the Q and T values at that point.

#### 9.2.1 OPEN A CURVE

You can open a curve either through the formula or through the input table.

1. Select **File** then **Open**.
2. To open an XML curve file, select **Formula** or to open a CRV or CSV curve file, select **Input Table**.
3. Select the required curve file. You can open several curves and the Curve Selection pane shows a list of those available. As you import or create more curves, they appear as rows in the table.
4. Check the checkbox to select a curve and the corresponding row is then highlighted. Selecting the curve displays it in the Curve Plot pane and makes it available for upload or download.
5. Select **View** then **Show Curve Details** to view the Curve Details.

#### 9.2.2 ZOOMING AND PANNING

To zoom in, drag a box around the area using the mouse.

To pan, press and hold the shift key and left mouse button while moving the mouse.

To un-zoom or un-pan, right-click the Curve Plot and select **Un-zoom** or **Un-pan**.

To revert to the original view, right-click the Curve Plot and select **Undo All Zoom/Pan**.

### 9.2.3 CHANGE THE GRAPH TO DEFAULT SIZE

To set the graph to its default size:

1. Right click the **Curve Plot** area.
2. Select **Set Scale to Default** from the context-sensitive menu.

### 9.2.4 CHANGE THE GRAPH GRID LINES

To change the grid lines:

1. Select **Graph Options** then **Grid Lines**.
2. Select **Major Grid Lines** or **Minor Grid Lines** to show the grid lines in a coarse or fine scale.

### 9.2.5 CHANGE THE GRAPH SCALE

To change the graph scale:

1. Select **Graph Options**.
2. Select the **X-Axis Scale** or **Y-Axis Scale**.
3. Select **Linear** or **Logarithmic**.

### 9.2.6 CHANGE CURVE COLOURS

To change curve colours:

1. Select **View** then **Show Curve Detail**. The **Curve Points Details** window appears in the left-hand pane.
2. Change the curve colour in the **Input Table View** and the **Product View**. The colour changes appear in the **Curve Plot**.
3. Select **File** then **Save**, then **Input Table View** to save the curve. Or select **Save As**.

### 9.2.7 PRINT A CURVE

To print a curve:

Select File then **Print** or **Print Preview**.

or

Right-click the **Curve Plot** area and select **Print** from the context-sensitive menu.

### 9.2.8 SAVE A CURVE AS AN IMAGE

To save a curve as a bitmap image:

1. Right click the **Curve Plot** area.
2. Select **Save Image As** from the context-sensitive menu.
3. Select the required image format and click **Save**.

---

## 9.3 CURVE POINTS DETAILS PANE

To show further details about the curves, select **View** then **Show Curve Detail**. This shows the curve as a table of points.

In the Curve Points Details pane you can give the curve a name and description using standard ASCII characters. The name allows up to 16 characters and the description up to 256 characters. If you do not enter a name, it uses

the default name **New Curve** and similarly the default description is **Curve Description**. The formula name and template version are also displayed if applicable.

To auto-hide the Curve Details, click the icon next to the cross. This shows the plot full size and only shows the curve detail when you position the cursor in the marked area in the left-hand margin.

To close the Curve Points Details pane, click the X in the right-hand corner.

### 9.3.1 CREATE A NEW CURVE

You can create a curve either through the formula or through the input table.

1. Select **File** then **New**. Then select either **Formula** or **Input Table**.
2. If you select Formula:
  - a. The **Formula Editor** appears.
  - b. Enter the required formula in the **Input Formula Editor** tab.
  - c. Select the required template from the **Curve Template** drop-down list.
  - d. Enter a name in the **Formula Name** text box.
  - e. Enter constant values in the **Input Constants** tab.
  - f. Click **Verify Formula** then click **Generate Curve**.
  - g. Select **File** then **Save**, then **Input Table View** to save the curve. Or select **Save As**.
3. If you select Input Table:
  - a. The **Curve Points Details** window appears in the left-hand pane.
  - b. Enter the required fields.
  - c. Select **File** then **Save**, then **Input Table View** to save the curve. Or select **Save As**.

### 9.3.2 ENTERING VALUES OF Q AND T INTO THE TABLE

The Curve Points dialog has three columns

**Index.** Each curve point has a unique index number associated with it, starting at 0, incrementing by 1 and ending with the last curve point.

**Q (multiples of setting).** Q, in this context stands for Quantity. It is the secondary current  $I_s$ , expressed in multiples of the nominal current  $I_n$ .

**T (Time in secs).** T is the imposed delay time, expressed in seconds.

To input values for Q and T to define a new table:

1. Select **File** then **New** then **Input Table**.
2. Insert the values for **Q** and **T** up to a maximum of 256 curve points (index 0 to 255). The tool instantaneously updates the graph view as points are entered. If fewer points are inserted, the tool automatically interpolates points using linear interpolation.

To copy and paste an entire table from Excel or other compatible table formats:

1. Copy the table to the clipboard.
2. Position the cursor in the top left-hand Q cell and paste.

### 9.3.3 EDIT A CURVE

To edit a curve:

1. Select **View** then **Show Curve Details**. The **Curve Points Details** window appears in the left-hand pane.
2. Enter or edit the required fields.
3. Change the curve colour in the **Input Table View** and the **Product View**.
4. Select **File** then **Save**, then **Input Table View** to save the curve. Or select **Save As**.

### 9.3.4 INTERPOLATING CURVE POINTS

To interpolate curve points:

1. Load the curve, select **View** then **Show Curve Details**. The Curve Points Details window opens.
2. Tick the **Show User Curve** tick box.
3. Tick the **Show Product Curve** tick box to interpolate points using the template file and linear interpolation.

### 9.3.5 IMPORT CURVE POINTS

To import curve points from other applications:

1. Select **View** then **Show Curve Details**. The **Curve Points Details** window appears in the left-hand pane.
2. Open the application, for example, Excel.
3. In the application, copy the curve points to the clipboard in the required format.
4. In the left-hand pane, in the **Curve Points** field, position the cursor in the top left-hand Q cell and paste the curve points.
5. Select **File** then **Save**, then **Input Table View** to save the curve. Or select **Save As**.

### 9.3.6 EXPORT CURVE POINTS

To export curve points to other applications:

1. Select **View** then **Show Curve Details**. The **Curve Points Details** window appears in the left-hand pane.
2. Open the application, for example, Excel.
3. In the left-hand pane, in the **Curve Points** field, copy the curve points to the clipboard.
4. Paste the curve points into the application.

---

## 9.4 FORMULA EDITOR

1. To open the Formula Editor select **View** then **Show Formula Editor**.
2. Enter the formula in the **T=** field. The formula is case sensitive, use only uppercase letters.
3. Select the required template from the **Curve Template** dropdown box. The curve you are creating with the formula must be associated with a predefined template. This must match the template of one of the curves stored in the IED. The template defines a curve with a specific spread of points which can be downloaded to the IED.
4. Enter the formula name into the **Formula Name** field. This can be any combination of standard ASCII characters up to 32 characters.
5. If you need a Definite Time characteristic, check the **DMT** (Definite Minimum Time) checkbox. Then enter fixed values for the tripping current multiplier (**Q**) and the delay time (**T**).
6. You can enter any constants into the formula and the first eight letters of the Greek alphabet are included in the formula editor as buttons. Click a button to enter the character in the **Formula** field.
7. Input the formula constants into the **Value** column.
8. To validate the formula, click the **Verify Formula** button at the bottom left corner of the screen. The names of the constants used in the formula are shown in the **Input Constants** table. The formula verifier checks the operators are valid but does not check if the formula is valid or if the results are out of range.
9. Select the **Options** tab, click **Save As** and enter a file name. The file is saved in XML format. Enter up to 16 standard ASCII characters.
10. Once the constants are entered and the file is saved, click the **Generate Curve** button (next to the Verify Formula button) to generate a curve. The curve appears in the Curve Plot pane.

## Allowed Formula Editor operators

Operators	Description
+	Plus
-	Minus
*	Multiply
/	Divide
^	Raise to the power of
sqrt()	Square Root
ln()	Natural logarithm
Sin	Sin function
Cos	Cos function
Tan	Tan function

### 9.4.1 PICK-UP SETTING AND TMS

The programmable curve is a set of points in a table which the software interpolates into a curve. It is treated in the same way as all the other standard curves stored in the IED. Each curve has a pick-up setting and a Time Multiplier Setting (TMS).

Most applications do not need the TMS feature, in which case you can set it to 1. However, the TMS can be useful in some applications. For example, one user overcurrent curve could be created for several IEDs and the TMS can then be set individually in each relay to achieve time grading.

## 9.5 CURVE TEMPLATES

Many protection functions use a graphical curve to define their Operate and Reset characteristics. These are inverse curves with current on the x-axis and time on the y-axis and each curve has 256 points.

In the Phasor tool, the curves created with the formula or points table must match the templates of their respective curves stored in the IED. Each curve is defined by 256 points with a specific spread of the points in different areas of the curve.

The following are examples of Curve Tool templates.

### Curve tool templates

Template	Description
Overcurrent Operate	Overcurrent protection IDMT operate curve
Overcurrent Reset	Overcurrent protection IDMT reset curve
Thermal Overload Operate	Thermal overload protection operate (heating) curve
Thermal Overload Reset	Thermal overload protection reset (cooling) curve
Undervoltage Operate	Undervoltage protection operate curve
Overflux Operate	Overfluxing (V/Hz) protection operate curve

The curve templates have a clearly defined number of graphical points to define certain portions of the curve. The following tables are examples of template definitions.

### Overcurrent operate

Range	Number of points
Range 1: 1x to 3x setting	128
Range 2: 3x to 32x setting	116

Range	Number of points
Range 3: 32x to 76x setting	12
Overall range	256

### Overcurrent reset

Range	Number of points
Range 1: 1x to 0.96x setting	116
Range 2: 0.96x to 0.7x setting	128
Range 3: 0.7x to 0x setting	12
Overall range	256

### Thermal overload operate

Range	Number of points
Range 1: 1x to 4x setting	150
Range 2: 4x to 5x setting	68
Range 3: 5x to 10x setting	32
Range 4: 10x to 32x setting	6

### Thermal overload reset

Range	Number of points
Range 1: 1x to 0.96x setting	116
Range 2: 0.96x to 0.7x setting	128
Range 3: 0.7x to 0x setting	12
Overall range	256

### Overflux operate

Range	Number of points
Range 1: 1x to 2x setting	128
Range 2: 2x to 5x setting	116
Range 3: 5x to 10x setting	12
Overall range	256

### Overflux reset

Range	Number of points
Range 1: 1x to 0.96x setting	116
Range 2: 0.96x to 0.7x setting	128
Range 3: 0.7x to 0x setting	12
Overall range	256

### Undervoltage operate

Range	Number of points
Range 1: 1x to 0.95x setting	66
Range 2: 0.95x to 0x setting	190
Overall range	256

### 9.5.1 SELECT A CURVE TEMPLATE

To select a curve template:

1. Select **View**, then **Show Formula Editor**.
2. Select a template from the **Curve Template** dropdown list.
3. The selected template also appears in the **Curve Points Details** pane, in the **Product View**.

---

## 9.6 CONNECTING TO AN IED

Depending on the model, MiCOM IEDs have one or more of the following ports which you can use to transfer curve files:

- Front USB
- Front serial
- Rear RS485
- Rear Ethernet

The front port is a temporary local connection used to set up the IED. The rear serial port is typically used for multi-drop SCADA. The Ethernet port runs at 10/100 Mbps and is typically used for network SCADA.

To configure the communication settings for downloading and uploading the curves to and from the IED

1. Select **Device** then **Connection Configuration**. The Edit Connection dialog appears.
2. In the Scheme dropdown box, select which port to configure.
3. Click the **Transaction Values** tab. These are the default values. If you make changes and need to revert to the default settings, click the **Restore Defaults** button.

The following is a list of transaction values and their definitions

**Busy Hold-off Time (ms)**. The time interval used by Courier between receiving a BUSY response and sending a subsequent POLL BUFFER command.

**Busy Count**. The maximum number of BUSY responses that will be accepted for a single Courier transaction before aborting the transaction.

To cope with abnormal situations where a device is not replying correctly to requests, a limit is placed on the number of BUSY responses that should be accepted. Without this limit the link to the device would be stuck in a loop.

**Reset Response Time (ms)**. The maximum time from sending the last byte of a Courier Reset Remote Link message to receiving the first byte of a response. When that time has elapsed, the request is aborted.

**Response Time (ms)**. The maximum time from a sending the last byte of a Courier message to receiving the first byte of a response. When that time has elapsed the request is aborted. The Response Time parameter is used for all messages except Courier Reset Remote Link messages.

**Try Count**. The number of tries before aborting the request.

**Transmit Delay Time (ms)**. The minimum delay that is put between receiving a response and transmitting the next request. Transmit delay is normally set to zero but can be set to a few milliseconds when using half duplex communication. This gives the other end of the link time to change from transmitting to receiving.

**Global Transmit Time (ms)**. The minimum delay that is put between transmitting a global message and the next transmission.

### 9.6.1 CONNECTING TO A SERIAL PORT

If you connect to a serial port, the **Serial** tab appears.

1. Click the **Serial** tab. The fields are already populated with the default settings.
2. Enter the **Relay Address**. This is an integer which represents the Courier address of the IED.

### 9.6.2 CONNECTING TO THE ETHERNET PORT

If you connect to the Ethernet port, the **Ethernet** tab appears.

1. There is no DHCP support so you must know the **IP address** and enter it manually.
2. The TCP port can be dynamic or static. If you need a static TCP port, check the **Use fixed incoming TCP port** checkbox and enter the **Fixed incoming port number**.
3. If the device is attached to a bay unit, click the **Device is attached to a bay unit** checkbox. Then select from the **Bus Address** dropdown box.
4. Enter the **Relay Address**. This is an integer which represents the Courier address of the IED.

---

### 9.7 SEND A CURVE TO AN IED

1. To open an existing curve, select **File** then **Open Curve**. You can open several curves and the **Curve Selection** pane has a list of those available. As you import or create more curves, they appear as rows in the table.
2. Check the checkbox to select a curve and the corresponding row is then highlighted. Selecting the curve displays it in the **Curve Plot** pane and makes it available for upload or download.
3. Click the **Device** tab and select **Send Curve**. The **Send Curve Form** appears.
4. The IED stores several curve characteristics. In the **Curve Characteristic** dropdown box, select which curve you want to overwrite.
5. Click **Send** to send the curve to the IED then click **Get Curve Ref**.
6. Check the **PC Curve Value** is the same as the **Relay Curve Value**. This shows that the send has been successful because it overwrites the existing Relay Curve Value.
7. To send a curve using a different template to the one stored in the device, go to the **USER CURVES DATA** menu option on the front panel of the device. Scroll to the programmable curve that requires editing and select the new template option.

---

### 9.8 EXTRACT A CURVE FROM AN IED

1. Select **Device** then **Extract Curve**.
2. Select **File** then **Save** then **Input Table View** to save the curve file in CSV format  
or  
select **File** then **Save** then **Product View** to save the curve file in CRV format.



---

## 10 S&R COURIER

---

Settings and Records - Courier enables you to connect to any Courier device, retrieve and edit its settings and send the modified settings back to a Courier device, including DNP 3.0 configuration if supported by the device.

Although each device has different settings, each cell is presented in a uniform style, showing the permissible range and step size allowed.

Settings and Records - Courier also enables you to:

- extract events from a device
- extract disturbance records from a device
- control breakers and isolators
- set the date and time on a device
- set the active group on a device
- change the address of a device
- save settings, protocol configuration, events and disturbance files to disk

---

### 10.1 SET UP IED COMMUNICATION

1. Select **Device** then **Communications Setup**. The Communications Setup dialog appears.
2. If the configuration you want to use already exists, select it from the Scheme drop-down list and click **OK**.
3. If the configuration you want to use does not exist, create a new communications setup.

---

### 10.2 CREATE A NEW COMMUNICATION SETUP

1. Select **Device** then **Communications Setup**. The **Communications Setup** dialog box appears.
2. Select the connection: **Serial, Modem** or **Internet**.

If using a serial connection,

1. Select the **Serial** tab.
2. In the **COM Port** drop-down list, select the serial port to which the device will be connected.
3. Select the **Baud rate** and **Framing**.

If using a modem,

1. Select the **Modem** tab.
2. Click **Configure...** to enter the phone number.

Then for all connection types,

1. Select the **Transaction Values** tab and complete the fields.
2. Click **Save As**.
3. Enter a name in the **Save Communications Parameters As** field and click **OK**.
4. Click **OK** to configure the communications port.

---

### 10.3 OPEN A CONNECTION

1. **Select Device** then **Open Connection**.
2. If known, enter the device address in the **Address** field, otherwise click **Browse** to scan available devices.

3. Click **OK** to open the connection.
4. Enter the password using four alphabetic characters.
5. Click **OK**. If the password is valid, the connection is made and the **On-line** window appears.

*Note:*

*If the device is set to the default password, the **Enter Password** dialog is not needed for enhanced DNP 3.0 devices.*

---

## 10.4 CREATE A NEW OR DEFAULT IED DNP 3.0 FILE

1. Select **File** then **New**.
2. Select **DNP File**. The **New DNP 3.0 File** dialog appears.
3. Select the required device type from the **Device Type** drop-down list. The model numbers for the device type are displayed.
4. Select the model number from the **Model Number** list or use the **Advanced** button to construct the required model number. If duplicate model numbers exist, the Header details give version numbers and other identifying information. The appropriate language is displayed in the **Language** drop-down list, showing the language of the file.
5. If more than one language type is supported, the **Language** drop-down list shows the languages for the device type.
6. Click **OK**. A new DNP 3.0 file is generated, based on the selected model.

---

## 10.5 EXTRACT A SETTINGS FILE FROM A DEVICE

1. **Select Device** then **Open Connection** to open a connection to the required device.
2. In the **Online Device** window, right-click the device name.
3. Select **Send To** then **New Settings File**.
4. The **New Settings File** dialog appears. Select the device model number.
5. Click **OK**.
6. Once the extraction is complete, a window appears showing the settings.

---

## 10.6 SAVE A SETTINGS FILE

1. Select **File** then **Save As**.
2. Edit the **File Name** or **Header** fields as required.
3. Click **Save**.

---

## 10.7 SEND A SETTINGS FILE TO A DEVICE

1. Open a connection to the required device.
2. Make sure the destination file is in the active window.
3. Select **File** then **Send To**
4. Click the appropriate device.

## 11 MONITORING MODULE

The Monitoring Module retrieves diagnostic data (either monitor or test data) from specific cells of any Courier device at predefined intervals and displays them as a list. The procedures for the operation and control of the Courier Monitoring Module are described in the next section.

### 11.1 OFFLINE AND ONLINE MONITORING MODULE

The Monitoring module enables you to display and print, measurements and diagnostic data from any Courier device. By setting the timer between 1 and 60 seconds, the device can be polled at regular intervals to display the current state.

The Offline module contains the following menu options:

Menu	Description
File	<b>Page Setup...</b> Display the <b>Page Setup</b> dialog, enabling print settings to be changed. <b>Exit</b> Exit the Monitoring module.
Device	<b>Open Connection...</b> Display the <b>Establish Connection</b> dialog, enabling the PC to retrieve data from the connected device. When the connection is made, a window is opened and measurement data is polled. <b>Communications Setup...</b> Display the <b>Communications Setup</b> dialog, enabling you to select or set up the communication settings and values to be used.
Polling	<b>Setup Timer...</b> Display the <b>Set Polling Timer</b> dialog, enabling you to enter the time interval between polls.
View	<b>Toolbar</b> Show/hide the toolbar. <b>Status Bar</b> Show/hide the status bar.
Help	<b>Contents</b> Display help topics. <b>About Monitoring...</b> Display version and copyright information about the Monitoring Module.

### 11.2 ONLINE MONITORING MODULE

The Online module contains the following menu options:

Menu	Description
File	<b>Print...</b> Print the contents of the selected window. <b>Print Preview</b> Display the Print Preview window, showing how the selected data will appear when printed. <b>Page Setup...</b> Display the <b>Page Setup</b> dialog, enabling print settings to be changed. <b>Exit</b> Exit the Monitoring module.
Edit	This menu is only available when a device is connected. <b>Copy</b> Copy the selected text to the clipboard.

Menu	Description
Device	<p><b>Close Connection...</b> Close the connection to the online device and the window or windows in use.</p> <p><b>Retrieve from Device &gt;</b></p> <p><b>Measurements</b> Open a window and retrieve measurement data.</p> <p><b>Tests</b> Open a window and retrieve the test items.</p> <p><b>Refresh</b> Retrieve the values for the selected window from the device immediately.</p> <p><b>Communications Setup...</b> Display the Communications Transaction Values dialog, enabling you to adjust the transaction values in use.</p>
Polling	<p><b>Setup Timer...</b> Display the <b>Set Polling Timer</b> dialog, enabling you to enter the time interval between polls.</p> <p><b>Start Polling</b> Start polling the device for information. Information will be obtained from the device at the time interval set by the <b>Set Polling Timer</b> dialog.</p> <p><b>Stop Polling</b> Stop requesting information from the device. You must stop polling before carrying out any other operations.</p>
View	<p><b>Toolbar</b> Show/hide the toolbar.</p> <p><b>Status Bar</b> Show/hide the status bar.</p>
Window	<p>This menu is only available when a device is connected.</p> <p><b>Cascade</b> Arrange data windows so that the titles bars are visible.</p> <p><b>Tile</b> Arrange data windows so they do not overlap.</p>
Help	<p><b>Contents</b> Display help topics.</p> <p><b>About Monitoring...</b> Display version and copyright information about the Monitoring Module.</p>

---

## 12 GOOSE EDITOR

---

Using the GOOSE Editor you can edit the UCA2 GOOSE settings for a MiCOM Px4x series IED. You can also map GOOSE inputs and outputs to the DDB signals of an IED.

The GOOSE Editor can extract settings from and send settings to an IED using a Courier port on the IED. It can also save IED settings to a file on your PC or print them.

---

### 12.1 SET UP IED COMMUNICATION

1. Select **Device** then **Communications Setup**. The Communications Setup dialog appears.
2. If the configuration you want to use already exists, select it from the Scheme drop-down list and click **OK**.
3. If the configuration you want to use does not exist, create a new communications setup.

---

### 12.2 CREATE A NEW COMMUNICATION SETUP

1. Select **Device** then **Communications Setup**. The **Communications Setup** dialog box appears.
2. Select the connection: **Serial**, **Modem** or **Internet**.

If using a serial connection,

1. Select the **Serial** tab.
2. In the **COM Port** drop-down list, select the serial port to which the device will be connected.
3. Select the **Baud rate** and **Framing**.

If using a modem,

1. Select the **Modem** tab.
2. Click **Configure...** to enter the phone number.

Then for all connection types,

1. Select the **Transaction Values** tab and complete the fields.
2. Click **Save As**.
3. Enter a name in the **Save Communications Parameters As** field and click **OK**.
4. Click **OK** to configure the communications port.

---

### 12.3 OPEN A CONNECTION

1. **Select Device** then **Open Connection**.
2. If known, enter the device address in the **Address** field, otherwise click **Browse** to scan available devices.
3. Click **OK** to open the connection.
4. Enter the password using four alphabetic characters.
5. Click **OK**. If the password is valid, the connection is made and the **On-line** window appears.

*Note:*

*If the device is set to the default password, the **Enter Password** dialog is not needed for enhanced DNP 3.0 devices.*

---

### 12.4 SCAN FOR AVAILABLE DEVICES

1. Select **Device** then **Open Connection**. The **Establish Connection** dialog appears.
2. Click **Browse**. The **Browse Available Relays** dialog appears.

3. Enter the first and last device addresses to be scanned in the **From** and **To** fields.
4. Click **Scan**. A list of devices in the range appears.
5. Highlight the required device and click **OK**. The **Open Connection** dialog appears with the number of the selected device in the **Address** field.

---

## 12.5 EXTRACT GOOSE SETTINGS FROM A DEVICE

1. Open a connection to the device. If GOOSE settings are not loaded, open a GOOSE file or create a new GOOSE file.
2. Select **Device** then **Receive from Relay**.
3. The GOOSE settings file is extracted from the device. It can then be edited and saved.

---

## 12.6 OPEN, EDIT AND SAVE A GOOSE FILE

1. Select **File** then **Open**.
2. Select the required file and click **Open**.
3. Edit the selected GOOSE settings file.
4. Select **File** then **Save** or **Save As**.

---

## 12.7 SEND GOOSE SETTINGS TO A DEVICE

1. Open a connection to the device. If GOOSE settings are not loaded, open a GOOSE file or create a new GOOSE file.
2. Select **Device** then **Send to Relay**. The **Send Settings to Relay** dialog appears.
3. Type in a Reference Identifier if required.
4. Click **OK**. The GOOSE settings are sent to the device.

---

## 13 GOOSE CONFIGURATOR

---

The GOOSE Configurator tool allows you to manage GOOSE schemes across multiple devices, with all connections shown graphically. It also provides a detailed list of GOOSE messages, which can be exported to assist with maintenance and commissioning.

---

### 13.1 OPEN AN MCL FILE

You can modify an MCL file if the data model is installed for that device. Unsupported MCL files are marked as NO ICD and although you can open them, most operations are blocked.

To open an existing MCL file, select the **File** tab then **Open** then **Browse**. You can open up to 20 MCL files at the same time.

To open MCL files exported from previous sessions in a single archive file, select the **File** tab then **Open** then **Import**. Files can be added to the current session or opened in a new one.

To import files to a folder with an archive name, select the **File** tab then **Options** and check the check box.

---

### 13.2 EXPORT FROM AN S1 SYSTEM TO GOOSE CONFIGURATOR

A quick way to create a GOOSE Configurator diagram is to export the MCL files from an S1 system directly into the GOOSE Configurator. This simplifies creating a one to one equivalent setup on GOOSE configurator for creating all the GOOSE connections.

Right click on the System name on the S1 System Explorer structure and select the **Show GOOSE connections** options. All relays with created MCL files will be shown.

You can now select which MCL files you want to export to the GOOSE configurator for each relay in the S1 system. You can also pick an associated PSL file, which can be used for quick logic configuration of the GOOSE signals in the PSL Editor.

---

### 13.3 PUBLISH A MESSAGE

The Goose Configurator tool allows you to modify an MCL file to publish a new message.

1. Select the IED from which you want to publish a message.
2. Click **Publish a message**.
3. Select the Goose Control Block from which you want to publish a message. Click **Next**.
4. From the tree structure, select which messages you want to publish. Click **Finish**. The messages are then published.
5. Once the message is successfully published, a horizontal line appears next to the device.
6. To view a list of published messages, click **Show published messages**.
7. To export the list of published messages as an Excel file, click **Export to Excel**.
8. Click **Close View** to return to the main menu..

---

### 13.4 SHOW PUBLISHED MESSAGES

1. To display all messages that are published from opened MCL files, click **Show published messages**.
2. To remove published messages from the list, select the message and click **Remove publishing**. A warning appears if any messages are subscribed to by other IEDs.
3. To export the list of published messages to an Excel file, click **Export to Excel**.
4. Click **Close View** to return to the main menu.

---

## 13.5 CLONE PUBLISHING

You can clone published messages across compatible MCL files which use the same source ICD file.

1. Click **Clone publishing**. A list of all published messages appears.
2. Select the IED from which you want to clone messages and click **Next**.
3. Select the target IED for clone messages. Only IEDs which use the same ICD file are listed.
4. Click **Finish**. Messages are cloned and results of the operation appear.

---

## 13.6 SUBSCRIBE TO A MESSAGE

To make connection between IEDs, you must first subscribe to a published message.

1. Click **Subscribe to a message**.
2. Select the IED to which you want to subscribe a message and click **Next**.
3. From the tree structure, select the subscribing block and click **Next**.
4. Select the IED which publishes the messages and click **Next**.
5. Select the message to which you want to subscribe and click **Finish**. Subscribing to a published message makes a connection between IEDs. The connection is marked with black dot.

---

## 13.7 SET A PSL FILE PATH

You can associate a PSL file to enable quick configuration of GOOSE signals.

Right click on an IED and select the **Set PSL file path** option. Locate the file using the explorer pop up window and select it.

---

## 13.8 OPEN A PSL FILE PATH

You can open a PSL file to enable quick configuration of GOOSE signals.

Right click on an IED and select the **Open PSL file**. This will launch PSL Editor with the associated PSL file.

---

## 13.9 MANAGE GOOSE CONNECTIONS

1. To display connections between IEDs click **Show Goose Connections**.
2. To remove connections from the list, select the connection and click **Unsubscribe from message**. A warning appears if any connections are subscribed to by other IEDs.
3. To export the list of connections to an Excel file, click **Export to Excel**.
4. Click **Close View** to return to the main menu.

---

## 13.10 SHOW IED DETAILS

To show the IED details, select the IED and click **Show IED details**.

---

## 13.11 WORKING WITH SCL FILES

The GOOSE Configurator also allows you to include non MiCOM devices by letting you import CID, IID or SCD files, External devices and MiCOM relays without a datamodel installed only allow to be used in GOOSE configurator as publishers.

The tool also allows you to export individual devices as CID, IID files or the entire diagram as SCD, if it was originally created from an SCD.



---

## 13.12 SAVE CHANGES

Publishing and subscribing messages changes the MCL files.

To save all MCL files, select the **File** tab, then **Info**, then **Save All**.

To save currently opened MCL files, select the **File** tab then **Info** then **Save Session**.

To save currently opened MCL files to a single archive file, select the **File** tab then **Info** then **Export**.

To save an individual MCL file:

1. Select the **File** tab then **Info**.
2. In the **Currently opened files** list, select the relevant file and click the **Save** link.

---

## 13.13 RESTORE MCL FILES

To restore MCL files to the previous session, select the **File** tab then **Open** then **Restore Session**.

To revert to a previous version of an individual MCL file:

1. Select the **File** tab then **Info**.
2. In the **Currently opened files** list, select the relevant file and click the **Reload** link.

---

## 13.14 CURRENTLY OPENED FILES

Select the **File** tab then **Info**. Currently opened files are listed in order of when they were opened.

---

## 13.15 RECENTLY USED FILES

Select the **File** tab then **Open**. Recently used files are listed in order of when they were last used.

To reopen recently used MCL files at startup, select the **File** tab then **Options** and check the check box.

---

## 13.16 CLOSE FILES

To close a single file:

1. Select the **File** tab then **Info**.
2. In the **Currently opened files** list, select the relevant file and click the **Close** link.

