ProSoft® TECHNOLOGY
A BELDEN BRAND

Where Automation Connects.

PLX51-HART-8I

Isolated 8-Channel HART Input

Multidrop HART Field Devices for EtherNet/IP™ or Modbus®

June 11, 2026

USER MANUAL

Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about our products, documentation, or support, please write or call us.

ProSoft Technology, Inc.
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
www.prosoft-technology.com
ps.support@belden.com

PLX51-HART-8I User Manual
For Public Use.

June 11, 2026

Content Disclaimer

This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither ProSoft Technology nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. Information in this document including illustrations, specifications and dimensions may contain technical inaccuracies or typographical errors. ProSoft Technology makes no warranty or representation as to its accuracy and assumes no liability for and reserves the right to correct such inaccuracies or errors at any time without notice. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of ProSoft Technology. All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components. When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use ProSoft Technology software or approved software with our hardware products may result in injury, harm, or improper operating results. Failure to observe this information can result in injury or equipment damage.

For professional users in the European Union

If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.

Warning – Cancer and Reproductive Harm – www.P65Warnings.ca.gov

Agency Approvals and Certifications

Please visit our website: www.prosoft-technology.com

Contents

1 Preface 7

1.1 Introduction to the PLX51-HART-8I 7
1.2 Features 8
1.3 Architecture 9
1.4 Additional Information 11
1.5 References 11
1.6 Support 12

2 Installation 13

2.1 Module Layout 13
2.2 Module Mounting 16
2.3 Power 17
2.4 Ethernet Ports 17
2.5 Analog (HART) 17
2.5.1 Voltage Input 18
2.5.2 Current Input 19
2.5.3 Current Input with external resistor 20
2.6 Analog (HART) – Multidrop 21
2.6.1 Series Configuration 21
2.6.2 Parallel Configuration 21
2.7 Non-Isolated Analog Configuration 22

3 Setup 23

3.1 Install Configuration Software 23
3.2 Network Parameters 23
3.3 Creating a New Project 28
3.4 General Parameters 30
3.5 Channel Configuration 32
3.5.1 Adding HART Device 33
3.5.2 HART Device Configuration 36
3.5.3 HART Device Parameterization 40
3.6 Channel Calibration 42
3.6.1 Current Calibration 42
3.6.2 Voltage Calibration 43
3.7 Primary Interface 44
3.7.1 EtherNet/IP Target 44
3.7.2 Modbus Server 57
3.7.3 Modbus Client 61
3.7.4 EtherNet/IP Originator 66
3.8 Internal Data Space Map 79
3.8.1 Copy From 80
3.8.2 Copy To 86
3.8.3 Constants 88
3.9 Advanced 90
3.10 Module Download 91

4 Firmware Update 93

5 SD Card Recovery 95

5.1 Firmware 95
5.2 Configuration....96
5.2.1 Manual Copy....97
5.2.2 PLX50CU Triggered Upload 98
5.3 Network Parameters 99

6 Security Services 100

6.1 Securing Process....102
6.1.1 Configuration....102
6.1.2 Download Security Configuration 111
6.1.3 Initialize User Authentication 113
6.2 Operation 116
6.2.1 Initial User Login 116
6.2.2 Role Specific Operations 118
6.2.3 Change Other Password 122
6.2.4 Clear All Security 123
6.3 Event Log....123
6.4 Reset Security Configuration 124

7 Device Type Manager (DTM) 125

7.1 Installation....125
7.2 Configuration....126
7.2.1 PLX51-HART-8I DTM 126
7.2.2 Adding Device DTMs 128
7.3 Operation 130

8 Operation 132

8.1 HART Devices 132
8.1.1 Process Variables....132
8.1.2 Advanced Messages 133
8.1.3 Multi-device HART Channel 133
8.1.4 Explicit HART Messaging 134
8.2 EtherNet/IP Target....136
8.2.1 Class 1 Assembly Mapping 136
8.2.2 Explicit Messaging 139
8.3 EtherNet/IP Originator 141
8.3.1 EtherNet/IP Class 1 Connections 141
8.3.2 Explicit EtherNet/IP Messaging 142
8.4 Modbus Client....143
8.5 Modbus Server....144

9 Diagnostics 145

9.1 LEDs 145
9.2 Module Status Monitoring in PLX50 Configuration Utility....147
9.2.1 General 148
9.2.2 Channels....150
9.2.3 EtherNet/IP Explicit....151
9.2.4 EtherNet/IP Map 152
9.2.5 EtherNet/IP Originator 153
9.2.6 Logix 154

9.2.7 Modbus 155
9.2.8 CIP Statistics....156
9.2.9 Ethernet Clients 156
9.2.10 TCP/ARP 157
9.3 Channel 0 - 7 157
9.3.1 General 158
9.3.2 Device List 158
9.3.3 HART Statistics....159
9.3.4 Calibration....159
9.4 HART Devices 160
9.4.1 General 161
9.4.2 Device Info....162
9.4.3 Device Status....163
9.4.4 Device Configuration 164
9.4.5 Advanced Status....165
9.4.6 HART Statistics....166
9.4.7 Advanced Messages 167
9.5 Target Device Status Monitoring in the PLX50 Configuration Utility 168
9.5.1 EtherNet/IP 168
9.6 Module Event Log....171
9.7 HART Packet Capture 172
9.8 Modbus Packet Capture 176
9.9 Module Status Report....178
9.10 Modbus Summary CSV 178
9.11 Modbus Expanded CSV 180
9.12 Port Mirror....181
9.13 Flash LED 182

10 Technical Specifications 183

10.1 Dimensions 183
10.2 Electrical 184
10.3 Environmental....184
10.4 Ethernet 184
10.5 Serial Port (RS232)....185
10.6 Serial Port (RS485)....185
10.7 Analog Input Channel 185
10.8 HART 185
10.9 Modbus Client....186
10.10 Modbus Server....186
10.11 EtherNet/IP Target....186
10.12 EtherNet/IP Originator 186
10.13 Certifications 186

11 What is HART? 187

11.1 Introduction to HART 187
11.2 HART Response Status....188

12 Security 189

12.1 Scope....189
12.2 Defense in Depth 190
12.2.1 Defense in Depth vs. Hardening 190
12.2.2 Responsibilities....190
12.2.3 Example....191
12.3 Impact of the System Lifecycle to the Device Lifecycle....192
12.4 Impact of Device Requirements on System Planning....193
12.4.1 Secure Installation Location 193

12.4.2 Dedicated User Account Login Policy 194
12.4.3 Dedicated User Account Password Policy 194
12.4.4 Dedicated User Account Name and Access Role Policy for Device Management 194

13 Device Security 195

13.1 Prerequisites 195
13.2 Recommended Installation Sequence 195
13.2.1 Reasons for the Recommended Installation Sequence 195
13.2.2 Recommended Preparation for Installation 196
13.3 Choice of a Secure Installation Location 196
13.3.1 Device Availability Requirements 196
13.4 Software Update 197
13.5 Security Configuration 198
13.5.1 Assign a Static IP Address for the Device Management 198
13.5.2 Disable Insecure Management Protocols 198
13.5.3 Configure Management IP Access Restrictions 199
13.5.4 Configure Dedicated User Account Names and Access Roles for Device Management 199
13.5.5 Create a Backup of Device-Specific Data 200
13.6 Possible Hardware Modifications for Security 200
13.6.1 Restrict Physical Access to Network Ports 200
13.6.2 Restrict Physical (Visual) Access to the Device and Port LEDs 200
13.7 Device Installation 201
13.8 Operation 201
13.8.1 Environmental Conditions 201
13.8.2 Connectivity 201
13.9 Maintenance 202
13.9.1 Software Update 202
13.9.2 Hardware Enhancement 202
13.9.3 Hardware Replacement 202
13.9.4 Hardware Repair 202
13.10 Decommissioning 203
13.10.1 Destruction of Confidential Data 203
13.10.2 Secure Physical Destruction of Device and Components 204

14 Support, Service & Warranty 205

14.1 Contacting Technical Support 205
14.2 Warranty Information 205

1 Preface

1.1 Introduction to the PLX51-HART-8I

The PLX51-HART-8I supports the interfacing of HART devices on each of the 8 analog HART channels with either EtherNet/IP™ (Target or Originator) or Modbus® Client/Server (TCP/IP, RTU232, RTU485) protocols. Each channel supports both voltage and current input options (e.g., 4-20mA, Voltage, etc.), with or without HART communication enabled.

The PLX51-HART-8I supports up to 8 HART devices per channel (multidrop).

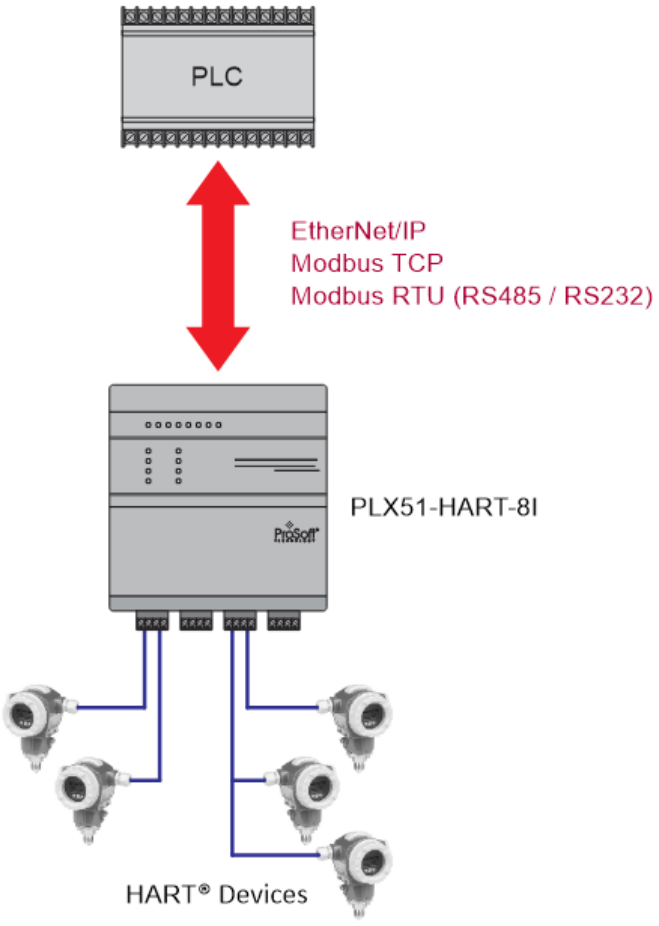


Figure 1.1 – PLX51-HART-8I multidrop typical architecture

1.2 Features

- The PLX51-HART-8I can interface analog / HART devices to either EtherNet/IP or Modbus Client or Server (TCP/IP, RTU485, RTU232).
- When operating as an EtherNet/IP target, the module will enable the HART devices to be accessed from the Logix controller using auto generated UDTs (which is created in a .L5X file from the PLX50CU software). The module can exchange up to 4KB input and 4KB output data with a Logix controller.
- When operating as an EtherNet/IP Originator, the module supports up to 10 Class 1 cyclic connections to EtherNet/IP IO as well as Explicit Messaging, including Direct-To-Tag Logix tag access, with up to 10 EtherNet/IP devices.
- When configured for Modbus Communication, the PLX51-HART-8I can be configured as either a Mobus Client or Modbus Server over TCP/IP, RS232, or RS485. The module supports the simultaneous operation of all Modbus ports.
- Each HART channel is electrically and logically isolated from the other HART channels.
- HART devices can be detected by scanning each HART channel and added to the HART channel in the PLX50 Configuration Utility software.
- Configurable HART commands can be sent and processed from the module to allow background updates of various variables and parameters.
- HART Burst mode is supported with configurable HART commands.
- Configurable HART device process variable (PV) update rates with up to 16 acyclic HART messages supported (per device) allowing for background status monitoring.
- Each channel can be configured as the following input:
  - 0 – 20mA
  - 4 – 20mA
  - 0 – 10Vdc
  - 0 – 20mA (with external resistor)
  - 4 – 20mA (with external resistor)
- SD Card backup is supported for disaster recovery (firmware, application configuration, and network parameters).
- Each channel supports dual HART masters allowing handheld programmers to operate with the existing HART communication.
- Dual Ethernet ports that support Device-Level-Ring (DLR) and port mirroring for diagnostics.
- Time Synchronization using either Simple Network Time Protocol (SNTP) or 1588 Precision Time Protocol (PTP).
- HART and Modbus packet captures and diagnostics allow for more efficient fault finding.
- A DTM (Device Type Manager) is available for simplifying device configuration and management using an FDT frame.
- The PLX51-HART-8I module is configured using the PLX50 Configuration Utility. This software can be downloaded from www.prosoft-technology.com free of charge.

1.3 Architecture

The following figure shows an example of the typical architecture for a PLX51-HART-8I interfacing to an EtherNet/IP device (e.g. Allen-Bradley Logix Controller).

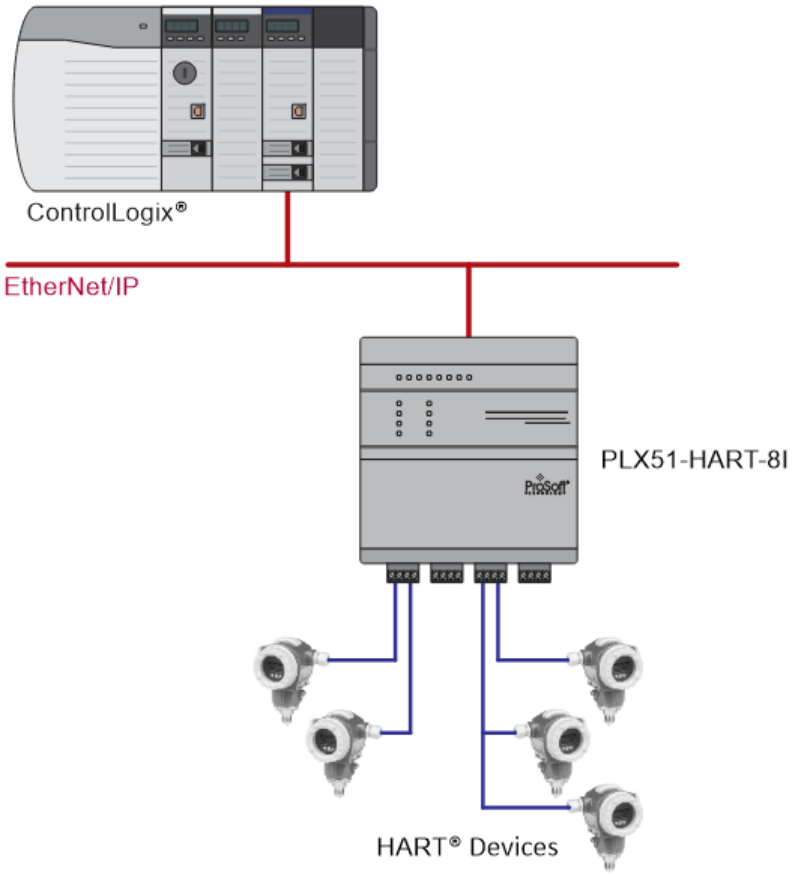


Figure 1.2 – PLX51-HART-8I EtherNet/IP typical architecture

The following figure shows an example of the typical architecture for a PLX51-HART-8I interfacing to a Modbus TCP/IP Client.

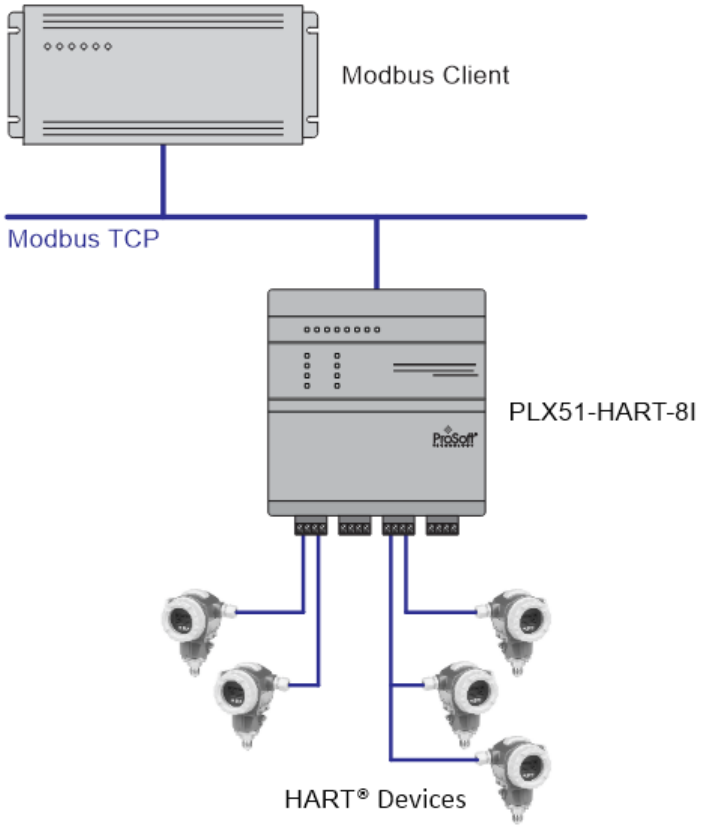


Figure 1.3 – PLX51-HART-8I Modbus TCP/IP typical architecture

The following figure shows an example of the typical architecture for a PLX51-HART-8I with Modbus RTU (RS232) communication.

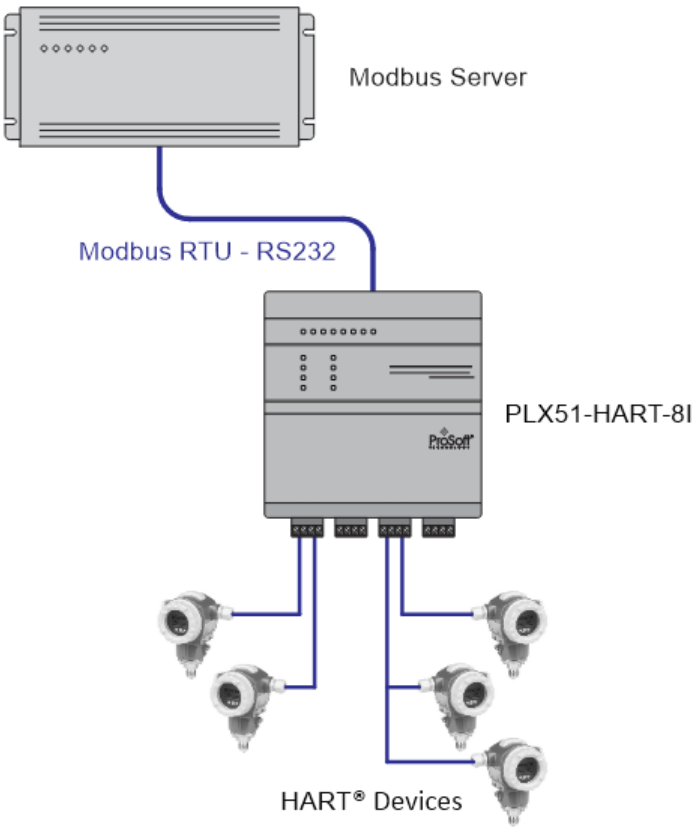


Figure 1.4 – PLX51-HART-8I Modbus RTU (RS232) architecture

1.4 Additional Information

The following documents contain additional information that can assist the user with the module installation and operation.

Resource	Link
PLX50 Configuration Utility Installation	www.prosoft-technology.com
User Manual Datasheet Example Code & UDTs	www.prosoft-technology.com

Table 1.1 - Additional Information

1.5 References

Resource	Link
FieldComm Group	https://www.fieldcommgroup.org/
CIP Routing	The CIP Networks Library, Volume 1, Appendix C: Data Management
Modbus	http://www.modbus.org

Table 1.2 – References

1.6 Support

Technical support is provided via the web (in the form of user manuals, FAQ, datasheets etc.) to assist with installation, operation, and diagnostics.

For additional support the user can use either of the following:

Resource	Link
Contact Us link	www.prosoft-technology.com
Support email	ps.support@belden.com

Table 1.3 – Support Details

2 Installation

2.1 Module Layout

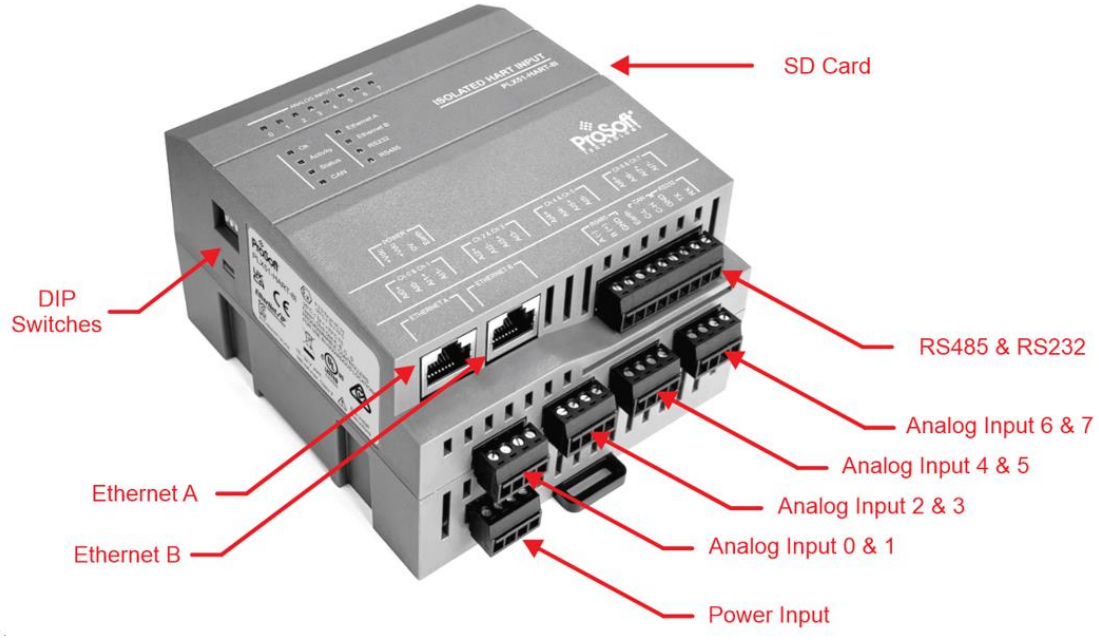


Figure 2.1 – Module top/front view

The module has three layers of connectors at the bottom.