To close all files that are open:

1. Select the **File** tab then **Info**.
2. Click **Close All**.

---

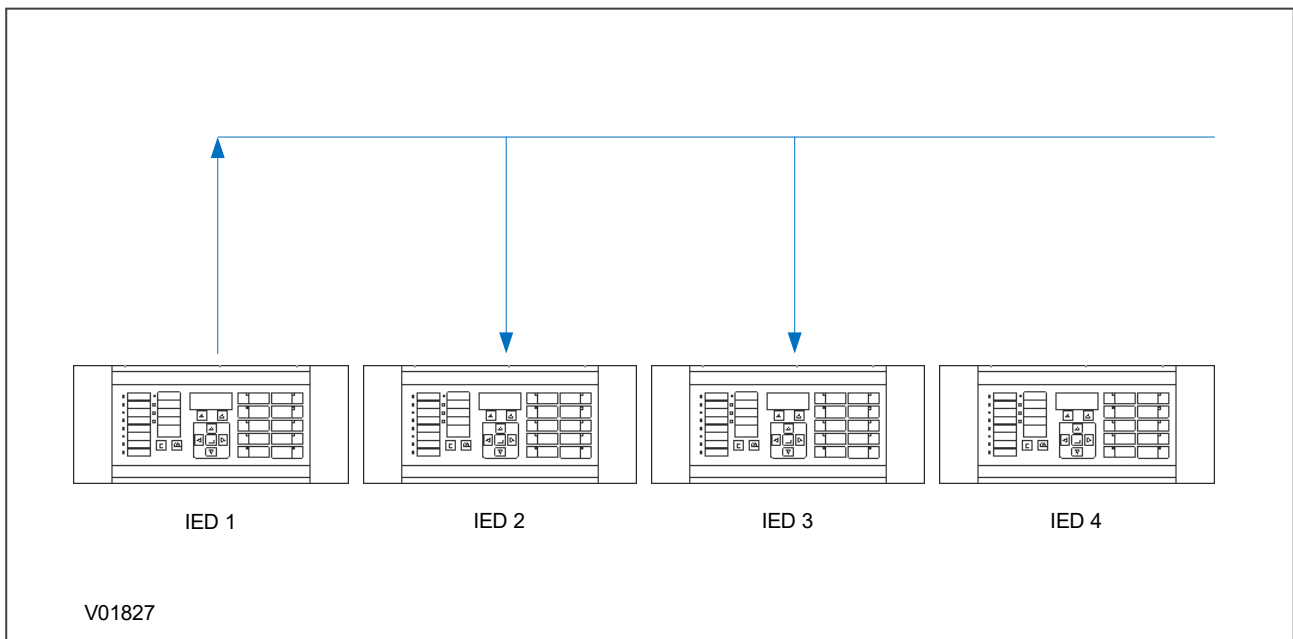
## 13.17 APPLICATION NOTE

This application note will explain how to use the GOOSE Configurator Tool in S1 Agile. You will be able to use the tool to simplify GOOSE configuration and to see in a system all the GOOSE correlations between publishers and subscribers. After reading this note you should be able to import MCL files as well as create, clone and subscribe a new GOOSE control block.

*Note:*

*At present only MiCOM compact and modular IEDs can be used with the S1 Agile tool.*

### 13.17.1 CONFIGURING THE IED

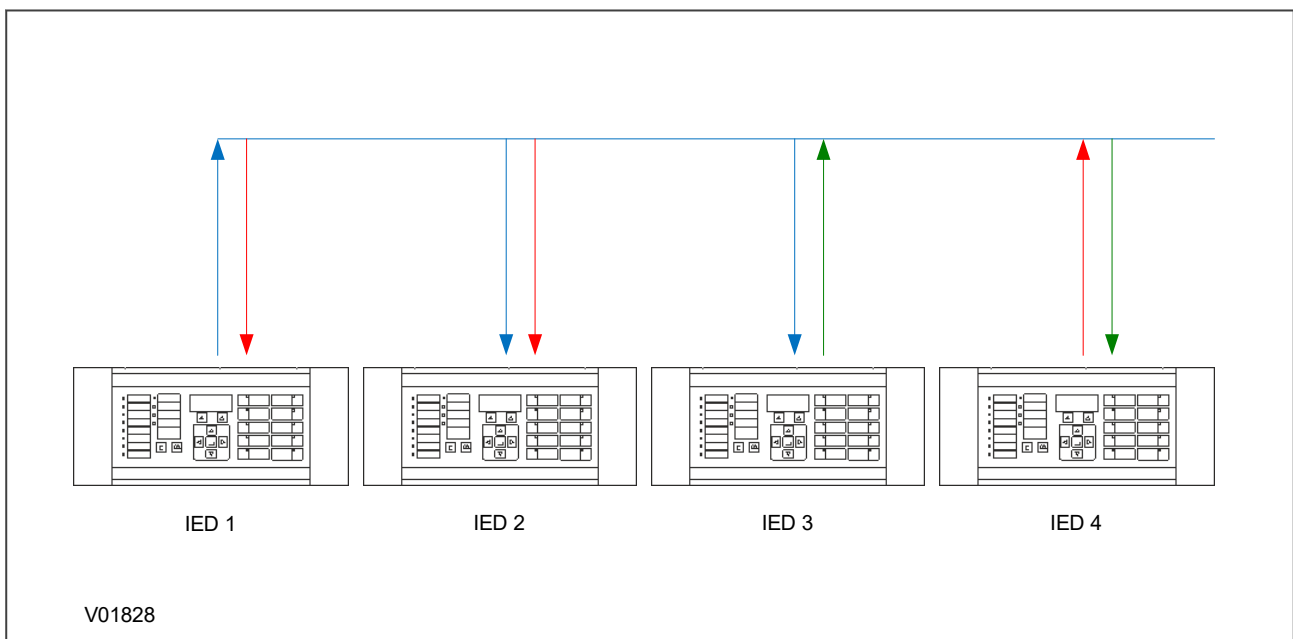


**Figure 19: Initial setup**

To explain how to use GOOSE configurator we will create a system with three IEDs. We will have a GOOSE published by IED 1 and it will be subscribed by IED 2 and IED 3. IED 4 will then be created directly on to the GOOSE configurator.

The following steps will:

- Create a new publication from IED 4
- Subscribe to the newly published GOOSE on IED 1 and IED 2
- Clone a new publication on IED 3 which will then be subscribed to by IED 4



**Figure 20: Final setup**

To simplify the system the GOOSE publishing from IED 1 will include the Boolean value associated with Function Key 1. The GOOSE published from IED 4 will contain Function Key 2.

The initial configuration for IED 1 covers the following:

- IED details
- Communications
- Dataset definition
- GOOSE control block

This is shown in the tables below:

SCL and IED Details	
SCL File ID	P44T
SCL File Version	2.37
Name	IED1

Template Details	
ICD Template	P44T_____03A.ICD
SCL Scheme Version	V1.7
IEC 61850 Edition	Edition 1
Description	P44T Railway Protection
Type	P44T
Configuration Revision	P44Tv03A
Supported Models	P44T???????030* (A)

Communications	
Connected Sub-Network	NONE
Access Point	AP1

Address configuration	
IP Address	192.168.0.1
SubNet Mask	255.255.255.0
Gateway Address	0.0.0.0

General configuration	
Media	Single Copper or Redundant (Fibre or Copper)
Ethernet Failover	Disable
Failover Timeout	2.0
TCP Keepalive	5
Database Lock Timeout	15

System\LLN0\IED1_DS	
Name	IED1_DS
Location	System\LLN0
Contents	System/FnkGGIO1.ST.Ind1.st.Val

System\LLN0\gcb01	
Multicast MAC Address	01 - 0C - CD - 01 - 00 - 00
Application ID (hex)	0
VLAN Identifier (hex)	0
VLAN Priority	4

Repeat message transmission parameters	
Minimum Cycle Time	20 ms
Maximum Cycle Time	1 s
Increment	900

Message Data parameters	
GOOSE Identifier	IED1System/LLN0\$GO\$gcb01
Dataset Reference	IED1System/LLN0\$IED1_DS
Configuration Revision	1

For IED 2 and IED 3 configuration is similar to IED 1. The tables below show you the configuration for GOOSE Subscription:

System\GosGGIO1\Ind1.stVal	
Multicast MAC Address	01 - 0C - CD - 01 - 00 - 00
Application ID (hex)	0

GOOSE Source parameters		
Source Path	IED1\System\FnkGGIO1\Ind1.stVal	
GOOSE Identifier	IED1System/LLN0\$GO\$gcb01	
Dataset Reference	IED1System/LLN0\$IED1_DS	
Configuration Revision	1	
Data Obj Index/Type	1	Boolean
Quality Obj Index	1	

### 13.17.2 EXPORTING A PRECONFIGURED SYSTEM TO GOOSE CONFIGURATOR

You can launch a preconfigured system to the GOOSE configurator by using the S1 tool.

1. Go to the S1 Agile Start Page and click on the **Ethernet Configuration** tile
2. Select the icon on the **GOOSE Configurator** tile

**Note:**

If a system is preconfigured or partially preconfigured it is easier to export the configuration to GOOSE configurator from the system. Otherwise you will need to add each individual MCL file to the tool.

In the **System Explorer** window right click on **System TEST** and select **Show Goose connections**. You can then select the MCL files that match the IEDs you want to export.

Device Name	MCL File
Test/IED 1	IED1.mcl
Test/IED 2	IED2.mcl
Test/IED 3	IED3.mcl

When you have selected the files they will open and an existing connection will be drawn. The figure below shows the chosen connections we described in the initial setup figure at the start of this note.

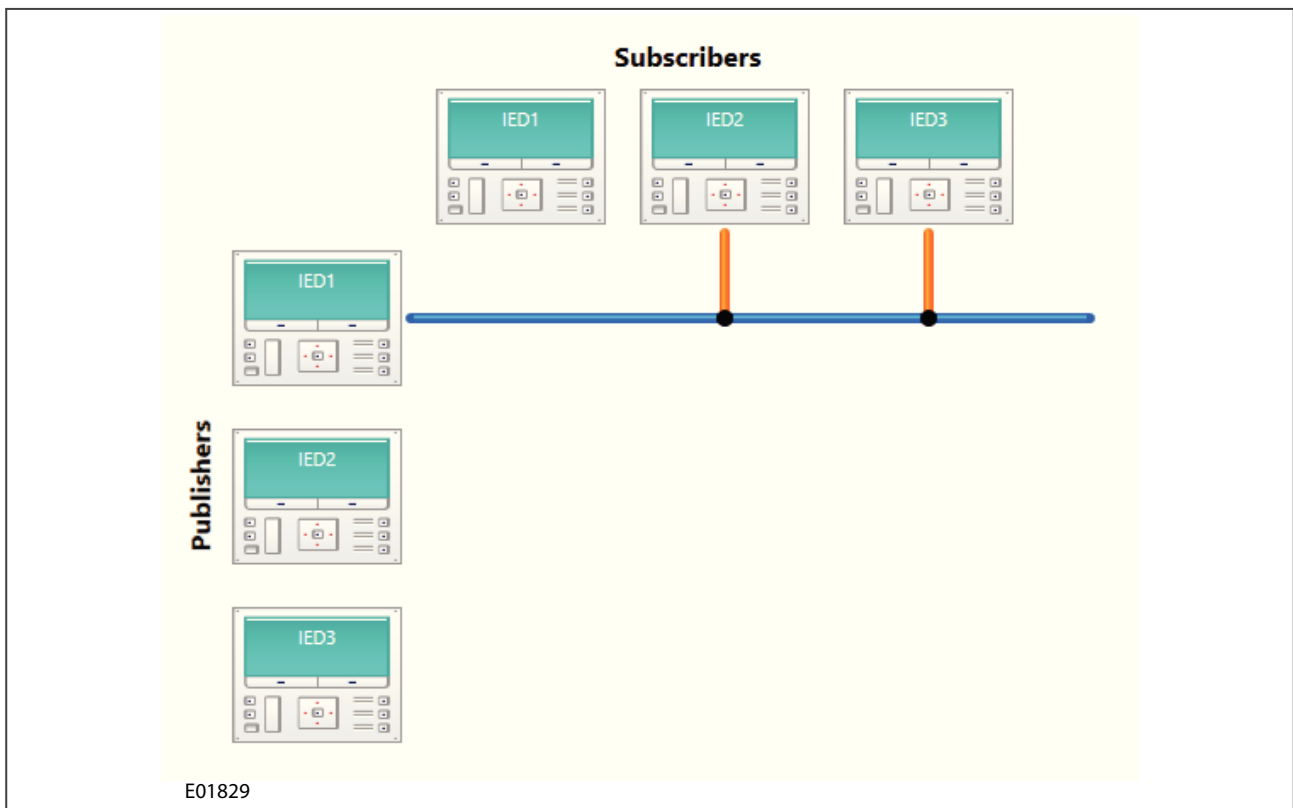


Figure 21: System exported into GOOSE configurator

### 13.17.3 ADDING A NEW IED TO THE GOOSE CONFIGURATOR

We can add a new MCL file to the GOOSE Configurator, but before we can add IED 4 we need to create the MCL file using the IED Configurator.

1. Click on **Tools** and select **IEC 61850 IED Configurator** from the drop down menu
2. Create a new file from the template
3. In the **Select Template using Model Number** window select the model from the drop-down list
4. Change the file name to **IED4** and make sure the IP address is listed as **192.168.0.4**
5. To open the MCL file go back to **Goose configurator** then select > **File > Open > Browse**
6. Select the MCL file created for IED 4

IED 4 has now been added and is part of the scheme.

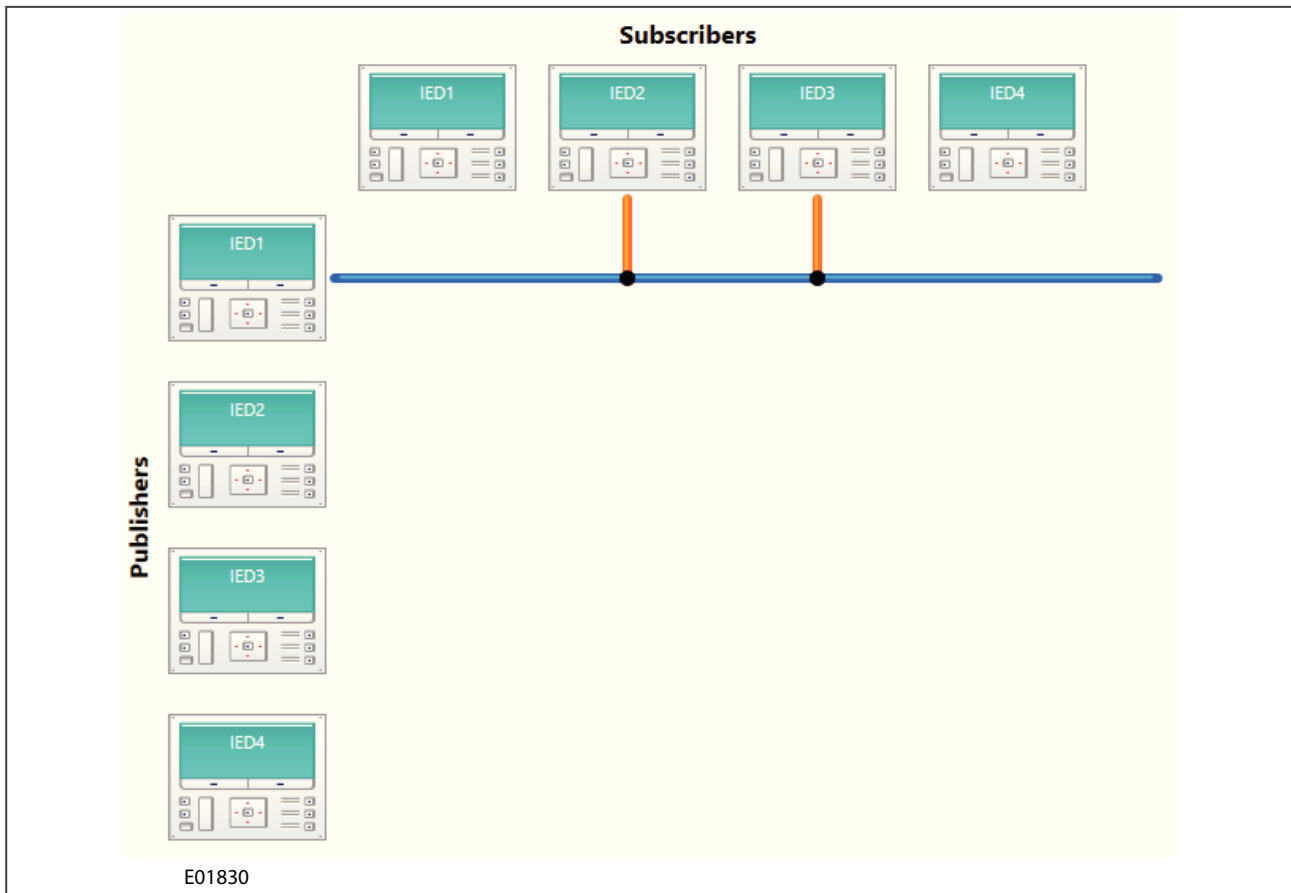


Figure 22: IED 4 added to scheme

### 13.17.4 CREATING A NEW GOOSE PUBLICATION

The next step is to create a new publication on IED 4. For this you will need to create the GOOSE control block publishing information and the dataset.

1. Right click on the device to be configured and choose **Publish a message** or select the IED with a left click and choose **Publish a message** from the tool bar
2. Select the GOOSE control block and choose the required communication parameters. Click **Next**

*Note:*

*The parameters are not editable in GOOSE configurator so you will need to switch to IED configurator to edit these values after they have been created.*

GCB selection	
GCB Name	System\LLN0 > System\LLN0\gcb01
Multicast MAC Address	01 - 0C - CD - 01 - 00 - 00
Application ID (hex)	0
VLAN Identifier (hex)	0
VLAN Priority	4
Minimum Cycle Time	20
Maximum Cycle Time	1,000
Increment	900
Configuration Revision	0

The dataset is now created and Function key 2 is published.

From the published list select **System > FnkGGIO1 > ST > Ind2** and from the tick list check **stVal**. The IED will now publish by a blue line in front of IED 4. You can also see this by selecting **Show published messages** in the tool bar.

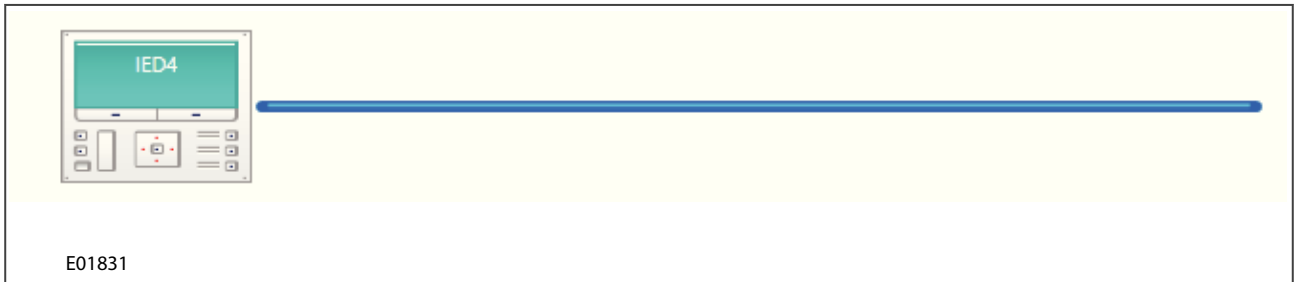


Figure 23: Publishing a GOOSE message

New publications will appear in the list, as shown in the table below:

Publishing IED	Goose Control Block	Message
IED1	System\LLN0\gcb01	System\FnkGGIO1.ST.Ind1.stVal
IED4	System\LLN0\gcb01	System\FnkGGIO1.ST.Ind2.stVal

You can export the publication to a spreadsheet by selecting **Export to Excel** on the tool bar or you can select the publication and choose to delete it from the list.

### 13.17.5 GOOSE SUBSCRIPTION

The new GOOSE published by IED 4 will be subscribed to by IED 1 and IED 2. To subscribe right click on the subscribing IED and select **Subscribe to a message**.

When the **Subscribe to a message** window opens find the data point and then drag it to the required GOOSE input in the subscribing IED. When the subscription is complete a line will appear connecting the points and the subscription will be visible in the view.

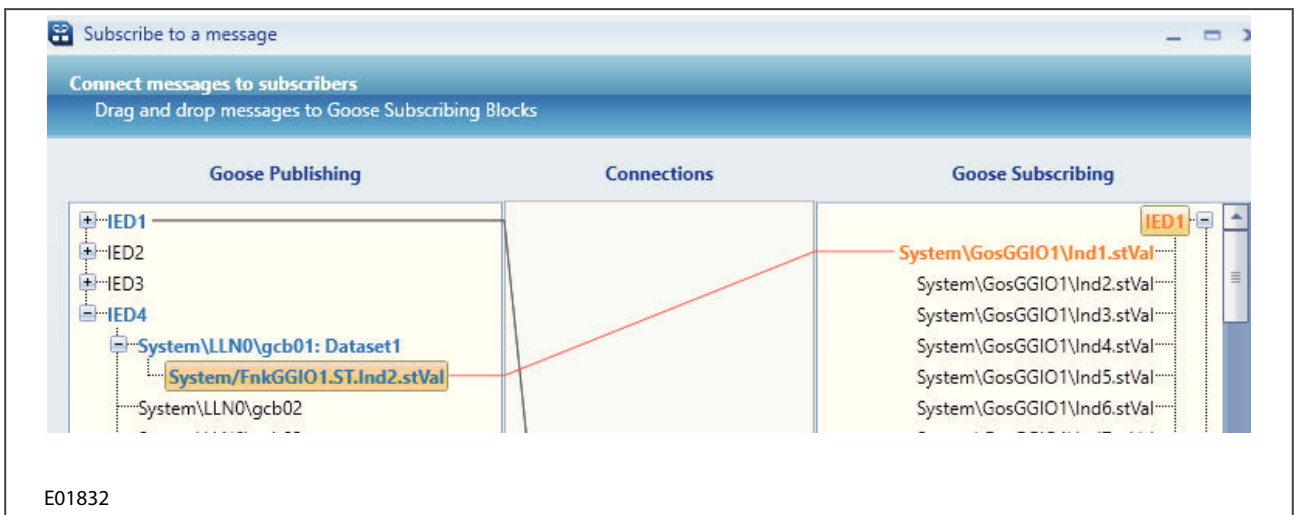


Figure 24: IED 1 subscribed to IED 4

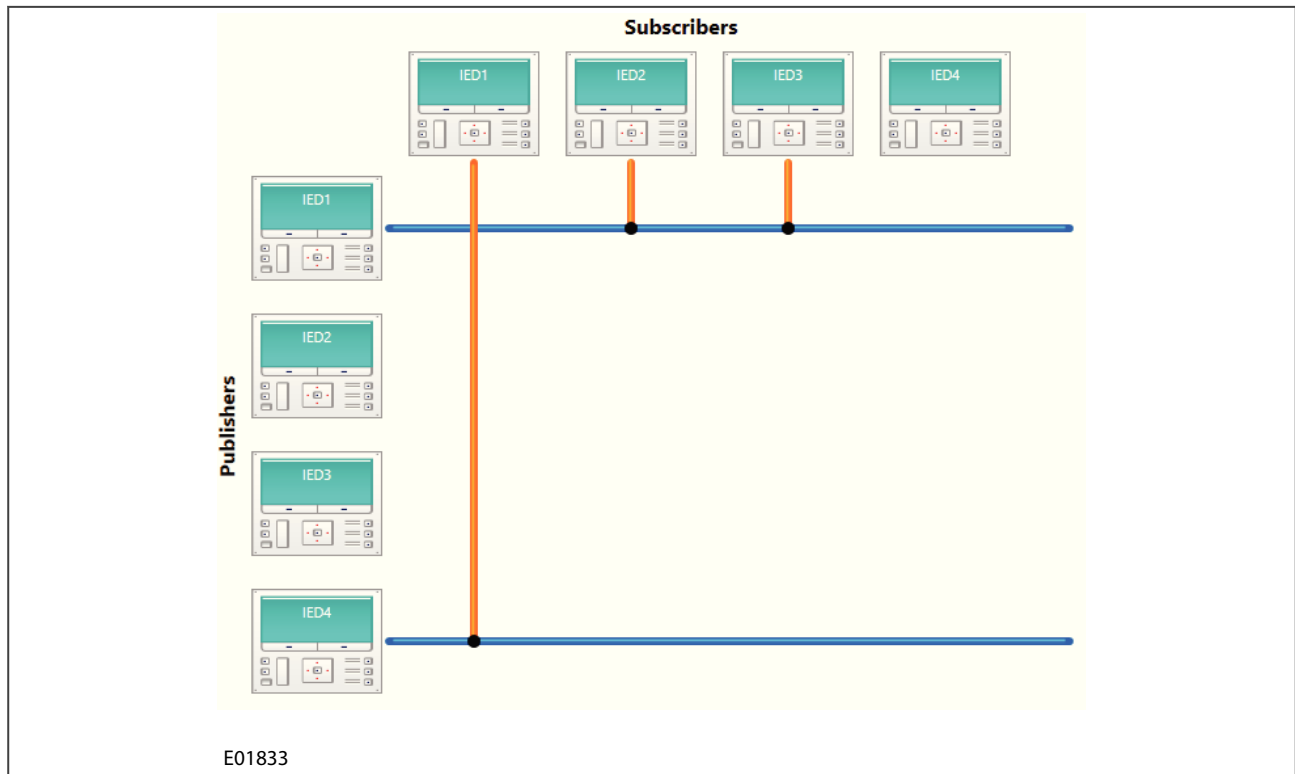


Figure 25: Subscription completed on IED 1

This process can be repeated for IED 2 using the **Subscribe to a message** button on the tool bar. When the subscription is complete IED 1 and 2 will have a connection to the blue line representing the GOOSE published by IED 4.



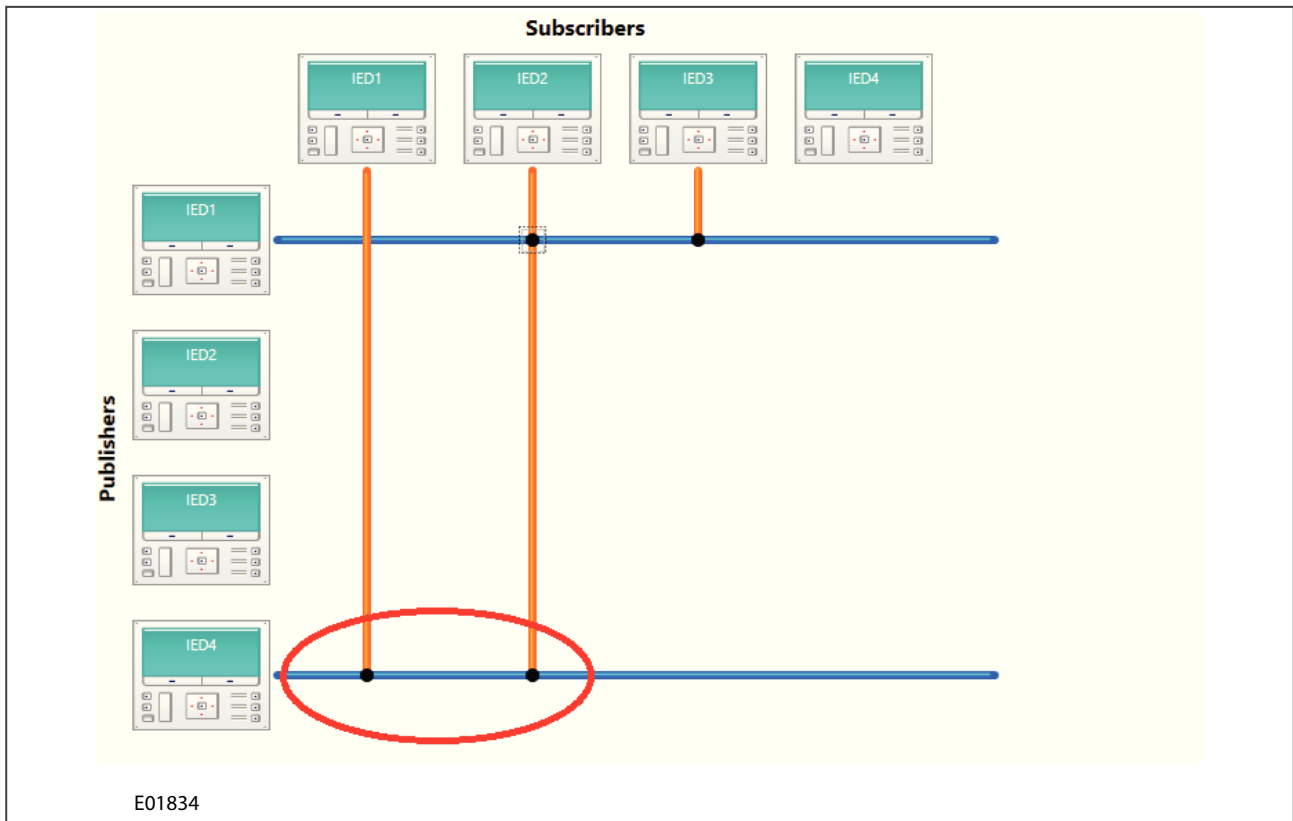
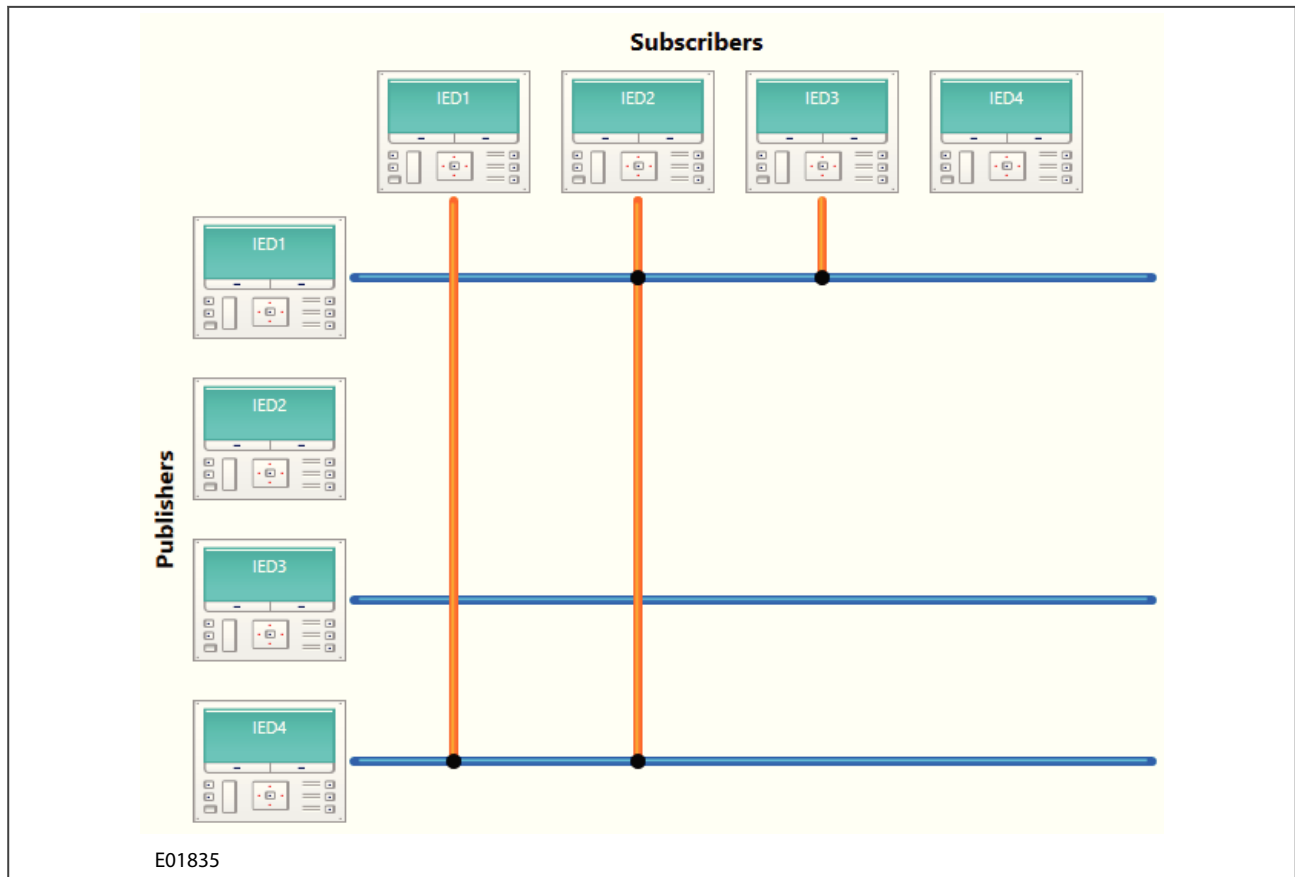


Figure 26: GOOSE subscriptions to IED 4

### 13.17.6 CLONING OF A PUBLISHER

Data shared through GOOSE by IEDs of a similar type across a substation will be the same. You can simplify the process by publishing one device, which can then be cloned to another device. In this example IED 3 uses the same GOOSE publication as IED 4.

1. Right click IED 3 and click **Clone publishing**. You can also select IED 3 and use the **Clone publishing** button on the tool bar.
2. In the **Select publishing IED** window select **IED 4** publication. You will see the location of the file under **File Path** and Yes under **ICD Available**
3. In the **Select target publishing IED** window select **IED 3** as the destination for the cloning process. Again the location will be displayed under **File Path** and Yes under **ICD Available**



**Figure 27: IED 3 cloned publication**

IED 4 will now subscribe to the message from IED 3. The diagram below shows the configuration as described in the final setup diagram, which is located at the start of this note.

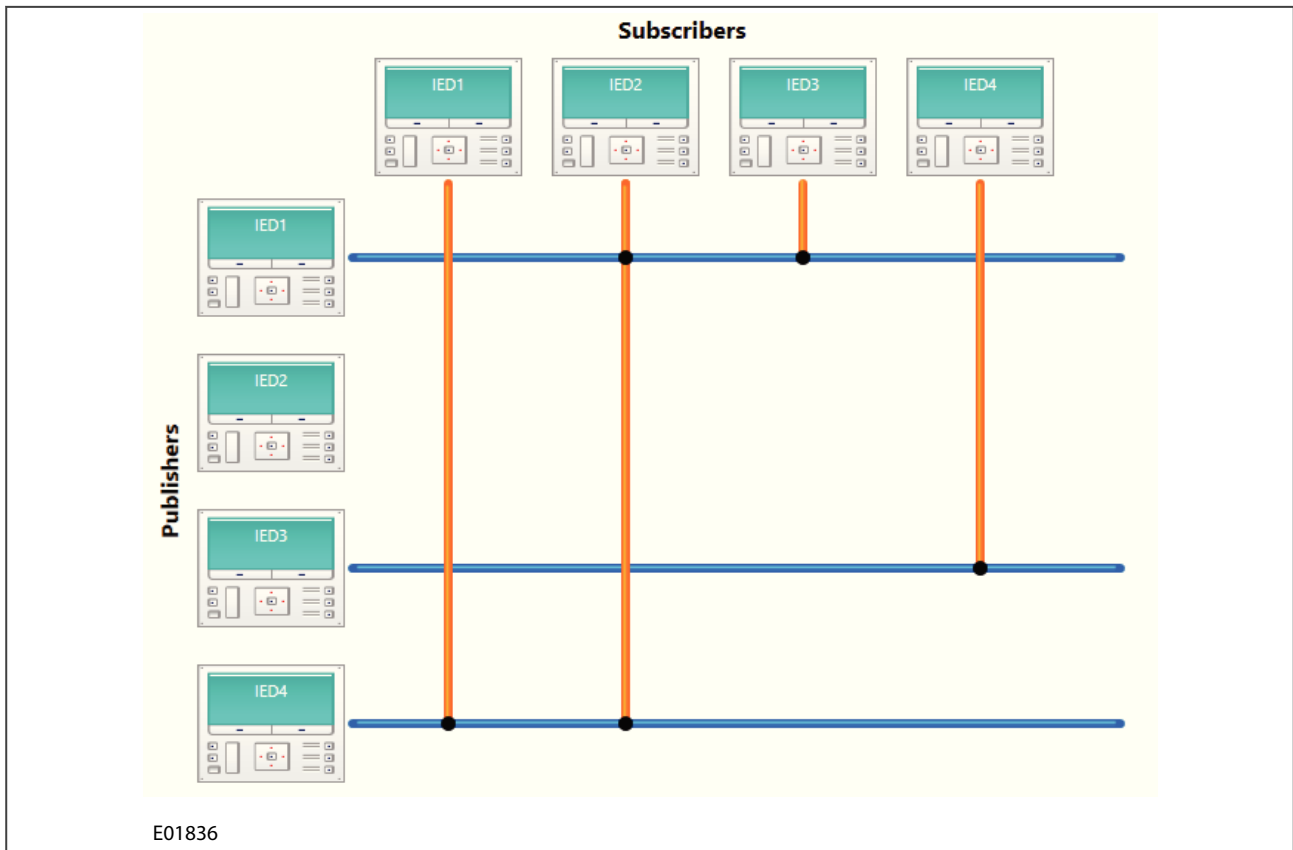


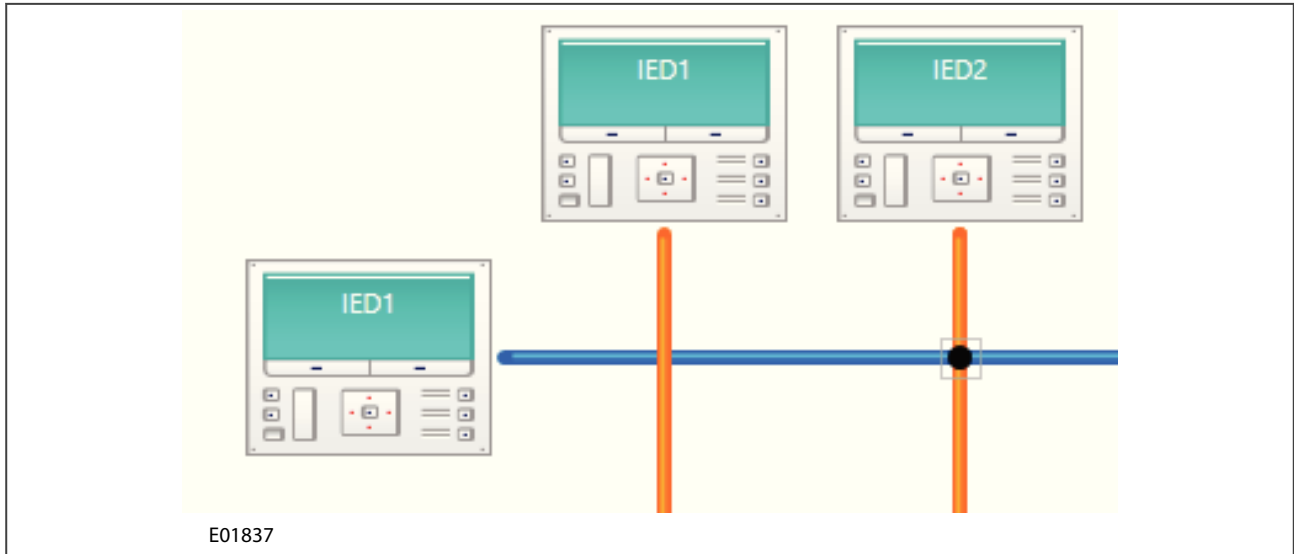
Figure 28: Final configuration

### 13.17.7 VIEW SUBSCRIPTIONS

To see all your subscriptions select **Show GOOSE connections** on the tool bar. In the summary table all the configured GOOSE messages will be displayed. From this point you can either **Export to Excel** or unsubscribe.

Publisher					Subscriber		
IED Name	GOOSE Control Block	Data Set	Message	File Path	IED Name	GOOSE Subscribing Block	File Path
IED1	System\LLN0\gcb01	IED1System/LLN0\$IED1_DS	System\FnkGGIO1\Ind1.stVal	C:\...	IED2	System\GosGGIO1\Ind1.stVal	C:\...
IED1	System\LLN0\gcb01	IED1System/LLN0\$IED1_DS	System\FnkGGIO1\Ind1.stVal	C:\...	IED3	System\GosGGIO1\Ind1.stVal	C:\...
IED4	System\LLN0\gcb01	IED4System/LLN0\$Dataset1	System\FnkGGIO1\Ind2.stVal	C:\...	IED1	System\GosGGIO1\Ind1.stVal	C:\...
IED4	System\LLN0\gcb01	IED4System/LLN0\$Dataset1	System\FnkGGIO1\Ind2.stVal	C:\...	IED2	System\GosGGIO1\Ind2.stVal	C:\...
IED3	System\LLN0\gcb01	IED3System/LLN0\$Dataset1	System\FnkGGIO1\Ind2.stVal	C:\...	IED4	System\GosGGIO1\Ind1.stVal	C:\...

If you double click on the join between the blue and orange bar you will see a sub list of all your subscriptions from the intersecting IEDs, as shown below.



**Figure 29: Interconnection view**

Select **Save Session** to save the diagram created GOOSE configurator. This will create a file extension “.gctsession” which you can open in the future. This is useful as the GOOSE configurator takes MCLs from multiple S1 systems. When you select **Export** the file will create a compressed version of “.gctsession” and the MCL files so they can easily be shared with other users.

When you select **Save All** it will save the changes performed to the MCL files without creating a new GOOSE configurator session. Select **Open** to see all the reverse actions for these features.

---

## 14 PHASOR TERMINAL

---

The Phasor Terminal (PMU Connection and Analysis) software tool is used to view and archive real-time IEEE C37.118 synchrophasor data. Multiple PMUs can be quickly and easily configured, connected and graphically compared.

Phasor Terminal can be connected with external devices using different types of transmission media and network protocols. It can communicate with many devices simultaneously in real time and show the connection quality.

---

### 14.1 SYSTEM STABILITY

Electrical power systems are becoming ever more complex and therefore ever more difficult to manage. This is due to various reasons, such as deregulation of the power industry, increasing requirements for high quality reliable energy, and increased supply from renewable sources which provide unpredictable quantities of energy to the grid. Also the grids of different countries and areas that were previously autonomous are becoming more interconnected. This provides great advantages for power distribution across boundaries but creates several energy management problems. Grid stability is therefore a major concern in the industry and a way of accurately predicting out-of-step conditions is becoming essential.

If the power system cannot provide suitable flows between generator and load, this can cause frequency instabilities. These instabilities can lead to underfrequency or overfrequency or out-of-step conditions, which often cause blackouts. The resulting overvoltages cause excessive stress on the equipment, affecting their reliability or operating life.

---

### 14.2 PHASOR MEASUREMENT UNITS

A Phasor Measurement Unit (PMU) can measure phasor quantities in real time. Measurements are timed to a common GPS clock generating 1 pulse per second. These measurements are then communicated back to a central Phasor Data Concentrator (PDC).

---

### 14.3 IEEE SYNCHROPHASOR STANDARD

The IEEE C37.118 standard defines synchronized phasor measurements used in power system applications. It provides a method to quantify the measurement, specifies tests to ensure the measurement conforms to the definition, and specifies error limits for the test. It also defines a data communication protocol, including message formats for communicating this data in a real-time system.

---

### 14.4 HARDWARE INSTALLATION

The PC on which Phasor Terminal is installed must be set up to communicate with the PMU devices. This is done using an Ethernet LAN, or directly using a serial connection (RS232). This document assumes the PMU devices to which you want to connect have already been configured and are available for connection. You will need to know the parameters of the connected devices.

---

### 14.5 USING THE MAIN WINDOW

The main Phasor Terminal window is blank until you create one or more PMU devices. Once you've installed a device, information specific to that device is displayed. If you install more than one device, select the device from the drop-down list.

To separate the Points Explorer window from the main window, double click its header bar. To return it to its original position, double click its header bar again.

The status bar uses an icon to show the device name, connection mode and connection quality. When connected it shows if data frames are received normally, stored as they are received or received with less than 10% of the nominal frame rate. Hover the mouse over the icon to see the current and nominal frame rates.

---

## 14.6 CREATING A NEW DEVICE

To create a new device:

1. Click the **Create new device configuration** icon. The **Edit device configuration** dialog appears.
2. The **Name** field is blank and the other fields have default values. Edit these as required.
3. The **Miscellaneous** panel gives you the option to **Autoconnect**.

In most cases the device is connected to the Phasor Terminal over the LAN by Ethernet.

Any network layer (layer 3) protocol can be used but most systems use IP, in which case an IP address will have been already assigned to the PMU device. A typical transport protocol would be TCP.

UDP is a protocol very similar to TCP but does not have the error-correcting abilities of TCP and it needs less overhead. UDP is often sufficient for real-time streaming so is often used in this type of application. All settings are the same as for TCP.

To connect by Ethernet:

1. Make sure the settings on the PMU tool host match the settings of the PMU device.
2. Make sure the name of the PMU tool host is set to **localhost**, or set the IP address of the PMU device.
3. The IEEE C37.118 standard specifies default port numbers for the network layer. By default, 4712 is used for TCP and 4713 is used for UDP however these can be configured as required.

The Phasor Terminal also supports serially connected PMU devices. To connect by serial port:

1. Set **Protocol** to **Serial**.
2. The **Serial Port** fields have default values. Set these as required.

*Note:*

*Restart the connection after applying a new device configuration.*

---

## 14.7 EDITING AN EXISTING DEVICE CONFIGURATION

To edit an existing device configuration, select the device and click the Edit device configuration icon.

This is the same dialog as invoked by the Create new device configuration icon but with the fields populated with existing parameters of the chosen device. You can change these as required.

---

## 14.8 MANAGE DEVICE CONNECTIONS

To view the configuration details of a device:

1. Select **Connection** then **Devices**.
2. The **Management of devices** window appears. The icons are identical to those in the main window but it provides information about the devices and their connections.

To edit the configuration details of a device:

1. Select **Connection** then **Devices**.
2. In the **Devices Explorer** view, double click the device.
3. Edit the device configuration and click **OK**.

---

## 14.9 USING PHASOR TERMINAL

There are two main windows used to select and display acquired quantities, also known as Points. These windows show the instantaneous current and voltage phasor magnitude measurements, and their associated phase angle with reference to a GPS time signal. The Point Explorer panel tree structure allows you to select which points are available for display and the Plot window shows the points selected in real time.

---

## 14.10 CHANGE A DEVICE NAME

To change a device name:

In the **Point Explorer**, select and edit the device name.

---

## 14.11 DISPLAYING QUANTITIES

A PMU can be wired to several different feeders at a substation and can send multiple channels of information depending on the PMU configuration chosen. The PMU measures the voltage and current of each feeder, then compares these with a GPS time reference to determine their phase angles. This information is sent back to the control unit (in our case, the Phasor Terminal) in the form of phasors (voltages and currents with their associated phase angles).

The PMU can send data at between 5 (minimum) and 50 (maximum) frames per second. To determine the data rate, hover the cursor over the connection icon in the status bar. A data rate of 50 frames per second is the maximum for 50 Hz power systems. Although the IEEE C37.118 standard specifies the data rates at which a PMU device should send data, the phasor terminal accepts the data at whatever rate it is received.

This information can be displayed in two different ways: a polar chart or a time chart. A polar chart is the most convenient, because you can easily display the magnitude and phase angle of the phasor. The magnitude is represented by the length of the line and the phase angle is represented by the line's angular deviation from the x-axis. This is updated once every second.

You can display a trace, marked by the end of the phasor, which allows you to see a history of its behaviour. The maximum and minimum quantity of the phasor is trapped as well as the instantaneous value. These are displayed in a moveable legend.

Time charts can also be displayed if required. For example, the magnitude and phase of a phasor can be displayed on different time charts, in a vertically tiled arrangement. This is updated in real time every second.

---

## 14.12 SELECTING ITEMS TO DISPLAY

To select which items to plot, select the item in the Point Explorer window and drag it into the plot window. It only allows you to do this if it is a valid operation. For example you cannot drag a time-based item (magnitude or angle) into a polar chart, and you cannot drag a polar-based function (phasor) into a time chart. If using a time chart, you can have either the magnitudes of different phasors or the angles, but not both. You need a separate time chart for the magnitude information and the angle information.

To display a quantity:

1. Select which quantity you want to display. The chart icon (polar or time) is enabled, depending on which quantity you select.
2. Click the chart icon to open a blank chart.
3. Drag the quantity into the chart window.
4. You can display many quantities in one chart window. However, the quantities must be the same type.

To remove a quantity from a window:

1. Right-click the plot window.
2. Select Remove then select the item you want to remove.

### 14.12.1 CHANGING PLOT PROPERTIES

To change the scaling and alignment of the plot, right-click the plot window and select **Plot properties**.

**Overlap chart** refers to overlapping the legend over the chart.

### 14.12.2 DISPLAYING DATA IN A RELATIVE VIEW

You can choose a particular quantity as the reference to be used.

To display values in a relative view:

1. Create a plot with at least two quantities.
2. Right-click the plot window and select **Data presentation**.
3. Select the reference data source.

Note:

*The reference quantity is underlined in the legend.*

To switch back to the default raw data view:

1. Right-click the plot window and select **Data presentation**.
2. Select **Raw data view**.

### 14.12.3 CHANGING PLOT NAME

To change the plot name, right click the plot tab and select **Rename** tab.

---

## 14.13 VIEW DEVICE PROPERTIES

To view the properties of a device:

In the **Point Explorer** double-click the point's name and the **Point properties** window appears. Parameters in black can be edited.

If the phasor is defined in Cartesian coordinates, the angle is converted to radians automatically. However, if a device sends angle values in **Angle Units**, the proper unit must be defined during the configuration process.

The timestamp **Adjustment** allows you to adjust for different time bases and affects all data points provided by a device. It has a default value of 0 and can be added to the timestamp received from a device.

---

## 14.14 VIEW POINT PROPERTIES

To view the properties of a point:

In the **Point Explorer** double-click the point's name and the **Point properties** window appears. Parameters in black can be edited.

**Value** represents the magnitude of the phasor.

**View mode** allows you to select **Peak** or **RMS** and applies to the magnitude of the voltage phasors only.

If the **Timestamp shift** is not equal to 0, this means the device is sending incorrect timestamps. This could be due to the clock being desynchronized from the GPS reference.

---

## 14.15 CONNECT TO A DEVICE

To connect to a device:

1. Select the device from the drop-down list on the main window's toolbar, or from the tree in the **Point Explorer** panel.
2. Click the **Connect to the device** icon.

The icon next to the device name in the Point Explorer and the connection indicator in the status bar both show the connection status.



---

## 14.16 DISCONNECT FROM A DEVICE

To disconnect from a device:

1. Select the device from the drop-down list on the main window's toolbar, or from the tree in the **Point Explorer** panel.
2. Click the **Disconnect from device** icon.

You can also disconnect and reconnect in one operation using the **Disconnect from device and reconnect** icon. This is used to reboot the connection in case of configuration changes.

---

## 14.17 CONTROL COMMANDS

The following commands control data collection:

- The **Data ON** icon requests the selected PMU device to start transmitting data.
- The **Data OFF** icon requests the selected PMU device to stop transmitting data.
- The **Configuration request** icon requests the selected device to send its configuration data.

Select **Connection** then **Devices** to view this data.

---

## 14.18 CAPTURING BINARY DATA

To start capturing data:

1. Click the **Start dumping** icon on the main window's toolbar.
2. Browse the destination file and location and click **Save**. The file capture process then begins.

To stop capturing data:

Click the **Stop dumping** icon from the main window's toolbar.

---

## 14.19 EXPORT DATA

The Phasor Terminal can export data to a MS Excel file using a wizard. This simplifies selection of the data range, the time period and the destination file. It also allows you to define the quantities to be exported.

To export data to MS Excel format:

1. Select **Tools** then **Export data** from the main menu, or press **CTRL+E**.
2. Drag and drop the points to be exported into the right-hand pane, or use **>** and **<**. This sets them as **Points to Export**. Click **Next**.
3. Select the time period and destination file.
4. Click **Export**. The progress bar shows when the process is complete.



**Caution:**  
Do not try and export to Excel if you do not have Excel installed. This will crash the application

---

## 14.20 MODIFY DATA ARCHIVE SETTINGS

The Archiving feature allows you to start collecting the data and placing it in a database file.

To start archiving:

1. Select **Tools** then **Archivisation**. The Archivisation setup dialog appears.
2. In the **Db name** field, enter the name of the SQLite database file.
3. In the **Space management policy** field, select one of the following:
  - None**. The disk usage is not being monitored.
  - 10% space left**. The terminal checks to see if there is 10% of the total storage space available on the target drive. If there is not enough space the oldest data is dropped to make more space available.
  - Grow to**. Set the maximum space
4. Check the **Collect Data** checkbox and click **Apply**. Archiving continues until the allocated storage space is reached or until you uncheck the **Collect data** check box and click **Apply**.

## 15 OFFLINE FAULT LOCATOR

The fault locator tool enables the user to model a power system network and, using the disturbance records obtained during a fault (in COMTRADE form), find the location of the fault offline. The tool supports a network with maximum 6 terminals and 4 junctions. Once a power system network is created, it can be saved and used to find the fault locations simply by replacing the disturbance records. The welcome page of the Fault Locator tool has three options:

1. New Network - creates a new network
2. Open Network - opens an existing network
3. Recent Networks - provides access to recently opened/created networks.

Once a network is created and saved, the user will be able to open that existing network and edit them as required.

### 15.1 CREATE A NEW NETWORK

On the Welcome window, clicking the **New Network** button will immediately open a **Save As** file save window. Enter a suitable network name into the **File name:** text entry box. The file will automatically be given a Network Files (\*.fln) file extension. Clicking the **Save** button will open the Fault Locator **Properties:** and **Topology:** window.

In **Properties:**, the **Name** of the network file and the **Unit system** are displayed. The name of the network file and unit system may be changed. The unit system option may be **km** or **miles**.

*Note:*

*The tool does not perform conversion between km and miles. It just provides an indication for the network parameter accuracy. If km is selected as the preferred unit then all line parameters must be entered in km and if miles is selected, then all line parameters must be entered in miles.*

In **Topology:**, there are two buttons to enter details of nodes and lines. The **NODES** button will open the **Define terminals and junctions** window, where all the terminals and junctions of the power system may be defined. The **LINES** button will open the **Define network Lines** window, where all the line parameters may be defined. Lines connect the terminals and junctions defined in the Nodes window, so terminals and junctions must be defined before lines.

### 15.2 DEFINE NODES

A terminal is any node which has the current and voltage measurements from where the disturbance records are obtained. A junction is any point that two terminals get connected (E.g. A busbar). These points will not usually have its own current and voltage measurements and they are used as reference points in any system that has more than two terminals.

*Note:*

*There can only be a maximum of 6 terminals and 4 junctions. Each terminal in the system must have its current and voltage measurements. A minimum of two terminals must be entered to make a valid system.*

In the Fault Locator home window, click the **NODES** button, then in the **Nodes** window, clicking the **ADD** button allows entry of terminal and/or junction details.

When the **ADD** button is clicked a **New Node** window will appear, providing a node **Name** entry text box and a drop-down box for node **Type**. If the node **Type** is **Terminal**, then the **VT Ratio**, **CT Ratio** and **Data Scaling (P/S)** text boxes and drop-down appear, allowing ratios and the format/data scaling comtrade (.cfg) file to be recorded. These details are required to be accurately provided as input. Clicking the **OK** will add each Junction/Terminal to the **Node** window list. To edit the selected node, click the **EDIT** button.

Type (terminal/junction)	Name (it should be unique)	VT Ratio (V)	CT Ratio (A)	Data Scaling (Primary/Secondary)
Terminal	T1	1,000.00	1,200.00	Primary
Terminal	T2	1,000.00	1,200.00	Primary
Terminal	T3	1,000.00	1,200.00	Primary
Junction	J1			

Once all the required terminals and junctions on the power system network are entered, the back button returns to the Fault Locator home window.

*Note:*  
It is advisable to save the network after any additions/modifications.

### 15.3 DEFINE LINES

A line is a defined connection between nodes.

In the Fault Locator home window, the **LINES** button will allow definition of the required line parameters connecting the power system terminals and junctions.

*Note:*  
Line definition requires terminals and junctions to be defined first.  
All impedance and shunt susceptance values should be given per mile/km  
CT and VT are not applicable for junction to junction lines  
At least one line must be defined  
Every terminal or junction must be connected to at least one terminal or junction

In the Define network lines window, click the **ADD** button, a New Line window will open allowing entry of details required to be entered as part of line parameters:

**From** - This defines one end of the line. It can either be a terminal or a junction.

**To** - This defines the other end of the line. This can also be a terminal or a junction.

**Imp. Magnitude** - This is the magnitude of positive sequence impedance of the line in terms of ohms/km or ohms/mile depending on which unit system the user created the system

**Imp. Angle** - This is the angle of positive sequence impedance of the line in degrees.

**Shunt Susceptance** - This is the magnitude of positive sequence Shunt Susceptance of the line in terms of S/km or S/miles depending on which unit system the user created the system

**Length** - This is the length of the line in km or miles depending on which unit system selected in the Fault Locator home window.

Click **OK** to add the Line to the Define network lines list. To edit the selected line, click the **EDIT** button.

From	To	Series Imp.Mag (ohms/km/mile)	Series Imp.Ang (° - degree)	Shunt Susceptance (S/km/mile)	Length (miles/km/mile)
T1	T2	5.000000000	4.000000000	10.000000000	10.0

Once all required lines are added, the back button returns to the Fault Locator home window.

*Note:*  
It is advisable to save the network after any additions/modifications.

## 15.4 NETWORK DESIGN REQUIREMENTS

Design requirements of power system networks modelled with this tool:

- Terminal or junction names must be unique. An error message will be displayed if the user tries to repeat used names in a network.
- All the terminals and junctions specified in the Define terminals and junctions window must be connected in the Define network lines window for the user to be able to save the model.
- In the Define network lines window always enter a terminal name in **From** column and the junction name in the **To** column. Only exceptions are two ended systems and when connecting multiple junctions.
- When a system has multiple junctions always connect the junctions in a left to right order when creating the table. If the network shown below at (a) as an example of correct connection and at (b) incorrect connection of the terminals.

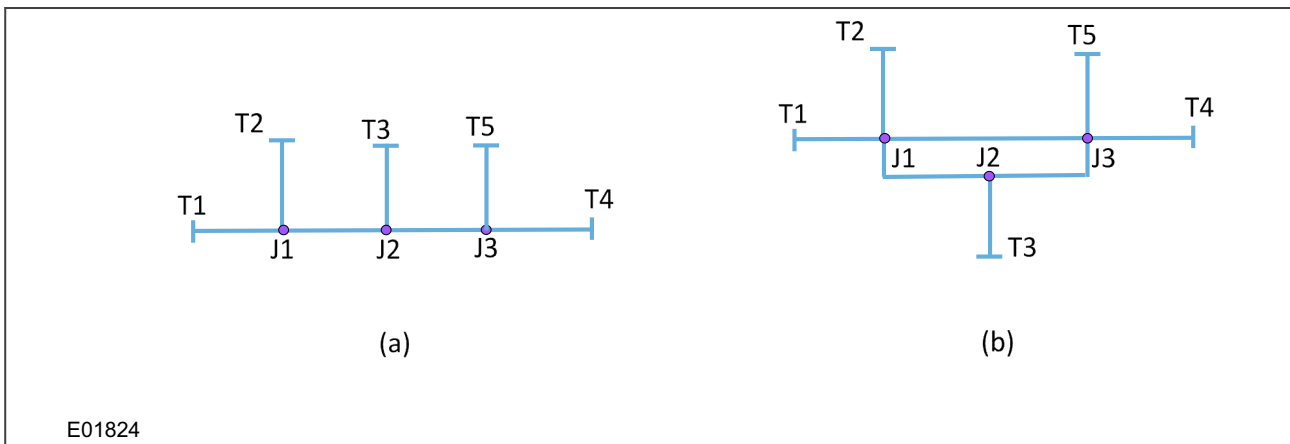


Figure 30: Two five terminal three junction power system networks

## 15.5 EXAMPLE NETWORKS

For any network that has less than two junctions, the order in which the terminals and junctions are entered in to the system does not have any significance. Therefore, while creating the network for the following network systems a specific order is not required.

- 2 terminals (Should not contain junctions)
- 3 terminals with 1 junction
- 4 terminals with 1 junction
- 5 terminals with 1 junction
- 6 terminals with 1 junction

For any other networks, the order must be correctly specified when creating the system.

**Note:**

*It is advisable to simplify network topologies into diagrams similar to those used in the following examples, as this will effectively identify the linearity of the network created. Therefore, reducing chances of making mistakes when creating networks using this tool in left to right order. It is also good practise to make sure that the order of terminals and junctions being created with the tool is maintained consistently when creating nodes and lines.*

### 15.5.1 EXAMPLE 1

In the example below, a 6 terminal 4 junction network, the tool will expect the values to put in from left to right in a linear order as specified before in this document. The first junction to line information entered will be counted as

the junction 1. It is imperative that the first input to the model should be the connection T1 to J1 or T2 to J1. In addition to that, while creating nodes, the order must be maintained.