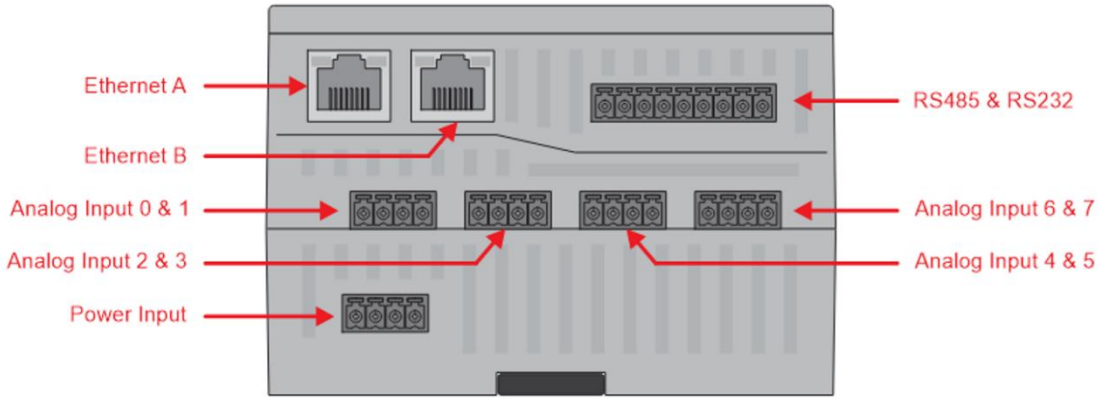


Figure 2.2 – Module bottom view

The bottom layer contains a 4-way power connector that supports redundant DC power inputs to the module.

The middle layer contains four 4-way connectors, each providing inputs for two analog inputs (mA or voltage).

The top layer contains two RJ45 connectors for Ethernet and one 9-way connector for RS232 and RS485 communications. The Ethernet cable must be wired according to industry standards, for more information see section *1.4 Additional Information*.

The module provides four DIP switches on the left-hand side of the enclosure.

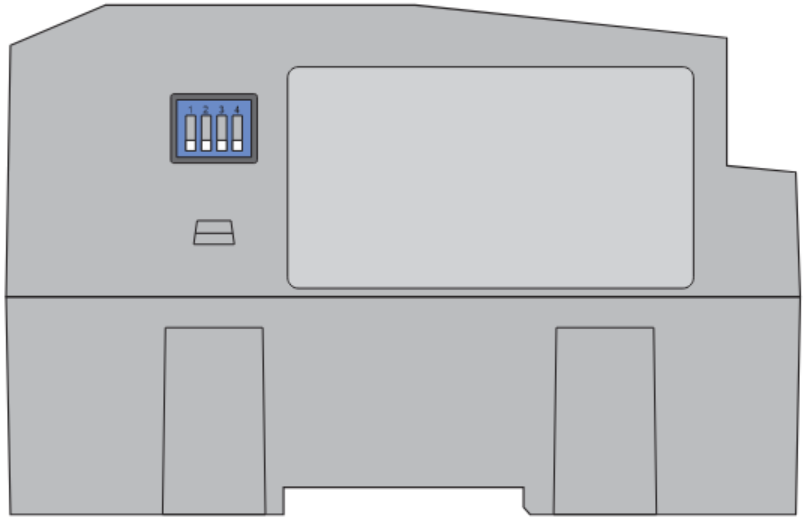


Figure 2.3 – Module side view

DIP Switch	Description
DIP Switch 1	Used to force the module into Safe Mode. When in Safe Mode the module will not load the application firmware and will wait for new firmware to be downloaded. This should only be used when a firmware update is interrupted at a critical stage.
DIP Switch 2	Used to force the module into DHCP mode which is useful when the user has forgotten the IP address of the module.
DIP Switch 3	Used to lock the configuration from being overwritten by the PLX50 Configuration Utility. When set the PLX50 Configuration Utility will not be able to download to the module.
DIP Switch 4	When set at bootup it will force the module Ethernet IP address to **192.168.1.100** and network mask **255.255.255.0**. The user can then switch the DIP switch off and assign the module a static IP address if needed.

Table 2.1 - DIP Switch Settings

The module provides eight communication and diagnostic LEDs as well as eight Analog Input / HART channel diagnostics and status LEDs. These LEDs are used to provide status of the module system operation, the Ethernet interface, and the status of each of the eight analog HART channels.

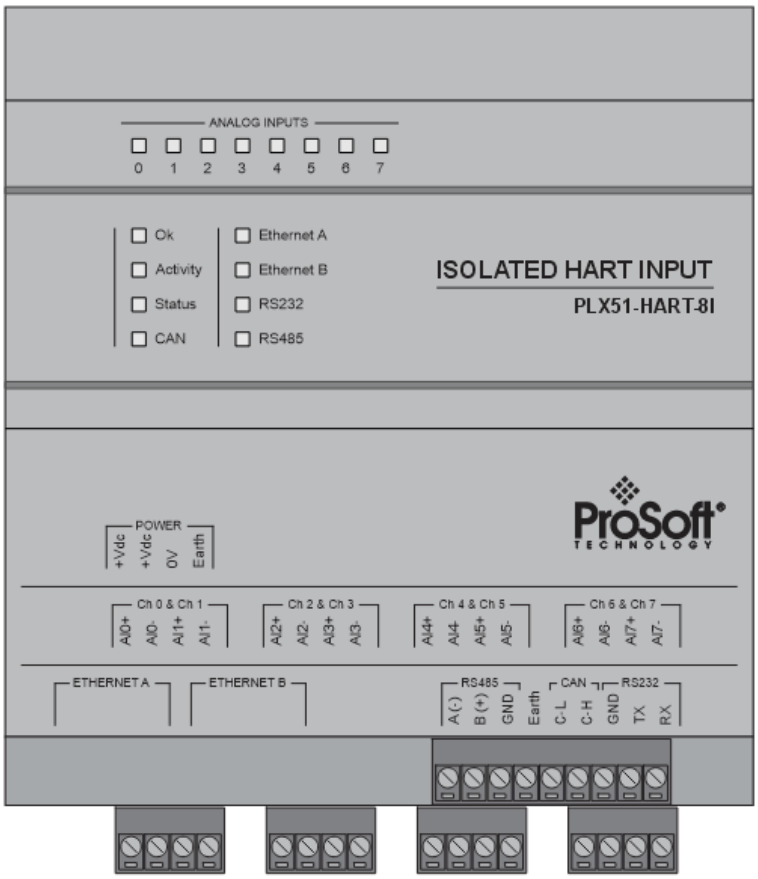


Figure 2.4 – PLX51-HART-8I front view

2.2 Module Mounting

The module provides a DIN rail clip to mount onto a 35mm DIN rail.

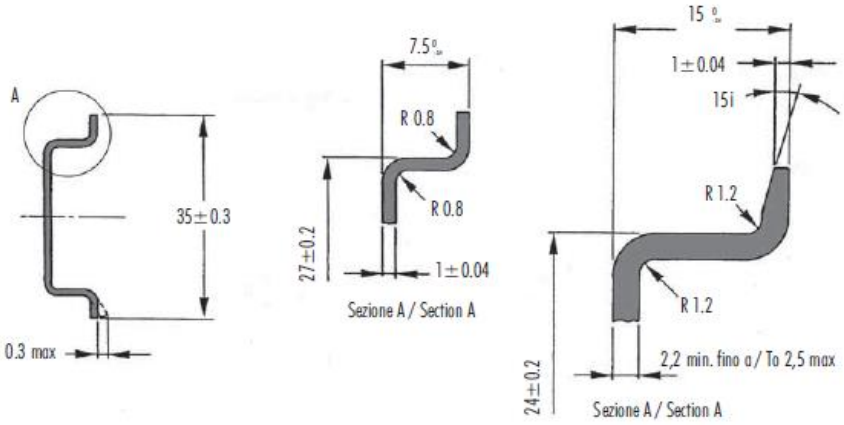


Figure 2.5 - DIN rail specification

The DIN rail clip is mounted on the bottom of the module. Use a flat screwdriver to pull the clip downward. This will enable the user to mount the module onto the DIN rail. Once the module is mounted onto the DIN rail the clip must be pushed upwards to lock the module onto the DIN rail.

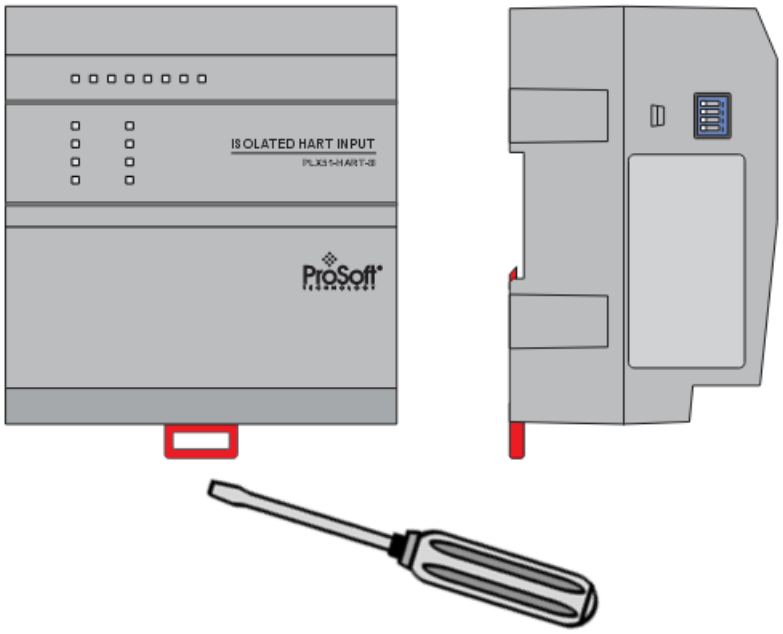


Figure 2.6 - DIN rail mouting

2.3 Power

A 4-way power connector is used to connect Power 1 +, Power 2 +, Power – (ground), and Earth. The module requires an input voltage of 10 – 32Vdc. Refer to the technical specifications in chapter *10 Technical Specifications*.

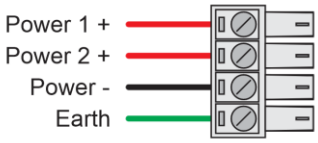


Figure 2.7 - Power connector

Note: The DC power supply or DC power source used by the PLX51-HART-8I must be classified as Limited-Energy Circuits and Safety Extra Low Voltage (SELV).

2.4 Ethernet Ports

The Ethernet connector should be wired according to industry standards. Refer to section *1.4 Additional Information* for more details.

2.5 Analog (HART)

The Analog HART channels are connected using a 4-way connector for two analog inputs.

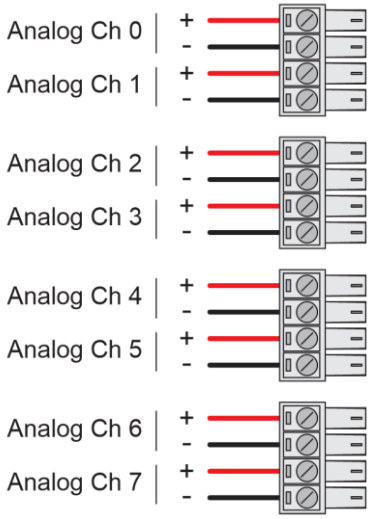


Figure 2.8 – Analog Input connectors

Each analog input channel can be represented by the following equivalent circuit:

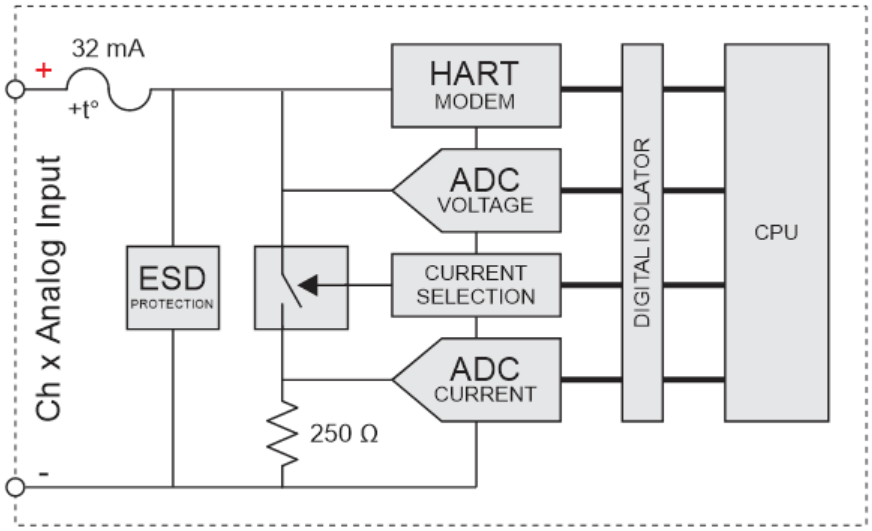


Figure 2.9 – Analog Input equivalent circuit

Note: All analog input channels are galvanically isolated from each other, and from the module's CPU.

Each channel can be configured for either voltage, current, or current with an external resistor.

2.5.1 Voltage Input

When configured for a Voltage input (0-10V), the wiring to the terminal must be like the examples shown below.

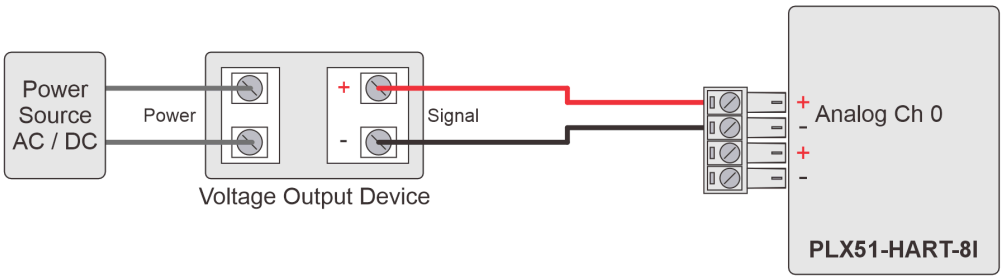


Figure 2.10 – Typical Volatge input

Note: Voltages more than 11V should not be applied to the inputs.

2.5.2 Current Input

When configured for current input types (0-20mA or 4-20mA), the wiring of 2-wire devices should be such that it is loop-powered with the device (as shown below).

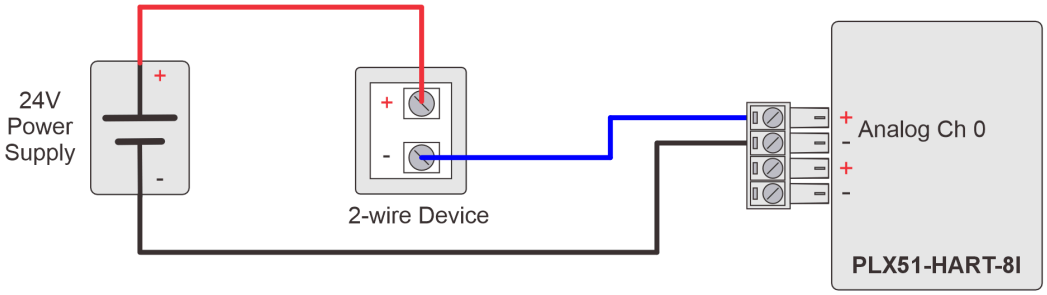


Figure 2.11 – Current Input – Loop-Powered (2-wire) device

Non-loop powered (4-wire) devices should be wired as follows:

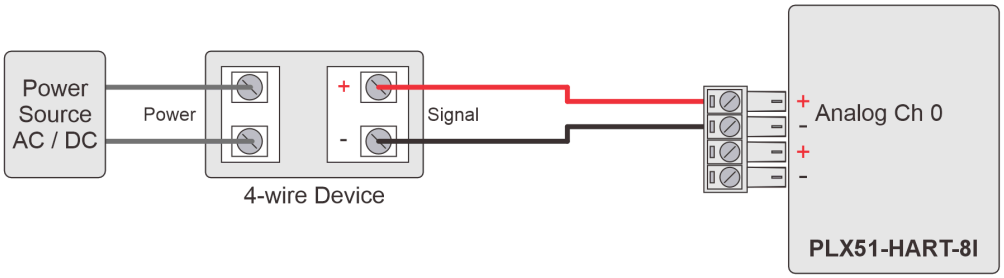


Figure 2.12 – Current Input – Non-Loop-Powered (4-wire) device

Note: Currents more than 32 mA should not be applied to the inputs.

2.5.3 Current Input with external resistor

When configured for current input type (0-20mA or 4-20mA) with an external resistor, the wiring of a loop-powered device should be as follows:

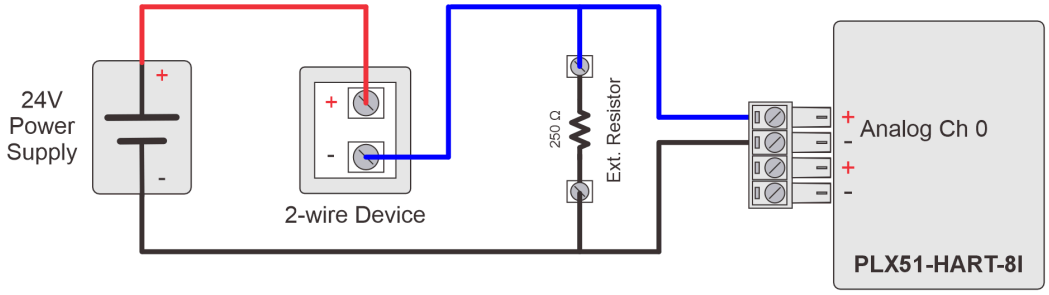


Figure 2.13 – Current Input – Loop-Powered (2-wire) device with External Resistor

The exact resistance of the external resistor must be entered into the channel's configuration.

This mode can also be used when adding the PLX51-HART-8I module to an existing analog device and PLC application.

Here, the exact input impedance of the PLC's analog card must be entered into the channel's configuration.

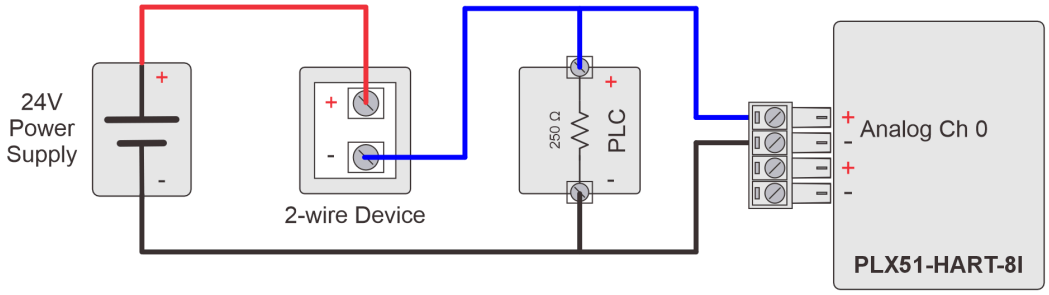


Figure 2.13 – Current Input – Loop-Powered (2-wire) device with PLC analog card

Note: The maximum current of the device and selected external resistor combination must be such to not result in Voltages more than 11V being applied to the inputs.

V = I x R

2.6 Analog (HART) – Multidrop

The PLX51-HART-8I module supports multiple HART devices being connected to a single channel – this is typically referred to as multidrop.

In a multidrop setup the field devices can be connected in either a series or parallel configuration. A maximum of 8 devices can be connected per channel.

2.6.1 Series Configuration

The series connection method has the advantage of the (4-20 mA) current still being controlled by one of the devices, which may be required in some applications. The disadvantage is that the supply voltage is divided by the devices, so the maximum device count would typically be 2. (Assuming a typical minimum of 10V, and a supply of 24V).

The following example shows 2 loop-powered (2-wire) devices connected in series.

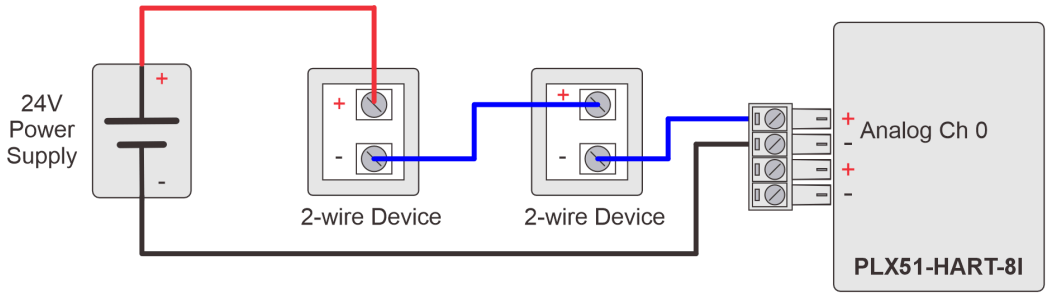


Figure 2.14 – PLX51-HART-8I - Multidrop Wiring – Series

Note: It is not recommended to multidrop 4-wire devices unless all devices make use of isolated power supplies.

2.6.2 Parallel Configuration

Connecting the field devices in parallel is more common although it has the disadvantage that the 4-20 mA cannot be controlled by any device. Here all the field devices should be set to 4 mA (current modulation disabled) and all share a common supply.

The PLX51-HART-8I can support 8 parallel devices per channel.

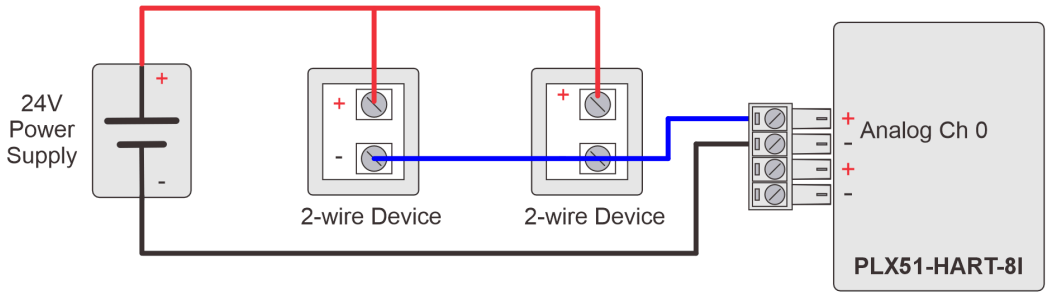


Figure 2.15 – PLX51-HART-8I - Multidrop Wiring – Parallel

2.7 Non-Isolated Analog Configuration

Although each analog channel is isolated, in some instances this isolation is not required, and the use of a single 24V power supply is preferred.