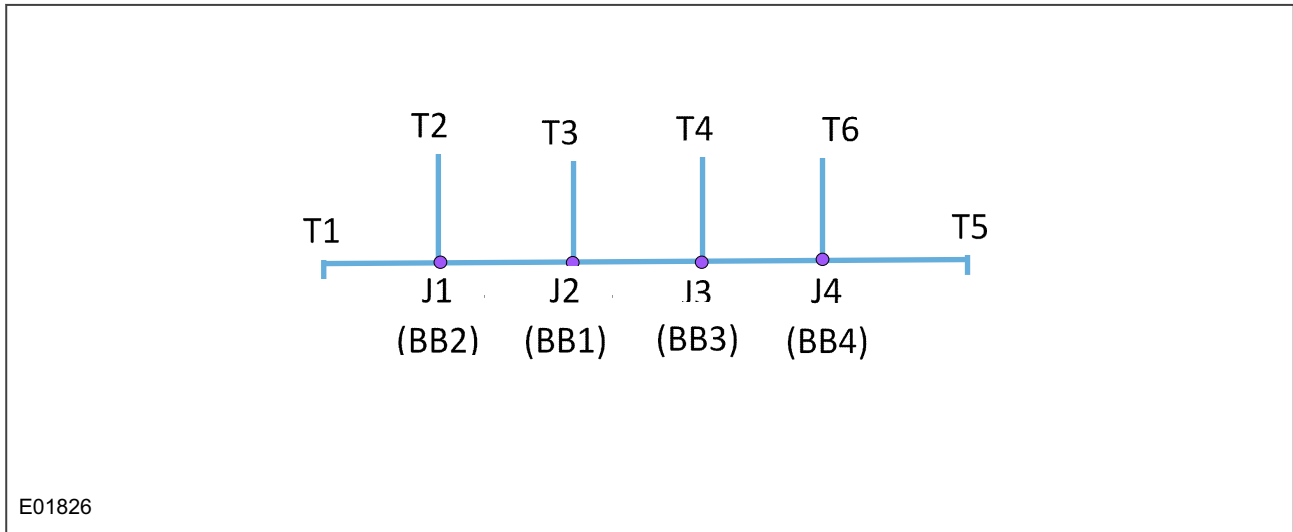


Figure 31: Example - simplified six terminal four junction network

Correctly entered nodes:

Type (terminal/junction)	Name (it should be unique)	VT Ratio (V)	CT Ratio (A)	Data Scaling (Primary/Secondary)
Junction	J1			
Junction	J2			
Junction	J3			
Junction	J4			
Terminal	T1	1,000.00	1,500.00	Primary
Terminal	T2	1,000.00	1,500.00	Primary
Terminal	T3	1,000.00	600.00	Primary
Terminal	T4	1,000.00	1,200.00	Primary
Terminal	T5	1,000.00	1,500.00	Primary
Terminal	T6	1,000.00	1,200.00	Primary

Note:  
Terminals and junctions are defined in order

Correctly entered lines:

From	To	Series Imp.Mag (ohms/km/mile)	Series Imp.Ang (° - degree)	Shunt Susceptance (S/km/mile)	Length (miles/km/mile)
T1	J1	0.501250000	77.280000000	0.000003440	100.0
T2	J1	0.501250000	77.280000000	0.000003440	40.0
T3	J2	0.501250000	77.280000000	0.000003440	10.0
J1	J2	0.501250000	77.280000000	0.000003440	32.0
J2	J3	0.501250000	77.280000000	0.000003440	32.0
T4	J3	0.501250000	77.280000000	0.000003440	40.0
T5	J4	0.501250000	77.280000000	0.000003440	40.0

T6	J4	0.501250000	77.280000000	0.000003440	20.0
----	----	-------------	--------------	-------------	------

Note:  
The first terminal and junction line entered will be counted as junction 1.

Incorrectly entered nodes:

Type (terminal/junction)	Name (it should be unique)	VT Ratio (V)	CT Ratio (A)	Data Scaling (Primary/Secondary)
Terminal	T3	1,000.00	600.00	Primary
Terminal	T4	1,000.00	1,200.00	Primary
Terminal	T5	1,000.00	1,500.00	Primary
Terminal	T6	1,000.00	1,200.00	Primary
Junction	J1			
Junction	J2			
Junction	J3			
Junction	J4			
Terminal	T1	1,000.00	1,500.00	Primary
Terminal	T2	1,000.00	1,500.00	Primary

Note:  
T1 & T2 should be created before T3, T4, T5 or T6.

Incorrectly entered lines:

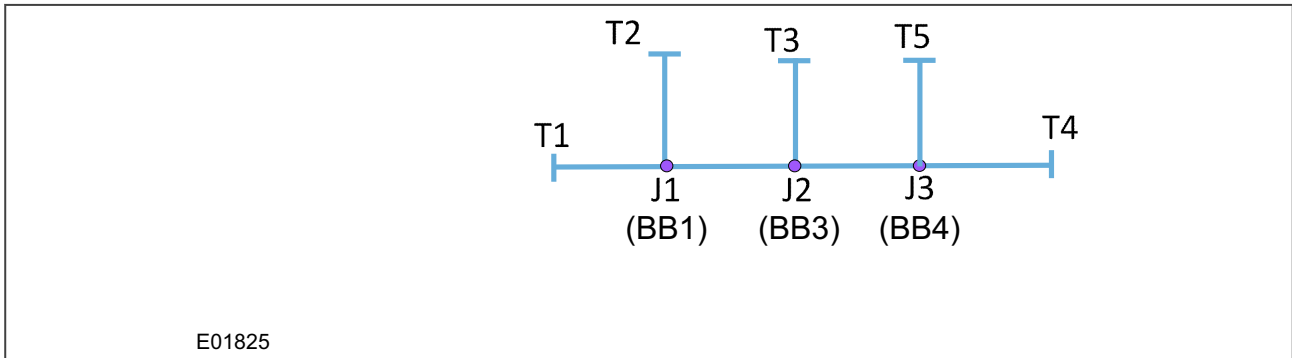
From	To	Series Imp.Mag (ohms/km/mile)	Series Imp.Ang (° - degree)	Shunt Susceptance (S/km/mile)	Length (miles/km/mile)
T3	J2	0.501250000	77.280000000	0.000003440	10.0
J1	J2	0.501250000	77.280000000	0.000003440	32.0
J2	J3	0.501250000	77.280000000	0.000003440	32.0
J3	J4	0.501250000	77.280000000	0.000003440	50.0
T4	J3	0.501250000	77.280000000	0.000003440	40.0
T5	J4	0.501250000	77.280000000	0.000003440	40.0
T6	J4	0.501250000	77.280000000	0.000003440	20.0
T1	J1	0.501250000	77.280000000	0.000003440	100.0
T2	J1	0.501250000	77.280000000	0.000003440	40.0

Note:  
The first junction entered is J2, so J2 will be considered to be in the position of J1.

## 15.5.2 EXAMPLE 2

In the example below, a 5 terminal 3 junction network, the tool will expect the values to put in from left to right in a linear order as specified before in this document. The first junction to line information entered will be counted as

the junction 1. It is imperative that the first input to the model should be the connection T1 to J1 or T2 to J1. In addition to that, while creating nodes, the order must be maintained.



**Figure 32: Example - simplified five terminal three junction network**

Correctly entered nodes:

Type (terminal/junction)	Name (it should be unique)	VT Ratio (V)	CT Ratio (A)	Data Scaling (Primary/Secondary)
Junction	J1			
Junction	J2			
Junction	J3			
Terminal	T1	1,000.00	1,500.00	Primary
Terminal	T2	1,000.00	1,500.00	Primary
Terminal	T5	1,000.00	1,500.00	Primary
Terminal	T3	1,000.00	1,500.00	Primary
Terminal	T4	1,000.00	1,200.00	Primary

*Note:*  
Terminals and junctions are defined in order

Correctly entered lines:

From	To	Series Imp.Mag (ohms/km/mile)	Series Imp.Ang (° - degree)	Shunt Susceptance (S/km/mile)	Length (miles/km/mile)
T1	J1	0.424375000	74.970000000	0.000002868	10.0
T2	J1	0.424375000	74.970000000	0.000002868	5.0
J1	J2	0.424375000	74.970000000	0.000002868	32.0
T5	J2	0.424375000	74.970000000	0.000002868	40.0
J2	J3	0.424375000	74.970000000	0.000002868	50.0
T3	J3	0.424375000	74.970000000	0.000002868	40.0
T4	J3	0.424375000	74.970000000	0.000002868	20.0

*Note:*  
The first terminal and junction line entered will be counted as junction 1.

Incorrectly entered nodes:



Type (terminal/junction)	Name (it should be unique)	VT Ratio (V)	CT Ratio (A)	Data Scaling (Primary/Secondary)
Terminal	T5	1,000.00	600.00	Primary
Terminal	T4	1,000.00	1,200.00	Primary
Terminal	T3	1,000.00	1,500.00	Primary
Junction	J1			
Junction	J2			
Junction	J3			
Terminal	T1	1,000.00	1,500.00	Primary
Terminal	T2	1,000.00	1,500.00	Primary

Note:

T1 & T2 should be created before T3, T4 or T5.

Incorrectly entered lines:



From	To	Series Imp.Mag (ohms/km/mile)	Series Imp.Ang (° - degree)	Shunt Susceptance (S/km/mile)	Length (miles/km/mile)
J2	J3	0.424375000	74.970000000	0.000002868	50.0
T5	J3	0.424375000	74.970000000	0.000002868	40.0
T3	J3	0.424375000	74.970000000	0.000002868	40.0
T4	J3	0.424375000	74.970000000	0.000002868	20.0
T1	J1	0.424375000	74.970000000	0.000002868	10.0
T2	J1	0.424375000	74.970000000	0.000002868	5.0
J1	J2	0.424375000	74.970000000	0.000002868	32.0

Note:

The first junction entered is J2, so J2 will be considered to be in the position of J1.

## 15.6 LOCATE FAULTS

To associate the current and voltage measurements obtained for each terminal, click the **LOCATE FAULTS...** button on the Fault Locator home window to open the **Select COMTRADE files for terminals** window..

Terminal	Path	
T1		
T2		

To upload the COMTRADE files for each terminal, either double-click on the required Terminal entry, or click the folder icon for the terminal entry required. Then navigate to and select the required COMTRADE file (.cfg).

To clear all associated COMTRADE file paths, click the **CLEAR COMTRADE PATHS** button. To change an associated COMTRADE file path, simply select a different file.

**Note:**

The COMTRADE channel selected for each terminal should have 3 phase voltages and 3 phase currents of that terminal. So, in total there should only be 6 analogue channels. In addition, the .cfg file should contain correct unit, phase and rating information. If any details are missing or incorrect, the tool will be unable to take in values accurately from the COMTRADE file and results will be incorrect.

With all required terminal(s) associated with corresponding COMTRADE file(s), click the **START ALGORITHM** button to find the fault location.

The final fault location information about detected fault consists of the line section or junction where the fault occurred and the faulty phases. In order to understand how to interpret the location of the fault, the user needs to understand all 5 different pieces of information displayed on the final output. The explanation for the contents displayed in the result view is as given below:

**Node 1** - This is one end of the line on which the fault is identified.

**Distance 1** - This is the distance of the fault from Node 1 (Units will either be in km or miles depending on the selection made by the user on the homepage).

**Node 2** - This is the other end of the line on which the fault is identified.

**Distance 2** - This is the distance of the fault from Node 2 (Units will either be in km or miles depending on the selection made by the user on the homepage).

**Fault Phases** - The phases that the fault affected.

In the example below, the fault is on the line segment T1J1 and the fault location is 0.41km away from T1 and 31.59km away from J1. The fault is on phase A.

Node 1	Distance 1 (km/miles)	Node 2	Distance 2 (km/miles)	Fault Phases
T1	0.41	J1	31.59	Fault is on phase A

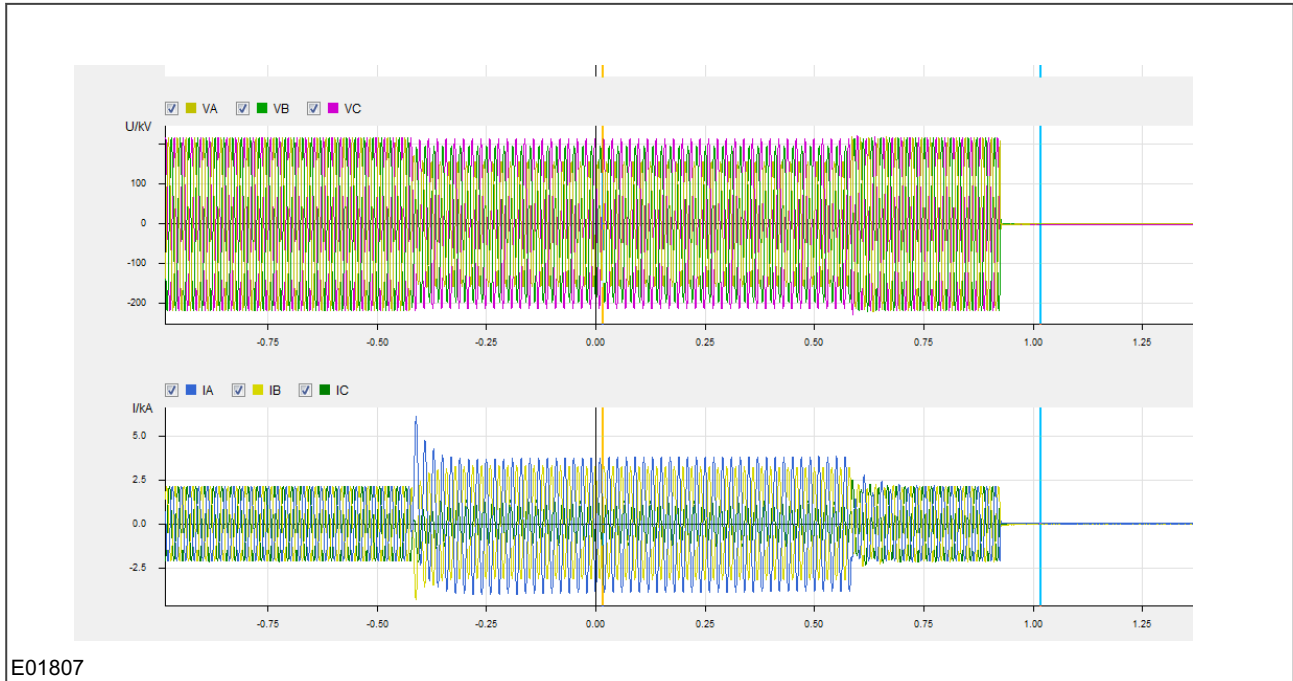
In the example below, the fault is on junction J1 and so node 1 and node 2 indicate the same location and both distance 1 and distance 2 are 0.00. The fault is on phases C and A.

Node 1	Distance 1 (km/miles)	Node 2	Distance 2 (km/miles)	Fault Phases
J1	0.00	J1	0.00	Fault is on phase C and phase A

### 15.6.1 COMTRADE REQUIREMENTS

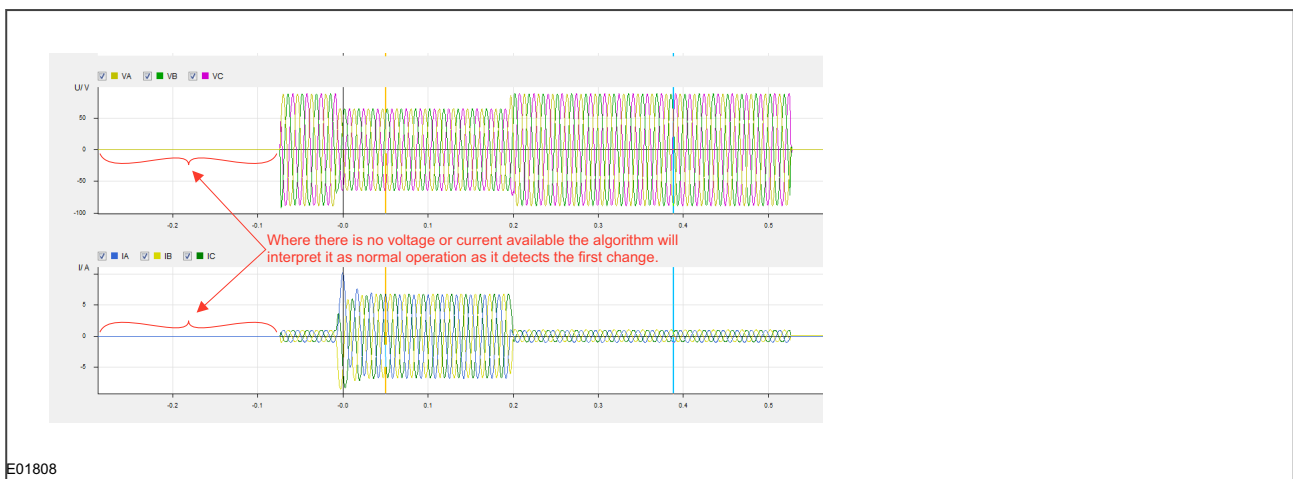
COMTRADE files used to upload to this tool need to satisfy the following conditions:

- The number of analogue channels on each terminal should exactly be 6. Those 6 channels are Va, Vb, Vc, Ia, Ib and Ic. The algorithm only requires these channels to compute the fault location.
- The order these channels (Va, Vb, Vc, Ia, Ib and Ic) can be different. However, if they are recorded in different order then on .cfg file, the phase identification and channel units should be present, because it will assume that it is recorded in phase A-B-C order for voltages and currents.
- Switch on to Fault cannot be identified. The beginning of the disturbance record or the COMTRADE file should have some nominal operating information before the fault, shown below.



**Figure 33: An acceptable COMTRADE file--for a terminal where the first disturbance is the fault**

- An unacceptable format is shown in the figure below, where there is a blank period before the system information starts. If the COMTRADE file contains such blank space before the recorded voltage and current information begins, then the inception of recorded current and voltage point will be perceived as the fault point, which will result in an incorrect result being produced.



**Figure 34: An Unacceptable COMTRADE file--where there is a blank period before the system voltage and current details**

- The inception of the fault on all the COMTRADE files recorded at different terminals should be within a cycle. The maximum variation between the COMTRADE files can be one cycle. If the faults occur at two different time points and the difference is greater than 1 cycle, then the output of the tool will be wrong.
- COMTRADE files should be stored in ASCII format.

*Note:*  
COMTRADE files saved in Binary format are not compatible with this tool.

## 15.7 NETWORK TOPOLOGIES AND RESTRICTIONS

Generally, faults on power system networks containing up to 6 terminals and 4 junctions can be accurately located using this tool. However, there are some requirements.

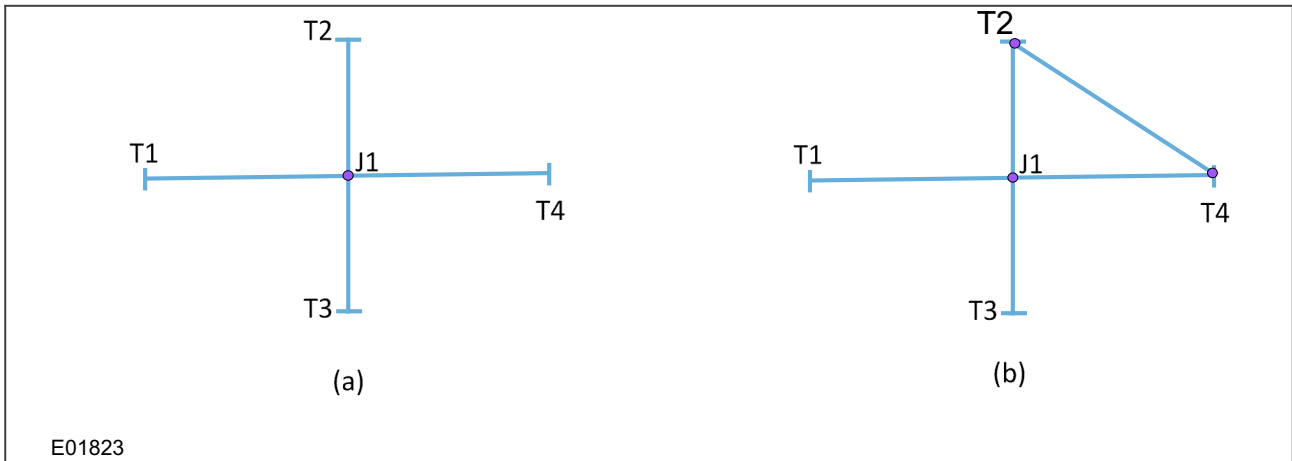
- Each terminal should only be connected to 1 junction (They cannot be connected to multiple junctions or to other terminals unless it is a two-terminal system).
- If the line length is shorter than 10km the accuracy of the algorithm may not be less than 2% as claimed.
- If the faults on the line occur close to the ends (<1km) of the line (either too close to terminal or junction), the fault section identification and fault distance identification may be inaccurate.
- Fault location detection would work accurately for solid faults. If they are resistive faults and if the fault resistance is above 50 Ohms, the fault location detection may be inaccurate.

*Note:*

*When creating networks that contain more than 3 terminals and 1 junction, it is advisable to reference networks detailed in the Supported Topologies section.*

## 15.8 LOOPED NETWORKS

It is vital that the topology of the power system network is linear and not looped. In the four terminal one junction system, shown below, the power system network shown on (a) is the type of accepted four terminal one junction system. If a user tries to create a topology as shown on (b), then the tool will give an error message warning that network validation has failed and that the network is cyclic. The reason for this is because the connections can only be linear, and they cannot be looped (a terminal can only be connected to one junction). In a nutshell when junctions are present, terminals cannot be directly connected. They can only be connected to each other through junctions (An exception is a two-terminal system).



**Figure 35: Example - two different four terminal one junction power system networks**

Another type of looped network is shown below, the power system shown on (a) and (b) don't have terminals directly connected to each other as in the example above. However, on the topology as shown on (b), junctions are interconnected therefore it is still considered as looped network. Hence, the tool will give an error message warning that network validation has failed and that the network is cyclic, when attempting to create such a network.

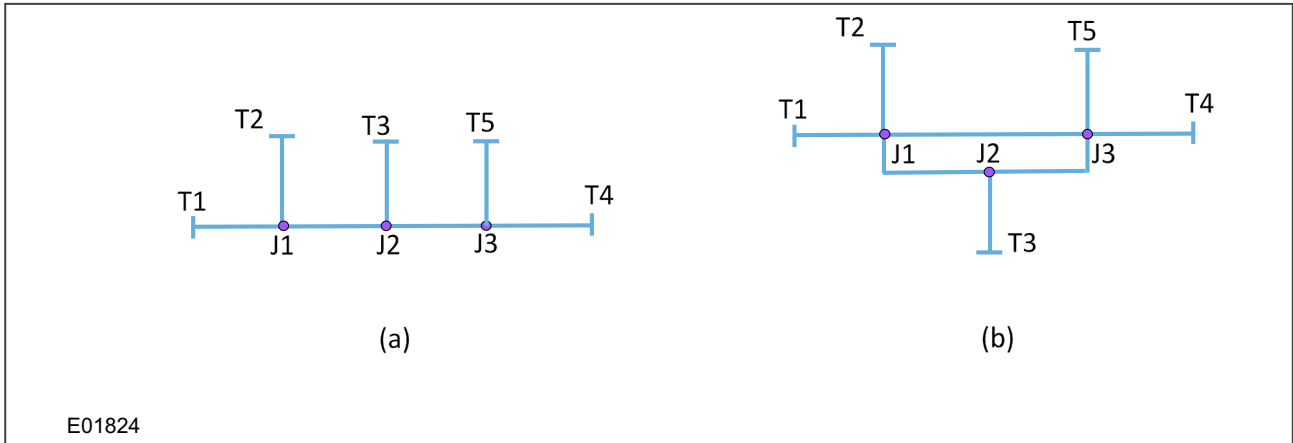


Figure 36: Example - two different five terminal three junction power system networks

## 15.9 SUPPORTED TOPOLOGIES

Supported topologies compatible with this tool are detailed in this section. While creating the topology, it is advisable that existing networks be matched to the network topologies given here.

### 15.9.1 TWO TERMINAL NETWORK

Two terminals are connected together and protection relays are placed at either end to record the respective voltages and currents, example below.

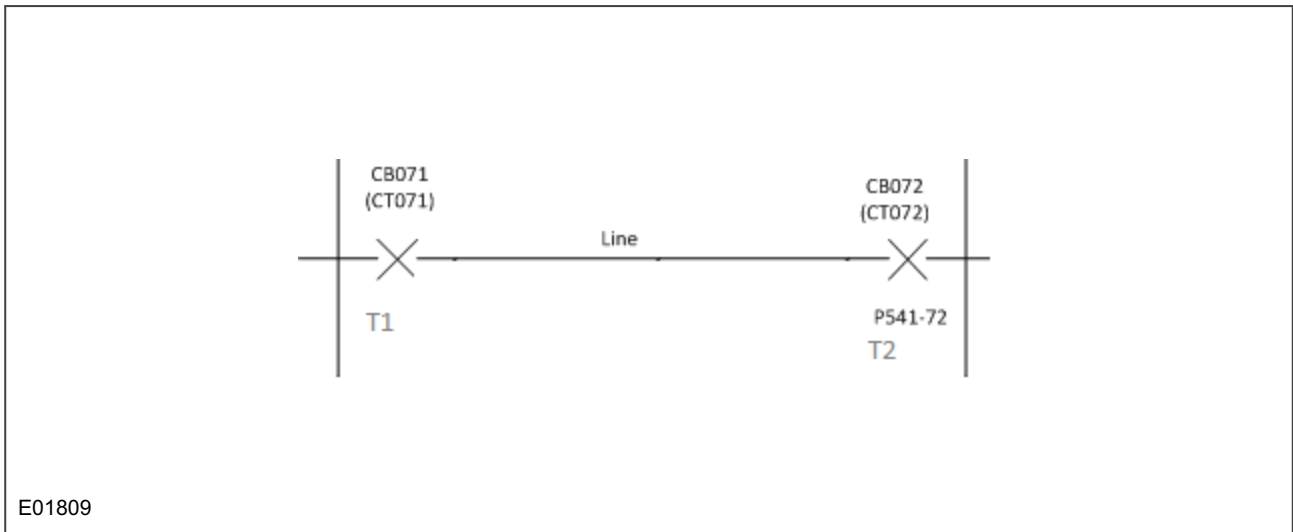


Figure 37: Example - two terminal network

### 15.9.2 THREE TERMINAL ONE JUNCTION NETWORK

A typical three terminal system would normally be connected through one junction. In the example below, busbar 3 (BB3) acts as a junction for terminals T1, T2 and T3. It is important note that BB3 is does not have any line length, hence it is defined as a junction.

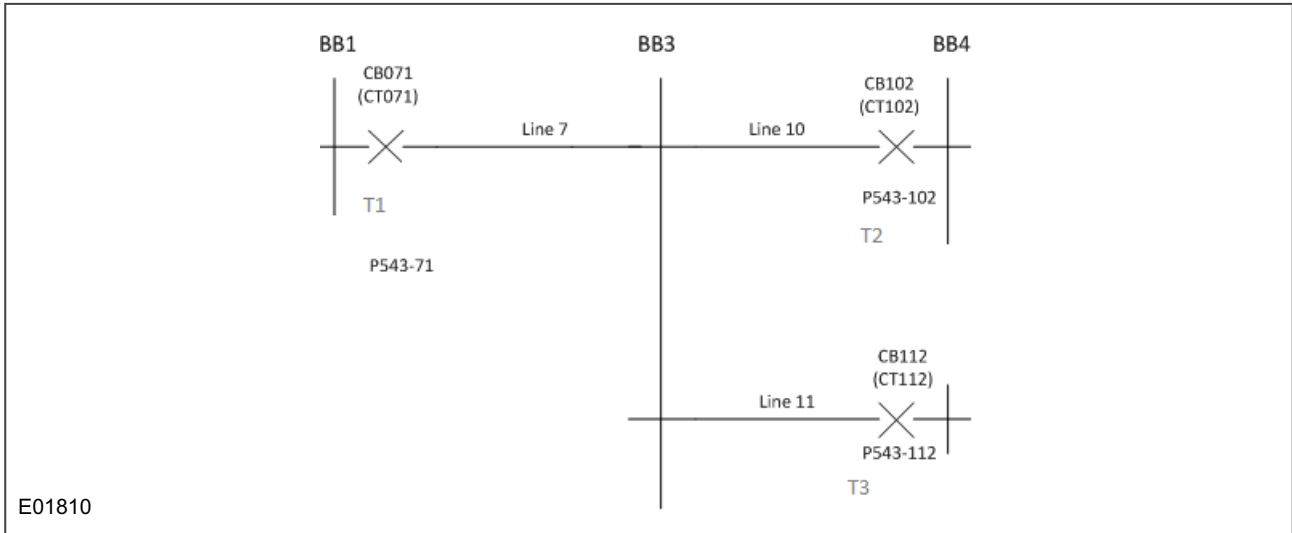


Figure 38: Example - three terminal one junction network

### 15.9.3 THREE TERMINAL TWO JUNCTION NETWORK

A three terminal system with two junctions, shown in the example below, with busbar 3 (BB3) acting as a junction for terminals T1 and T2 and busbar 2 (BB2) connected to T3 acting as the second junction. Note the line section that connects the two junctions (BB2 and BB3).

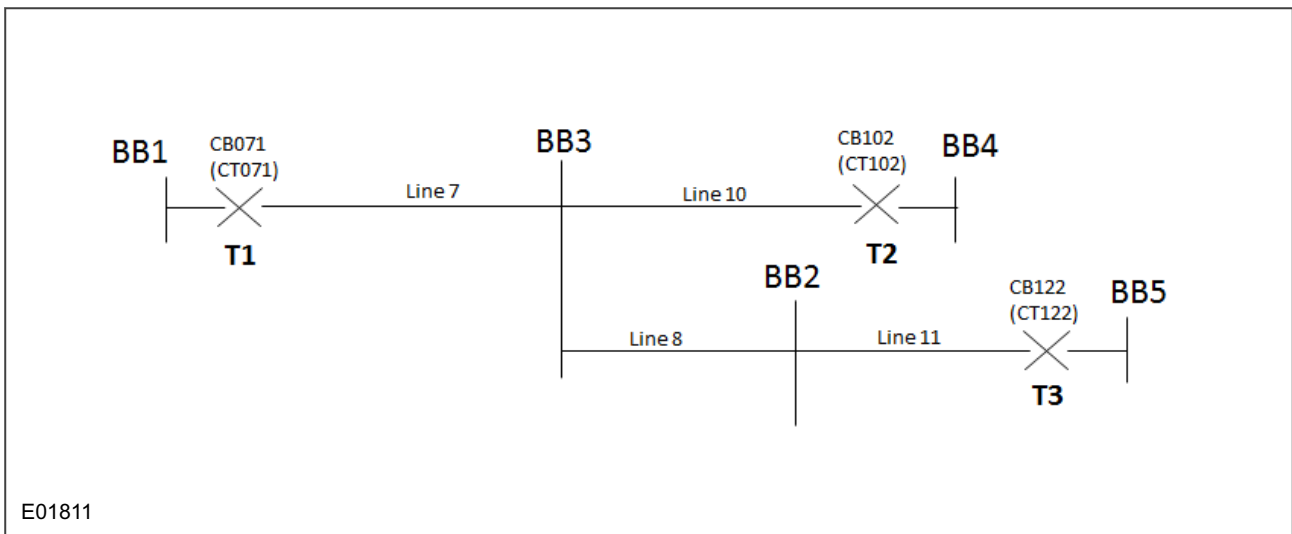


Figure 39: Example - three terminal two junction network

### 15.9.4 FOUR TERMINAL ONE JUNCTION NETWORK

Like the three terminal one junction network, a four-terminal network with one junction is also connected by one busbar (BB1 in this case), which acts as a junction. Busbars that act as junctions do not have any length to them, whereas lines (Lines 6, 7, 8 & 9) that connect to the junction do have their own lengths.

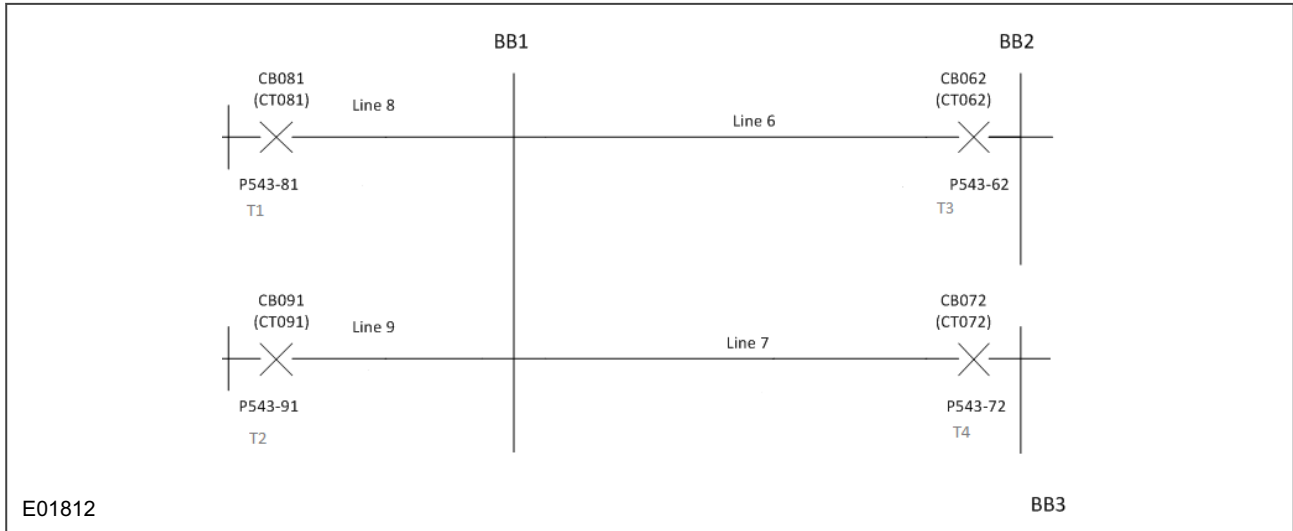


Figure 40: Example - four terminal one junction network

### 15.9.5 FOUR TERMINAL TWO JUNCTION NETWORK

In a four terminals system with two junctions there will be line section connecting two junctions, shown in the example below.

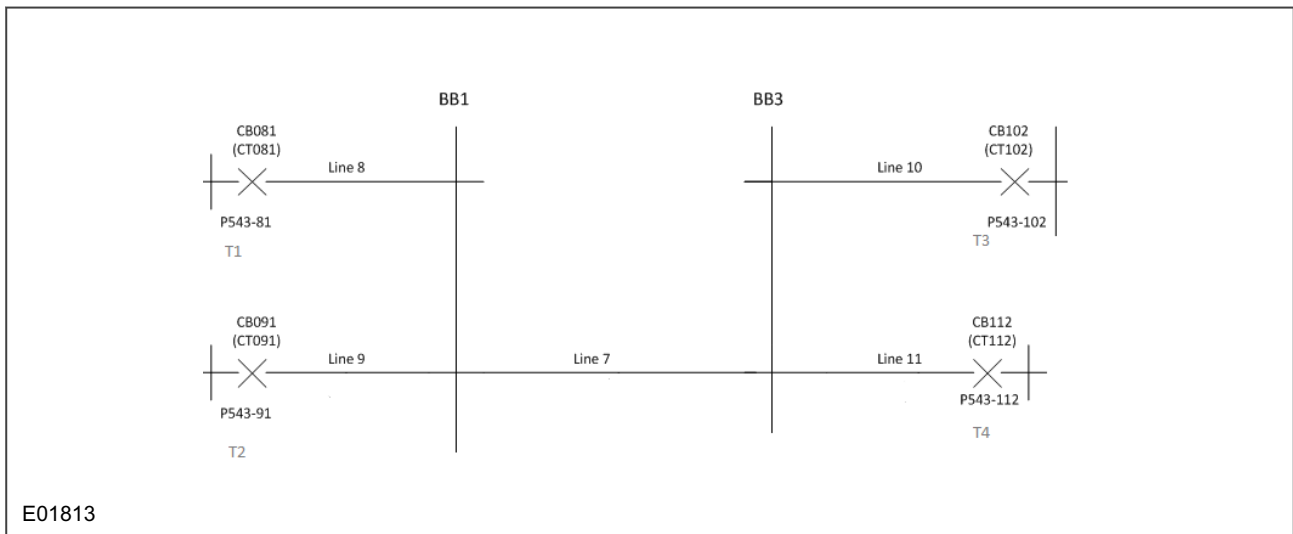


Figure 41: Example - four terminal two junction network

### 15.9.6 FOUR TERMINAL THREE JUNCTION NETWORK

In a four terminals system with three junctions, shown below, Busbar 2 (BB2), Busbar 3 (BB3) and Busbar 6 (BB6). Following the left to right order, BB3 should be assigned as junction1, BB2 as junction2 and BB6 as junction3. T1 and T2 are connected to junction 1, T3 connected to Junction 2 and T4 connected to Junction 3.

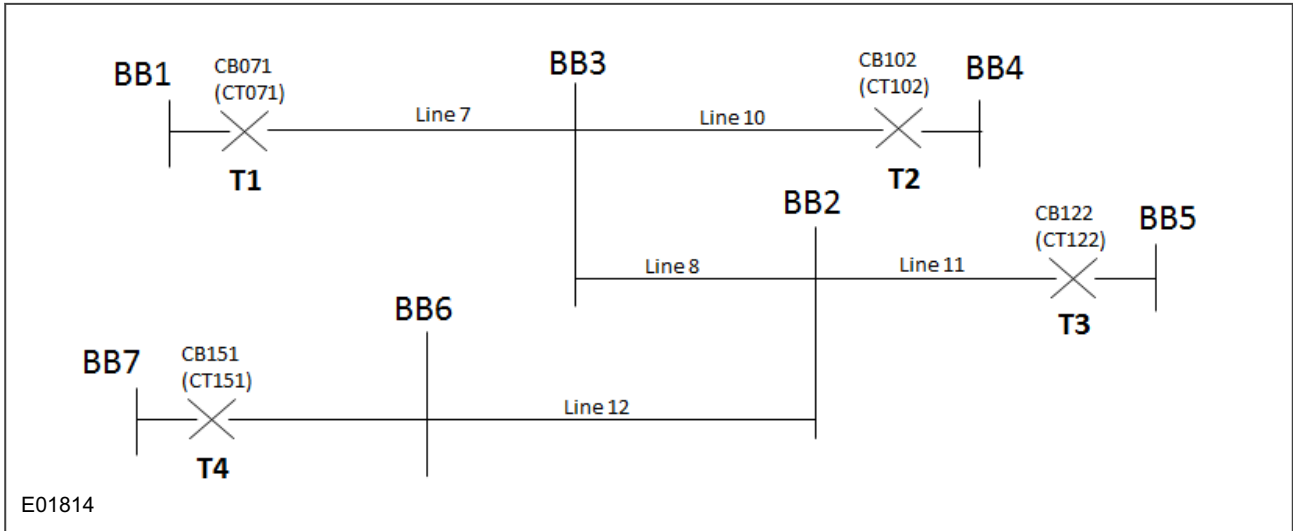


Figure 42: Example - four terminal three junction network

### 15.9.7 FIVE TERMINAL ONE JUNCTION NETWORK

Like other one junction networks, all five terminals will be connected to one Busbar (BB2), shown below.

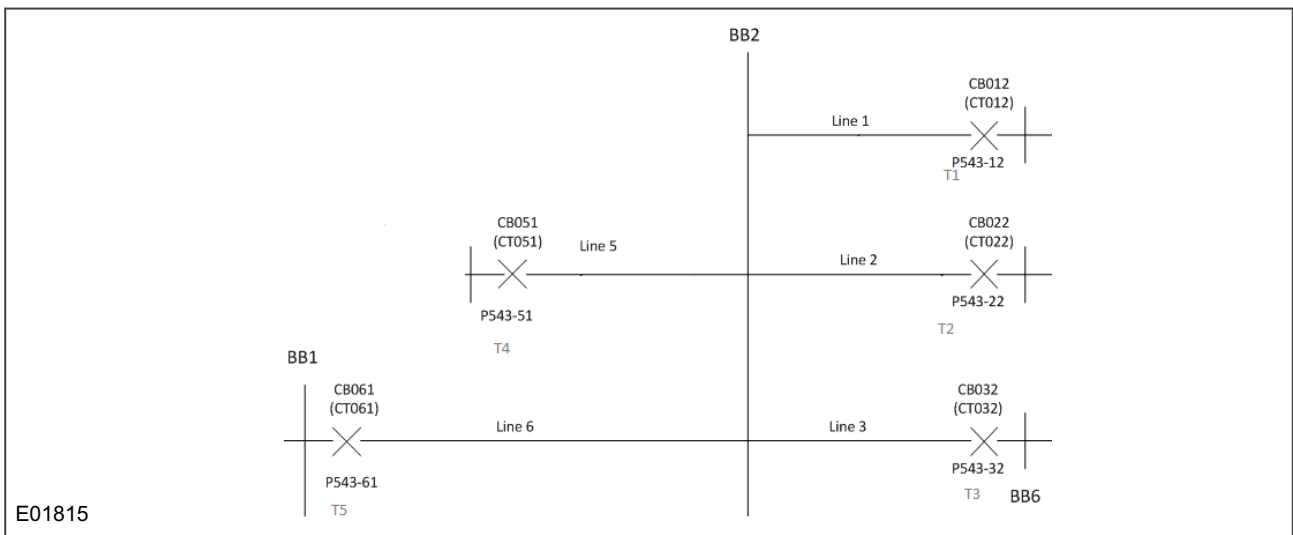


Figure 43: Example - five terminal one junction network

### 15.9.8 FIVE TERMINAL TWO JUNCTION NETWORK

In the five terminal and two junction network, shown below. T1, T2 and T3 are connected to busbar 1 (BB1), which acts as one junction. Terminals T4 and T5 are connected to BB3 and then BB1 and BB3 are connected by Line 7.



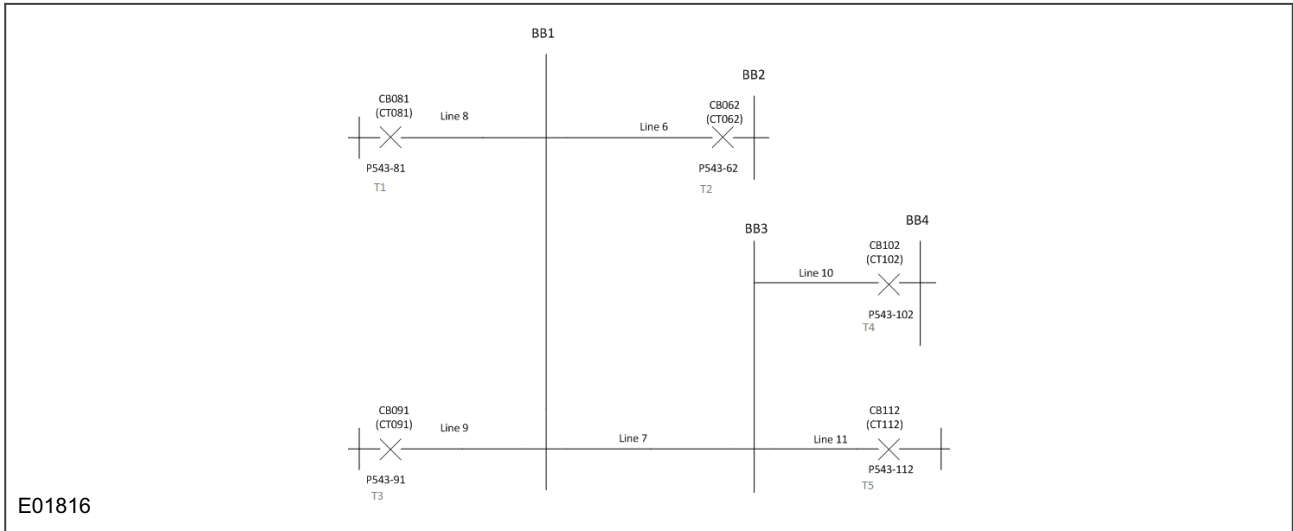


Figure 44: Example - five terminal two junction network

### 15.9.9 FIVE TERMINAL THREE JUNCTION NETWORK

In the five terminal three junction network, shown below. Three junctions are BB1, BB3 and BB4. Terminal T1 and T2 are connected to BB1 and terminals T3 and T4 are connected to BB4 and Terminal T5 is connected BB3. Line 7 connects BB1 and BB3 and line 10 connects BB3 and BB4.

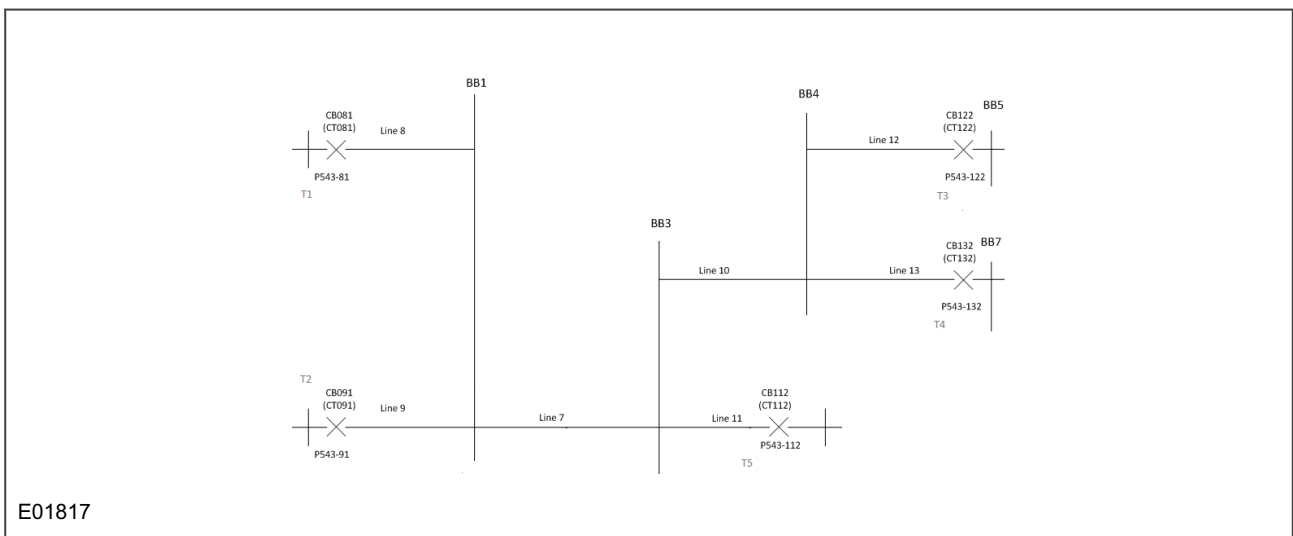


Figure 45: Example - five terminal three junction network

### 15.9.10 FIVE TERMINAL FOUR JUNCTION NETWORK

In the five terminal four junction network, shown below. Four junctions are BB2, BB3, BB6 and BB7. Terminal T1 and T2 are connected to BB3 and terminal T3 connected to BB2, and terminal T4 is connected to BB6 and Terminal T5 is connected BB7. Line 8 connects BB3 and BB2, Line 12 connects BB2 and BB6 and line 13 connects BB6 and BB7.

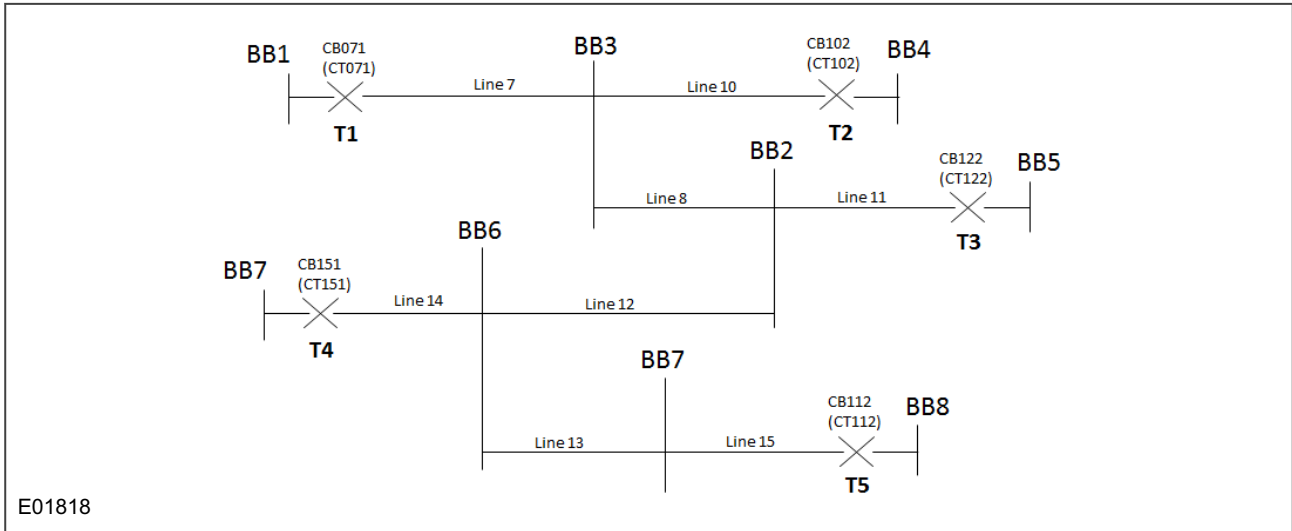


Figure 46: Example - five terminal four junction network

### 15.9.11 SIX TERMINAL ONE JUNCTION NETWORK

Like other one junction networks, all the terminals will be connected to one busbar, which acts as a junction (BB2 in this example).

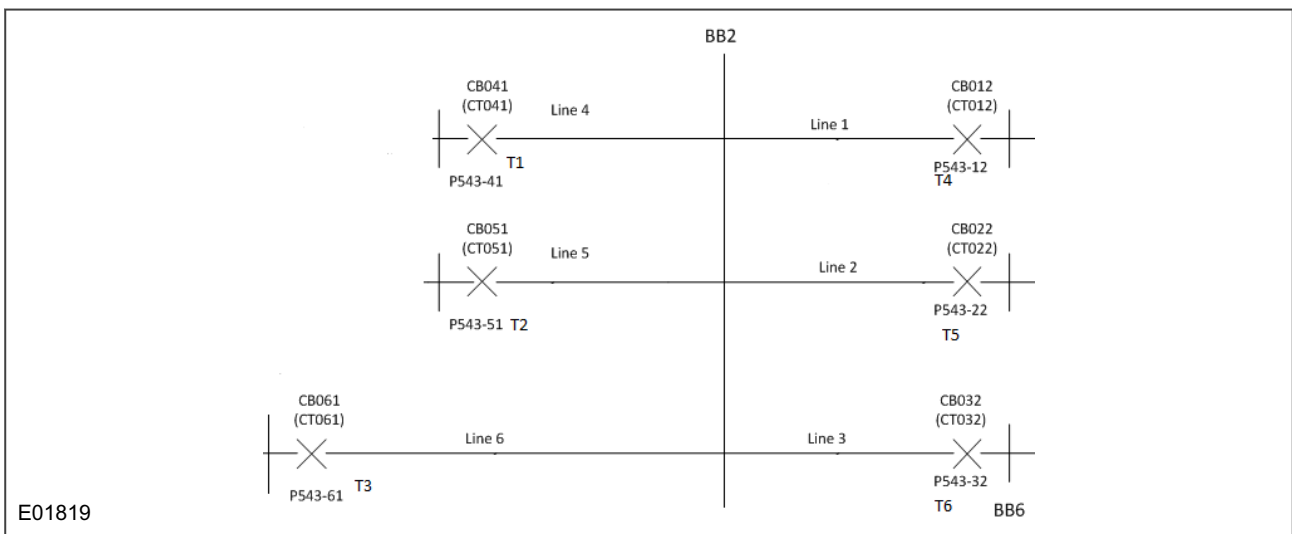


Figure 47: Example - six terminal one junction network

### 15.9.12 SIX TERMINAL TWO JUNCTION NETWORK

In the six terminal two junction network, given below. T1, T2, T3 and T4 are connected to junction BB2 and T5 and T6 are connected to Junction BB1.

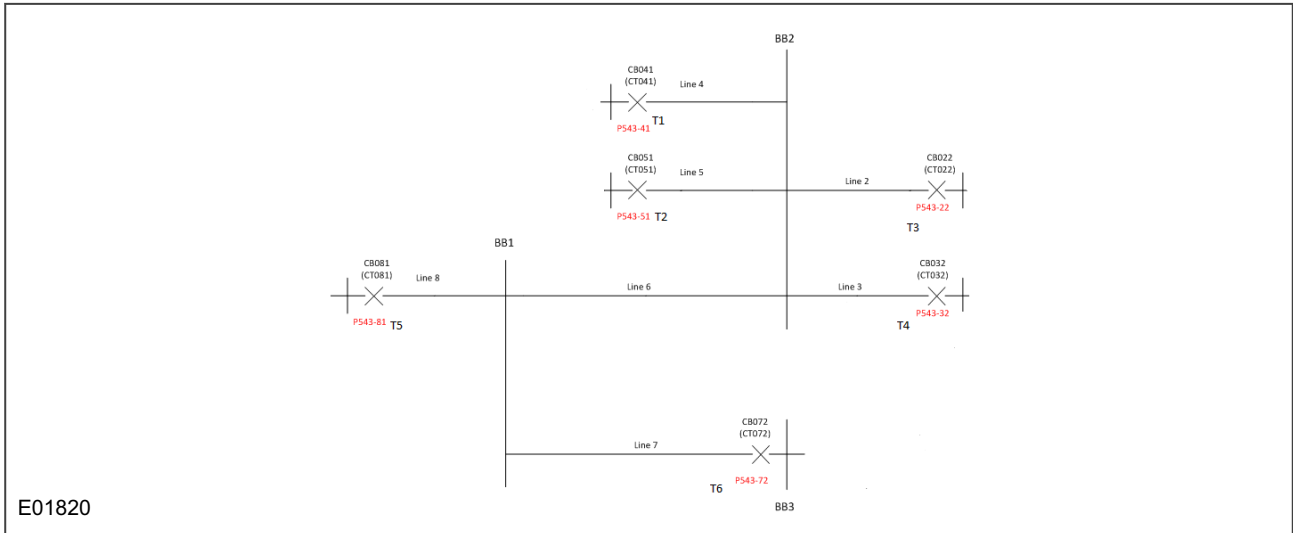


Figure 48: Example - six terminal two junction network

### 15.9.13 SIX TERMINAL THREE JUNCTION NETWORK

In the six terminal three junction network, given below. T1 and T2 are connected to junction BB2, T3 and T4 are connected junction BB1 and T5 and T6 are connected to Junction BB3. BB2 is connected to BB1 by Line 6 and BB1 is connected to BB3 by Line7.

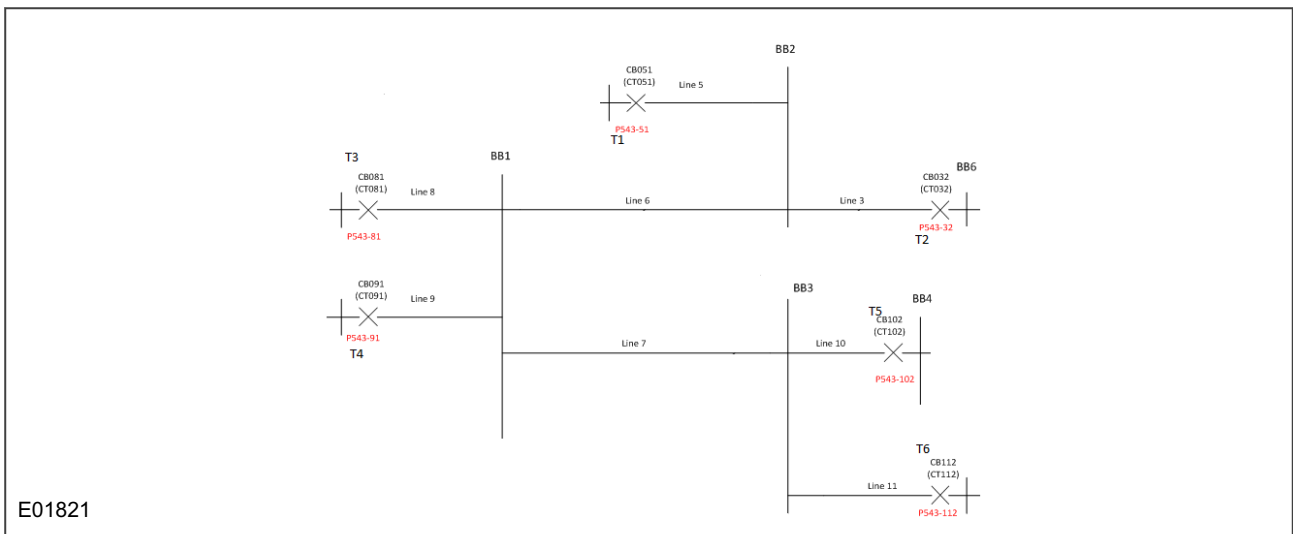


Figure 49: Example - six terminal three junction network

### 15.9.14 SIX TERMINAL FOUR JUNCTION NETWORK

In the six terminal four junction network, given below. T1 and T2 are connected to junction BB2, T3 is connected to Junction BB1 and T4 is connected junction BB3 and T5 and T6 are connected to Junction BB4. BB2 is connected to BB1 by Line 6 and BB1 is connected to BB3 by Line7 and BB3 is connected to BB4 by line 10.

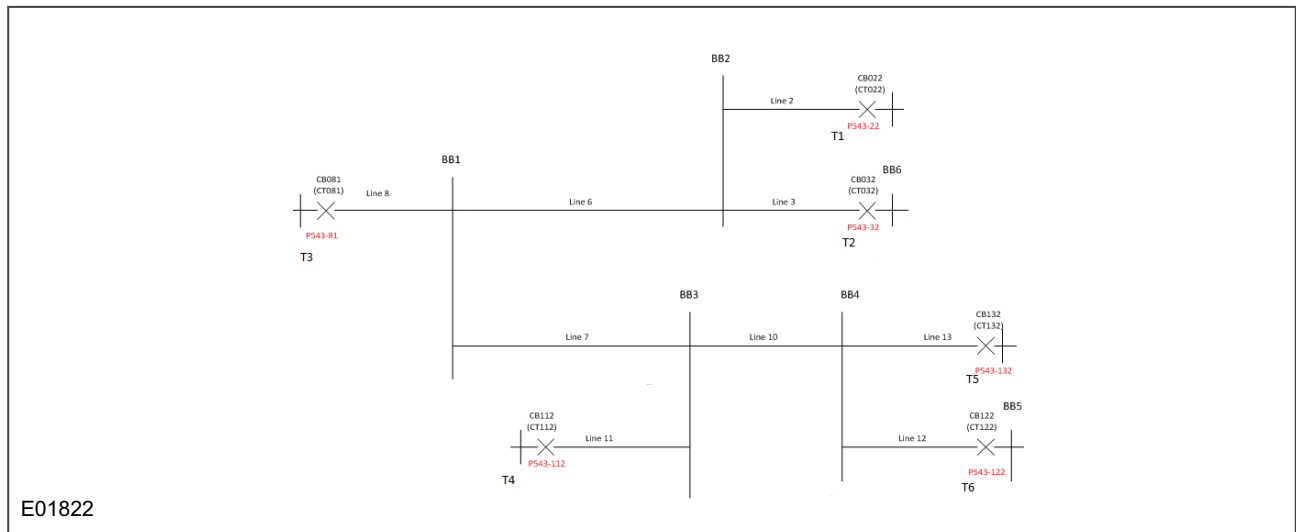


Figure 50: Example - six terminal four junction network

## 16 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.

### 16.1 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.

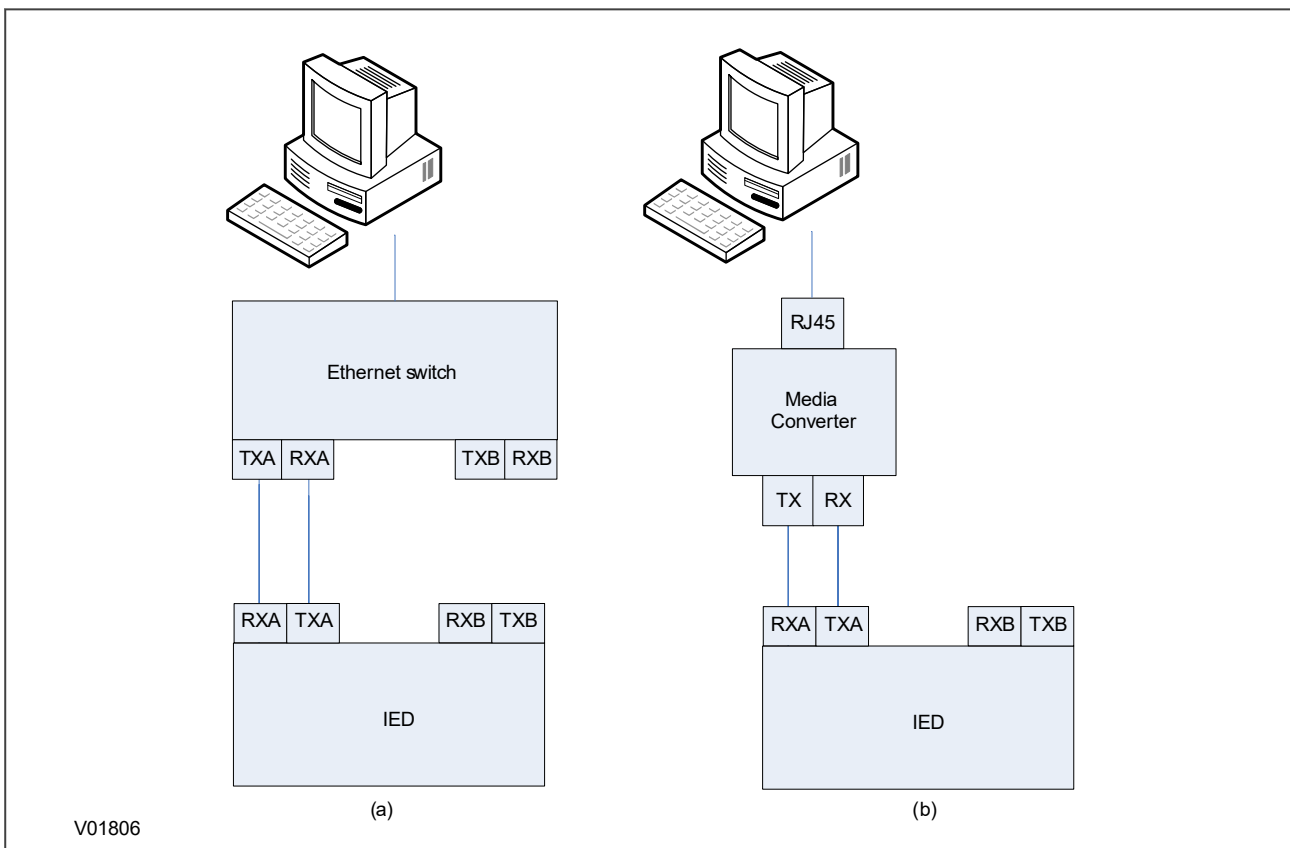


Figure 51: Connection using (a) an Ethernet switch and (b) a media converter

### 16.2 INSTALLING THE CONFIGURATOR

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

---

## 16.3 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.

---

## 16.4 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.

---

## 16.5 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.

---

## 16.6 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.

---

## 16.7 PASSWORD CONFIGURATION

To assign a password the current password needs to be input first, then a new password can be given. The default password is AAAA.