The unit can then be configured as follows:

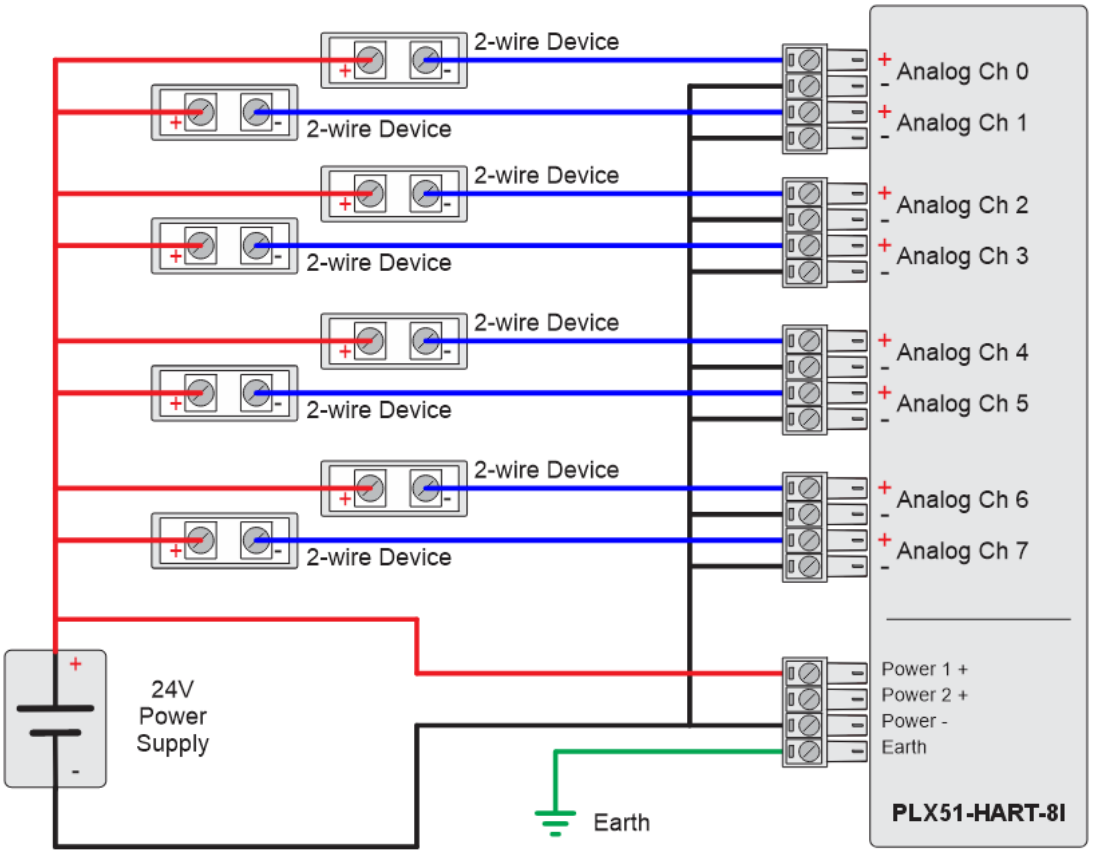


Figure 2.16 – PLX51-HART-8I – Non-Isolated Wiring

3 Setup

3.1 Install Configuration Software

The PLX51-HART-8I network setup and configuration is achieved by means of the PLX50 Configuration Utility (PLX50CU). This software can be downloaded from: www.prosoft-technology.com.

Figure 3.1 - PLX50 Configuration Utility

3.2 Network Parameters

The module will have DHCP (Dynamic Host Configuration Protocol) enabled as factory default. Thus, a DHCP server must be used to provide the module with the required network parameters (IP address, subnet mask, etc.). There are several DHCP utilities available, however it is recommended that the DHCP server in the PLX50 Configuration Utility be used.

Note: When DIP Switch 4 is set at bootup, it will force the module's IP address to **192.168.1.100** and network mask **255.255.255.0**. The user can then switch the DIP switch **OFF** and assign the module a static IP address.

Within the PLX50 Configuration Utility, the **DHCP SERVER** can be found under the *Tools* menu.

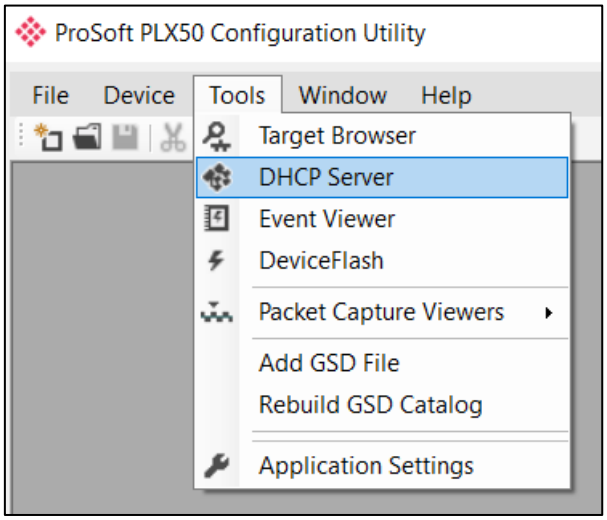


Figure 3.2 - Selecting DHCP Server

Once opened, the DHCP server will listen to all available network adapters for DHCP requests and display their corresponding MAC addresses.

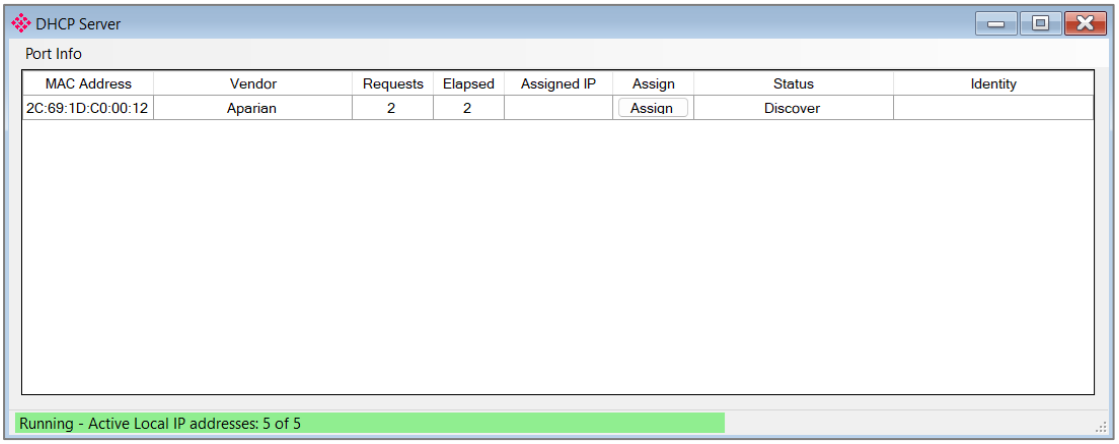


Figure 3.3 - DHCP Server

Note: If the DHCP requests are not displayed in the DHCP Server, it may be due to the local PC's firewall. During installation, the necessary firewall rules are automatically created for the Windows firewall. Another possibility is that another DHCP Server is operational on the network, and it has assigned the IP address.

To assign an IP address, click on the corresponding **ASSIGN** button to open the *Assign IP Address for MAC* window.

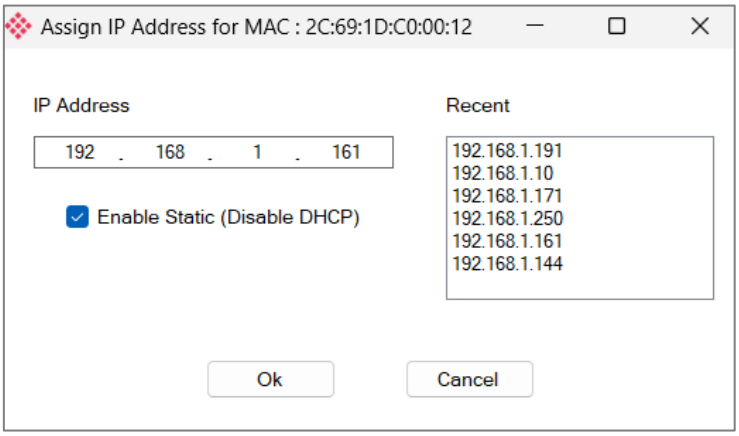


Figure 3.4 - Assigning IP Address

The required IP address can then be either entered, or a recently used IP address can be selected by clicking on an item in the *Recent* list. If the **ENABLE STATIC** checkbox is checked, then the IP address will be set to static after the IP assignment, thereby disabling future DHCP requests.

Once the IP address window has been accepted, the DHCP server will automatically assign the IP address to the module and then read the Identity Object Product name from the device.

The successful assignment of the IP address by the device is indicated by the green background of the associated row.

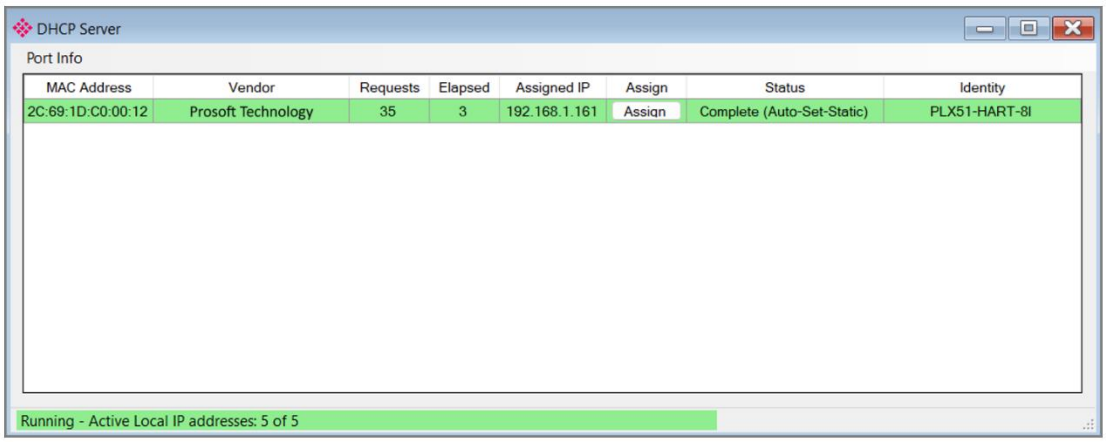


Figure 3.5 - Successful IP address assignment

It is possible to force the module back into DHCP mode by powering up the device with DIP switch 2 set to the **ON** position.

A new IP address can then be assigned by repeating the previous steps.

Important: It is important to return DIP Switch 2 back to **OFF** position, to avoid the module returning to a DHCP mode after the power is cycled again.

In addition to setting the IP address, several other network parameters can be set during the DHCP process. These settings can be viewed and edited in the PLX50 Configuration Utility's Application Settings, in the DHCP Server tab.

Once the DHCP process has been completed, the network settings can be set using the Ethernet Port Configuration via the Target Browser. The **TARGET BROWSER** can be accessed under the *Tools* menu.

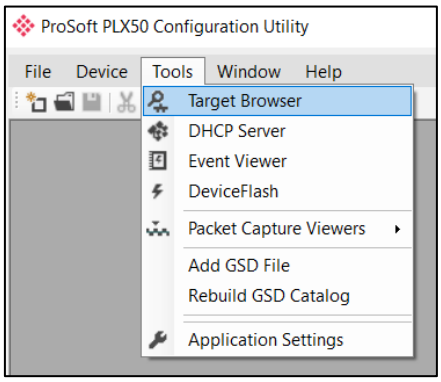


Figure 3.6 - Selecting the Target Browser

The *Target Browser* automatically scans the Ethernet network for EtherNet/IP devices.

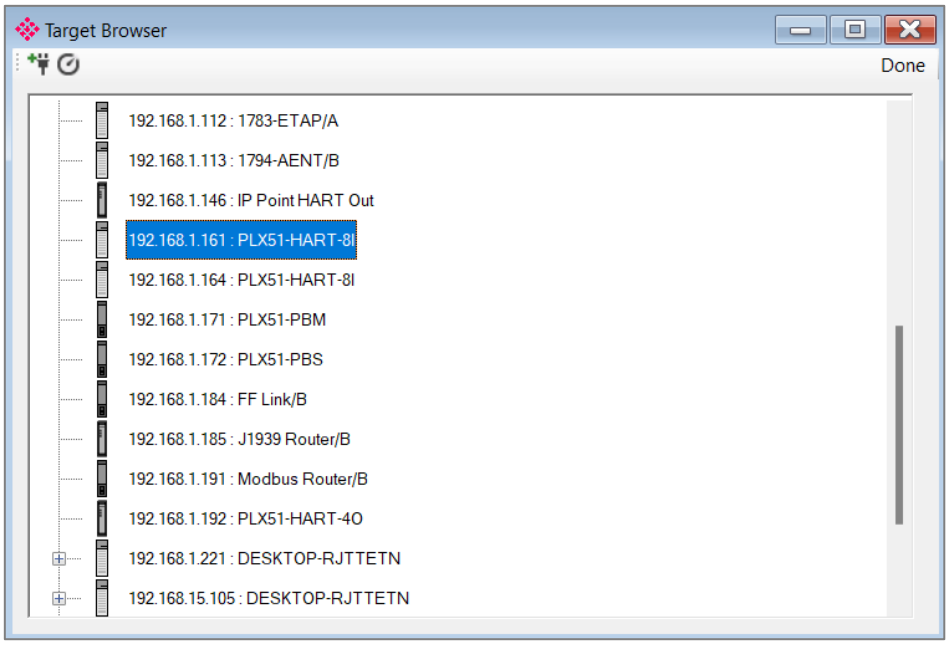


Figure 3.7 - Target Browser

Right-clicking on a device, reveals the context menu, including the **PORT CONFIGURATION** option.

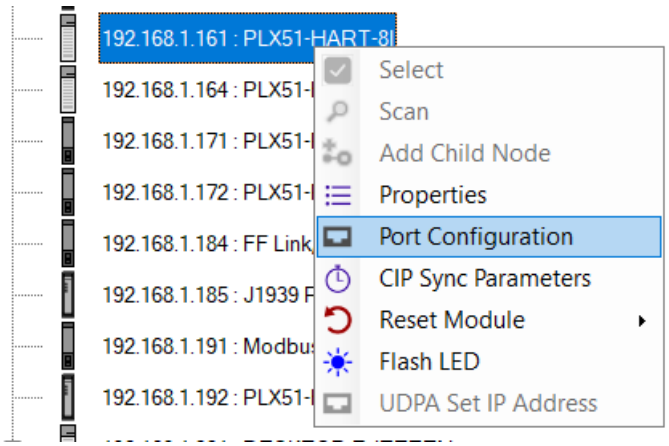


Figure 3.8 - Selecting Port Configuration

The relevant Ethernet port configuration parameters can be modified using the *Port Configuration* window.

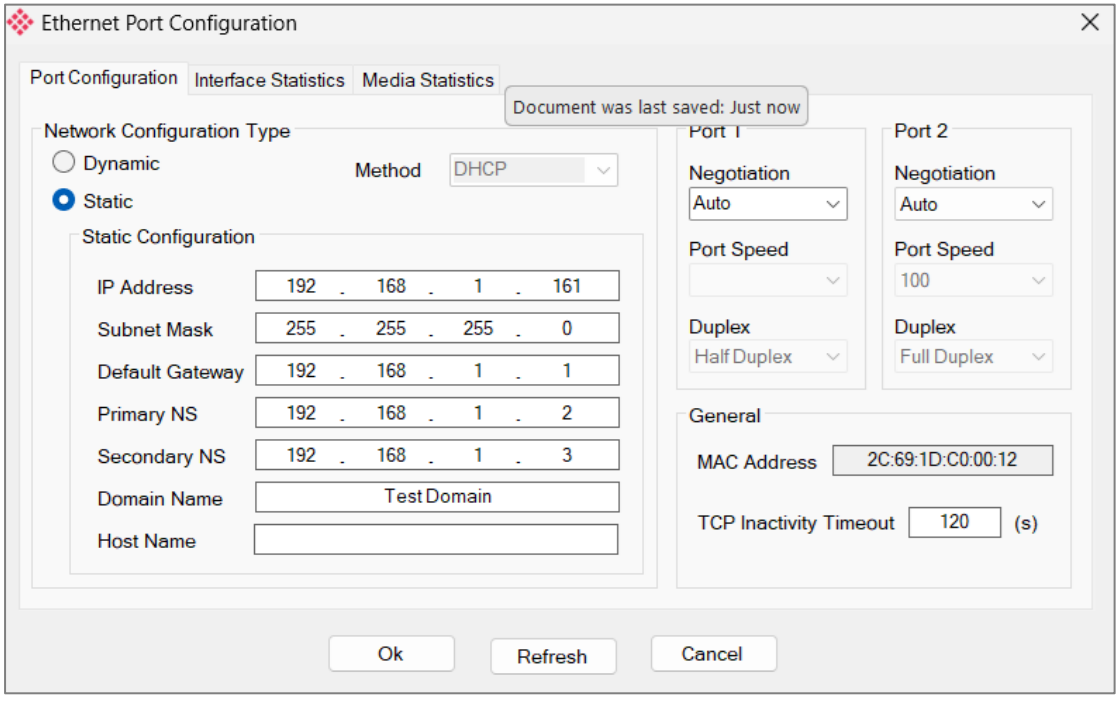


Figure 3.9 - Port Configuration

Alternatively, these parameters can be modified using Rockwell Automation's RSLinx software.

3.3 Creating a New Project

Before the user can configure the module, a new PLX50 Configuration Utility project must be created. Under the *File* menu, select **NEW**.

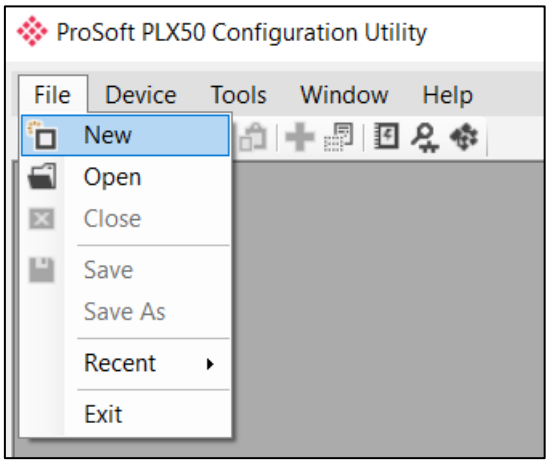


Figure 3.10 - Creating a new project

A PLX50 Configuration Utility project will be created, showing the Project Explorer tree view. To save the project use the **SAVE** option under the *File* menu. A new device can now be added by selecting **ADD** under the *Device* menu.

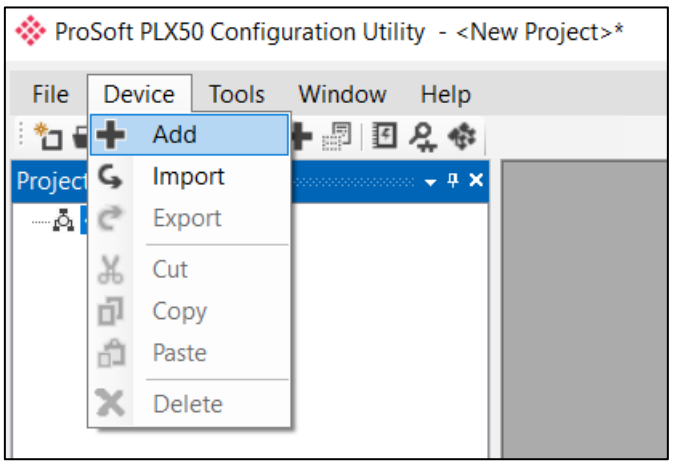


Figure 3.11 - Adding a new device

In the *Add New Device* window select the PLX51-HART-8I and click the **OK** button.

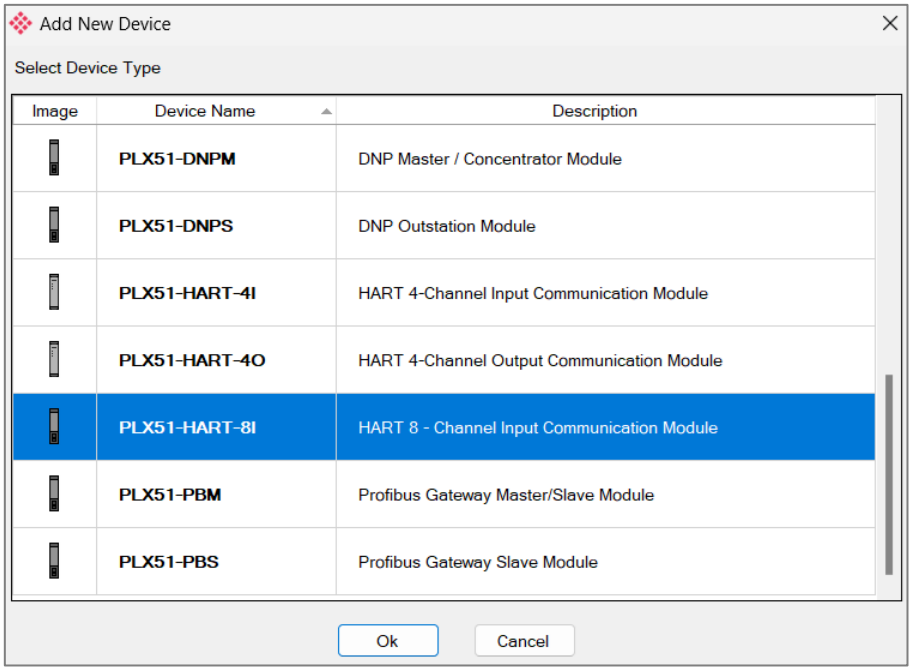


Figure 3.12 – Selecting a new module

The device will appear in the Project Explorer tree, and its configuration window opens. The device configuration window can be reopened by either double-clicking the module in the Project Explorer tree or right-clicking the module and selecting **CONFIGURATION**.

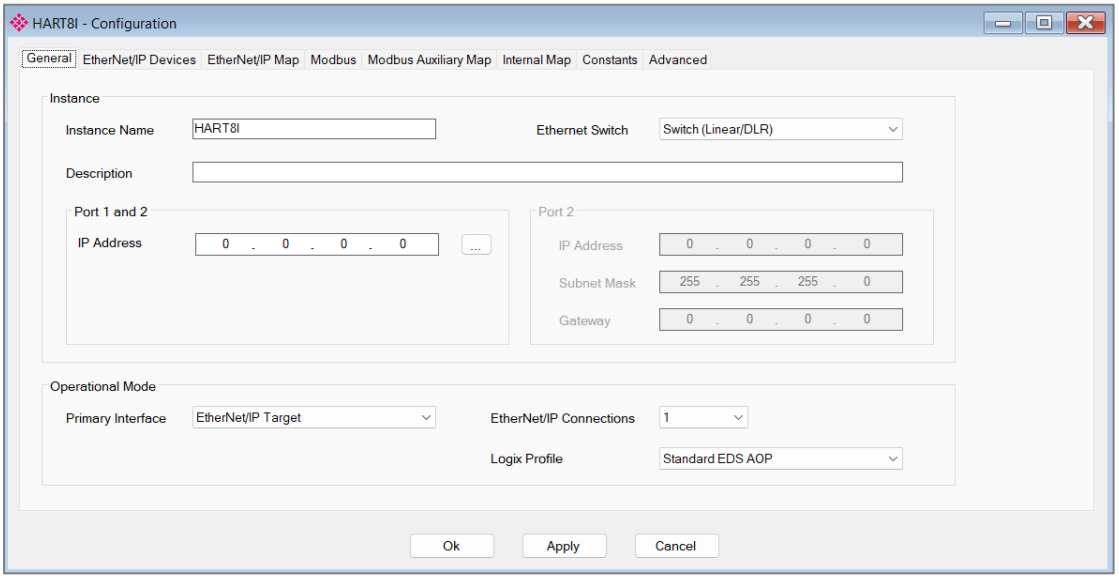


Figure 3.13 – Module configuration

3.4 General Parameters

The PLX51-HART-8I parameters are configured by the PLX50 Configuration Utility software. When downloading this configuration into the module it will be saved in non-volatile memory that persists when the module is powered down.

Important: When a firmware upgrade is performed the module will clear all configuration.

The general configuration is shown in the figure below. The general configuration window is opened by either double-clicking on the module in the tree, or right-clicking the module and selecting **CONFIGURATION**.

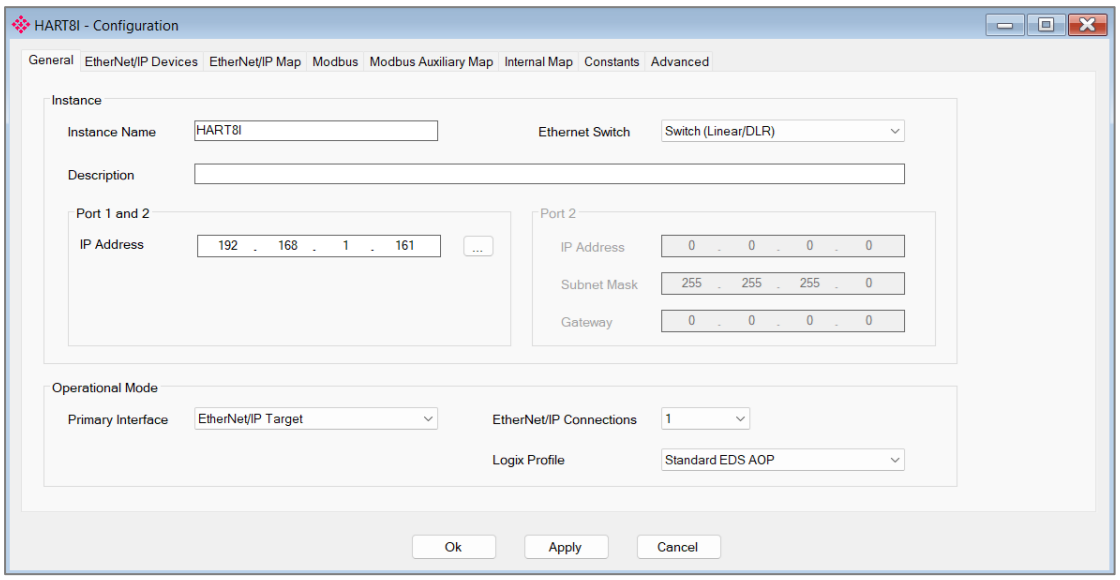


Figure 3.14 – General configuration

The general configuration consists of the following parameters:

Parameter	Description
Instance	
Instance Name	This parameter is a user-defined name to identify between various modules.
Description	This parameter is used to provide a more detailed description of the application for the module.
Ethernet Switch	The operational mode of the embedded Ethernet switch. **Switch** (Linear/DLR) This is the default mode where the embedded switch is enabled. The two Ethernet ports are identical in functionality and (external) traffic received on one port is transmitted out the other. Both ports use the IP address configured using DHCP or set the Target browser. **Split** (Dual-IP) In this mode the embedded switch is disabled. Traffic received at one port is not transmitted to the other. *Port 1*: The IP address is the one configured using DHCP or via the Target browser. EtherNet/IP requests and connections will be processed. Modbus TCP requests will be processed.

	Port 2: The IP address is the one contained within the configuration below (Port 2). EtherNet/IP requests and connections will not be processed. Modbus TCP requests will be processed.
Port 1 IP Address	The IP address of the local module when the embedded switch is set to **LINEAR** or Ethernet Port 1 when the switch is set to **SPLIT**.
Port 2 IP Address	The IP address used on Port 2 when the embedded switch is set to **SPLIT**.
Port 2 Subnet Mask	The Subnet Mask used on Port 2 when the embedded switch is set to **SPLIT**.
Port 2 Gateway	The Default Gateway used on Port 2 when the embedded switch is set to **SPLIT**.
Operational Mode	
Primary Interface	**EtherNet/IP Target**: A Logix controller can own the PLX51-HART-8I over EtherNet/IP using up to 8 class 1 connections. **Modbus Server**: An external Modbus Client can read and write data to the module which can then be mapped to one or more Analog/HART devices. The module can operate as a Modbus Server on Ethernet TCP, RTU232, and RTU485. **Modbus Client**: The module can read and write data from various external Modbus devices which can then be mapped to one or more Analog/HART devices. The module can operate as a Modbus Client on Ethernet TCP, RTU232, and RTU485 **EtherNet/IP Originator**: As an EtherNet/IP originator, the module can use two methods to read and write data to and from an EtherNet/IP device (IO): **EtherNet/IP Class 1 Connection**: The PLX51-HART-8I can own EtherNet/IP IO by using the PLX50CU software to configure the IO connections. **EtherNet/IP Explicit Messaging**: The PLX51-HART-8I can exchange data with up to 10 EtherNet/IP devices using explicit messaging.
EtherNet/IP Connections	The number of class 1 CIP connection established between the ControlLogix CPU and the module. (1 to 8). **Note:** This value must match that configured in the Logix IO tree.
Logix Profile	The Studio 5000 profile used to instantiate the PLX51-HART-8I. **Standard AOP**: This is the preferred profile which allows the user to configure between 1 and 8 connections. **Generic Profile**: This option provides only a single connection and is required for older versions of Logix.

Table 3.1 - General configuration parameters

3.5 Channel Configuration

The analog channel specific configuration is shown below. Each of the 8 channels has the same configuration options. The channel configuration window is opened by either double-clicking on the specific channel of the module in the tree, or right-clicking on the specific channel and selecting **CONFIGURATION**.

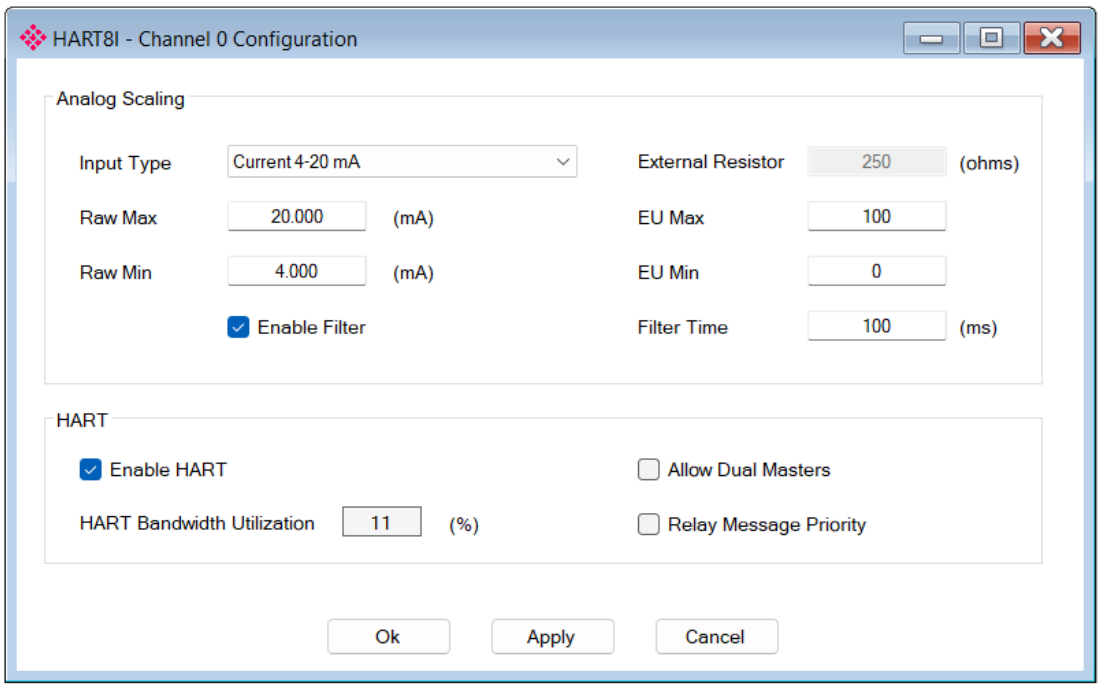


Figure 3.15 – Channel configuration

The Channel configuration consists of the following parameters:

Parameter	Description
Analog Scaling	
Input Type	*Current* or *Voltage*
Raw Max	The upper analog value to be used for the scaling to engineering units. The scaling to engineering units (EU) is calculated as follows: EU = EUMin + (RawValue – RawMin) * ((EUMax – EUMin) / (RawMax – RawMin))
Raw Min	The lower analog value to be used for the scaling to engineering units.
External Resistor	Used to specify the exact value of the external resistor when using one of the Current - Ext. Resistor input types.
EU Max	The upper engineering value used for the scaling to engineering units. The scaled engineering value will equal this value when the analog value is equal to the *Raw Max* value.
EU Min	The lower engineering value used for the scaling to engineering units. The scaled engineering value will equal this value when the analog value is equal to the *Raw Min* value.
Enable Filter	Enable or Disable Analog Filtering.
Filter Time	The time constant, in milliseconds, of the first order filter applied to the analog signal. A value of zero implies no filtering.
HART	
Enable HART	Used to Enable or Disable the HART Communication. This should be disabled when using standard (non-HART) analog field devices.

Allow Dual Masters	When set, the PLX51-HART-8I module (as the primary HART Master) will allow communication to be shared with a secondary HART Master (e.g., a handheld programmer or calibrator).
Relay Message Priority	This option will allow relay messages (e.g., from Asset Managers like FDT/DTMs) that are sent to the HART device to be prioritized, resulting in a faster response time.
HART Bandwidth Utilization	An indication of the approximate bandwidth utilization of all the devices on this HART channel. This value considers the PV Updates and the configured Advanced Messages for each device. An indicted value near or above 100% indicates that the channel is oversubscribed and that the configured device update rates will not be able to be achieved. In this case, the configured update rates of the underlying devices will need to be adjusted accordingly.

Table 3.2 - Channel configuration parameters

3.5.1 Adding HART Device

HART devices can either be added manually or directly from the device scan list.

3.5.1.1 Manually

When right-clicking on a specific channel, the user can select **ADD DEVICE** to add a HART device at a specific HART node address. Each channel can have a maximum of eight HART devices.

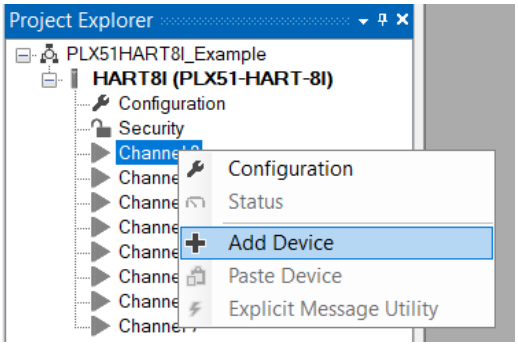


Figure 3.16 – Manually adding HART device

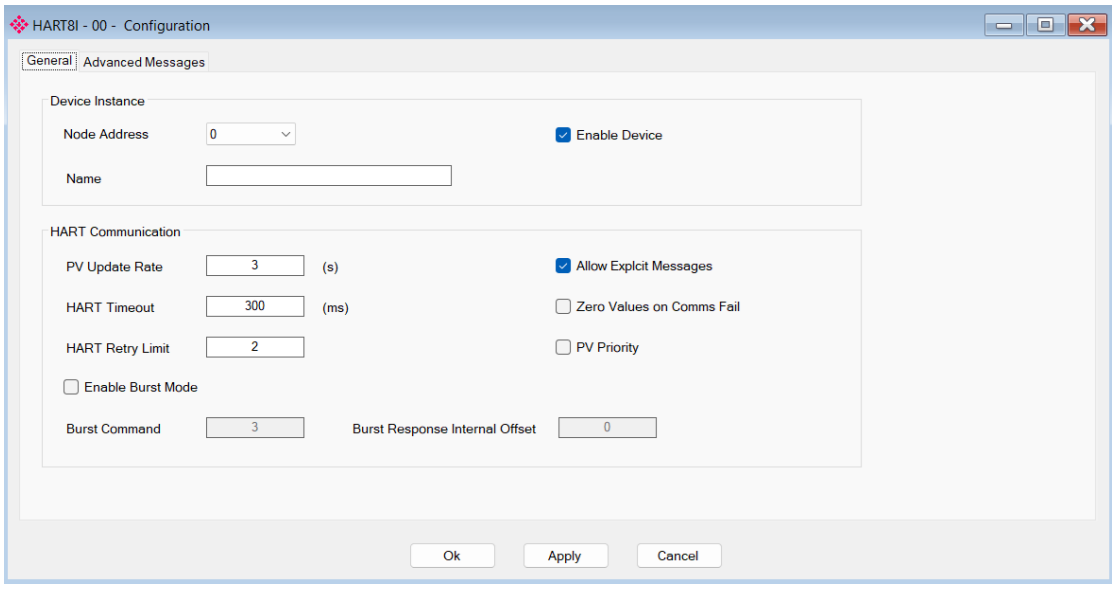


Figure 3.17 – HART Device General Configuration

Once the **OK** button is pressed, then the HART device will be added to the Channel.

Figure 3.18 – HART Device added to Channel

3.5.1.2 Device List Scanning

When online with the module, the *Device List* can be accessed by right-clicking on the channel, selecting **STATUS**, and clicking the **DEVICE LIST** tab.

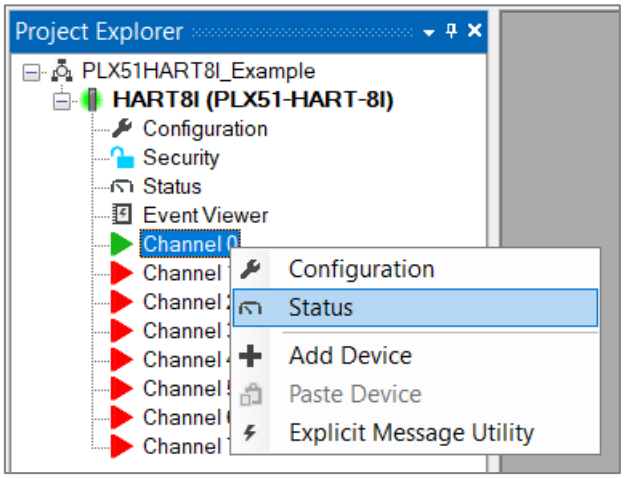


Figure 3.19 – Channel Status selection

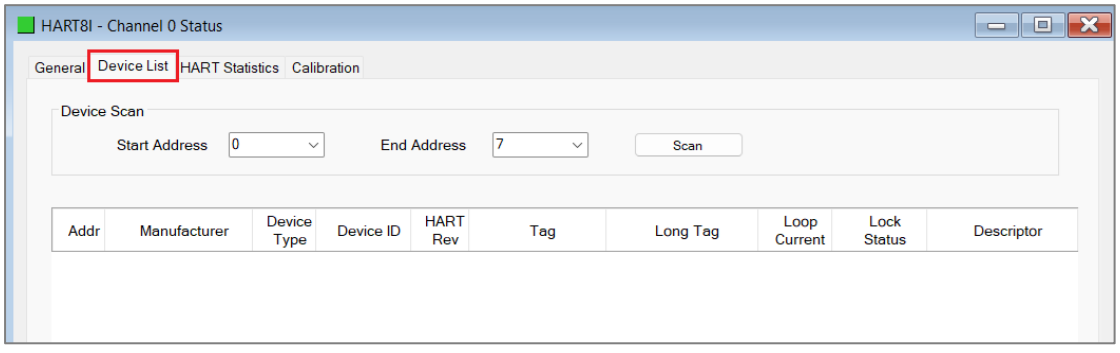


Figure 3.20 – Channel Device List

Once the **SCAN** button is pressed, the module will scan the specific channel from the selected *Start Address* to the *End Address*. If a device is found, it will be listed in the table.

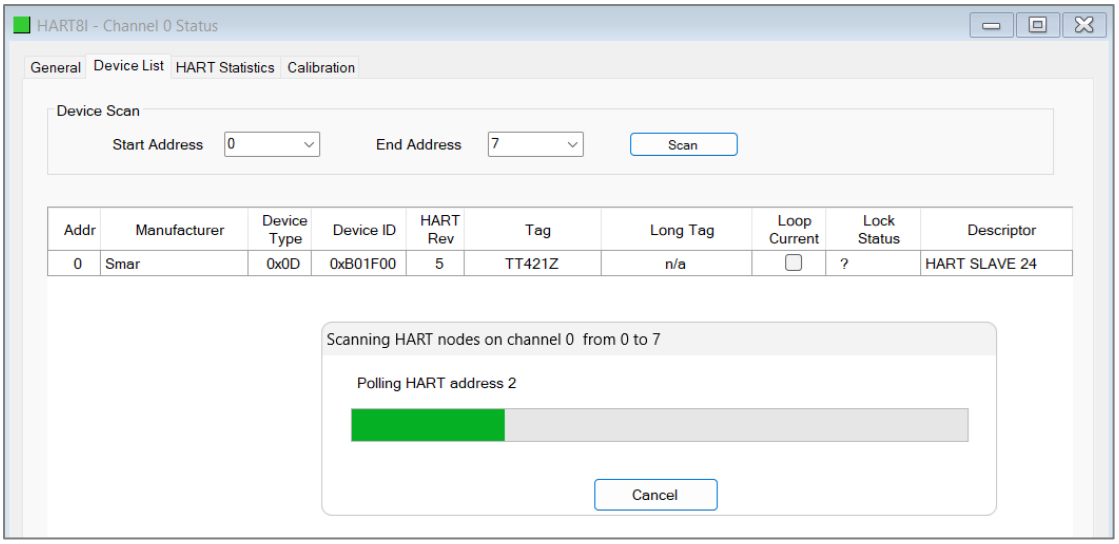


Figure 3.21 – Channel Device List Scanning

When right-clicking on a HART device that was found on the channel, the user can select **ADD** to add the HART device to the module configuration.

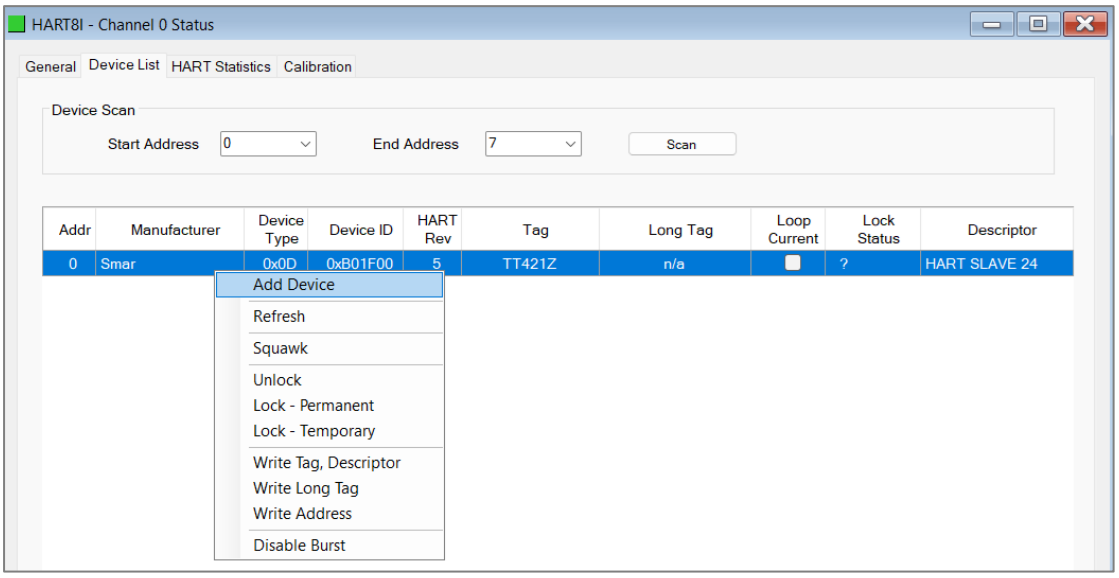


Figure 3.22 – Add HART device from Device List

3.5.2 HART Device Configuration

Once a HART device has been added to the module configuration, the HART device configuration can be opened by either double-clicking on the device, or right-clicking on the device and selecting **CONFIGURATION**.

3.5.2.1 General

The HART device general configuration is shown in the figure below.

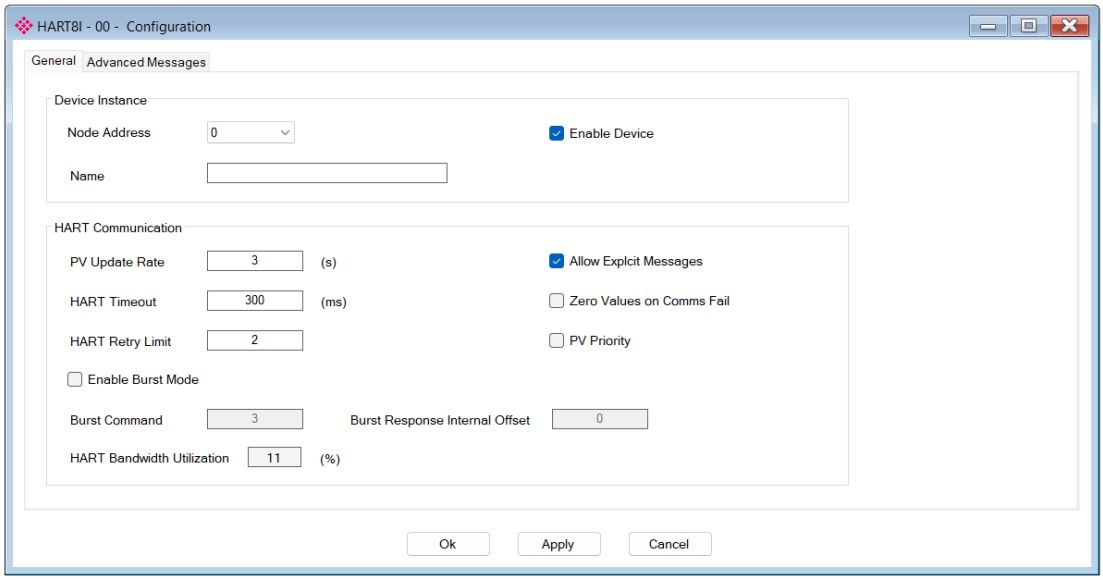


Figure 3.23 – HART Device General configuration

The HART Device general configuration consists of the following parameters:

Parameter	Description
Device Instance	
Node Address	The short address of the HART device.
Name	User configurable name given to the HART device in the configuration software (which will also be used when generating the Logix L5X UDTs). **Note:** This name is not linked to the HART tag name of the device.
Enable Device	Enable or Disable HART communication to the device.
HART Communication	
PV Update Rate	The update rate of the HART process Variable (HART Command 3) in seconds. A value of zero would indicate as fast as possible. **Note:** When the PV update rate is low (i.e., fast) on a high traffic channel (e.g., multiple HART devices), it will cause the other HART communication on the channel to update at a slower rate. **Note:** When multiple devices are connected on the same channel it is not recommended to use a PV Update Rate of zero.
HART Timeout	The time in milliseconds that the module will wait for a HART device to respond. A ***No Response*** will be declared after the timeout has expired.
HART Retry Limit	The number of consecutive no responses from the specific HART device, before the status of HART device is set to offline.
Allow Explicit Messages	Allow or block explicit HART messages (e.g., FDT/DTM asset management) being requested via the Ethernet interface of the module.
Zero Values on Comms Fail	When selected, if the specific HART device goes offline, then all the PV values will be forced to zero.