If the password does not follow NERC rules a message will be shown. Click on the **NERC Rules** button to review the rules.

If the password is not known then the password can be recovered by using the **Recover Password** button and following the instructions.

---

## 16.8 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.

---

## 16.9 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.

---

## 16.10 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.

---

## 16.11 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.

---

## 16.12 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.

### 16.13 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

### 16.14 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.

### 16.15 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.



---

## 16.16 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.

---

## 16.17 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.

---

## 16.18 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.

---

## 16.19 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.

## 17 PRP/HSR CONFIGURATOR

The PRP/HSR Configurator tool is intended for MiCOM Px4x IEDs with redundant Ethernet using PRP (Parallel Redundancy Protocol), or HSR (High-availability Seamless Redundancy). This tool is used to identify IEDs, switch between PRP and HSR or configure their parameters, configure the redundancy IP address, or configure the SNTP IP address.

### 17.1 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.

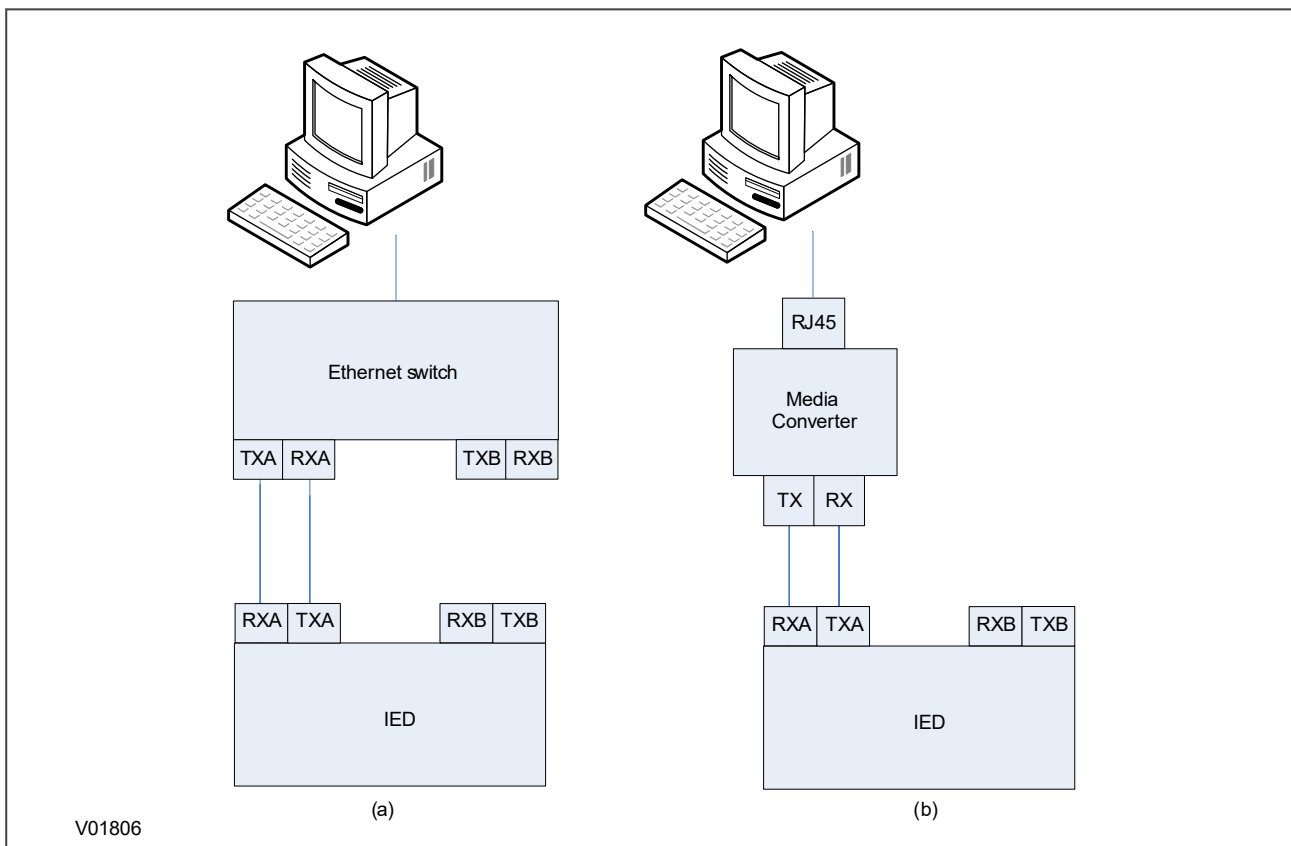


Figure 52: Connection using (a) an Ethernet switch and (b) a media converter

### 17.2 STARTING THE CONFIGURATOR

To start the configurator:

1. Select the Configurator from the Windows **Programs** menu.
2. The Login screen appears. For user mode login, enter the **Login name** as **User** and click **OK** with no password.
3. If the login screen does not appear, check all network connections.
4. The main window appears. In the bottom right-hand corner of the main window, click the **Language** button to select the language.
5. The **Network Board** drop-down list shows the Network Board, IP Address and MAC Address of the PC in which the Configurator is running.

---

### 17.3 PRP/HSR 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.

---

### 17.4 SELECTING THE DEVICE MODE

You must now select the device mode that you wish to use. This will be either PRP or HSR. 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

---

### 17.5 PRP/HSR 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 redundancy network address, not the IEC 61850 IP address.
3. The board network address is updated and displayed in the main window.

---

### 17.6 SNTP IP ADDRESS CONFIGURATION

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.

---

### 17.7 CHECK 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 **Equipment** button.
3. At the bottom of the main window, a box shows the ports where devices are connected and their MAC addresses.

---

### 17.8 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.

---

## 17.9 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.

---

## 17.10 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.

---

## 17.11 END OF SESSION

To finish the session:

1. In the main window, click the **Quit** button, a new screen appears.
2. If a database backup is required, click **Yes**, a new screen appears.
3. Click the ... button to browse the path. Enter the name in the text box.

## 18 RSTP CONFIGURATOR

The RSTP Configurator tool is intended for MiCOM Px4x IEDs with redundant Ethernet using RSTP (Rapid Spanning Tree Protocol). This tool is used to identify IEDs, configure the redundancy IP address, configure the SNTP IP address and configure the RSTP parameters.

### 18.1 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.

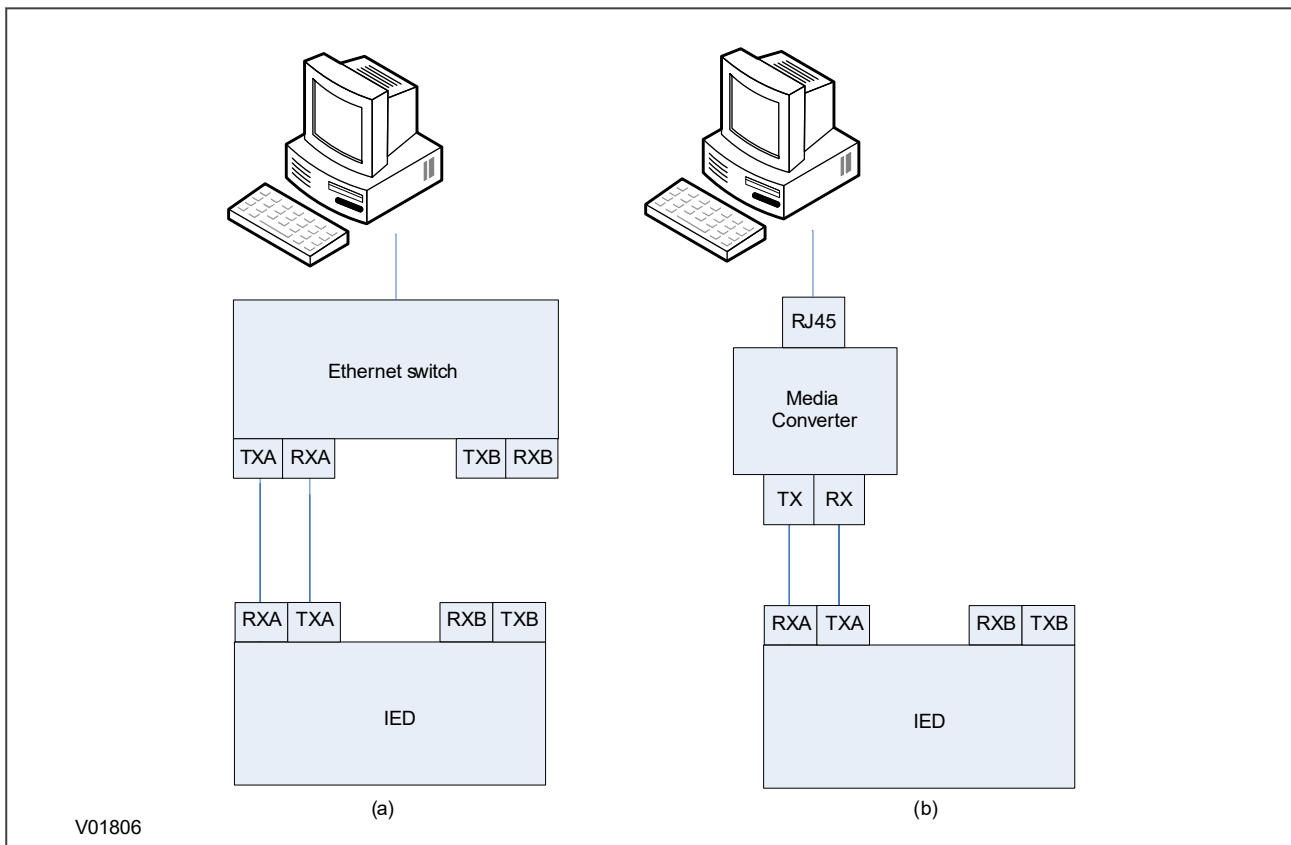


Figure 53: Connection using (a) an Ethernet switch and (b) a media converter

### 18.2 STARTING THE CONFIGURATOR

To start the configurator:

1. Select the Configurator from the Windows **Programs** menu.
2. The Login screen appears. For user mode login, enter the **Login name** as **User** and click **OK** with no password.
3. If the login screen does not appear, check all network connections.
4. The main window appears. In the bottom right-hand corner of the main window, click the **Language** button to select the language.
5. The **Network Board** drop-down list shows the Network Board, IP Address and MAC Address of the PC in which the Configurator is running.

---

### 18.3 RSTP DEVICE IDENTIFICATION

To configure the redundant Ethernet board, go to the main window and click **Identify Device**.

*Note:*

*Due to the time needed to establish the RSTP protocol, wait 25 seconds between connecting the PC to the IED and clicking the Identify Device button.*

The redundant Ethernet board connected to the PC is identified and its details are listed.

- Device address
- MAC address
- Version number of the firmware
- SNTP IP address
- Date & time of the real-time clock, from the board

---

### 18.4 RSTP IP ADDRESS CONFIGURATION

To change the network address component of the IP address,

1. From the main window click the **IP Config** button.
2. The **Device Setup** screen appears showing the **IP Base Address**. This is the board redundancy network address, not the IEC 61850 IP address.
3. Enter the required board IP address.
4. Click **OK**. The board network address is updated and displayed in the main window.

---

### 18.5 SNTP IP ADDRESS CONFIGURATION

To configure the SNTP server IP address:

1. From the main window click the **SNTP Config** button. The **Device setup** screen appears.
2. Enter the required **MAC SNTP address** and server **IP SNTP Address**. Click **OK**.
3. The updated MAC and IP SNTP addresses appear in the main screen.

---

### 18.6 CHECK 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 **Equipment** button.
3. At the bottom of the main window, a box shows the ports where devices are connected and their MAC addresses.

---

### 18.7 RSTP CONFIGURATION

1. To view or configure the RSTP Bridge Parameters, from the main window, click the device address to select the device. The selected device MAC address appears highlighted.
2. Click the **RSTP Configuration** button. The **RSTP Configuration** screen appears.
3. To view the available parameters in the board that is connected, click the **Get RSTP Parameters** button.
4. To set the configurable parameters such as Bridge Max Age, Bridge Hello Time, Bridge Forward Delay, and Bridge Priority, modify the parameter values according to the following table and click **Set RSTP Parameters**.



S.No	Parameter	Default value (second)	Minimum value (second)	Maximum value (second)
1	Bridge Max Age	20	6	40
2	Bridge Hello Time	2	1	10
3	Bridge Forward Delay	15	4	30
4	Bridge Priority	32768	0	61440

### 18.7.1 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.

### 18.7.2 PORT PARAMETERS

This function is useful if you need to view the parameters of each port.

1. From the main window, click the device address to select the device. The **RSTP Configuration** window appears.
2. Select the **Port Parameters** tab, then click **Get Parameters** to read the port parameters. Alternatively, select the port numbers to read the parameters.

### 18.7.3 PORT STATES

This is used to see which ports of the board are enabled or disabled.

1. From the main window, click the device address to select the device. The **RSTP Configuration** window appears.
2. Select the **Port States** tab then click the **Get Port States** button. This lists the ports of the Ethernet board. A tick shows they are enabled.

## 18.8 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.

---

## 19 SWITCH MANAGER

---

Switch Manager is used to manage Ethernet ring networks and MiCOM H35x-V2 and H36x-V2 SNMP facilities. It is a set of tools used to manage, optimize, diagnose and supervise your network. It also handles the version software of the switch.

The Switch Manager tool is also intended for MiCOM Px4x IEDs with redundant Ethernet using Self Healing Protocol (SHP) and Dual Homing Protocol (DHP). This tool is used to identify IEDs and GE Switches, and to configure the redundancy IP address for the GE proprietary Self Healing Protocol and Dual Homing Protocol.

### Switch hardware

GE switches are stand-alone devices (H3xx, H6x families) or embedded in a computer device rack, for example MiCOM C264 (SWDxxx, SWRxxx, SWUxxx Ethernet boards) or PC board (MiCOM H14x, MiCOM H15x, MiCOM H16x).

### Switch range

There are 3 types of GE switches:

- Standard switches: SWU (in C264), H14x (PCI), H34x, H6x
- Redundant Ring switches: SWR (in C264), H15x (PCI), H35x,
- Redundant Dual Homing switches: SWD (in C264), H16x (PCI), H36x

Switch Manager allows you to allocate an IP addresses for GE switches. Switches can then be synchronized using the Simple Network Time Protocol (SNTP) or they can be administrated using the Simple Network Management Protocol (SNMP).

All switches have a single 6-byte MAC address.

### Redundancy Management

Standard Ethernet does not support a loop at the OSI link layer (layer 2 of the 7 layer model). A mesh topology cannot be created using a standard Hub and switch. Redundancy needs separate networks using hardware in routers or software in dedicated switches using STP (Spanning Tree Protocol). However, this redundancy mechanism is too slow for one link failure in electrical automation networks.

GE has developed its own Redundancy ring and star mechanisms using two specific Ethernet ports of the redundant switches. This redundancy works between GE switches of the same type. The two redundant Ethernet connections between GE switches create one private redundant Ethernet LAN.

The Ethernet ports dedicated to the redundancy are optical Ethernet ports. The GE redundancy mechanism uses a single specific address for each Ethernet switch of the private LAN. This address is set using DIP switches or jumpers.

Switch Manager monitors the redundant address of the switches and the link topology between switches.

---

## 19.1 INSTALLATION

### Switch Manager requirements

- PC with Windows XP or later
- Ethernet port
- 200 MB hard disk space
- PC IP address configured in Windows in same IP range as switch

### Network IP address

IP addressing is needed for time synchronization of GE switches and for SNMP management.

Switch Manager is used to define IP addresses of GE switches. These addresses must be in the range of the system IP, depending on the IP mask of the engineering PC for substation maintenance.

GE switches have a default multicast so the 3rd word of the IP address is always 254.

---

## 19.2 SETUP

1. Make sure the PC has one Ethernet port connected to the GE switch.
2. Configure the PC's Ethernet port on the same subnet as the GE switch.
3. Select **User** or **Admin** mode. In User mode enter the user name as **User**, leave the password blank and click **OK**. In Admin mode you can not upload the firmware on the Ethernet repeaters.
4. In Admin mode enter the user name as **Admin**, enter the password and click **OK**. All functions are available including Expert Maintenance facilities.
5. Click the **Language** button in the bottom right of the screen and select your language.
6. If several Ethernet interfaces are used, in the **Network** board drop-down box, select the PC Network board connected to the GE switch. The IP and MAC addresses are displayed below the drop-down box.
7. Periodically click the **Ring Topology** button (top left) to display or refresh the list of GE switches that are connected.

---

## 19.3 NETWORK SETUP

To configure the network options:

1. From the main window click the **Settings** button. The Network Setup screen appears.
2. Enter the required board IP address. The first two octets can be configured. The third octet is always 254. The last octet is set using the DIP switches (SW2) on the redundant Ethernet board, next to the ribbon connector.
3. Click **OK**. The board network address is updated and displayed in the main window.
4. From the main window click the **SNTP Config** button. The Device setup screen appears.
5. Enter the required **MAC SNTP Address** and server **IP SNTP Address**. Click **OK**.
6. The updated MAC and IP SNTP addresses appear in the main screen.
7. Click the **Saturation** button. A new screen appears.
8. Set the saturation level and click **OK**. The default value is 300.

---

## 19.4 BANDWIDTH USED

To show how much bandwidth is used in the ring,

Click the **Ring%** button, at the bottom of the main window. The percentage of bandwidth used in the ring is displayed.

---

## 19.5 RESET COUNTERS

To reset the switch counters,

1. Click **Switch Counter Reset**.
2. Click **OK**.

---

## 19.6 CHECK 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 **Equipment** button.
3. At the bottom of the main window, a box shows the ports where devices are connected and their MAC addresses.

---

## 19.7 MIRRORING FUNCTION

Port mirroring is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of the repeater to another port where the data can be studied. Port mirroring is managed locally and a network administrator uses it as a diagnostic tool.

To set up port mirroring:

1. Select the address of the device in the main window.
2. Click the Mirroring button, a new screen appears.
3. Click the checkbox to assign a mirror port. A mirror port copies the incoming and outgoing traffic of the port.

---

## 19.8 PORTS ON/OFF

To enable or disable ports:

1. Select the address of the device in the main window.
2. Click **Ports On/Off**, a new screen appears.
3. Click the checkbox to enable or disable a port. A disabled port has an empty checkbox.

---

## 19.9 VLAN

The Virtual Local Area Network (VLAN) is a technique used to split an interconnected physical network into several networks. This technique can be used at all ISO/OSI levels. The VLAN switch is mainly at OSI level 1 (physical VLAN) which allows communication only between some Ethernet physical ports.

Ports on the switch can be grouped into Physical VLANs to limit traffic flooding. This is because it is limited to ports belonging to that VLAN and not to other ports.

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port. You must define outgoing ports allowed for each port when using port-based VLANs. The VLAN only governs the outgoing traffic so is unidirectional. Therefore, if you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. An egress port is an outgoing port, through which a data packet leaves.

To assign a physical VLAN to a set of ports:

1. Select the address of the device in the main window.
2. Click the **VLAN** button, a new screen appears.
3. Use the checkboxes to select which ports will be in the same VLAN. By default all the ports share the same VLAN.

## 19.10 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.

## 20 AE2R

Automatic Extraction of Event Records (AE2R) automatically reads event files from the communication ports of GE devices with either the Courier protocol or the IEC 60870-5-103 protocol.

AE2R is configured with an initialisation file. This file contains all settings, file names and file directories needed for configuration. This file can be created and edited using a standard text editor.

Once configured, event files can be automatically extracted according to a schedule by creating a batch file and feeding it to the windows Task Scheduler or other mechanisms that can run batch files periodically. This procedure is outside the scope of the manual.

AE2R also has a tool that allows setting simple passwords (for relays that support cybersecurity phase 1 or in other words, relays that have AAAA as default level 3 password) and test the communications to ensure the initialisation file has been properly configured. The command line can be used to manually execute the AE2R application on demand.

### 20.1 INITIALISATION FILE

The first step is to create or edit the initialisation file (AE2R.INI) with a text editor such as Microsoft® Notepad. It needs to be configured for each application and for the communication requirements of the connected devices.

The AE2R.INI file contains 3 sections: the common section headed [AE2R\_GENERAL], the communications section that can be serial [AE2R\_SERIAL], through a modem [AE2R\_MODEM] or via Ethernet [AE2R\_ETHERNET] and finally the password section [AE2R\_PASSWORDS]. Section entries are only included when non-default values are needed. There is a demo .ini file installed in the AE2R installation folder that can be used as a guide.

### 20.2 COMMON SECTION

The common section is formed from the following options:

Function	Description	Parameter Type	Permissible Values/Strings	Default Value
ErrorLogPathname	The error log file name must contain only valid filename characters. The name may contain spaces. When ErrorLogPathname is set to a blank string the path name is as follows. If S1 Agile is installed then the default directory is the AE2R subdirectory in the root directory for the event files as set by S1 Agile. If it is not installed then the default is the directory defined by EventRootDir. The file name in both circumstances is AE2R_Errors.log.	String		<blank string>
EventRootDir	EventRootDir is ignored if S1 Agile is installed on the same PC as AE2R. If S1 Agile is installed the root directory for the event files is set by S1 Agile. When EventDir is set to a blank string the directory containing the AE2R executable is used.	String		<blank string>
UseEthernet	This parameter indicates whether an Ethernet connection is to be used: 1 - Ethernet connection 0 - direct COM port or Modem connection	Integer	0 or 1	0
CommPort	This parameter specifies the COM port to be used. Ignored if UseEthernet is set to 1.	String	Any valid communication port string, e.g. COM1	COM1 (when CommPort key name does not exist)

Function	Description	Parameter Type	Permissible Values/Strings	Default Value
BaudRate	Ignored if UseEthernet is set to 1. This value can normally be confirmed from the connection parameter of the relay in the S1 Agile system	Integer	Any valid Baud rate	9600
ElevenBits	Ignored if UseEthernet is set to 1. This value can normally be confirmed from the connection parameter of the relay in the S1 Agile system.	Integer	0 or 1 1-11 bits 0-10 bits	1
BusyHoldoff	The time interval used by Courier between receiving a BUSY response and sending a subsequent POLL BUFFER command. It only affects RS485 daisy chains used in rear port connections	Integer	0 to 65535	50
BusyCount	The maximum number of BUSY responses that will be accepted for a single Courier transaction before aborting the transaction. To cope with abnormal situations where a device is not replying correctly to requests, a limit is placed on the number of BUSY responses that should be accepted. Without this limit the link to the device would be stuck in a loop. It only affects RS485 daisy chains used in rear port connections	Integer	0 to 65535	100
ResetResponse	The maximum time from sending the last byte of a Courier Reset Remote Link message to receiving the first byte of a response. When that time has elapsed, the request is aborted. The recommended value for all connections is 1000ms.	Integer	0 to 65535	100
Response	The maximum time from a sending the last byte of a Courier message to receiving the first byte of a response. When that time has elapsed the request is aborted. The Response Time parameter is used for all messages except Courier Reset Remote Link messages.	Integer	0 to 65535	0 to 65535
TryCount	The number of tries before aborting the request.	Integer	0 to 65535	3
TransmitDelay	The minimum delay that is put between receiving a response and transmitting the next request. Transmit delay is normally set to zero but can be set to a few milliseconds when using half duplex communication. This gives the other end of the link time to change from transmitting to receiving	Integer	0 to 65535	5
GlobalTransmit	The minimum delay that is put between transmitting a global message and the next transmission.	Integer	0 to 65535	10
UseModem	Defines whether the connection is going through a modem or not.	Integer Ignored if UseEthernet is set to 1	0 or 1 1 - modem connection 0 - direct COM port connection	0

Function	Description	Parameter Type	Permissible Values/Strings	Default Value
TAPI_ModemName	This key entry must be set the name of the modem. The name should be exactly as it appears in the Windows modem setup dialog. Ignored if UseModem is set to 0.	String		<blank string>
TAPI_LineAddress	This parameter is ignored for most modems. The value is required by specific modems. Ignored if UseModem is set to 0.	Integer		0
TAPI_NumberToDial	Ignored if UseModem is set to 0.	String	A valid telephone number. Commas may be used to indicate a one second delay.	<blank string>
TAPI_UseCountryAndAreaCodes	Ignored if UseModem is set to 0.	Integer	0 or 1 1 - TAPI_AreaCode and TAPI_CountryCode are used 0 - TAPI_AreaCode and TAPI_CountryCode are not used	0
TAPI_AreaCode	Ignored if UseModem is set to 0.	String	A valid area code telephone number. Commas may be used to indicate a one second delay.	<blank string>
TAPI_CountryCode	Ignored if UseModem is set to 0.	String	A valid country code telephone number. Commas may be used to indicate a one second delay.	<blank string>

## 20.3 COMMUNICATIONS SECTION

The communications section is formed from the following options:

Function	Description	Parameter Type	Permissible Values	Default Value
AE2R_SERIAL	Enables polling of events on a serial port. This section is used if UseEthernet in section [AE2R_GENERAL] is set to 0 and UseModem in section [AE2R_GENERAL] is set to 0. Each section entry in the [AE2R_SERIAL] section defines the device address for one device. The first key name is AE000, the second AE001, and so on to AE999.	Integer	1 to 254	<No default value>
AE2R_MODEM	This section is used if UseEthernet in section [AE2R_GENERAL] is set to 0 and UseModem in section [AE2R_GENERAL] is set to 1. Each section entry in the [AE2R_MODEM] section defines the device address for one device. The first key name is AE000, the second AE001, and so on to AE999.	Integer	1 to 254	<No default value>
AE2R_ETHERNET	This section is ignored if UseEthernet in section [AE2R_GENERAL] is set to 0. Each section entry in the [AE2R_ETHERNET] section defines the Ethernet connection parameters for one device. The first key name is AE000, the second AE001, and so on to AE999.			



---

## 20.4 SETTING THE PASSWORD

To set the password on the .ini file:

1. Navigate to the installation folder of S1 Agile and locate the AE2R folder. The default location is C:\Program Files (x86)\GE\MiCOM S1 Agile\AE2R.
2. Run AE2R Config.exe
3. When prompted, select the **browse** option and open the .ini file
4. Click on the **Change** button
5. Set the cybersecurity phase 1 password for the relay, typically the default is AAAA. On a non-cybersecurity or bypassed relay, select the option to disable the password.
6. Use the **Test** button to verify the .ini file is correct and the password has been set properly.

*Note:*

*This is not applicable to RBAC cybersecurity relays, unless the password is bypassed.*

---

## 20.5 RUNNING AE2R

There are three different ways to run AE2R:

- **Running AE2R from the Windows command line:**

1. Type command in the Windows search bar and right click on the Command Prompt, select **Run as Administrator**.
2. Once in the command line, navigate to the location of AE2R. If installed in the default installation folder use the following command `cd C:\Program Files (x86)\GE\MiCOM S1 Agile\AE2R`.
3. Type `AE2R.exe AE2R_ini_file.ini` where `AE2R_ini_file.ini` is the name of the .ini file.

- **Running AE2R from a batch file:**

1. Create a text file using notepad and type `AE2R.exe AE2R_ini_file.ini` where `AE2R_ini_file.ini` is the name of the .ini file. Save the file in the default AE2R installation folder.
2. Change the extension of the file from .txt to .bat.
3. Feed the batch file to any program desired, normally this would be a task scheduler.

- **Running AE2R from a shortcut:**

1. Navigate to the default installation AE2R folder.
2. Right click on AE2R.exe and create a shortcut.
3. Right click on the shortcut and select **Properties**.
4. In the **Target** section add at the end the name of the .ini file, this is equivalent to using the .ini file as an argument when running the executable.
5. When running the shortcut, it is advised to run it as administrator.

The default AE2R installation folder pathway is:

C:\Program Files (x86)\GE\MiCOM S1 Agile\AE2R.

---

## 20.6 INSPECTING THE EXTRACTED EVENT FILES

After the files have been extracted using AE2R, they are saved in C:\ProgramData\GE\MiCOM S1 Agile\S1 Security Events\AE2R. Navigate to this folder to retrieve the event files.

## 21 AEDR2

AutoExtract Disturbance Records 2 (AEDR2) automatically reads COMTRADE disturbance records from the rear serial communication ports GE devices with either the Courier protocol or the IEC 60870-5-103 protocol.

AEDR2 is configured with an initialisation file. This file contains all settings, file names and file directories needed for configuration. This file can be created and edited using a standard text editor. Log files are also defined in the initialisation file which are used by AEDR2 to record a history of events and errors.

Once configured, disturbance records are automatically extracted according to a schedule from devices connected in a defined range of addresses. This is done using the Windows® Scheduled Task facility which can be used to execute one or several schedules. All new disturbance records are saved to a user-defined drive and filename.

AEDR2 also has a test function to ensure the initialisation file has been properly configured. The command line is used to execute the test function and validate the initialisation file. The command line can also be used to manually execute the AEDR2 application on demand.

WinAEDR2 is a management facility for AEDR2. It shows the history of all previous extractions and has shortcut buttons to launch WaveWin, Windows Explorer and the Scheduled Task facility. It can also be used to view log files, and edit and test the initialisation file.

### 21.1 INITIALISATION FILE

First of all you need to create or edit the initialisation file (AEDR2.INI) with a text editor such as Microsoft® Notepad. It needs to be configured for each application and for the communication requirements of the connected devices.

The AEDR2.INI file contains 3 sections: the common section headed [AEDR2], the Courier section headed [Courier] and the IEC 60870-5-103 section headed [IEC-103]. Section entries are only included when non-default values are needed.