PV Priority	When this option is set, the updating of Process Variables for the specific HART device will be prioritized over any other explicit or advanced HART messages that need to execute.
Enable Burst Mode	Burst HART communication will be enabled on the specific device. Burst communication will send the response for a configured HART command continuously without the need for the module to send the request for the HART command. **Note:** When HART Burst mode is enabled, then only one HART device can communicate on the specific analog channel and Multidrop architectures are invalid for the specific analog channel.
Burst Command	Generally, HART command 3 responses will be continuously sent by the device when Burst is enabled, but certain devices allow different HART commands to be returned in Burst mode. If supported by the HART device, this will provide the option to enter the specific HART command.
Burst Response Internal Offset	The data received from the HART Burst Response will be placed in the Internal Data Space (IDS) Offset configured here. This can then be mapped to any Primary Communication interface using the internal mapping. **Note**: When HART command 3 is set to Burst, then all the normal PV values will also be automatically updated in addition to writing the values to the IDS offset configured.
HART Bandwidth Utilization	An indication of the approximate bandwidth utilization of this device on the HART channel. This value considers the PV Updates and the configured Advanced Messages.

Table 3.3 – HART Device General configuration parameters

3.5.2.2 Advanced Messages

The PLX51-HART-8I module supports configurable HART commands that can be sent and processed in the background. These HART commands are configured in the *Advanced Messages* tab. Up to 16 Advanced Messages can be configured per HART device with configurable update rates.

To configure each Advanced Message, click on the **BUILD** button as shown below:

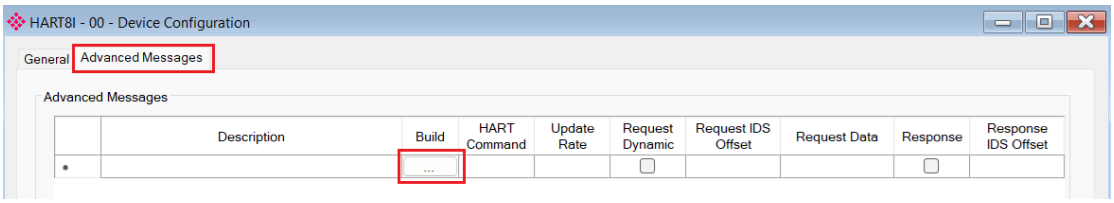


Figure 3.24 – HART Device Advanced Message Configuration

Once the **BUILD** button is pressed, then the *Advanced Message Builder* is opened as shown below.

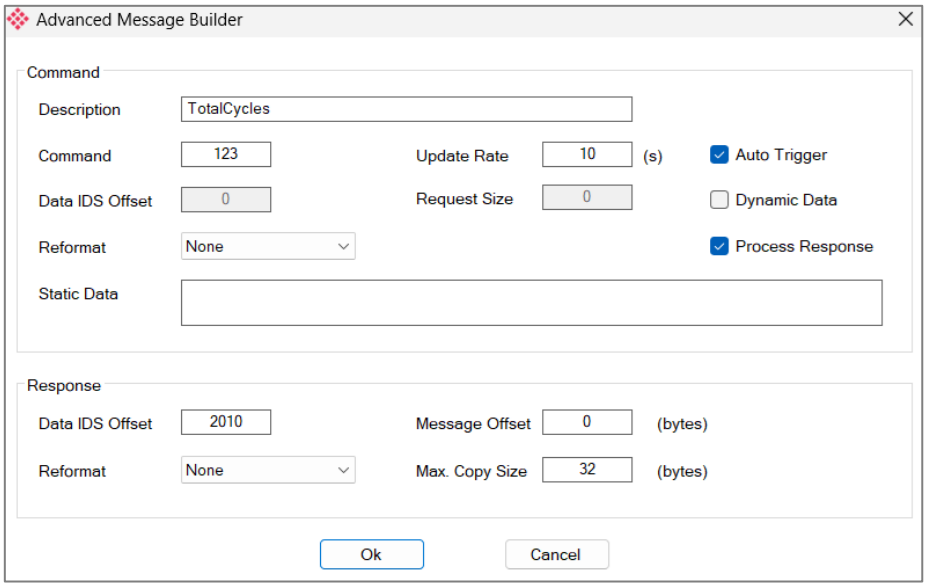


Figure 3.25 – HART Device Advanced Message Builder

The HART Device Advanced Message configuration consists of the following parameters:

Parameter	Description
Command	
Description	The user description of the specific Advanced Message
Command	The HART command to be sent
Data IDS Offset	If the *Dynamic Data* option has been selected, then the data to be sent with the HART command (with the *Request Size* number of bytes) will be read from this Internal Data Space Offset.
Reformat	Used to specify how the data is formatted before sending with the HART command. **None**: No reformatting applied. (AA BB CC DD) **BB AA**: 16bit Byte swap **BB AA DD CC**: 32bit Byte Pair Swap **CC DD AA BB**: Word Swap **DD CC BB AA**: Word and Byte Pair Swap

Update Rate	The period (in seconds) between the specific HART message being sent.
Request Size	The number of data bytes to follow the HART command.
Static Data	If the *Dynamic Data* option has not been selected, then the user can enter fixed data to be sent with the HART command. The data will need to be entered as a space-delimited, hexadecimal string. For example: 0A 0D 12 EE
Auto Trigger	When this option has been selected, then the HART message will be sent at the update rate. If Auto Trigger has not been selected, then the specific HART message will only be sent once, when the HART device starts-up.
Dynamic Data	Data will be read from the *Data IDS Offset* to be sent with the HART command when *Request Size* is greater than 0.
Process Response	The response received from the HART device for the command sent will be processed if this option is selected. Otherwise, the response will be discarded.
Response	**Note:** This section is relevant only if *Process Response* has been selected.
Data IDS Offset	Where the response HART data will be stored.
Reformat	Used to specify how the HART response data is formatted before writing it to the Internal Data Space. **None**: No reformatting applied. (AA BB CC DD). **BB AA:** 16bit Byte swap **BB AA DD CC**: 32bit Byte Pair Swap **CC DD AA BB**: Word Swap **DD CC BB AA**: Word and Byte Pair Swap
Message Offset	Specifies the byte offset of the response, that will be copied.
Max. Copy Size	The maximum number of bytes to copy.

Table 3.4 – HART Device Advanced Message parameters

Once the configuration is done and the **OK** button is pressed, the *Advanced Messages* will appear in the list.

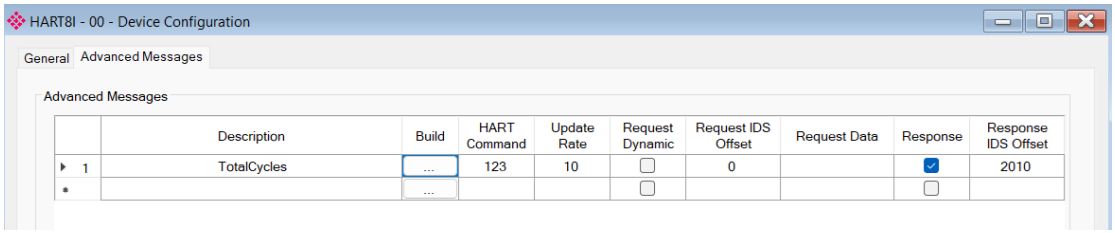


Figure 3.26 – HART Device Advanced Message List

3.5.3 HART Device Parameterization

There are certain standard HART parameters that can be updated and read from the HART device (e.g., Tag, Units, Damping, Node Address, etc.) by the PLX50CU software. Some parameters can be accessed in the *Device List* of the Channel Status and others by the *Device Configuration* tab in the *Status* window (once the HART device has been added).

3.5.3.1 Device List

It is important to note that the HART device node address can be changed from this list via the **WRITE ADDRESS** option.

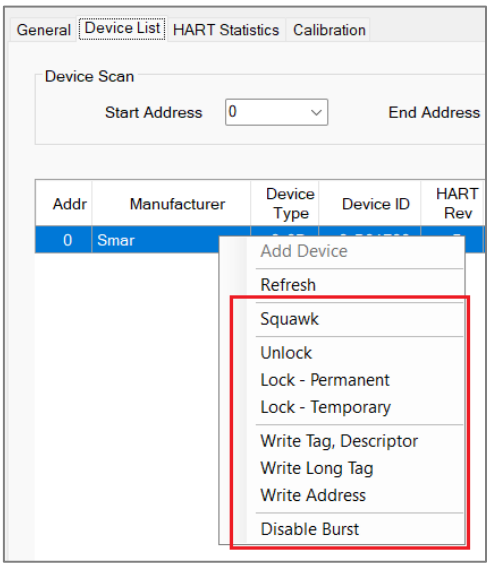


Figure 3.27 – HART Device Parameterization – Device List

Option	Command	Description
Refresh	-	Update the displayed parameters
Squawk	72	Request the HART device to visually identify itself, typically by flashing its display or LEDs. Usually used to locate the device in a field installation.
Unlock	71	Unlocks the device allowing configuration changes to be made.
Lock - Permanent	71	Locks the device's configuration, preventing any changes to its configuration. The Lock will remain in place following a device reset or power cycle.
Lock - Temporary	71	Locks the device's configuration, preventing any changes to its configuration. The Lock will be removed following a device reset or power cycle.
Write Tag, Descriptor	18	Updates (writes) the Tag and Descriptor of the device.
Write Long Tag	22	Updates (writes) the Long Tag of the device.
Write Address	6	Updates (writes) a new Polling Address (short address) of the device and specifies the Current Signaling Mode. When using multidrop, the Current Signaling Mode should be disabled.
Disable Burst	109	Used to disable Burst mode. When a device has Burst mode enabled, it will continuously and autonomously transmit data with a master requesting it. Burst mode must disabled on all devices on a multidrop channel.

Table 3.5 – HART Device Commands

3.5.3.2 Status Window

When a HART device has been added, certain device parameters can be updated from the *Status* window. It is also important to note that the HART device can be reset from this window by pressing the **MASTER RESET** button.

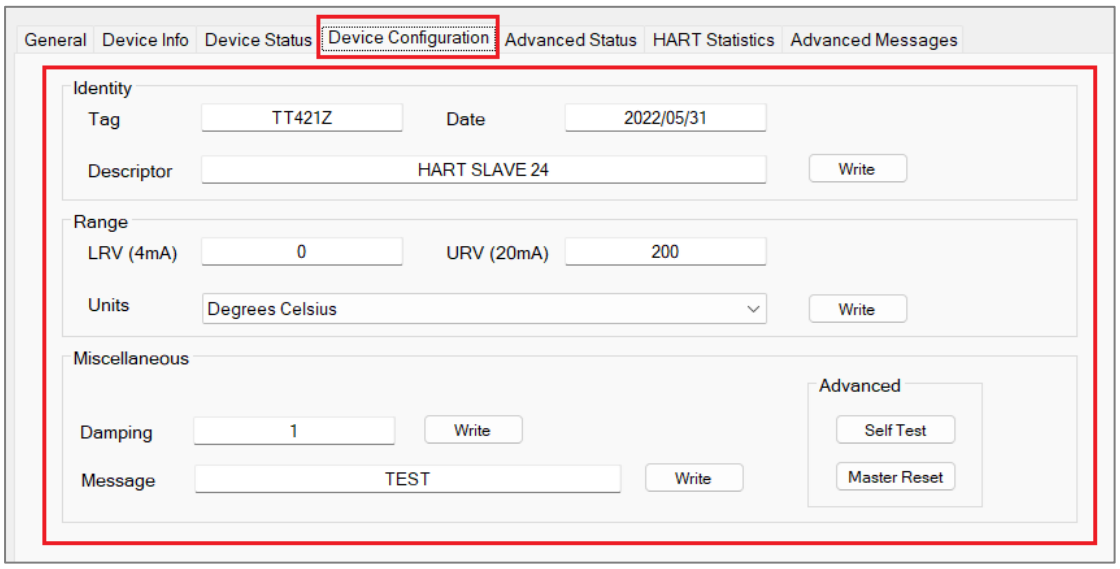


Figure 3.28 – HART Device Parameterization – Status Window - Device Configuration

The HART Device Configuration consists of the following parameters:

Parameter	Description
Identity	
Tag	The user tag name configured in the field device. (8 characters). **Note:** The Tag, Descriptor and Date are updated together.
Descriptor	The user descriptor configured in the field device. (16 characters). **Note:** The Tag, Descriptor and Date are updated together.
Date	The date when the tag and descriptor configuration was last modified. **Note:** The Tag, Descriptor and Date are updated together.
Range	
LRV	The Lower Range Value in engineering units represented by the 4-mA analog signal. **Note:** The LRV, URV and Range Units are updated together.
URV	The Upper Range Value in engineering units represented by the 20-mA analog signal. **Note:** The LRV, URV and Range Units are updated together.
Units	The engineering units in which the LRV and URV values are specified. **Note:** The LRV, URV and Range Units are updated together.
Miscellaneous	
Damping	The damping value is specified in seconds. Damping refers to the digital filtering of process variables to remove transient and potentially erroneous deviations from the actual measure variable.
Message	A user defined 32-character message stored in the field device.

Table 3.6 – HART Device Advanced Message parameters

3.6 Channel Calibration

Important: Before commencing with calibration ensure that it is safe to do so. The simulated current values could translate to extreme process variables in the connected control system which may cause unexpected results. Failure to do so could result in severe equipment damage and personal injury.

3.6.1 Current Calibration

To re-calibrate a PLX51-HART-8I module to current:

1. Using an external milliamp source, adjust the current to 4 mA, or as close as possible to 4 mA.
2. Enter the exact milliamp value, read from an external meter, into the *Low Value Actual* numeric inputs.
3. Press the **LOW VALUE** (4 mA) **CAPTURE** button, to capture the current (un-calibrated value) into the *Capture* field.
4. Using the external milliamp source, adjust the current to 20 mA, or as close as possible to 20 mA.
5. Enter the exact milliamp value, read from an external meter, into the *High Value Actual* numeric inputs.
6. Press the **HIGH VALUE** (20 mA) **CAPTURE** button, to capture the current (un-calibrated value) into the *Capture* field.
7. The new *Span* and *Offset* calibration settings will be automatically calculated. (See figure below).
8. Press **ACCEPT** to write these new calibration figures to the module.
9. The *Calibration Type* will then change to **User Calibration**, to reflect the changes.

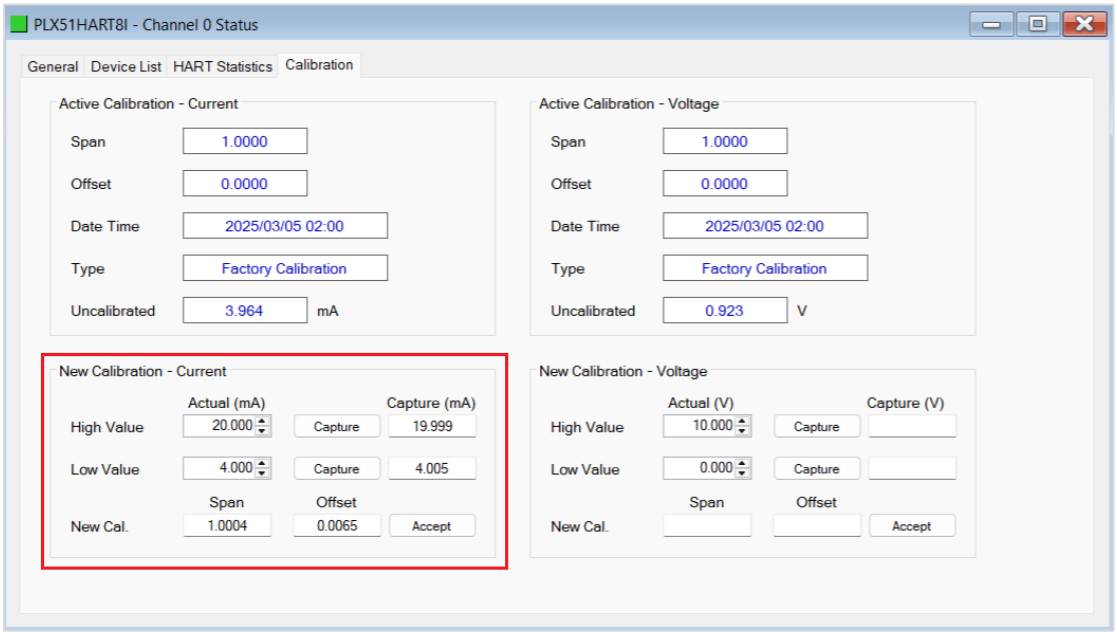


Figure 3.29 – User Calibration – Current

3.6.2 Voltage Calibration

To re-calibrate a PLX51-HART-8I module for voltage, the steps below must be followed:

1. Using an external voltage source, adjust the voltage to 0 Vdc, or as close as possible to 0 Vdc.
2. Enter the exact voltage value, read from an external meter, into the *Low Value Actual* numeric inputs.
3. Press the **LOW VALUE** (0 Vdc) **CAPTURE** button, to capture the voltage (un-calibrated value) into the *Capture* field.
4. Using the external voltage source, adjust the voltage to 10 Vdc, or as close as possible to 10 Vdc.
5. Enter the exact voltage value, read from an external meter, into the *High Value Actual* numeric inputs.
6. Press the **HIGH VALUE** (10 Vdc) **CAPTURE** button, to capture the voltage (un-calibrated value) into the *Capture* field.
7. The new *Span* and *Offset* calibration settings will be automatically calculated. (See figure below).
8. Press **ACCEPT** to write these new calibration figures to the module.
9. The *Calibration Type* will then change to **User Calibration**, to reflect the changes.

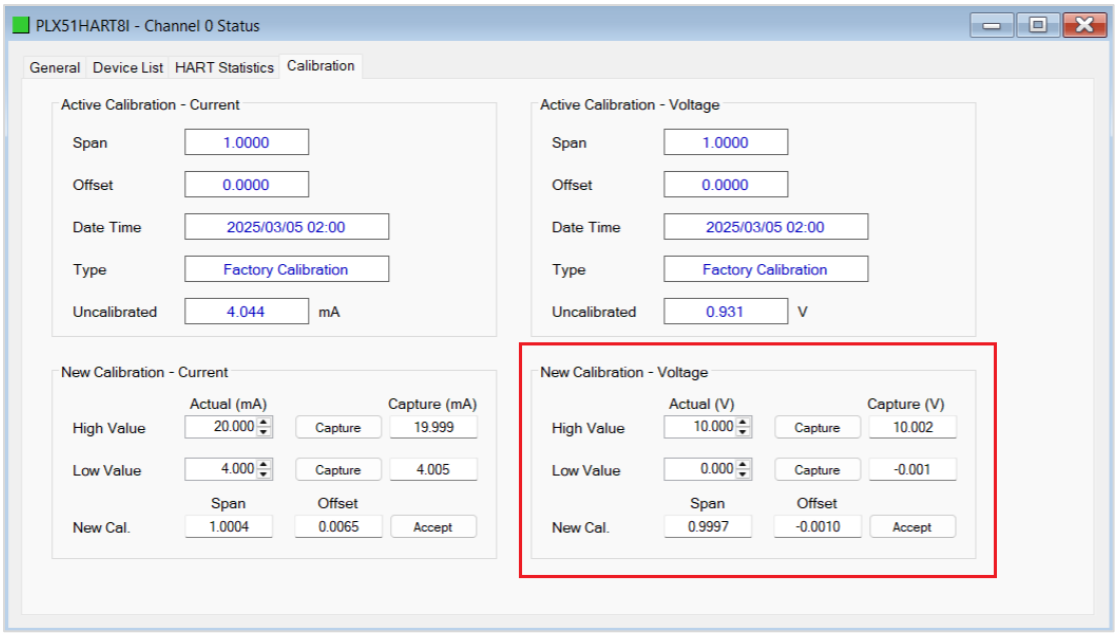


Figure 3.30 – User Calibration – Voltage

3.7 Primary Interface

The PLX51-HART-8I module supports four Primary Interface options.

3.7.1 EtherNet/IP Target

A controller (e.g. Logix controller) can own the PLX51-HART-8I over EtherNet/IP using up to 8 Class 1 EtherNet/IP connections when the Primary Interface is set to EtherNet/IP target. This will allow the PLX51-HART-8I to exchange data with the controller using the input and output assembly of the Class 1 EtherNet/IP connections. Analog Input Channel Data as well as data from HART devices can be mapped to the Logix controller over EtherNet/IP.

The user will need to add the PLX51-HART-8I to the Logix IO tree under an EtherNet/IP bridge (e.g. 1756-EN2TR) or Ethernet Logix controller (e.g. 1756-L85E).

3.7.1.1 Studio / Logix 5000 Configuration

3.7.1.1.1 Add Module to EtherNet/IP I/O Configuration

The PLX51-HART-8I can be easily integrated with Allen-Bradley Logix family of controllers. Integration with the Logix family in Studio5000 makes use of the EDS Add-On-Profile (AOP) or a Generic Module Profile.

3.7.1.1.1.1 EDS AOP (Logix V21+)

Before the module can be added to the tree, the module's EDS file must be registered.

Using RSLinx, the EDS file can be uploaded from the device after which the ***EDS Hardware Installation*** tool will be invoked to complete the registration.

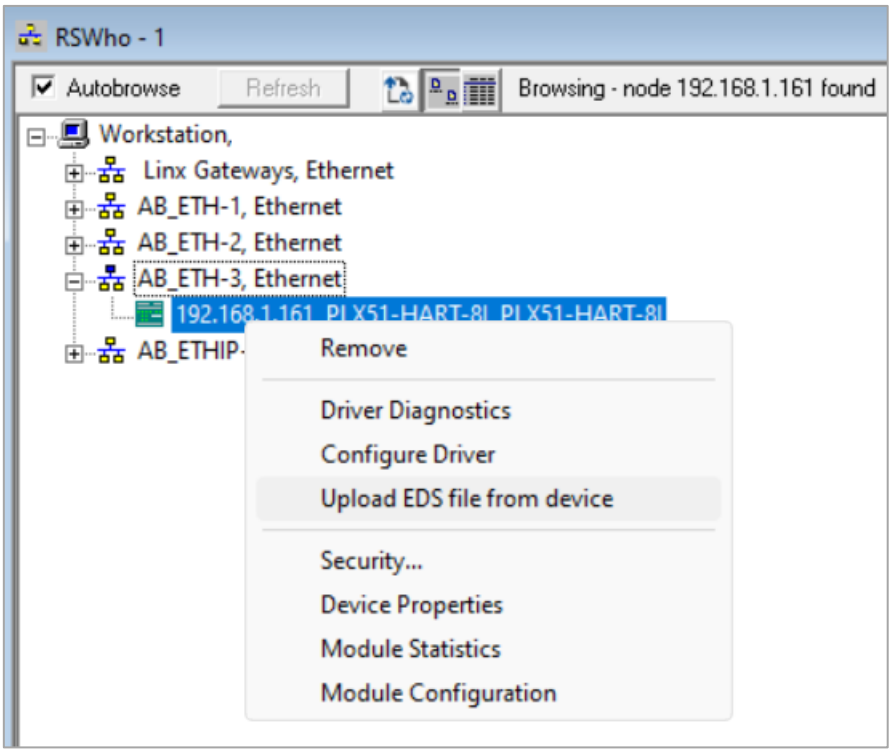


Figure 3.31 – EDS file upload from PLX51-HART-8I

Alternatively, the EDS file can be downloaded from the product webpage at www.prosoft-technology.com and registered manually using the **EDS HARDWARE INSTALLATION TOOL** shortcut under the *Tools* menu in Studio 5000.

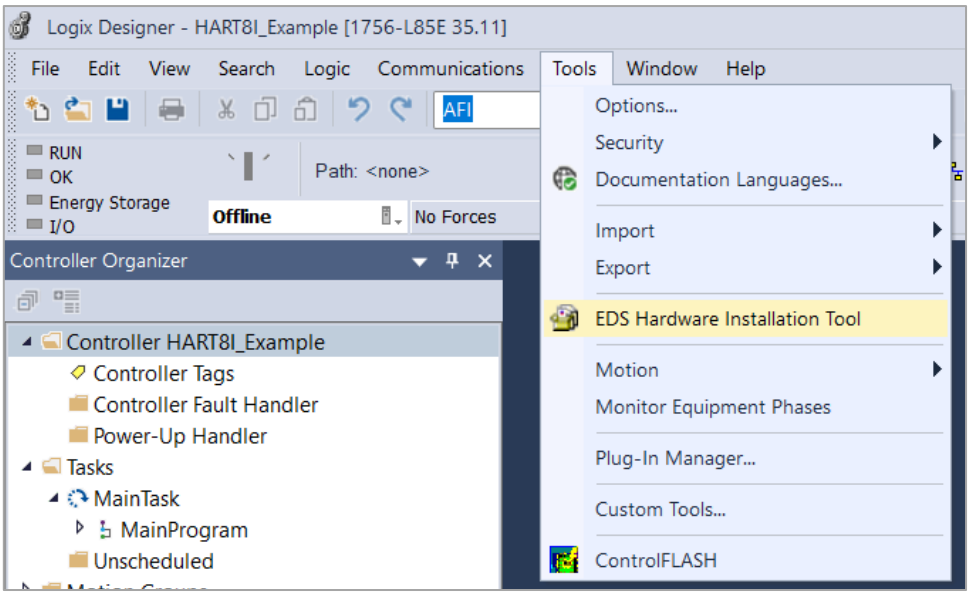


Figure 3.32 – EDS Hardware Installation Utility

After the EDS file has been registered, the module can be added to the Logix IO tree in Studio 5000. Under a suitable Ethernet bridge module in the tree, select the Ethernet network, right-click and select the **NEW MODULE** option.

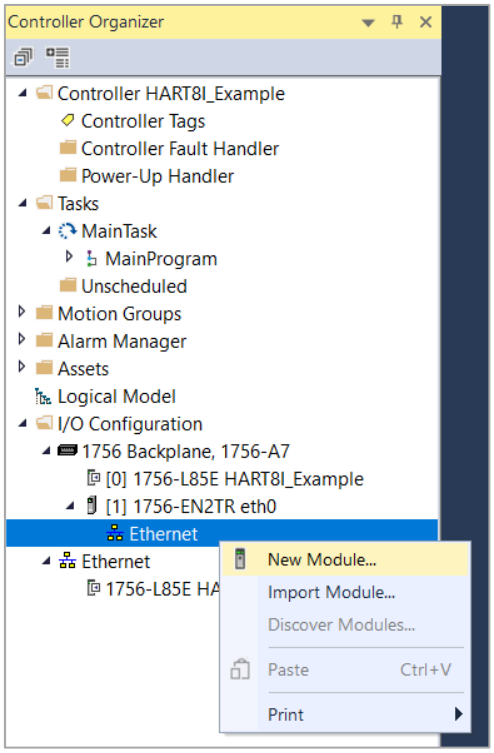


Figure 3.33 – Adding a module

The module selection dialog will open. To find the module, use the *Vendor* filter to select only the **Prosoft Technology** modules, or the search criteria “PLX51” as shown in the figure below.

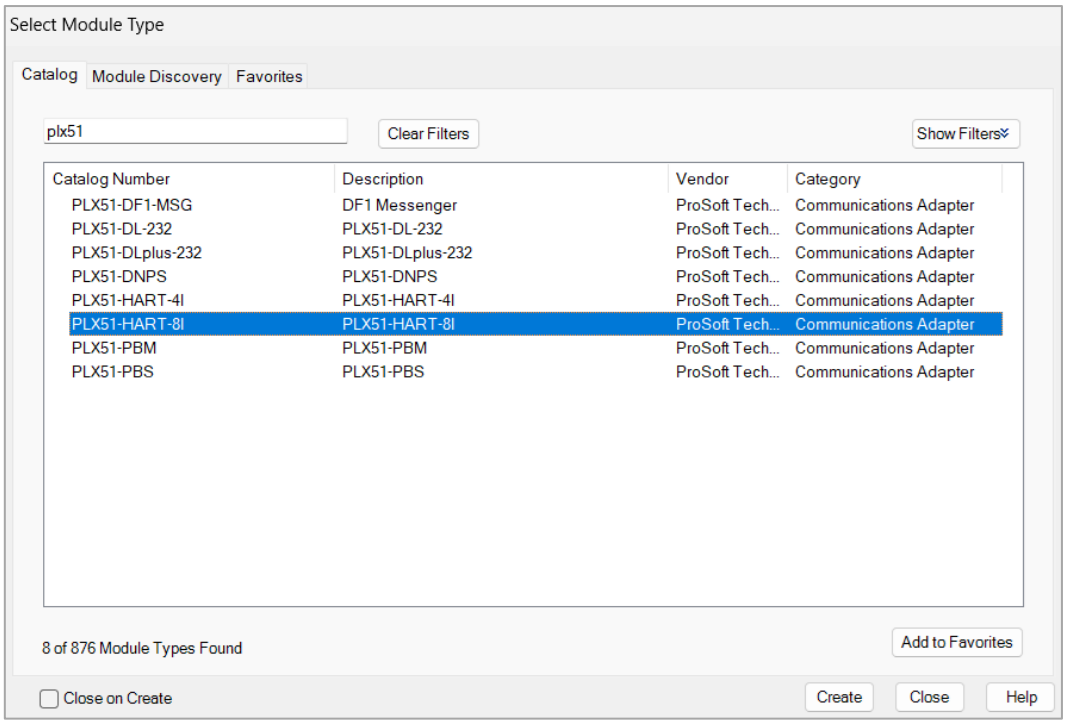


Figure 3.34 – Selecting the module

Locate and select the PLX51-HART-8I module and select the **CREATE** option. The module configuration dialog will open, where the user must specify the *Name* and *IP Address* as a minimum to complete the instantiation.

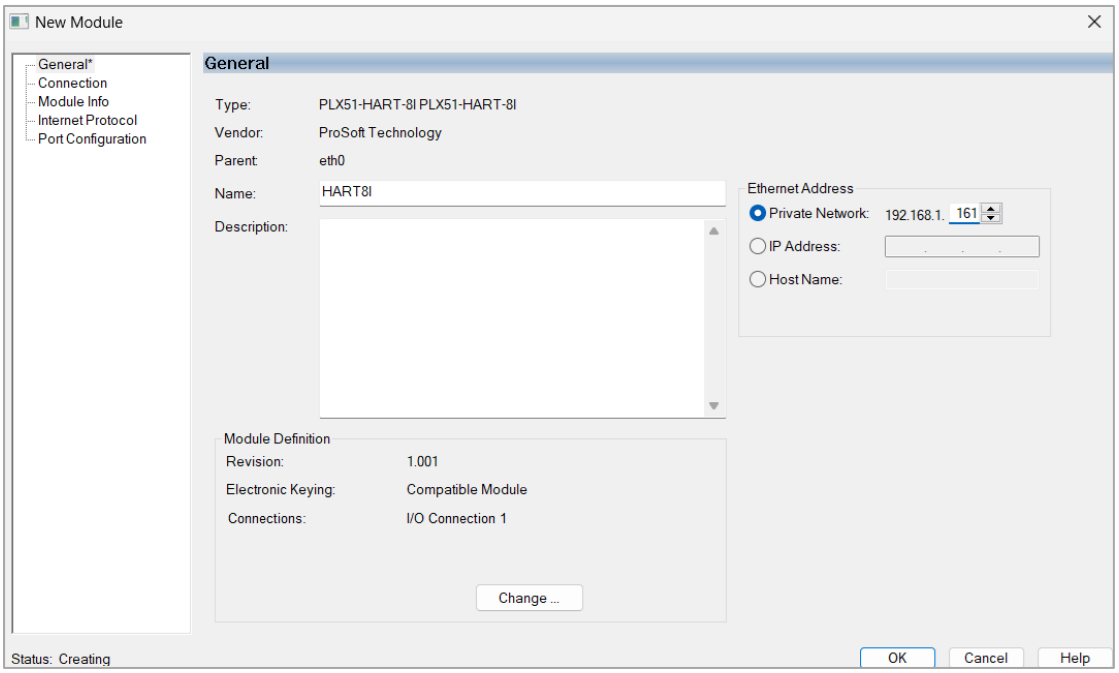


Figure 3.35 – Module instantiation

The PLX51-HART-8I supports up to 8 class 1 EtherNet/IP connections.

Important: The user will need to ensure that the number of connections configured in the *General* tab of the module configuration (PLX50 Configuration Utility) matches the selected connection count in Logix (Studio 5000).

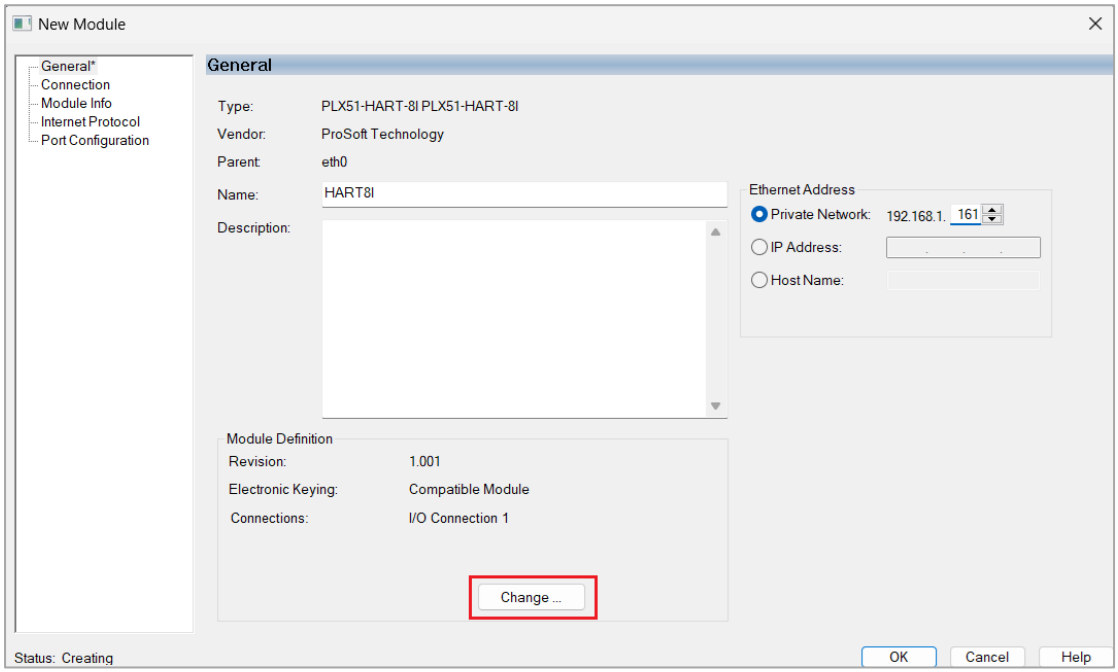


Figure 3.36 – Change number of IO Connections

Select the number of required connections.

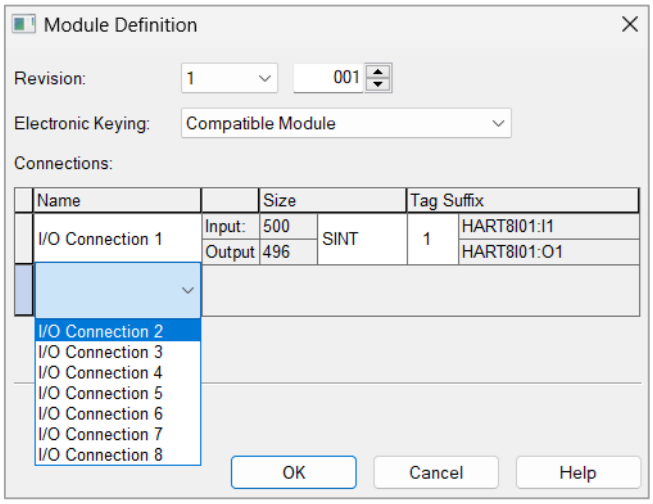


Figure 3.37 – Selection of IO Connections

The PLX51-HART-8I module will be in the Logix IO tree.

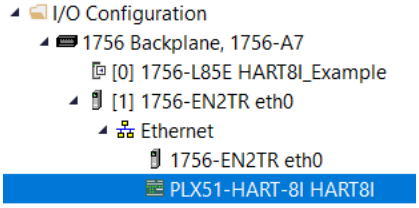


Figure 3.38 – Logix IO tree

The Module Defined Data Types will automatically be created during the instantiation process. These defined tags will need to be copied to and from meaningful structures.

3.7.1.1.1.2 Generic Module Profile (Logix Pre-V21)

Important: When using a Generic Module Profile only a **single** connection is supported limiting the total HART data that can be exchanged.

Important: When using the Generic Profile, ensure that the PLX51-HART-8I's ***Logix Profile*** has been set to the ***Generic Profile*** option, otherwise the generated L5X Logix code will import with errors.

When using Logix versions prior to version 21, then the PLX51-HART-8I module must be added to the RSLogix 5000 I/O tree as a generic Ethernet module. This is achieved by right clicking on the Ethernet Bridge in the RSLogix 5000 and selecting *New Module* after which the *ETHERNET-MODULE* is selected to be added as shown in the figure below.

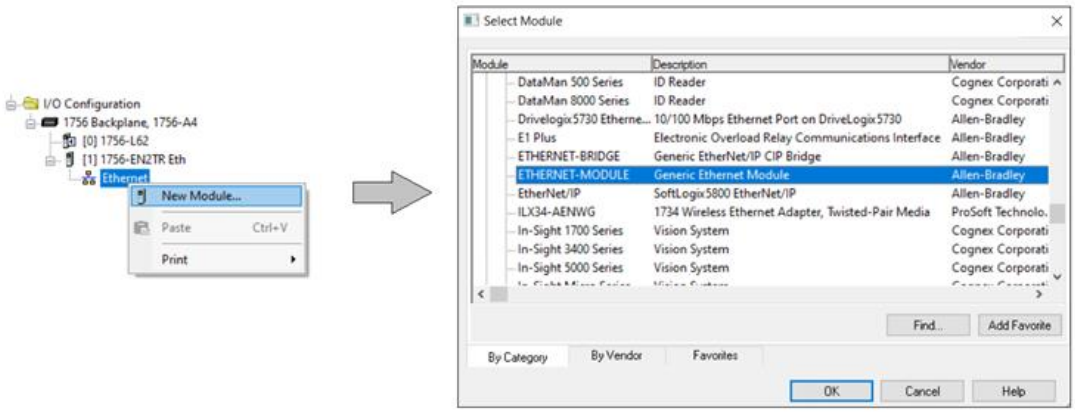


Figure 3.39 - Add a Generic Ethernet Module in RSLogix 5000

The user must enter the ***IP Address*** of the PLX51-HART-8I module that will be used. The assembly instance and size must also be added for the input, output, and configuration in the connection parameters section.

The required connection parameters for the PLX51-HART-8I module are shown below:

Connection Parameter	Assembly Instance	Size
Input	110	500 (8-bit)
Output	111	496 (8-bit)
Configuration	102	0 (8-bit)

Table 3.7 - RSLogix class 1 connection parameters for the PLX51-HART-8I module

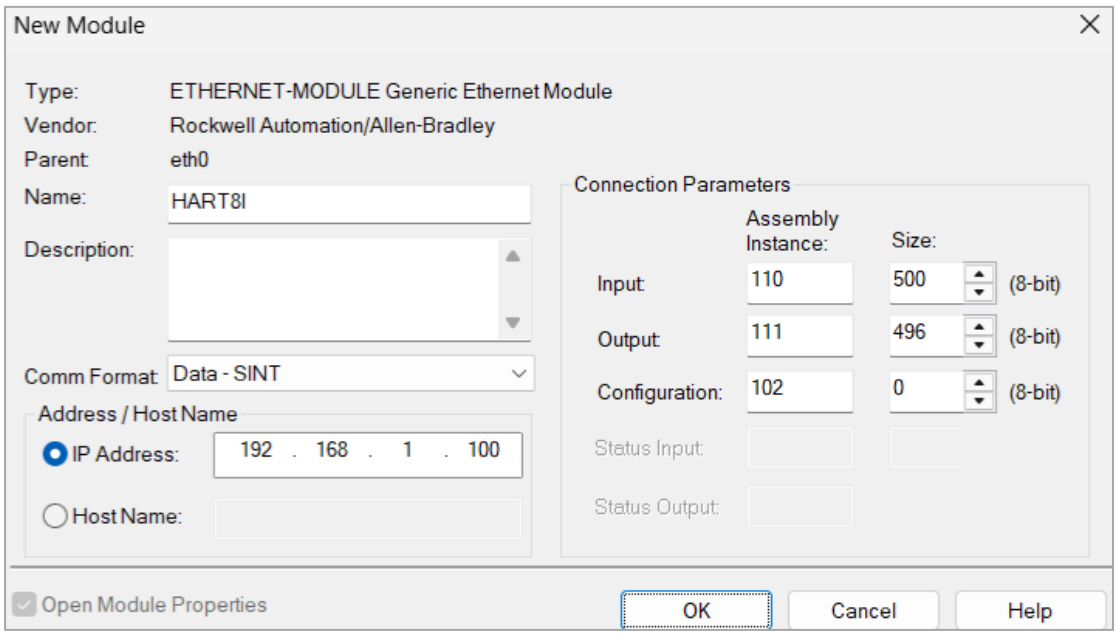


Figure 3.40 - RSLogix 5000 General module properties for PLX51-HART-8I module

Important: The user will need to enter the exact connection parameters before the module will establish a class 1 connection with the Logix controller.

Next the user needs to add the connection requested packet interval (***RPI***). This is the rate at which the input and output assemblies are exchanged. Refer to the technical specification section in this document for further details on the limits of the RPI.

3.7.1.1.2 Logix Mapping

PLX50 Configuration Utility (PLX50CU) will generate the required UDTs and Routines (based on the Internal Map) to map the required analog and HART data. The user will need to select the **RECOMMEND** button in the *Internal Map* tab to automatically populate the Internal Mapping and generate the .L5X file for Logix mapping, routines, and UDTs.

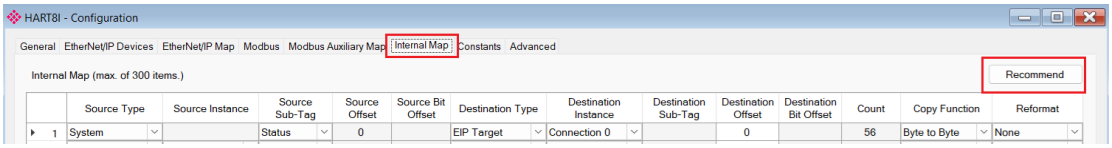


Figure 3.41 – Internal Mapping Recommend

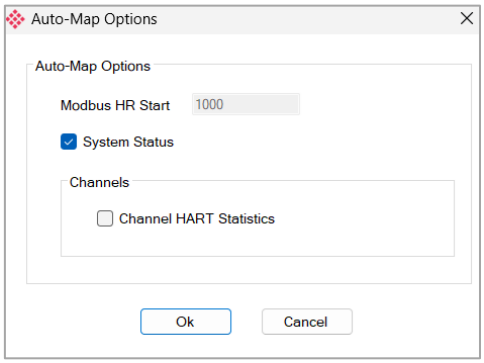


Figure 3.42 – Auto-Map Options popup

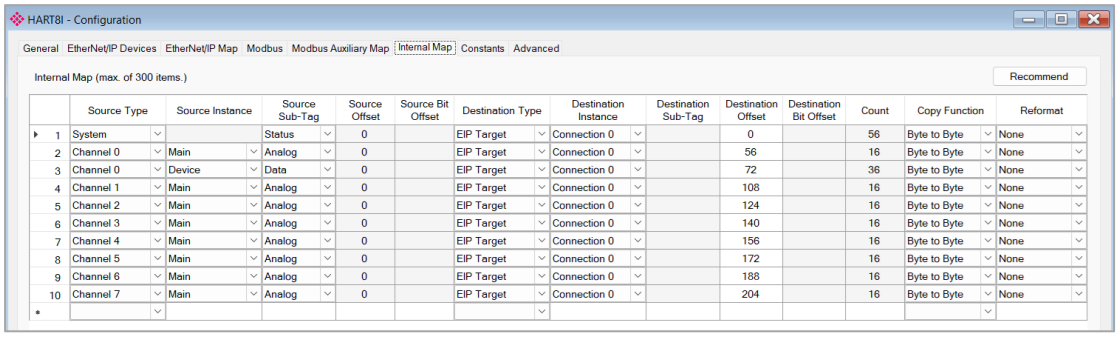


Figure 3.43 – Internal Mapping Auto Populated

Note: If the Auto Mapping for EtherNet/IP Target has been selected in the *Advanced* tab of the PLX50CU configuration, then the **RECOMMEND** button will be greyed out and the auto mapping will automatically be generated. The Auto Mapping for EtherNet/IP Target will be enabled by default.