#### 21.1.1 COMMON SECTION

Function	Description	Values		Default
ErrorLogFileName	Filename of Error Log	Valid filename	1	Error.log
ExtractionLogFileName	Filename of Extraction Log	Valid filename	1	Extraction.log
StatusLogFileName	Filename of Status Log	Valid filename	1	Status.log
ComtradeName	Used to create Comtrade short filenames	Part of valid filename	2	DR
ComtradeDir	Where to store the resulting Comtrade files	Valid directory	1	empty
ComtradeFormat	Defines Comtrade format	1991 or 1999		1999
ReportMissingDevices	1 indicates that any device not found between MinAddress and MaxAddress is reported as "not found" in the Error Log	0 or 1	3	0
LongFileNames	1 indicates Comtrade long filenames	0 or 1	4	0
LFN_TCode	For long filenames, defines the Time Zone with respect to UTC	Valid time zone		0z
LFN_Substation	For long filenames, the substation name or code where the originating device is located	Part of valid filename		empty
LFN_Company	The company of the specified substation	Part of valid filename		empty

Use full pathnames for files or directories (e.g. "C:\Directory\SubDir"). If relative paths are used, they are assumed to be relative to the directory in which the applications are installed.

Short filenames use the following format:

DEV\_XX\_TIMESTAMP

**DEV** identifies the device – C for Courier or I for IEC 60870-5-103 followed by the 3-digit device address.

For example 061001,231941657,0z, South Park,C001,Stafford Power,,,,.DAT

**XX** denotes the value of the ComtradeName key

**TIMESTAMP** expresses the date and time when the disturbance was recorded, in the format YYYY-MM-DD--HH-MM-SS. For example,

C001\_DR\_2006-10-01--23-19-41.DAT

Function	Value	Description
ReportMissingDevices	0	Missing devices are not reported as errors.
	1	Arrange all device addresses consecutively without gaps.
LongFileNames	0	Records are saved using the short file name format.
	1	Records are saved using the long file name format as defined by the IEEE.

### 21.1.2 COURIER SECTION

Key	Purpose	Values		Default
MinAddress	Minimum device address	1 to 254	1	empty
MaxAddress	Maximum device address	1 to 254	1	empty
CommPort	Which COM port to use	Valid COM port	2	COM1
BaudRate	Baud rate to use	Valid baud rate		9600
ElevenBits	Ten or Eleven bits	0 or 1	3	1
BusyHoldoff	Standard Courier parameter	Integer		50
BusyCount	ditto	Integer		100
ResetResponse	ditto	Integer		100
Response	ditto	Integer		100
TryCount	ditto	Integer		3
TransmitDelay	ditto	Integer		5
GlobalTransmit	ditto	Integer		10
UseModem	Whether to use a Modem	0 or 1		0
TAPI_ModemName	Modem Name	String		empty
TAPI_LineAddress	Line Address	Integer		0
TAPI_NumberToDial	Number to Dial	String		empty
TAPI_UseCountryAndAreaCodes	Whether to use Country/Area codes	Integer		0
API_AreaCode	Area Code to dial	String		empty
TAPI_CountryCode	Country Code to dial	String		empty
SecondaryPort	Defines which devices (if any) uses Secondary Port extraction	ALL or NONE or a sequence of numbers e.g. 1,4,7,12	4	NONE

The MinAddress and MaxAddress entries must either be both included or both omitted. If included, MaxAddress must be greater than MinAddress. All Courier addresses between MinAddress and MaxAddress (inclusive) are tried. If omitted, no Courier address is tried.

Both Courier and IEC 60870-5-103 disturbance extraction can use the same COM port. This is because all Courier devices are polled first, each time the AEDR2 application runs, followed by all IEC 60870-5-103 devices.

If ElevenBits = 0, serial data is set to 1 start bit, 8 data bits, no parity and 1 stop bit.

If ElevenBits = 1, serial data is set to 1 start bit, 8 data bits, even parity and 1 stop bit.

Secondary Port Extraction means the disturbance records can be read from the device but not deleted.

Primary Port Extraction means that disturbance records are deleted from the device once read. The value SecondaryPort can be set in one of three ways:

- **NONE** All devices are connected using their primary port.
- **ALL** All devices use the secondary port upload mechanism.
- **<comma separated list of device addresses>** e.g. 11,4,5,23,121

If the value is a list of addresses, the listed addresses use the secondary port upload mechanism. All other addresses between MinAddress and MaxAddress use the standard primary port Courier disturbance record method of extraction.

A device connected to AEDR2 through its primary port, but set using its primary port to free its secondary port, operates as if it were connected to its secondary port. A device connected to AEDR2 through its secondary port, but set using its secondary port to free its primary port, fails to upload records and the same record is uploaded repeatedly.

### 21.1.3 IEC 60870-5-103 SECTION

Key	Purpose	Possible Values		Default
MinAddress	Minimum device address	0 .. 254	1	empty
MaxAddress	Maximum device address	0 .. 254	1	empty
CommPort	Which COM port to use	Valid COM port		COM1
BaudRate	Baud rate to use	Valid baud rate		9600
ElevenBits	Ten or Eleven bits	0 or 1	2	1
DModDirectory	Defines where the DMod directory is found	Valid directory	3	see note
LeaveInDevice	Defines which devices (if any) have disturbance records left in	ALL or NONE or a sequence of numbers e.g. 1,4,77,12	4	NONE
ComtradeDataFormat	Defines the Comtrade data format	BINARY or ASCII		ASCII

The MinAddress and MaxAddress entries must either be both included or both omitted. If included, MaxAddress must be greater than MinAddress. All IEC 60870-5-103 addresses between MinAddress and MaxAddress (inclusive) are tried. If omitted, no IEC 60870-5-103 address is tried.

If ElevenBits = 0, serial data is set to 1 start bit, 8 data bits, no parity and 1 stop bit.

If ElevenBits = 1, serial data is set to 1 start bit, 8 data bits, even parity and 1 stop bit.

The DModDirectory value defines where the DMod files are. This is used for the descriptions of the signals in the disturbance records.

The default directory is:

C:\Program Files\GE\MiCOM S1 Agile\S&R-103\DMod

"Leave in Device" means that the disturbance records can be read from the device but not deleted. Otherwise, disturbance records are deleted from the device once read. The value LeaveInDevice can be set in one of three ways:

- **NONE** (all records are extracted and deleted)
- **ALL** (no records will be deleted from devices)
- **<comma separated list of device addresses>** e.g. 11,4,5,23,121

If the value is a list of addresses, the disturbance records of the listed addresses are left after extraction. For all other addresses between MinAddress and MaxAddress, records are extracted and deleted.

#### 21.1.4 EXAMPLE INI FILE

The following is an example of an INI file for a serial connection on COM 1 and for a 103 connection using a modem.

```
[AEDR2]
ErrorLogFileName = TestError.log
ExtractionLogFileName = TestExtraction.log
StatusLogFileName = TestStatus.log
ComtradeDir = C:\Project\AEDR2\WinAEDR2
ReportMissingDevices = 1
LongFileNames = 1
LFN_Substation = "South Park"
LFN_Company = "Stafford Power"
ComtradeFormat = 1999

[Courier]
CommPort = COM1
BaudRate = 19200
ElevenBits = 1
MinAddress = 1
MaxAddress = 2
SecondaryPort = 1,3,5

[IEC-103]
CommPort = COM1
BaudRate = 115200
ElevenBits = 1
MinAddress = 1
MaxAddress = 2
LeaveInDevice = ALL
DModDirectory = C:\Program Files\GE\MiCOM S1 Agile\S&R-103\DMod
ComtradeDataFormat = ASCII
UseModem = 0
TAPI_ModemName = Standard 56000 bps Modem
TAPI_NumberToDial = 01223503445
```

Clicking in the Edit .ini file button for the first time opens a default file.

---

## 21.2 CONNECTION

The PC running AEDR2 can be connected to either to the Rear Port 1 or the Rear Port 2 (if fitted) of a Courier device. AEDR2 can not be used with the front port of Px40 IEDs. Rear Port 1 allows the disturbance records to be extracted or saved. Rear Port 2 can only save disturbance records. Extracted records are saved to the local PC then deleted from the device. Saved records are copied to the local PC but not deleted from the device. AEDR2 can extract or save disturbance records from IEC 60870-5-103 devices. It maintains a list of previously extracted records so it can only extract such records once. Devices using IEC 60870-5-103 and Courier use a single direct connection to the same or different COM ports. Devices using Courier can also connect using a modem link. AEDR2 can run on more than one COM port but it needs to be run separately for each, with each port or modem using its own initialisation file.

---

## 21.3 OPERATION

AEDR2 scans all the Courier and IEC 60870-5-103 device addresses in a specified range. If it does not find a device at an address it goes to the next address. You only need to specify the lowest and highest addresses, even if there are devices missing in the sequence.

AEDR2 does not keep a list of known devices. Each time it runs, it scans all addresses in the specified range. You can add new devices or remove existing devices and AEDR2 extracts disturbance records from all addresses it finds in the range each time it operates.

If a device is found at an address in the specified range and an error is found while extracting a record, the error is reported to a log file.

When executed directly or by the Scheduled Task facility, the AEDR2 application runs invisibly in the background, without the WinAEDR2 interface running. The only communication between AEDR2 and WinAEDR2 is through three log files written by AEDR2 which are as follows:

#### Error Log

This contains errors reported by the Courier or IEC 60870-5-103 transfer mechanisms, or errors caused by missing devices. Each entry contains date, time and an error description.

#### Extraction Log

This has an entry for every record that is uploaded. Each entry contains date, time, communication type, device address, trigger date and time information.

#### Status Log

This file has one line showing the time and date that AEDR2 was last run. The Status Log is overwritten each time AEDR2 is run.

---

## 21.4 DISTURBANCE RECORD FILES

For each disturbance record, a set of two or three files are created in standard COMTRADE format (\*.CFG, \*.HDR, \*.DAT).

Filenames in a set use the following format,

<AAA>\_<ComtradeName>\_<Date and Time>

<AAA> Is the decimal address of the device, always three digits.

<ComtradeName> Is the name specified by the ComtradeName section entry in the INI file.

<Date and Time> Is the date and time of the extraction in the following format,

YYYY-MM-DD--HH-MM-SS

where (HH) use the 24 hour clock.

Lists of filenames are sorted into chronological order for each device address.

---

## 21.5 LOG FILE

All errors are output to a log file. Some errors may create more than one error in the log file. The log file name is user settable. See the LogFileName entry in the INI file.

---

## 21.6 USING THE SCHEDULED TASKS PROGRAM

1. Select **Start** then **Settings** then **Control Panel**.
2. Double-click **Scheduled Tasks**. The Scheduled Tasks program starts. The Task Scheduler varies from each version of Windows so check Windows help to learn how to use this tool.

3. Double click **Add Scheduled Task**. The Scheduled Tasks Wizard starts. This lets you schedule the program to run at regular intervals from once a day to once a year (inclusive). Once the task has been created, it can be scheduled more frequently than once a day.
4. Double-click **AEDR2**, the **Properties** dialog appears.
5. Select **Schedule** then **Advanced** to configure it to run at intervals which can be as small as one minute.

*Note:*

*The Scheduled Tasks facility can also be run directly from the WinAEDR2 application.*

The Scheduled Tasks program is a component that is included with Windows®. It allows programs to be run automatically at predetermined times. Other programs are available from independent companies that provide more comprehensive facilities and these can be used as alternatives to run AEDR2.

---

## 22 WINAEDR2

---

WinAEDR2 is a management facility for AEDR2. It shows the history of all previous extractions and has shortcut buttons to launch WaveWin, Windows Explorer and the Scheduled Task facility. It can also be used to view log files, and edit and test the initialisation file.

---

### 22.1 FUNCTIONS

The main window lists the most recently extracted records in the order of extraction. There are also buttons to launch the following functions.

**WaveWin** launches the WaveWin COMTRADE viewer application

**ExtractionLog** launches notepad to view the extraction log

**ErrorLog** launches notepad to view the error log

**Explorer** launches Windows Explorer

**Scheduler** launches the "Scheduled Tasks" application

**Edit .INI File** launches notepad to edit INI file

**Test .INI File** tests the INI file for errors and logs any errors

**Run AEDR2** launches the AEDR2.exe application

**AEDR2 Status** shows the run status of AEDR2



---

## 23 WAVEWIN

---

Wavewin is used for viewing and analysing waveforms from disturbance records. It can be used to determine the sequence of events that led to a fault.

Wavewin provides the following functions.

- File management
- Query management
- Log management
- Report generation
- Sequence of Events(SOE)
- Conversion of COMTRADE files
- Waveform summary

---

### 23.1 FILE MANAGER FEATURES

The File Manager is used to manage files, search the contents of a drive or directory, and edit, plot or draw the contents of a file. This feature is similar to Windows Explorer with application-specific functions tailored for the Power Utility industry.

The functions include automatic event file association, specialized copy or move, intelligent queries, report files, COMTRADE conversion and compression routines, merge and append waveform and load files, event summaries and calibration reports.

The File Manager supports the IEEE long file naming format.

---

### 23.2 SAVE AS COMTRADE

Oscillography formats supported by the software can be converted to the COMTRADE ASCII or Binary format. Two Comtrade versions are supported: the older 1991 format and the newer 1999 format. The Comtrade format can be selected from the Data Plotting Window's Properties dialog. The default format is the newer 1999 format.

To create a COMTRADE file,

1. Place the cursor on the event file or mark the desired files
2. Select **Options** then **Save As COMTRADE** (ASCII or Binary).
3. Enter the destination path and filename (do not enter a filename extension).
4. Click **OK**. The .DAT and .CFG files are created automatically. If a path is not defined, the COMTRADE files are saved in the active directory.

If the sample values in the selected file(s) are RMS calibrated and the desired COMTRADE file must have instantaneous values, set the Comtrade Settings fields to automatically convert the RMS data to instantaneous values.

To set the **Comtrade Settings** fields,

1. In the **Analysis** display, open the **Window Properties** dialog.
2. Select the **Comtrade** tab.
3. In the **Convert RMS Calibrated Data to Peak Data** dropdown box, select **Yes**.

To automatically convert the selected file(s) to COMTRADE using the IEEE long filename format,

1. In the **Save As Comtrade** dialog, check the **Use the ComNames Naming Convention to Name the Comtrade File(s)** field
2. Leave the **File Name** field empty.
3. Click **OK**.

All files marked in the table are converted to the selected COMTRADE format and are named using the IEEE long file naming convention.

---

## 24 DEVICE (MENU) TEXT EDITOR

---

The Menu Text Editor enables you to modify and replace the menu texts held in MiCOM Px4x IEDs. For example, you may want to customise an IED so that menus appear in a language other than one of the standard languages.

By loading a copy of the current menu text file in one of the standard languages into the reference column, you can type the appropriate translation of each menu entry into the target column.

This can then be sent from the PC to the IED, replacing one of the current standard languages. New menu text files created this way can also be saved to disk for later use or further editing.

---

### 24.1 OPEN A CONNECTION

1. Select **Device** then **Open Connection**. The Open Connection dialog appears.
2. Select the port to which the device is connected.
3. Select the **Device Timeout** in minutes.
4. Click **OK**. The Password dialog is displayed.
5. Type the Password. This is displayed as asterisks.
6. Click **OK**. A message appears confirming the connection has been opened.

---

### 24.2 CHANGE CONNECTION PASSWORD

1. Open a connection with the device.
2. Select **Device** then **Change Password**. The Change Password dialog appears.
3. In the **New Password** box, enter the new password. This is displayed as asterisks.
4. In the **Verify New Password** box, enter the password again.
5. Click **OK** to accept.

---

### 24.3 OPEN A MENU TEXT FILE AS A REFERENCE

1. Select the **Reference** column.
2. Select **File** then **Open**. The Open File dialog appears.
3. Select the required menu text file then click the **Open** button.
4. The menu text file appears in the **Reference** column.

---

### 24.4 EDIT TEXT FILE OF DEVICE

1. Select File then **New** to create a default menu text file for the required device or select File then **Open** to open an existing file.
2. The menu text file appears in the **Target** column. Select the required text cell in the **Target** tab corresponding to the text in the **Reference** tab. Edit the file as required.
3. Select **File** then **Save As**.
4. Edit the File Name or Header fields as required.
5. Click **Save**.

---

### 24.5 SEND EDITED TEXT FILE TO DEVICE

1. Connect a PC to the required device.
2. Select **Device** then **Open Connection** to open a connection to the required device.

3. Select **Send To Device**.
4. Click **OK**.
5. Once the sending of the text file is complete, the new text appears in the menu on the IED screen.

---

## 25 SETTINGS EXCEL EXPORT

---

System Explorer allows you to import or export Excel files of settings in various formats.

The Settings File Import/Export Mapping tile allows you to create custom mapping files. These xml files map each setting to an Excel cell.

---

### 25.1 MAPPING FILES

The mapping file is an xml file which maps each setting to an Excel cell.

#### 25.1.1 EXPORT DEFAULT MAPPING

This xml file maps each setting to an Excel cell.

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Export** then **Export Default Excel Mapping**.
3. Enter a filename for the output Excel mapping file, browse where to save it and click **Save**.
4. Click **Close**.

#### 25.1.2 CREATE CUSTOM MAPPING

This xml file maps each setting to an Excel cell.

1. Click the **Settings File Import/Export Mapping** tile.
2. Select the **File** tab then click **Open**.
3. Select the required settings file and click **Open**.
4. Select the **Home** tab.
5. Edit the **Excel Mapping** column as required. This contains values from the mapping file.

#### 25.1.3 CREATE CUSTOM MAPPING FROM DEFAULT MAPPING

This xml file maps each setting to an Excel cell.

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Export** then **Export Default Excel Mapping**.
3. Enter a filename for the output Excel mapping file, browse where to save it and click **Save**.
4. Click **Close**.
5. Click the **Settings File Import/Export Mapping** tile.
6. Select the **File** tab then click **Open**.
7. Select the required settings file and click **Open**.
8. Click **Load**, select the mapping file you want to load, then click **Open**.
9. Edit the **Excel Mapping** column as required. This contains values from the mapping file.
10. Click **Save**.

#### 25.1.4 HIDE OR SHOW MAPPED SETTINGS

1. Click the **Settings File Import/Export Mapping** tile.
2. Select the **File** tab then click **Open**.
3. Select the required settings file and click **Open**.
4. In the ribbon, check or uncheck the **Show Mapped** or **Hide Mapped** filters.

---

## 25.2 EXPORTING AN EXCEL FILE

The structure of the settings file is defined by the template. Some of the settings are global, which apply to all devices, and some are local, which are device-specific. If you need to make individual changes to a settings file that is controlled by templates, you can export the settings to an Excel file.

You can then edit values in the Excel file, keeping the same structure. This is important because each cell is controlled by a mapping file. This is an xml file which maps each Excel cell to a cell in the settings file. Once you have made the changes you can then reimport the Excel file.

If you include a custom mapping file:

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Export** then **Export to Excel**.
3. Browse for the mapping file. This xml file maps each setting to an Excel cell.
4. Enter a filename for the output Excel file, browse where to save it and click **Save**.
5. Click **Close**. All editable settings are exported to Excel.

If you include the default mapping file:

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Export** then **Quick Export to Excel**.
3. Enter a filename for the output Excel file, browse where to save it and click **Save**.
4. Click **Close**. All editable settings are exported to Excel.

### 25.2.1 EXPORT TO XRIO

When testing an IED, you can enter the IED settings into the test equipment software manually. The Settings Application Software can output an XRIO file which allows you to import the settings into the test equipment software. This can significantly reduce the time required to commission IEDs.

To export an XRIO file:

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Export** then **Export to XRIO**.
3. Enter a filename for the output XRIO file, browse where to save it and click **Save**.
4. Click **Close**.

### 25.2.2 ABOUT XRIO

RIO is a standard data format for different manufacturers to exchange protection devices settings. It is a plain text file with a common structure which allows devices to be tested with similar procedures. It defines the device and its characteristics, then it can define the settings to test a particular protection function.

XRIO is an extension of RIO and models physical test objects in the Omicron Test Universe (OTU) 2.0 protection environment. A test object can be a measurement or protection device. XRIO is based on XML and uses the basic structure of a RIO plain text file but with additions.

Where RIO allows you to test one protection function with each file, XRIO allows you to test several protection functions with each file. It also allows you to define custom settings which are specific to that device rather than generic settings. Also, whereas RIO limits you to using the test object once, XRIO allows you to repeat the test object several times.

A converter is used to convert the settings of the protection device into RIO format. However, XRIO files can have the converter built in. These converters are specific to individual protection devices from each manufacturer but are dependent on the Omicron Test Universe. The converter converts the device-specific settings to the Omicron Test Object parameters.

XRIO uses a hierarchical tree structure with the following three sections.

**Script Function section.** You can declare global functions used to transform the device-specific settings into RIO parameters.

**Custom section.** This can be freely defined. It maps the device-specific settings which you use to configure the test object, You can also use formulae. This is the section that is exported by the Settings Application Software.

**RIO section.** This holds conventional RIO blocks for test modules intended for a specific protection function. These are used by the test modules in the OTU. The structure is based on the RIO specification.

### 25.2.3 EXPORT TO CSV

To export a CSV file:

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Export** then **Export to CSV or CAPE**.
3. Check the **CSV** checkbox and select any required options, then click **OK**.
4. Enter a filename for the output file, browse where to save it and click **Save**.
5. Click **Close**.

### 25.2.4 EXPORT TO CAPE

To export a CAPE file:

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Export** then **Export to CSV or CAPE**.
3. Check the **CAPE** checkbox and select any required options, then click **OK**.
4. Enter a filename for the output file, browse where to save it and click **Save**.
5. Click **Close**.

---

## 25.3 IMPORTING AN EXCEL FILE

If you include a custom mapping file:

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Import** then **Import from Excel**.
3. Browse for the mapping file. This xml file maps each setting to an Excel cell.
4. Browse for the input Excel file and click **Save**.
5. Click **Close**.

If you include the default mapping file:

1. In **System Explorer**, under **Device**, right-click the Settings file.
2. Select **Import** then **Quick Import from Excel**.
3. Browse for the input Excel file and click **Save**.
4. Click **Close**.

---

## 25.4 HIDE OR SHOW READ ONLY SETTINGS

1. Click the **Settings File Import/Export Mapping** tile.
2. Select the **File** tab then click **Open**.
3. Select the required settings file and click **Open**.
4. In the ribbon, check or uncheck the **Show Read Only** or **Hide Read Only** filters.

---

## 25.5 SELECT LANGUAGE

1. Click the **Settings File Import/Export Mapping** tile.
2. Select the **File** tab then click **Options**.
3. Select the language from the drop-down list.



## 26 P747 BUSBAR COMMISSIONING TOOL (REMOTE HMI)

This tool is intended for busbar commissioning. It allows you to create a scheme and display the measured data. It consists of a scheme editor and a monitor that shows protection data in real time. The scheme editor allows you to quickly draw schemes from a library of elements, then validate the scheme. The monitor continually updates information about the scheme and shows the status of DDBs and values of measured data.

### 26.1 SCHEME EDITOR

The Scheme Editor allows you to quickly draw schemes from a library of elements, then validate the scheme.

To select your language, select **File** then **Options** then **Language**.

To create, open, save or print a scheme, select the **File** tab.

#### 26.1.1 CONNECTIONS

To enable connection bridges:

1. Select **File** then **Options** then **Diagram Settings**.
2. Check **Enable Connection Bridges**.

The following table shows which elements can be connected together.

Element	Busbar	Feeder Isolator (Q)	Circuit Breaker	Current Transformer	Voltage Transformer	Busbar Isolator (Qbus)
Busbar	No	Always	No	No	Busbar can be connected to max 1 VT element. VT has only one end connected	Always
Feeder Isolator (Q)	Always	No	CB can be connected to 1 to 4 isolators	CT can be connected to 1 to 2 isolators	VT has only one end connected	No
Circuit Breaker	No	CB can be connected to 1 to 4 isolators	No	Always. Max 1 CB to 1 CT	No	No
Current Transformer	No	CT can be connected to 1 to 2 isolators	Always. Max 1 CB to 1 CT	No	No	No
Voltage Transformer	Busbar can be connected to max 1 VT element. VT has only one end connected	VT has only one end connected	No	No	No	No
Busbar Isolator (Qbus)	Always	No	No	No	No	No

##### 26.1.1.1 MANUAL CONNECTIONS

To connect two elements:

1. Select **File** then **Options** then **Diagram Settings**.
2. Uncheck **Enable Auto Connections**.
3. Drag and drop two objects onto a scheme.
4. Drag a connection to each element. A green border shows the connection is complete.

### 26.1.1.2 AUTOMATIC CONNECTIONS

To connect two elements:

1. Select **File** then **Options** then **Diagram Settings**.
2. Check **Enable Auto Connections**.
3. Drag and drop two objects next to each other onto a scheme. The connection is made automatically.

### 26.1.1.3 REMOVE CONNECTION

To remove a connection:

1. Select a connection.
2. Press the **Delete** key or click the **Remove** icon.

## 26.1.2 SCHEME ELEMENTS

The following table shows the number of elements allowed in a scheme.

Element	Minimum number	Maximum number
Busbar	1	4
Isolator	2	74
Circuit Breaker	2	18
Current Transformer	2	18
Voltage Transformer	0	4

### 26.1.2.1 ADD ELEMENTS TO A SCHEME

To add elements to a scheme, drag and drop them from the toolbox.

### 26.1.2.2 REMOVE AN ELEMENT

To remove an element from a scheme:

1. Select an element.
2. Press the **Delete** key or click the **Remove** icon.

### 26.1.2.3 GROUP ELEMENTS IN A SCHEME

To group elements in a scheme:

1. Drag and drop the elements into the scheme.
2. Add any connections between them.
3. Select the elements you want to group.
4. Click the **Group** icon.

### 26.1.2.4 ROTATE ELEMENTS IN A GROUP

To rotate an element or group, select the item and click the **Rotate Left** or **Rotate Right** icon.

## 26.1.3 WORKING WITH TEXT ON THE SCHEME

You can add labels or free text onto the scheme:

- Circuit Breakers can be labelled CB1 to CB18.
- Current Transformers can be labelled CT1 to CT18.

- Voltage Transformers can be labelled VT1 to VT4.
- Feeder Isolators can be labelled QxZy where x=1 to 18 and y=1 to 4.
- Busbar Isolators can be labelled QBus1 to Qbus2.

#### 26.1.3.1 ADD A LABEL TO AN ELEMENT

To add a label to an element:

1. Double-click the element and select a label from the drop-down list.  
If many labels are available it can sometimes be difficult to find a specific one from the drop-down list. A search function helps you to find the one you need.
2. Double-click the element.
3. Enter the search text in the box at the top of the drop-down list.

#### 26.1.3.2 REMOVE A LABEL FROM AN ELEMENT

To remove a label from an element, right-click the element and select **Remove Label**.

#### 26.1.3.3 CHANGE AN ELEMENT'S LABEL

To change the label of an element, right-click the element and select **Edit Label**.

#### 26.1.3.4 ADD OR REMOVE FREE TEXT

To add or remove free text, drag and drop the **Free Text** object onto the scheme and enter the text.

To edit the text, double click it.

To remove the text block, right-click it and select **Remove**.

#### 26.1.3.5 VALIDATE A SCHEME

This checks for potential errors in the scheme and makes suggestions of how to correct them.

To validate scheme elements and the connections between them, click the **Validate** icon. To display the latest validation results, click the **Validation Report** icon.

---

## 26.2 PROTECTION DATA MONITOR

The Protection Data Monitor shows the status of DDBs and measured data in the scheme.

To start the Protection Data Monitor:

1. Select **File** then **Save** or **Save As** to save the scheme.
2. Click the icon **Switch to Dynamic Synoptic Mode**.

### 26.2.1 CONNECT TO THE IED

To read the IED data, first set up the connection:

1. Click the **Connect to P747** icon.
2. Select **Single Device** or **Many Devices**.
3. From the drop-down list select **Front Serial Port**, **Rear Serial Port** or **Ethernet**.  
The table is populated with default values. Check they are suitable for your application. You can set the Device Address from 1 to 255.
4. Click the **Connect** button. The connection status appears in the bottom left-hand corner of the screen. Green shows the IED is connected.

### 26.2.1.1 POLLING TIMER

The Protection Data Monitor polls the IED and updates the states of the elements in the scheme. The Polling Timer sets the time in seconds between each update.

To set the polling timer:

1. Click the **Polling Timer** icon.
2. Select the polling time in seconds from the drop-down list and click **OK**.

To stop or restart polling, click the **Stop Polling** icon or **Resume Polling** icon.

### 26.2.1.2 READ IED DATA

To read the IED data, click the Get Device Data icon.

This shows the Device Address, Model Number, Serial Number and device Description for each device that is connected.

### 26.2.1.3 MEASUREMENTS DATA

The Measurements Panel is on the left-hand side of the screen. The top left-hand corner shows the measurements for each zone and for each phase. The bottom left-hand corner shows the protection data and any alarms. The phase angle and magnitude are shown at each CT on the scheme.

## 27 DYNAMIC SYNOPTIC

This tool allows you to monitor the substation electrical components and analogue values in real time.

This is the user manual for the topology configurator, which is used by the P740 numerical busbar protection.

The main window is composed of three parts:



- The internal windows for the scheme, the logical and analogue values.
- The menu bar
- A toolbar

### 27.1 SYNOPTIC MAIN WINDOW



This window is used to display the topology of the substation. The scheme is updated periodically with information that is available in the connected device.



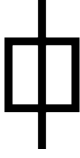
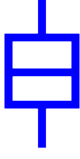
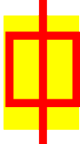


### 27.2 SYNOPTIC MAIN WINDOW

#### Feeder




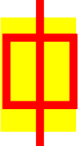


Symbol	Function	Explanation
	Feeder	Feeder with PU Not Connected
	Feeder	Feeder with PU Connected

#### Current Transformer



Symbol	Function	Explanation
	Current Transformer	CT with PU Not Connected
	Current Transformer	CT Healthy

Symbol	Function	Explanation
	Current Transformer	CT with PU Not Connected
	Circuit Breaker	CB with PU Not Connected
	Circuit Breaker	CB Closed
	Circuit Breaker	CB Open
	Circuit Breaker	CB Open and Unavailable
	Circuit Breaker	CB Closed and Unavailable
	Circuit Breaker	CB Status Alarm

## Circuit Breaker

Symbol	Function	Explanation
	Circuit Breaker	CB with PU Not Connected
	Circuit Breaker	CB Closed
	Circuit Breaker	CB Open
	Circuit Breaker	CB Open and Unavailable
	Circuit Breaker	CB Closed and Unavailable
	Circuit Breaker	CB Status Alarm

The CB is unavailable when the logic input "CB Not Available" is active. When the PU is in Commissioning mode "50BF disabled", the CB is unavailable too.

Symbol	Function	Explanation
	Isolator	with PU Not Connected
	Isolator	when Qx is Closed
	Isolator	when Qx is Opened
	Isolator	when Qx is Status Alarm

If the DDB signal Qx status alarm is not used in the PSL, the isolator can be opened or closed but never in alarm.