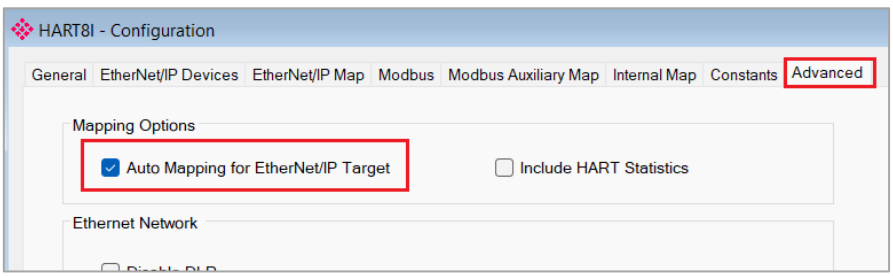


Figure 3.44 – Auto Mapping for EtherNet/IP Target

The user can then generate the required Logix and UDTs by right-clicking on the module in PLX50CU and selecting the **GENERATE LOGIX L5X** option.

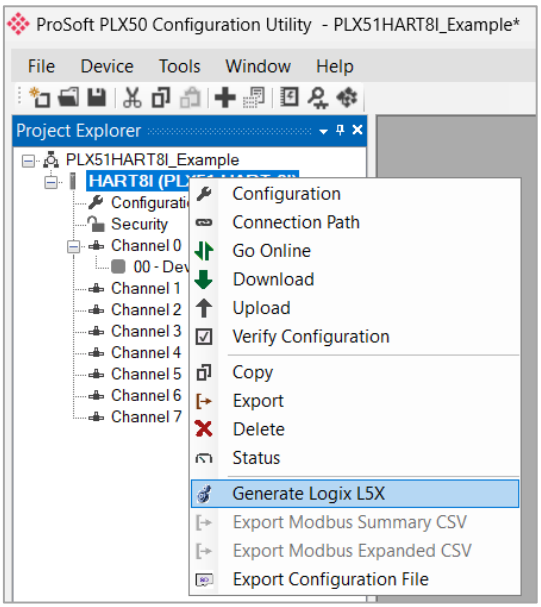


Figure 3.45 – Selecting Generate Logix L5X

The user will then be prompted to select a suitable file name and path for the .L5X file.

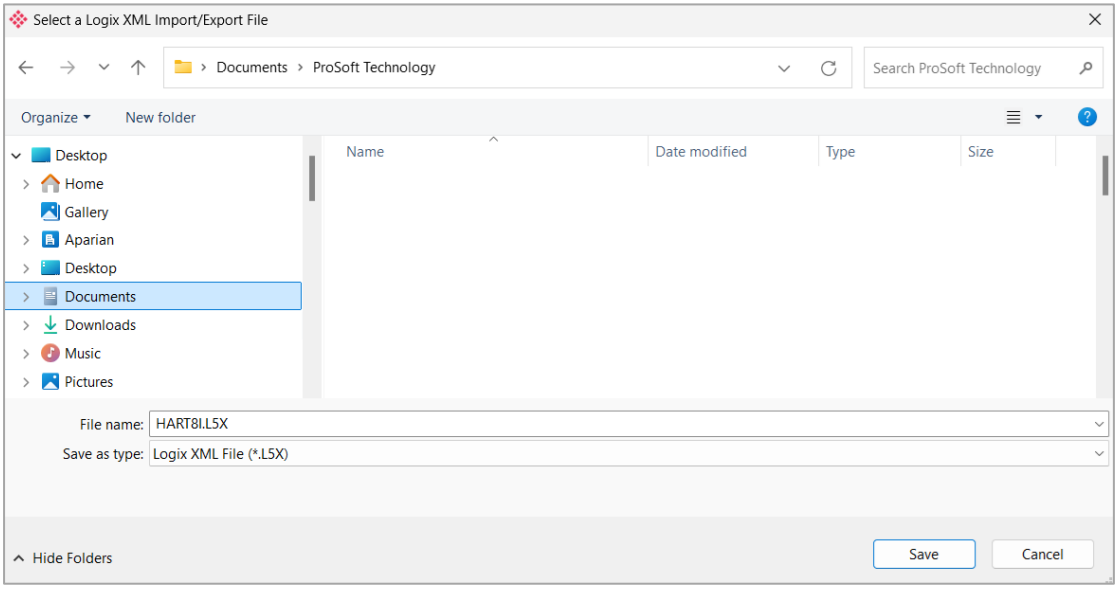


Figure 3.46 – Selecting the Logix .L5X file name

This .L5X file can now be imported into the Studio 5000 project by right-clicking on a suitable **PROGRAM** > **ADD** > **IMPORT ROUTINE**.

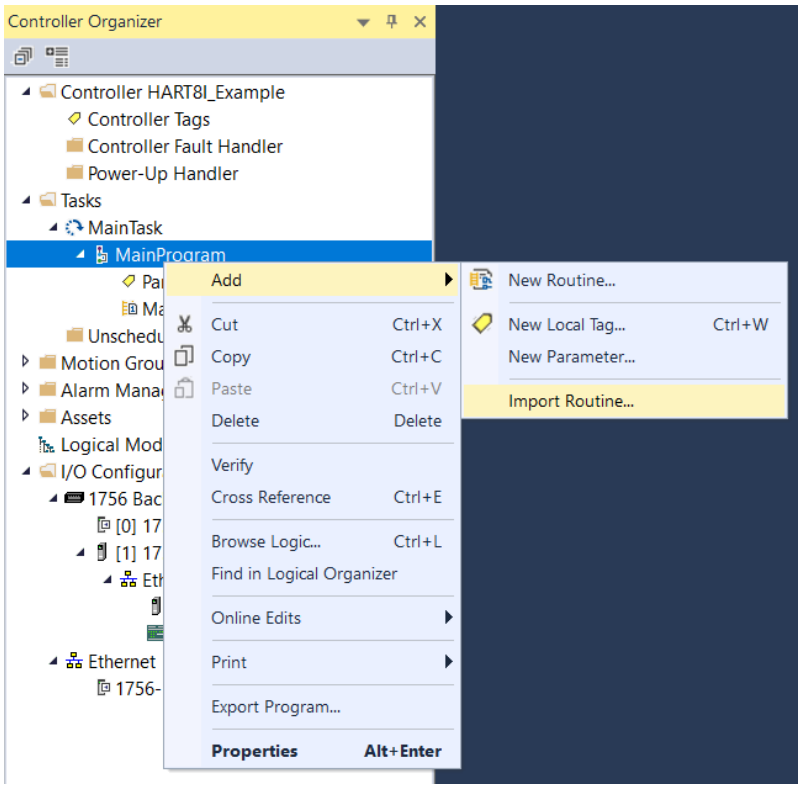


Figure 3.47 – Importing the .L5X file into Studio 5000

Select the previously created .L5X file and accept the import by pressing **OK**.

The import will create the following:

- Mapping Routine
- Multiple UDT (User-Defined Data Types)
- Multiple Controller Tags

Since the imported mapping routine is not a Main Routine, it will need to be called from the current Main Routine.

Figure 3.48 – Calling the mapping routine

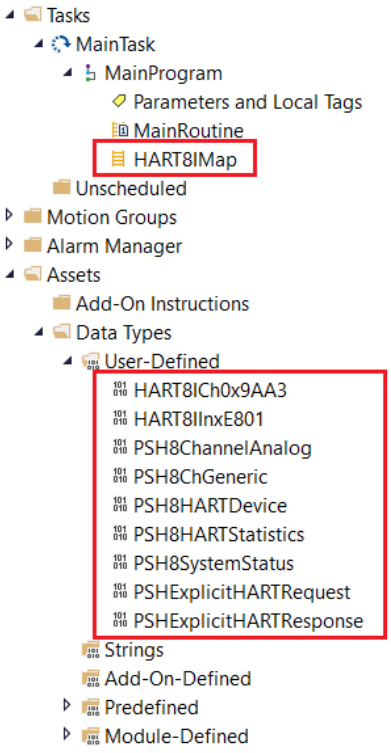


Figure 3.49 – Imported Logix Objects

Several PLX51-HART-8I specific (UDT) tags are created that reside under the main PLX51-HART-8I UDT.

Name	Value	Style	Data Type
HART8IIn	{...}		HART8IInxE801
HART8IIn.Status	{...}		PSH8SystemStatus
HART8IIn.Ch0	{...}		HART8ICh0x9AA3
HART8IIn.Ch1	{...}		PSH8ChGeneric
HART8IIn.Ch2	{...}		PSH8ChGeneric
HART8IIn.Ch3	{...}		PSH8ChGeneric
HART8IIn.Ch4	{...}		PSH8ChGeneric
HART8IIn.Ch5	{...}		PSH8ChGeneric
HART8IIn.Ch6	{...}		PSH8ChGeneric
HART8IIn.Ch7	{...}		PSH8ChGeneric

Figure 3.50 – PLX51-HART-8I tag overview

The Status tag displays the status and diagnostics information of the PLX51-HART-8I.

Name	Value	Style	Data Type	Description
HART8IIn.Status	{...}		PSH8SystemStatus	
HART8IIn.Status.ConfigValid	0	Decimal	BOOL	Configuration Valid (0=Invalid, 1=Valid)
HART8IIn.Status.EIPOriginatorCommsOk	0	Decimal	BOOL	EtherNet/IP Originator (0=Fail,1=Ok)
HART8IIn.Status.ModbusOnline	0	Decimal	BOOL	Modbus Status (0=Offline,1=Online)
HART8IIn.Status.EIPOwned	0	Decimal	BOOL	EtherNet/IP Target: (0=Not-Owned, 1=Owned)
HART8IIn.Status.Power1Ok	0	Decimal	BOOL	Power Input 1 (0=Off, 1=On)
HART8IIn.Status.Power2Ok	0	Decimal	BOOL	Power Input 2 (0=Off, 1=On)
HART8IIn.Status.ControllerRunMode	0	Decimal	BOOL	Controller Mode (0=Program, 1=Run)
HART8IIn.Status.NTPOK	0	Decimal	BOOL	NTP Status (0=Fail, 1=Ok)
HART8IIn.Status.CANBusOk	0	Decimal	BOOL	CAN Bus Status (0=Fail, 1=Ok)
HART8IIn.Status.RTCValid	0	Decimal	BOOL	Real-Time Clock Status (0=Fail, 1=Ok)
HART8IIn.Status.ConfigCRC	16#0000	Hex	INT	Configuration Checksum
HART8IIn.Status.CurrentCANBaud	0	Decimal	INT	Current CAN bus BAUD (0=10k,1=20k,2=50k,3=125...
HART8IIn.Status.Uptime	0	Decimal	DINT	Uptime
HART8IIn.Status.FreeRunCounter	0	Decimal	DINT	Free Running Counter
HART8IIn.Status.DateYear	0	Decimal	INT	Date Year
HART8IIn.Status.DateMonth	0	Decimal	INT	Date Month
HART8IIn.Status.DateDay	0	Decimal	INT	Date Day
HART8IIn.Status.TimeHour	0	Decimal	INT	Time Hour
HART8IIn.Status.TimeMinute	0	Decimal	INT	Time Minute
HART8IIn.Status.TimeSecond	0	Decimal	INT	Time Second
HART8IIn.Status.DeviceTemperature	0.0	Float	REAL	Device Temperature (Degrees Celsius)
HART8IIn.Status.DIPSwitchesAtStartup	0	Decimal	INT	DIP Switches at startup
HART8IIn.Status.DIPSwitchesCurrent	0	Decimal	INT	DIP Switches current
HART8IIn.Status.EthPort1Status	0	Decimal	INT	Ethernet Port 1 Status (Bit0: 0=LinkDown, 1=LinkUp...
HART8IIn.Status.EthPort2Status	0	Decimal	INT	Ethernet Port 2 Status (Bit0: 0=LinkDown, 1=LinkUp...
HART8IIn.Status.EthSwitchMode	0	Decimal	INT	Ethernet Switch Mode (0=Switch, 1=Split)
HART8IIn.Status.DLRStatus	0	Decimal	INT	Device Level Ring Status (Bit0: 0=Disable,1=Enabl...
HART8IIn.Status.NTPStatus	0	Decimal	INT	NTP Status (Bit0: 0=Disabled,1=Enabled; Bit1: 0=N...
HART8IIn.Status.PTPStatus	0	Decimal	INT	PTP Status (Bit0: 0=Disabled,1=Enabled; Bit1: 0=N...

Figure 3.51 – Status tag

The Channel tag will provide the analog input data as well as any HART device connected to that specific analog input channel.

Name	Value	Style	Data Type	Description
HART8IIn	{...}		HART8IInxE801	
HART8IIn.Status	{...}		PSH8SystemStatus	
HART8IIn.Ch0	{...}		HART8ICh0x9AA3	
HART8IIn.Ch0.Analog	{...}		PSH8ChannelAna...	
HART8IIn.Ch0.Analog.HARTEnabled	0	Decimal	BOOL	HART Communication (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.AnalogFilter	0	Decimal	BOOL	Analog Filter (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.EnableDUALMasters	0	Decimal	BOOL	Dual Master Support (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.UnderRange	0	Decimal	BOOL	Channel UnderRange (0=Ok, 1=UnderRange)
HART8IIn.Ch0.Analog.OverRange	0	Decimal	BOOL	Channel OverRange (0=Ok, 1=OverRange)
HART8IIn.Ch0.Analog.LoopOpen	0	Decimal	BOOL	Loop Open (0=Ok, 1=Open Circuit)
HART8IIn.Ch0.Analog.LoopShorted	0	Decimal	BOOL	Loop Shorted (0=Ok, 1=Short Circuit)
HART8IIn.Ch0.Analog.BurstModeActive	0	Decimal	BOOL	Burst Mode (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.RelayMsgPriority	0	Decimal	BOOL	Relay Message (0=Normal, 1=Priority)
HART8IIn.Ch0.Analog.CalibrationFactoryCurrentOk	0	Decimal	BOOL	Factory Current Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CalibrationFactoryVoltageOk	0	Decimal	BOOL	Factory Voltage Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CalibrationUserCurrentOk	0	Decimal	BOOL	User Current Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CalibrationUserVoltageOk	0	Decimal	BOOL	User Voltage Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CurrentValue	0.0	Float	REAL	Raw Current Value (mA)
HART8IIn.Ch0.Analog.ScaledValue	0.0	Float	REAL	Scaled Value
HART8IIn.Ch0.Analog.VoltageValue	0.0	Float	REAL	Raw Voltage Value (V)

Figure 3.52 – Analog Input Channel Specific tags

Name	Value	Style	Data Type	Description
HART8IIn	{...}		HART8IInxE801	
HART8IIn.Status	{...}		PSH8SystemStatus	
HART8IIn.Ch0	{...}		HART8ICh0x9AA3	
HART8IIn.Ch0.Analog	{...}		PSH8ChannelAna...	
HART8IIn.Ch0.Device	{...}		PSH8HARTDevice	
HART8IIn.Ch0.Device.NodeAddress	0	Decimal	INT	Node Address
HART8IIn.Ch0.Device.HARTStatus	16#0000	Hex	INT	HART Status
HART8IIn.Ch0.Device.DeviceOnline	0	Decimal	BOOL	Device Online (0=Offline, 1=Online)
HART8IIn.Ch0.Device.RelayMessageInhibited	0	Decimal	BOOL	Relay Message Control (0=Normal,1=Inhibited)
HART8IIn.Ch0.Device.PV	0.0	Float	REAL	Primary Variable
HART8IIn.Ch0.Device.SV	0.0	Float	REAL	Secondary Variable
HART8IIn.Ch0.Device.TV	0.0	Float	REAL	Tertiary Variable
HART8IIn.Ch0.Device.FV	0.0	Float	REAL	Fourth Variable
HART8IIn.Ch0.Device.PVUnitsCode	0	Decimal	INT	Primary Variable Units Code
HART8IIn.Ch0.Device.SVUnitsCode	0	Decimal	INT	Secondary Variable Units Code
HART8IIn.Ch0.Device.TVUnitsCode	0	Decimal	INT	Tertiary Variable Units Code
HART8IIn.Ch0.Device.FVUnitsCode	0	Decimal	INT	Fourth Variable Units Code
HART8IIn.Ch0.Device.AdvMsgSuccess	2#0000_0000_0000_0000	Binary	INT	Advanced Message Success (1 bit per Adv Msg Ite...
HART8IIn.Ch0.Device.AdvMsgActivity	2#0000_0000_0000_0000	Binary	INT	Advanced Message Activity (1 bit per Adv Msg Ite...

Figure 3.53 – Analog Input Channel – HART Device Specific tags

3.7.1.2 Internal Data Space Mapping

When the module is operating as an EtherNet/IP Target, the data from the originator device (e.g. Logix Controller) can be mapped to the PLX51-HART-8I using the Internal Map. The Internal Map configuration window is opened by either double-clicking on the module in the tree or right-clicking the module and selecting **CONFIGURATION** and selecting the *Internal Map* tab.

3.7.1.2.1 IDS Copy – EtherNet/IP Target Source

When copying data from a connection originator (e.g. the output assembly from the Logix Controller) to the module, the *Source Type* must be set to **EIP TARGET**.

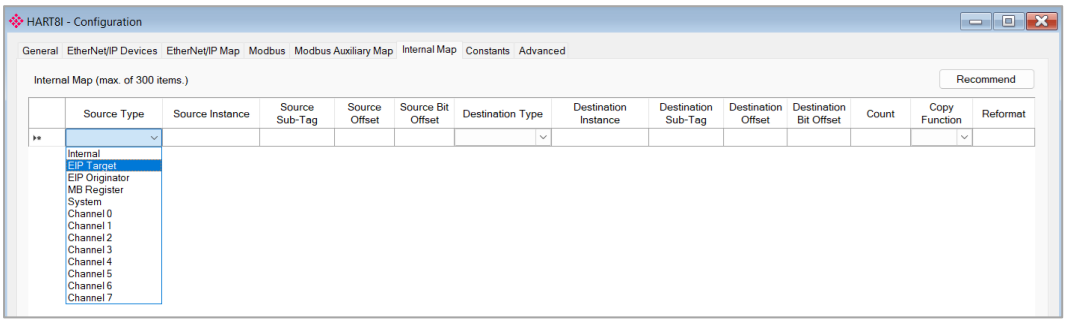


Figure 3.54 – IDS Copy – EtherNet/IP Target Source Type

The *Source Instance* will be the connection number, which can be connection 0 to 7, based on the number of connections configured.

The *Source Offset* is the offset in the EtherNet/IP output assembly from where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.7.1.2.2 IDS Copy – EtherNet/IP Target Destination

When copying data from the module to the EtherNet/IP Target input assembly, the *Destination Type* must be set to **EIP TARGET**.

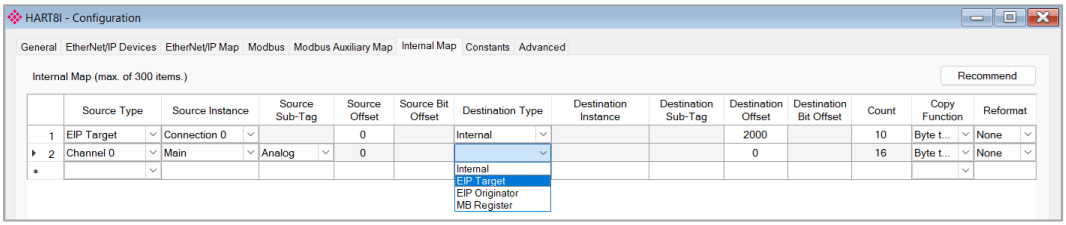


Figure 3.55 – IDS Copy – EtherNet/IP Target Destination Type

The *Destination Instance* will be the connection number, which can be connection 0 to 7, based on the number of connections configured.

The *Destination Offset* is the offset of the EtherNet/IP input assembly from where the data must be copied.

The *Count* is the number of bytes that will be copied.

Note: If the *Auto Mapping* for EtherNet/IP Target has been selected in the *Advanced* tab of the PLX50CU configuration, then the auto mapping will automatically be generated, and no mapping setup is required from the user. This is recommended.

3.7.2 Modbus Server

The PLX51-HART-8I can operate as a Modbus Server for Modbus TCP, RTU232, and RTU485. An external Modbus Client can read and write to the full Modbus Register range in the PLX51-HART-8I. The PLX51-HART-8I can operate as a Modbus Server for Modbus TCP, Modbus RTU232, and Modbus RTU485 simultaneously. The user will need to configure the relevant Modbus Parameters as shown below.

The Modbus configuration window is opened by either double-clicking on the module in the tree or right-clicking the module and selecting **CONFIGURATION** and selecting the *Modbus* tab.

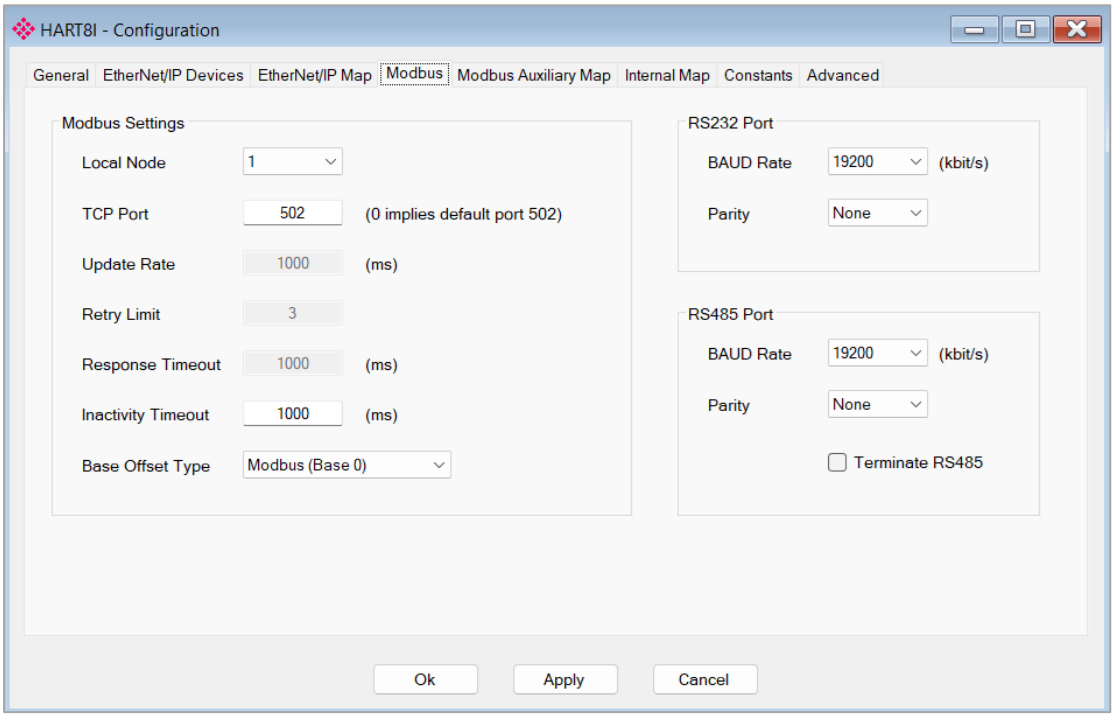


Figure 3.56 – Modbus Configuration

The Modbus Communication configuration consists of the following parameters:

Parameter	Description
Local Node	The Modbus Node address assigned to the module.
TCP Port	The TCP port to be used for the Modbus TCP communication. By default, the module will use the standard TCP port 502.
Update Rate	The period (in milliseconds) between Client requests to the target Modbus device. (Modbus Client mode only)
Retry Limit	The number of successive Modbus request retries before the request is set to have failed. (Modbus Client mode only)
Response Timeout	The time (in milliseconds) the module will wait for a valid Modbus response. (Modbus Client mode only)
Inactivity Timeout	The amount of time during which no Modbus requests have been received before the module indicates that the connection to the Modbus Client is no longer active. (Modbus Server mode only)
Base Offset Type	Modbus (Base 0) Conventional Modbus addressing where the first address is 0.