## 27.3 MENU

The menu is composed of 5 sub-menus:

- File
- Device
- Tools
- View
- Help

### 27.3.1 FILE

The File menu contains the following actions:

- **Open:** To open a dynamic synoptic file .dyn. No action except exit is available before the opening of a scheme.
- **Close:** To close the dynamic synoptic file
- **Exit:** To close the application



## 27.3.2 DEVICE

The File menu contains the following actions:

- **Communications Setup:** To configure the communication.
- **Open Connection to PU:** For a front port connection to a PU
- **Open Connection to CU:** For a front port connection to the CU
- **Open Connection to System:** For a rear port connection to the CU and/or PU

### 27.3.2.1 COMMUNICATIONS SETUP

This dialog is used to set the communications connection details and save them in the communication setup:

- **COM Port:** Select the port to which the relevant device is connected.
- **Baud Rate:** Select the baud rate used.

### 27.3.2.2 OPEN CONNECTIONS TO PU

Open Connection to PU opens a dialog box for the address of the PU.

Enter the address of the PU then confirm with OK to open the communication. If the communications are opened successfully, the refresh starts automatically.

### 27.3.2.3 OPEN CONNECTIONS TO CU

Open Connection to CU opens the communication with the central unit address 6. If the communications are opened successfully, the refresh starts automatically.

### 27.3.2.4 OPEN CONNECTIONS TO SYSTEM

Open Connection to CU opens the communication with the central unit address 6. If the communications are opened successfully, the refresh starts automatically.

---

## 27.4 TOOLS

The Tools menu contains the following actions:

- **Polling Timer:** To change the refresh period of all data. If the processing time is longer than the refresh period, then the process restarts immediately.
- **Start/Stop Polling:** To start or stop polling.
- **Zoom:** To reset the zoom magnification, or to increase or decrease it.

---

## 27.5 VIEW

The View Menu allows you to see the measured values of the units in the system. This is only possible after connecting.

- Analogue Values of PU
- Analogue Values of CU
- Logic Values of PU
- Logic Values of CU
- Device Data

### 27.5.1 DEVICE DATA

Information about the equipment connected is available in this window. This includes:

- Description and plant reference, which is set in the settings
- Model and serial number
- Software version

### 27.5.2 LOGIC VALUES OF THE CU



The window for Logic values of CU is divided into five parts:

1. **Monitor bit:** The value displayed is identical to the **Test Port Status** cell in the *COMMISSIONING TESTS* column.
2. **Trip and Trip Zone:** The first line indicates the protection which is operated: **87BB**, **50BF** or **manual tripping**. The symbol turns red when the trip occurs. The second line indicates the tripping zone. Both trip signals, zone and protection, are maintained for five seconds.
3. **Alarm:** The default status of the LED is grey. When there is an alarm on the PU, the LED turns yellow and the list of alarms is available in the Combo box on the right.
4. **Protection Status:** The first line indicates which of the protections are locked:
  - **87BB:** When there is a blocking for a circuitry fault or a PU error or when the mode **Lck Level 1** or **Lck Level 2** is active
  - **50BF:** When the mode **Lck Level 2** is active
  - **P740:** When the mode **All Prot Disabled** is selected in the CU

The second line indicates the zone.

1. **PU connected:** The address of the PUs connected to the CU are displayed in this field

### 27.5.3 LOGIC VALUES OF THE PU

The window for Logic values of PU is divided into four parts:

1. **Monitor bit:** The value displayed is identical to the **Test Port Status** cell in the *COMMISSIONING TESTS* column.
2. **Trip:** The default status of the LED is grey. When a trip occurs on the PU, the LED turns red. There is a five second drop-off on the **Any trip** DDB signal to display this information.
3. **Alarm:** The default status of the LED is grey. When there is an alarm on the PU, the LED is turns yellow and the list of alarms is available in the Combo box on the right.
4. **Protection Status:** This line indicates if the PU is in service (Green = ON) or if a commissioning mode is active (Red = OFF)
  - **50BF:** In red when the mode **50BF Disabled** is selected in the PU
  - **PU:** In red when the mode **Out of Service** is selected in the PU
  - **P740:** In red when the mode **All Prot Disabled** is selected in the CU

### 27.5.4 CU ANALOGUE VALUES

From the CU, the differential and bias currents for the Check Zone (CZ) and all the zones (Z1 to Zx) are available.

From the PU, only the currents of the connected zone are available.

The display in primary or secondary value depends on the setting in the Measurement Setup column.

### **27.5.5 PU ANALOGUE VALUES**

This window displays the magnitude of the currents in the PU.

---

### **27.6 HELP**

Contains the Help section and the About section.

---

## 28 REMOTE HMI

---

The MiCOM P746 Remote HMI is an application that is used to define and create schemes as well as display the measured data. This application operates in two modes:

- **Scheme Editor:** This mode allows the user to define a scheme with the predefined Busbars, Tie Groups and Feeder Groups.
- **Dynamic Synoptic:** This tool is used to display the measured analogue quantities and DDB (Digital Data Bus) status information based on the scheme designed in Scheme Editor mode.

---

### 28.1 COMMUNICATION SETTINGS

The Remote HMI application can communicate with the device through SERIAL COM port and ETHERNET TUNNELING.

You can select the settings before starting to communicate with the device in the Scheme Editor or Dynamic Synoptic mode. The selected communication option and their settings are displayed in the left-hand side of the Status Bar.

#### 28.1.1 SERIAL SETTINGS

The following settings can be set for SERIAL communication with P746:

**COM port:** The list of COM ports available in the system will be displayed. Select the port to which P746 is connected.

**Baud Rate:** Select the Baud Rate to be used. The options are 19200 and 9600.

**BusyHoldoff:** The time interval used by Courier between receiving a BUSY response and sending a subsequent POLL BUFFER command. It only affects RS485 daisy chains used in rear port connections

**Permissible values:** 0 to 65535

**Default value:** 50

**BusyCount:** The maximum number of BUSY responses that will be accepted for a single Courier transaction before aborting the transaction. To cope with abnormal situations where a device is not replying correctly to requests, a limit is placed on the number of BUSY responses that should be accepted. Without this limit the link to the device would be stuck in a loop. It only affects RS485 daisy chains used in rear port connections.

**Permissible values:** 0 to 65535

**Default value:** 100

**ResetResponse:** The maximum time from sending the last byte of a Courier Reset Remote Link message to receiving the first byte of a response. When that time has elapsed, the request is aborted. The recommended value for all connections is 1000ms.

**Permissible values:** 0 to 65535

**Default value:** 100

**Response:** The maximum time from a sending the last byte of a Courier message to receiving the first byte of a response. When that time has elapsed the request is aborted. The Response Time parameter is used for all messages except Courier Reset Remote Link messages.

**Permissible values:** 0 to 65535

**Default value:** 100

**TryCount:** The number of tries before aborting the request.

**Permissible values:** 0 to 65535

**Default value:** 3

**TransmitDelay:** The minimum delay that is put between receiving a response and transmitting the next request. Transmit delay is normally set to zero but can be set to a few milliseconds when using half duplex communication. This gives the other end of the link time to change from transmitting to receiving.

**Permissible values:** 0 to 65535

**Default value:** 5

**GlobalTransmit:** The minimum delay that is put between transmitting a global message and the next transmission.

**Parameter type:** Integer

**Permissible values:** 0 to 65535

**Default value:** 10

### 28.1.2 ETHERNET SETTINGS

The following settings can be set for "ETHERNET" communication:

**IP Address (Mandatory):** Set the IP address through which P746 can be connected.

**TCP Port number (Optional):** Select this option if specific ETHERNET TCP port has to be used. If this option is not selected, default ETHERNET port 0 will be used.

**Bay Address (Optional):** Select this option if P746 is connected through a Bay Unit and set the Bay Unit's address.

**BusyHoldoff:** The time interval used by Courier between receiving a BUSY response and sending a subsequent POLL BUFFER command. It does not affect Ethernet connections

**Permissible values:** 0 to 65535

**Default value:** 0

**BusyCount:** The maximum number of BUSY responses that will be accepted for a single Courier transaction before aborting the transaction. To cope with abnormal situations where a device is not replying correctly to requests, a limit is placed on the number of BUSY responses that should be accepted. Without this limit the link to the device would be stuck in a loop. It does not affect Ethernet connections.

**Permissible values:** 0 to 65535

**Default value:** 0

**ResetResponse:** The maximum time from sending the last byte of a Courier Reset Remote Link message to receiving the first byte of a response. When that time has elapsed, the request is aborted. The recommended value for all connections is 1000ms.

**Permissible values:** 0 to 65535

**Default value:** 100

**Response:** The maximum time from a sending the last byte of a Courier message to receiving the first byte of a response. When that time has elapsed the request is aborted. The Response Time parameter is used for all messages except Courier Reset Remote Link messages.

**Permissible values:** 0 to 65535

**Default value:** 5000

**TryCount:** The number of tries before aborting the request.

**Permissible values:** 0 to 65535

**Default value:** 3

**TransmitDelay:** The minimum delay that is put between receiving a response and transmitting the next request. Transmit delay is normally set to zero but can be set to a few milliseconds when using half duplex communication. This gives the other end of the link time to change from transmitting to receiving.

**Permissible values:** 0 to 65535

**Default value:** 0

**GlobalTransmit:** The minimum delay that is put between transmitting a global message and the next transmission.

**Parameter type:** Integer

**Permissible values:** 0 to 65535

**Default value:** 15

## 28.2 SCHEME EDITOR

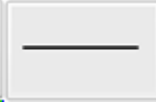

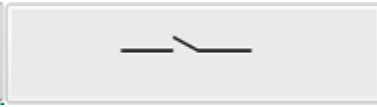




The Scheme Editor window is used to design the scheme for the device using the Busbar, Feeder Group and Tie Group graphical icons.


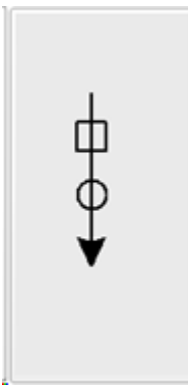
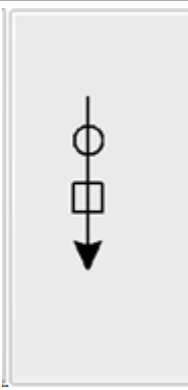
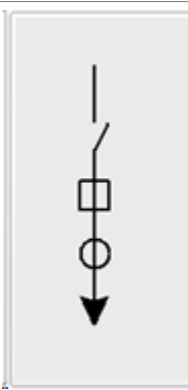
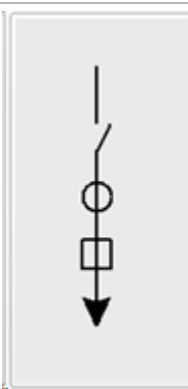
The Main Window is composed of following parts:

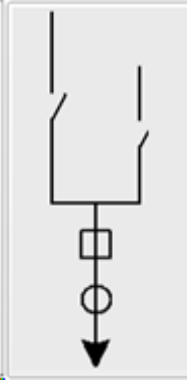
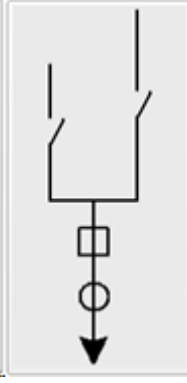
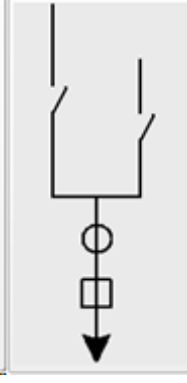
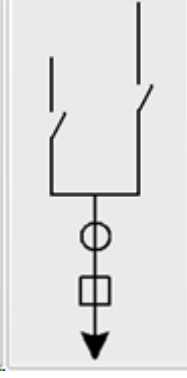
- The Menu Bar
- A Toolbar
- Toolbox
- Scheme Design Window

### 28.2.1 PRINCIPLE OF OPERATION



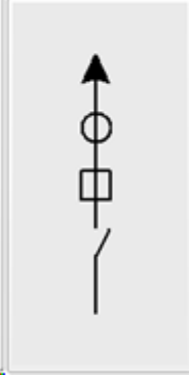
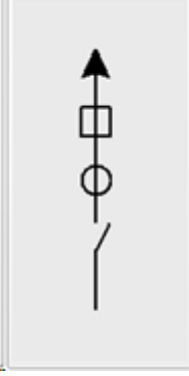
A library of predefined symbols allows the scheme to be created. This library is located in the form of toolbox located in the left side of the main window. These symbols can be easily dragged and dropped into the Scheme Window.

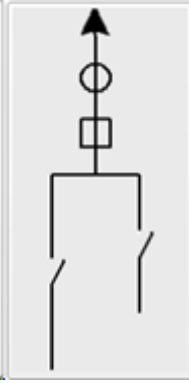
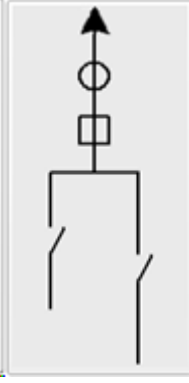
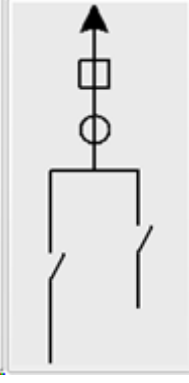
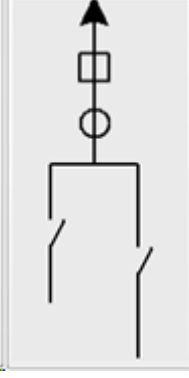
Symbol	Description
	Busbar
	Busbar Link
	Tie Group 1
	Tie Group 2
	Tie Group 3
	Tie Group 4
	Tie Group 5

Symbol	Description
	Tie Group 6
	Feeder Group 1
	Feeder Group 2
	Feeder Group 3
	Feeder Group 4

Symbol	Description
	<p>Feeder Group 5</p>
	<p>Feeder Group 6</p>
	<p>Feeder Group 7</p>
	<p>Feeder Group 8</p>



Symbol	Description
	Feeder Group 9
	Feeder Group 10
	Feeder Group 11
	Feeder Group 12

Symbol	Description
	<p>Feeder Group 13</p>
	<p>Feeder Group 14</p>
	<p>Feeder Group 15</p>
	<p>Feeder Group 16</p>

## 28.2.2 CONSTRAINTS

There are a number of constraints to consider:

- The maximum number of Busbars that can be created in the scheme is restricted to two. Only one Tie Group can be created in the scheme.
- The initial drag and drop placement of an object onto the scheme editor page is not possible if the 'grey boundary box' of such an object is touching or overlapping with another object already placed on the page.
- Feeder Group cannot be created before creating at least one busbar in the scheme.
- The Feeder group and Tie group components can not be resized.
- The number of Feeder groups that can be created is restricted to six in 1 box mode and 18 in 3 box mode.
- If vertical Busbar links are used within a scheme then they must be applied to both Busbar ends. for example, zone 1 and zone 2.
- Objects that are placed within a scheme must be positioned with sufficient space to allow measurements to be displayed when in the Dynamic Synoptic mode.

---

## 28.3 SCHEME DESIGN

### 28.3.1 CREATING A NEW SCHEME

To create a new scheme go to **Select File > New menu** or New icon in the toolbar. The **Select Scheme Mode** window is displayed

1. If the device is connected, select the **Relay Connected** option and then press the **OK** button. The P746 mode is retrieved from the unit and a new scheme is created.
2. If the device is not connected, select the **Relay Not connected** option, **One Box Mode** or **3 Box Mode** and then press the **OK** button to create a new scheme.

In both cases the newly created scheme is displayed.

### 28.3.2 CREATING A BUSBAR

The only difference between **Busbar Left** and **Busbar Right** is that the Busbar Labels on these symbols is displayed on left side and right side respectively. To create a Busbar, drag and drop the **Busbar Left** or **Busbar Right** symbol from **Busbar Toolbox** into the Scheme Window. The **Set Busbar Properties** window is displayed.

Select either the **BB1** or **BB2** option and then press the **OK** button to create the Busbar. To increase the length of the Busbar, click on the endpoint and drag the mouse.

### 28.3.3 CREATING A BUSBAR LINK

To create a Busbar link, drag and drop the **Busbar Link** symbol from the **Busbar Toolbox** into the Scheme Window.

*Note:*

*Only two Busbar Links are allowed in a scheme.*

### 28.3.4 CREATING A TIE GROUP

To create a Tie Group, drag and drop the **Tie Group** symbol from **Tie Group Toolbox** into the Scheme Window.

1. If the selected Tie Group does not have a CT, it will be created immediately.
2. If the selected Tie Group has one CT, the **Tie Group Properties** window will be displayed with one CT.
3. If the selected Tie Group has two CTs, the **Tie Group Properties** window will be displayed with two CTs.
4. Select **CT** for CT1 and CT2 and press the **APPLY** button to create the Tie Group.

*Note:*

*Only one Tie Group is allowed in a scheme. The same CTs are not allowed for CT1 and CT2 for Tie Groups with double CTs.*

### 28.3.5 CREATING A FEEDER GROUP

To create a Feeder Group, drag and drop the **Feeder Group** symbol from the **Feeder Group Toolbox** into the Scheme Window. The **Feeder Group Properties** window is displayed.

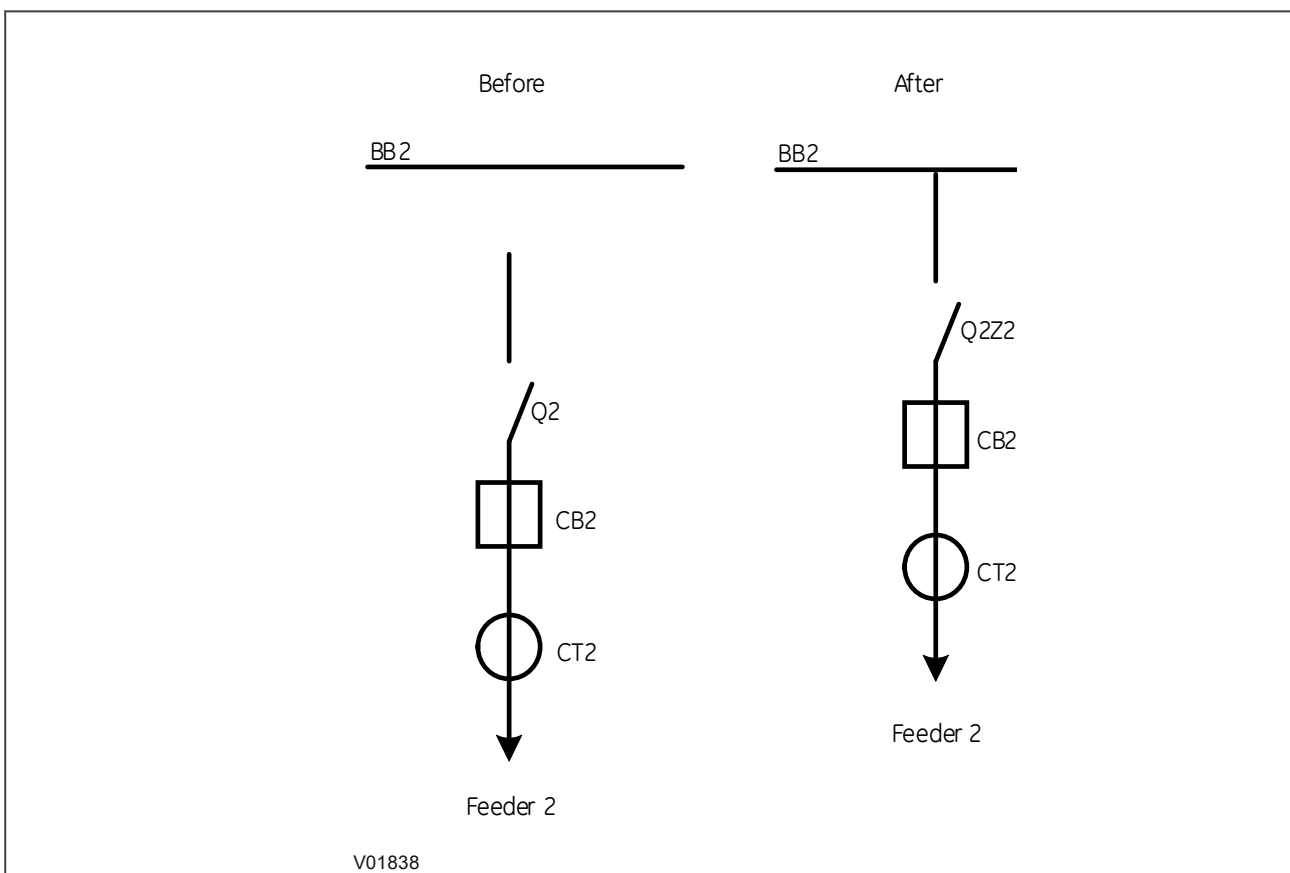
1. Select **Feeder** and press the **APPLY** button to create the Feeder Group.

Only six 1 Box mode and 18 3 Box Feeder Groups can be created.

### 28.3.6 ASSOCIATION OF ZONES FOR ISOLATORS

The Zone information for isolators in Feeder Groups and Tie Groups is associated dynamically when they are moved nearer to the Busbar.

The following diagram shows an example of association of Zone for Isolators in Feeder Groups.



**Figure 54: Association of Feeder Group with Single Isolator Group**

The following diagram shows an example of association of Zone for Isolators in Tie Groups.

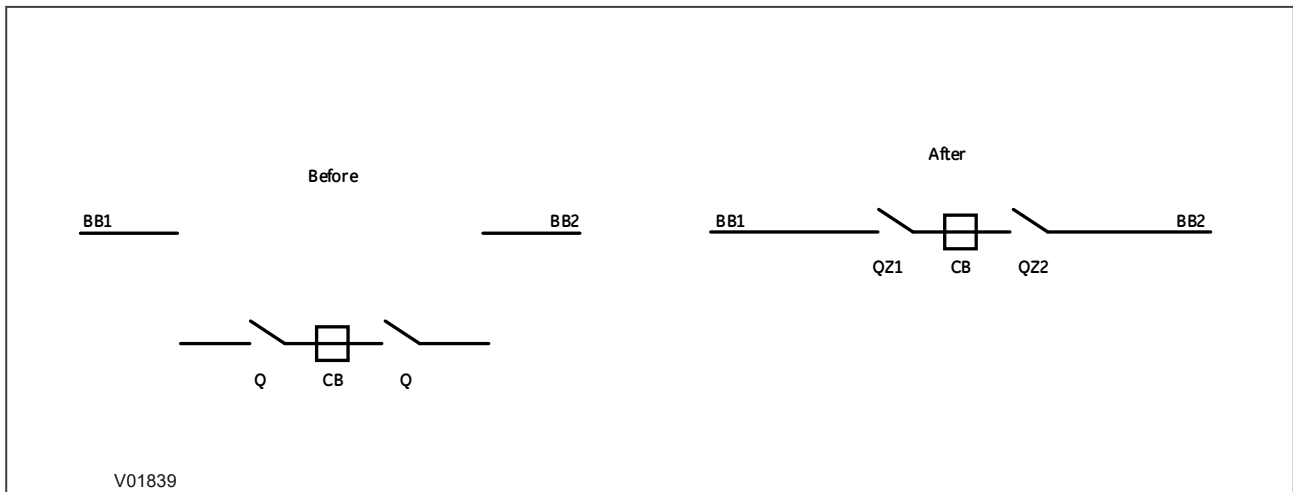


Figure 55: Association of Tie Group without Busbar Links

### 28.3.7 EDIT OPTIONS

**To move an object:** All objects can be moved anywhere in the scheme by following these steps:

1. Select the objects to be moved
2. Click the object using mouse and drag it to the new position
3. Use the **UP**, **DOWN**, **LEFT** and **RIGHT** arrow keys to move in any direction
4. If the new position of the object overlaps with any other object, the object won't move

**To copy and paste an object:**

1. Only one object can be copied at a time.
2. Select the object to be copied.
3. Copy the object by selecting **Edit >Copy** menu or right click the mouse on the selected object and choose **Copy Selection** from the submenu that appears.
4. Select **Edit >Paste** menu or right click the mouse and choose **Paste Selection** from the submenu that appears.
5. Left click the mouse on the point where the object is to be pasted.
6. If the new position of the object overlaps with any other object, the object will not be pasted and a "beep" will sound.

**To add new text:**

1. Select the 'Alphabet' character from the tool bar menu and then select the location in the scheme for new text to be placed. The **Insert Text** dialog box will then appear making it possible to insert the new text.

**To modify text in the text object:**

1. Select the text object whose text to be modified.
2. Right click the mouse on the selected text object and choose "Edit Text" option from the submenu that appears.
3. "Insert Text" dialog box appears, making it possible to modify the text.

**To remove an object:**

1. Select a single object or multiple objects to be removed.
2. Press "Del" button or select "Edit->Clear" menu to remove the selected objects.
3. To remove all objects at a time, select "Edit->Clear All" menu.

**To cancel last operation:**

1. Press **Ctrl + Z** or select **Edit > Undo** menu to cancel the last operation.

---

## 28.4 DYNAMIC SYNOPTIC

The Dynamic Synoptic polls states of CBs (Circuit Breaker), CTs (Current Transformer) with their Primary ratios and load currents, CB Bus Coupler and Isolators present in the scheme. The respective icons are animated based on the states polled from P746 and the load currents are displayed near each CT. These values are updated periodically with the information polled from the P746 unit connected it.

Dynamic Synoptic polls P746 relay and displays P746 Mode Configuration, differential and bias currents per phase, neutral values of each zone and CZ (Check Zone), voltages for connected zone, DDB Status information for Protection Status, Trip Status, Blocked Zone, Trip Zone and Alarm DDB Signals.

Zone Measurements:

- In 1 Box mode, Differential and Bias Currents per phase and neutral values of Zone1, Zone2 and Check Zone are displayed.
- In 3 Box mode, Differential and Bias Currents for the Protected phase of Zone1, Zone2 and Check Zone are displayed.
- The voltage values for connected zone are displayed.

Protection Status:

- This indicates the blocked state of 87BB and 50BF signals.
- The colours used are GREEN for "OK" and RED for "BLOCKED" state.

Trip Status:

- This indicates the trip state of 87BB and 50BF signals.
- The colours used are GREEN for "NO TRIP" and RED for "TRIPPED" state.

Blocked Zone:

- This indicates which zone is blocked.
- The colours used are GREEN for "OK" and RED for "BLOCKED" state.

Trip Zone:

- This indicates which zone is tripped.
- The colours used are GREEN for "NO TRIP" and RED for "TRIPPED" state.

Alarm Signals:

- The active alarms are displayed in the "ALARMS LIST BOX".
- On clicking the button next to the list box, the list of active alarms will be displayed.
- The ALARM icon will be in GREEN colour if no alarm is active. If at least 1 alarm is active, ALARM icon will be displayed in RED in colour.

---

## 28.5 DYNAMIC SYNOPTIC

### 28.5.1 FILE

The FILE menu proposes the following actions:

- New: Click File -> New menu or Click New icon in the Toolbar to create a new Scheme in the Scheme Editor mode. No actions except open and exit are available before creating a new scheme.
- Open: Click File -> Open menu or Click Open icon in the Toolbar to open the saved scheme. No actions except new and exit are available before opening a scheme.

- **Save:** If the scheme is open the File -> Save menu or Save icon in the Toolbar saves the scheme permanently.
- **Save As...:** If the scheme is open the File -> Save As... menu saves the scheme with different names.
- **Close:** If the scheme is open the File -> Close menu closes the it.
- **Page Setup:** If the scheme is open the File -> Page Setup menu, the Page Setup window opens. This allows to setup the page settings for printing.
- **Print:** Select File->Print to display a dialog box that allows to select the printer.
- **Print Preview:** Select File->Print Preview to preview the scheme in Print Preview dialog box.

### 28.5.2 EDIT

The EDIT is enabled in the Scheme Editor mode. All submenus under this menu are disabled in Dynamic Synoptic mode.

**Undo:** Select Edit -> Undo menu or Type "CTRL + Z" or Undo icon in the Toolbar to cancel the last action.

**Redo:** Select Edit -> Redo menu or Type "CTRL + Y" or Redo icon in the Toolbar to restore the undone action.

**Cut:** Select **Edit** > Cut menu or Cut icon in the Toolbar to cut the selected symbol in the scheme.

**Copy:** Select **Edit** > Copy menu or Copy icon in the Toolbar to copy the selected symbol in the scheme.

**Paste:** Select **Edit** > Paste menu or Paste icon in the toolbar to paste the cut or copied symbol in the scheme.

**Select All:** Select **Edit** > Select All menu or type **CTRL + A** to select all the symbols in the scheme.

**Clear:** Select **Edit** > Clear menu or press the **Delete key** to delete the selected symbol in the scheme.

**Clear All:** Select **Edit** > Clear All to delete the all the symbols in the scheme.

### 28.5.3 VIEW

#### Zoom In:

Click **View** > **Zoom** > Zoom In or "Zoom In" icon in the Toolbar to enlarge the scheme from 25% to 200%.

#### Zoom Out:

Click **View** > **Zoom** > Zoom Out menu or "Zoom Out" icon in the Toolbar to minimize the scheme from 200% to 25%.

#### Grid:

Click **View** > Grid menu to view and hide the grid in the scheme.

### 28.5.4 DEVICE

**Communication Setup:** Select Device > Communication Setup menu to display **Communication Setup** dialog box to set the communication settings in Scheme Editor and Dynamic Synoptic mode.

**Connect to P746:** Select Device > Connect to P746 to connect to the relay through the selected communication option. After connecting to the relay, the tool starts to poll the data, animates the scheme and displays the measurement data received.

**Get Device Data:** This menu is enabled only when the data is being polled from P746. Select Device > Get Device Data to display the device information in a dialog box.

**Set Polling Timer:** Select Device > Set Polling Timer menu to set the polling frequency using **Set Polling Timer** dialog box.

**Stop polling:** This menu is enabled only when the data is being polled from P746. Select Device > Stop Polling menu to stop polling in the Dynamic Synoptic mode.

### 28.5.5 MODE

The MODE menu contains only one sub-menu that differs in idle condition, Scheme Editor Mode and Dynamic Synoptic Mode.

If there is no scheme present, the submenu will be disabled.

If Scheme Editor Mode is active, **Switch to Dynamic Synoptic Mode** will be displayed. Select this menu item to switch from Scheme Editor mode to Dynamic Synaptic mode.

If Dynamic Synaptic Mode is active, **Switch to Scheme Editor Mode** will be displayed. Select this menu item to switch from Dynamic Synaptic Mode to Scheme Editor mode.

### 28.5.6 LANGUAGE

To select the following languages:

- **English:** Select **Language** > English menu to choose English language.
- **French:** Select **Language** > Français menu to choose French language.
- **Spanish:** Select **Language** > Español menu to choose Spanish language.
- **German:** Select **Language** > Deutsch menu to choose German language.
- **Russian:** Select **Language** > Русский menu to choose Russian language.
- **Chinese:** Select **Language** > 简体中文 menu to choose Chinese language.







## Imagination at work

Grid Solutions  
St Leonards Building  
Redhill Business Park  
Stafford, ST16 1WT, UK  
+44 (0) 1785 250 070  
[contact.centre@ge.com](mailto:contact.centre@ge.com)

© 2023 General Electric. 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.

P40-MCR-SAS-UG-EN-6