	PLC (Base 1) PLC addressing, where the first address is 1.
RS232 Port	
BAUD Rate	The RS232 serial port's BAUD rate. (Modbus RTU232)
Parity	The RS232 serial port's Parity configuration. (Modbus RTU232)
RS485 Port	
BAUD Rate	The RS485 serial port's BAUD rate. (Modbus RTU485)
Parity	The RS485 serial port's Parity configuration. (Modbus RTU485)
Terminate RS485	Enables the on-board 125Ω RS485 terminating resistor.

Table 3.8 – Modbus parameters

The *Modbus Node Number* will need to be configured in the parameters above to allow a Modbus Client to access the module as a Modbus Server device.

3.7.2.1 Internal Data Space Mapping

When the module is operating as a Modbus Server, the data from the Modbus Registers (used to exchange data with the Modbus Client) can be mapped to the module using the Internal Map. The Internal Map configuration window is opened by either double-clicking on the module in the tree or right-clicking the module and selecting **CONFIGURATION** and selecting the *Internal Map* tab.

Note: The user can select the **RECOMMEND** button in the Internal Map to auto map the module status and analog input channel data as well as each HART device that is connected to the channel to the recommended Modbus Registers.

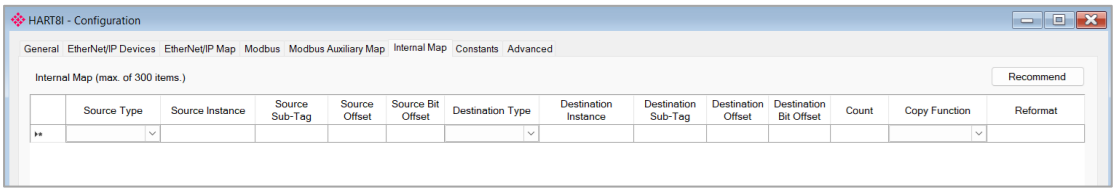


Figure 3.57 – Modbus Server – Internal Mapping Recommend

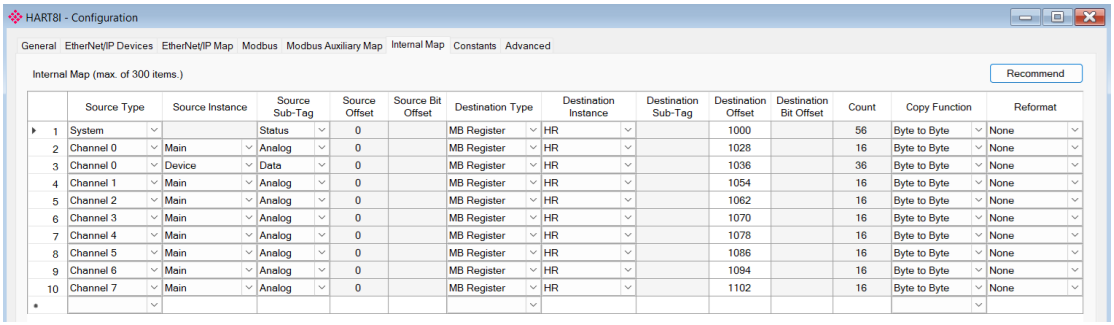


Figure 3.58 – Modbus Server – Internal Mapping Updated

3.7.2.1.1 IDS Copy – Modbus Source

When copying Modbus data to the module, the *Source Type* must be set to **MB REGISTER**.

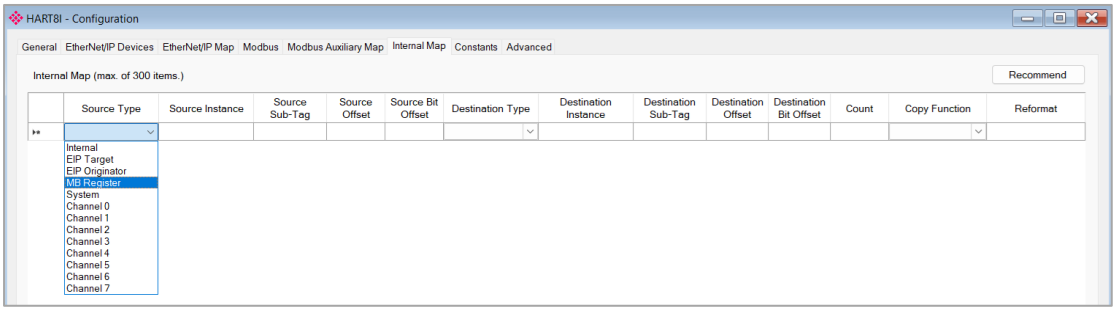


Figure 3.59 – IDS Copy - Modbus Source Type

The *Source Instance* will be the Modbus register type required.

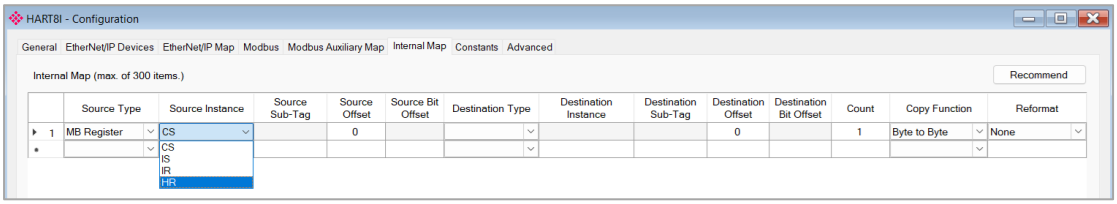


Figure 3.60 – IDS Copy - Modbus Source Instance

The *Source Offset* is the Modbus Register offset from where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.7.2.1.2 IDS Copy – Modbus Destination

When copying data from the module to a Modbus Register, the *Destination Type* must be set to **MB REGISTER**.

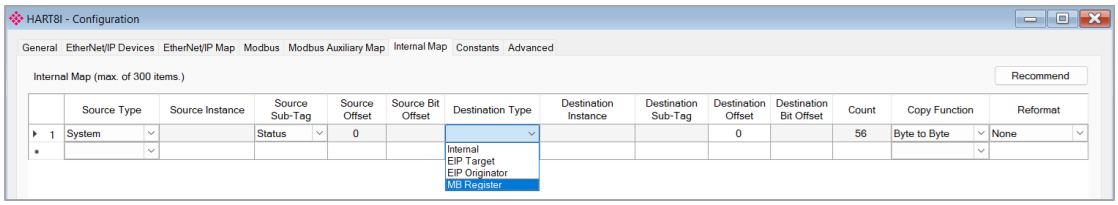


Figure 3.61 – IDS Copy - Modbus Destination Type

The *Destination Instance* will be the Modbus register type required.

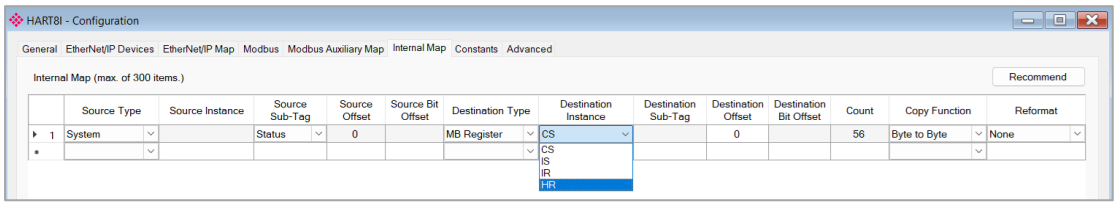


Figure 3.62 – IDS Copy - Modbus Destination Instance

The *Destination Offset* is the Modbus Register offset to where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.7.3 Modbus Client

The PLX51-HART-8I can operate as a Modbus Client for Modbus TCP, RTU232, and RTU485. The user will need to configure the relevant Modbus Parameters as shown below followed by the configuration of the Modbus Auxiliary Map. This map will allow the user to configure various read and write functions to external Modbus Registers, to and from the internal Modbus registers.

The Modbus configuration window is opened by either double-clicking on the module in the tree or right-clicking the module and selecting **CONFIGURATION** and selecting the *Modbus* tab.

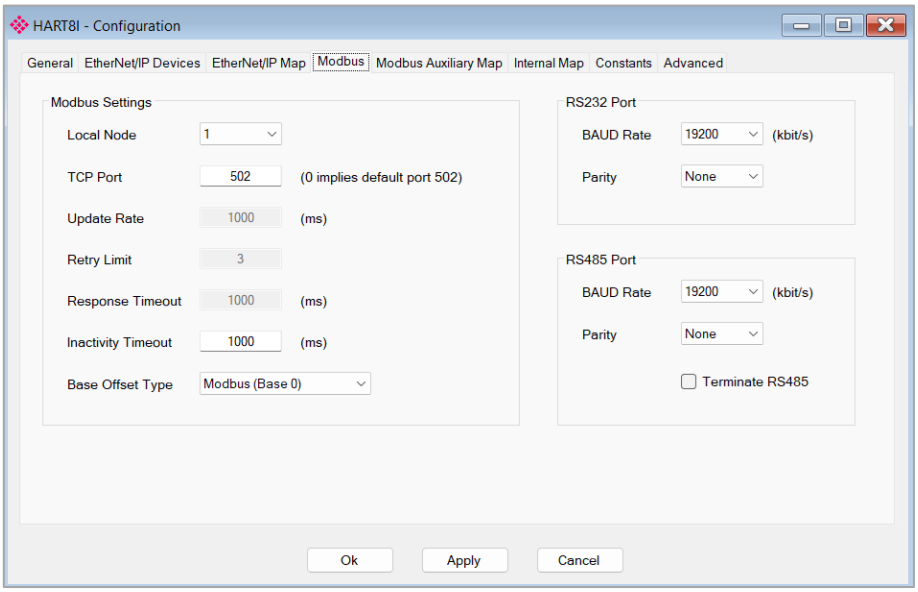


Figure 3.63 – Modbus Configuration

The Modbus Communication configuration consists of the following parameters:

Parameter	Description
Local Node	The Modbus Node address assigned to the module.
TCP Port	The TCP port to be used for the Modbus TCP communication. By default, the module will use the standard TCP port 502.
Update Rate	The period (in milliseconds) between Client requests to the target Modbus device. (Modbus Client mode only)
Retry Limit	The number of successive Modbus request retries before the request is set to have failed. (Modbus Client mode only)
Response Timeout	The time (in milliseconds) the module will wait for a valid Modbus response. (Modbus Client mode only)
Inactivity Timeout	The amount of time during which no Modbus requests have been received before the PLX51-HART-8I indicates that the connection to the Modbus Client is no longer active. (Modbus Server mode only)
Base Offset Type	Modbus (Base 0) Conventional Modbus addressing where the first address is 0. PLC (Base 1) PLC addressing, where the first address is 1.
RS232 Port	
BAUD Rate	The RS232 serial port's BAUD rate. (Modbus RTU232)
Parity	The RS232 serial port's Parity configuration. (Modbus RTU232)
RS485 Port	
BAUD Rate	The RS485 serial port's BAUD rate. (Modbus RTU485)
Parity	The RS485 serial port's Parity configuration. (Modbus RTU485)
Terminate RS485	Enables the on-board 125Ω RS485 terminating resistor.

Table 3.9 – Modbus parameters

3.7.3.1 Modbus Auxiliary Map

The Modbus Auxiliary Map configuration is shown in the figure below. The Modbus configuration is only applicable when the module has a Modbus Client operating interface. Up to 100 mapping items can be configured. Within the 100 mapping items, a maximum of 20 Modbus TCP Server devices can be configured.

The Modbus Aux Map will be executed in a sequential manner, and a mapped item will be executed at the *Update Rate* in the Modbus parameters. That is, the *Update Rate* is the time between two successive mapped item executions.

The *Modbus Auxiliary Map* configuration window is opened by either double-clicking on the module in the tree or by right-clicking the module and selecting **CONFIGURATION**.

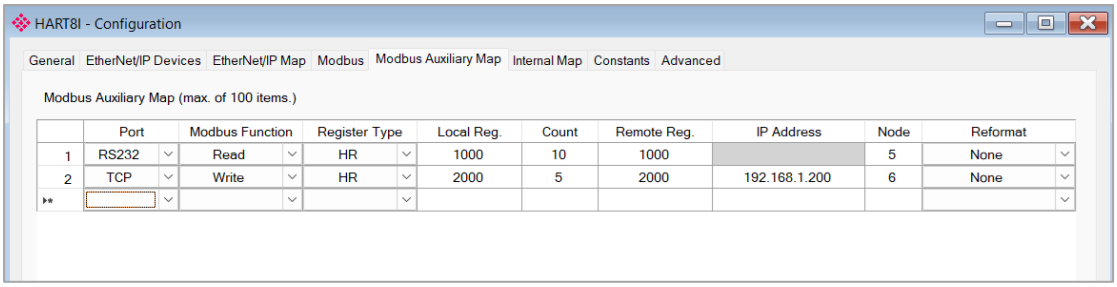


Figure 3.64 – Modbus Auxiliary Map Configuration

The Modbus Auxiliary Map configuration consists of the following parameters:

Parameter	Description
Port	The external port to be used: **TCP**: Modbus TCP (Ethernet) **RS232**: Modbus RTU232 **RS485**: Modbus RTU485
Modbus Function	This is the Modbus function that is sent to the Modbus Server. **Read**: Read a Modbus Register (e.g. HR, IR, CS, or IS) from a Modbus Server. **Write**: Write a Modbus Register (e.g. HR or CS) to a Modbus Server.
Register Type	Modbus Register Type: **CS**: Coil Status **IS**: Input Status **IR**: Input Register **HR**: Holding Register
Local Reg.	The local (internal) module Modbus register address.
Count	The number of Modbus elements to read or write.
Remote Reg.	The remote Server Modbus address register.
IP Address	The IP address of the remote Modbus Server.
Node	The Modbus Node address of the remote Modbus Server.
Reformat	Used to specify how the data is formatted before writing to, or after reading from, the Modbus Server. **None**: No reformatting applied. (AA BB CC DD). **BB AA**: 16bit Byte swap **BB AA DD CC**: 32bit Byte Pair Swap **CC DD AA BB**: Word Swap **DD CC BB AA**: Word and Byte Pair Swap

Table 3.10 – Modbus Auxiliary Map parameters

3.7.3.2 Internal Data Space Mapping

When the module is operating as a Modbus Client, the data from the Modbus Registers (used to exchange data with the Modbus Servers) can be mapped to the module using the Internal Map. The Internal Map configuration window is opened by either double-clicking on the module in the tree or right-clicking the module and selecting **CONFIGURATION** and selecting the *Internal Map* tab.

Note: The user can select the **RECOMMEND** button in the Internal Map to auto map the module status and analog input channel data as well as each HART device that is connected to the channel to the recommended Modbus Registers.

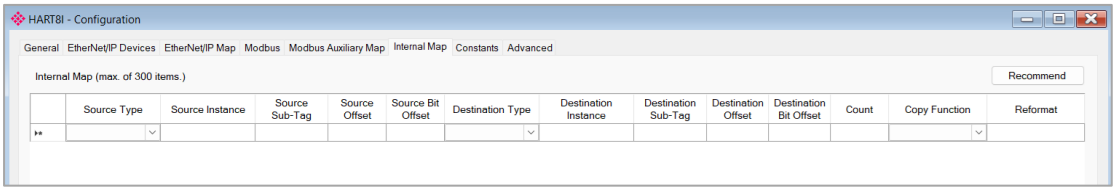


Figure 3.65 – Modbus Client – Internal Mapping Recommend

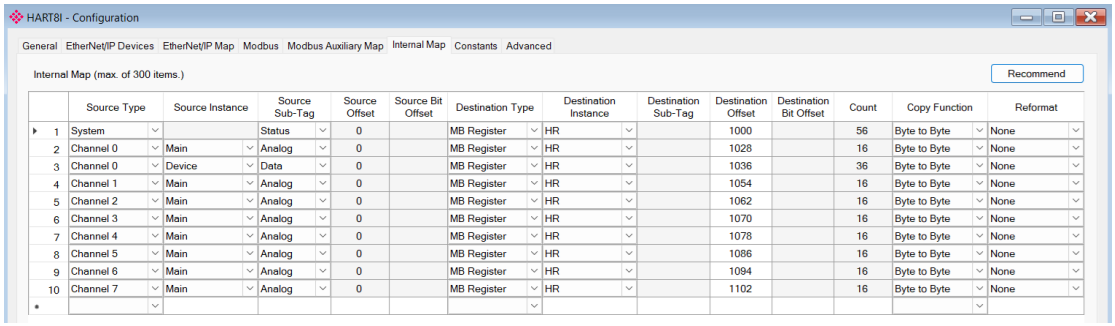


Figure 3.66 – Modbus Client – Internal Mapping Updated

3.7.3.2.1 IDS Copy – Modbus Source

When copying Modbus data to the PLX51-HART-8I, the *Source Type* must be set to **MB REGISTER**.

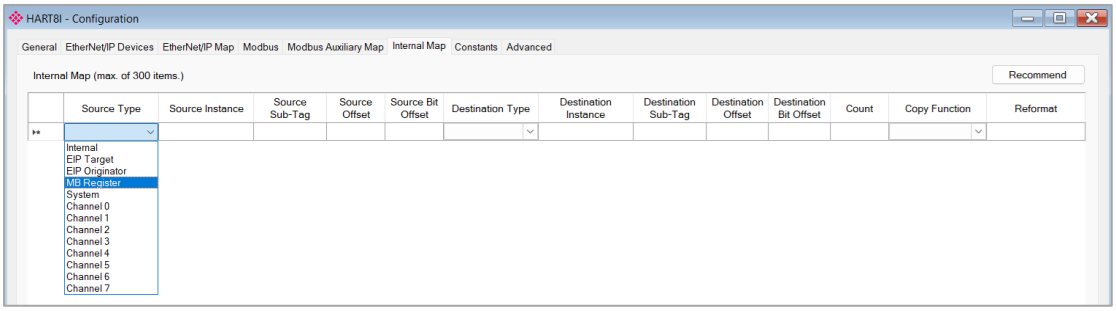


Figure 3.67 – IDS Copy - Modbus Source Type

The *Source Instance* will be the Modbus register type required.

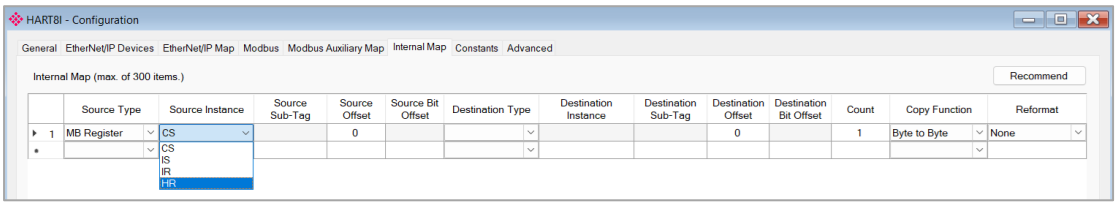


Figure 3.68 – IDS Copy - Modbus Source Instance

The *Source Offset* is the Modbus Register offset from where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.7.3.2.2 IDS Copy – Modbus Destination

When copying data from the module to a Modbus Register, the *Destination Type* must be set to **MB REGISTER**.

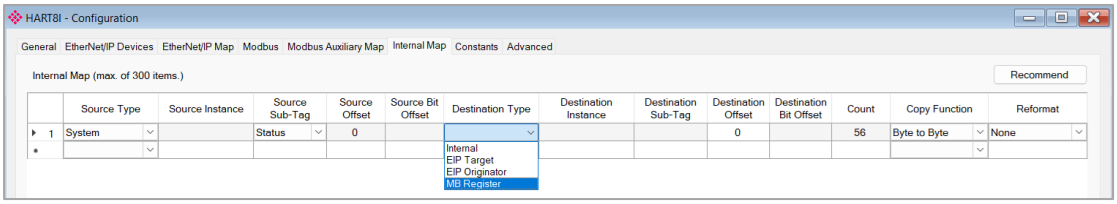


Figure 3.69 – IDS Copy - Modbus Destination Type

The *Destination Instance* will be the Modbus register type required.

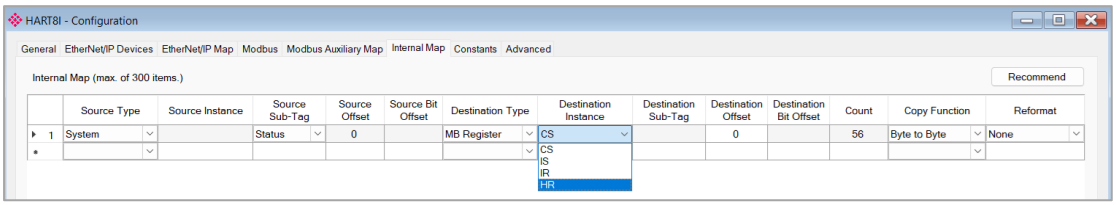


Figure 3.70 – IDS Copy - Modbus Destination Instance

The *Destination Offset* is the Modbus Register offset to where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.7.4 EtherNet/IP Originator

The PLX51-HART-8I can operate as an EtherNet/IP connection originator for cyclic (Class 1) or explicit (Class 3 or UCMM) data exchange. The explicit messaging can be configured in the *EtherNet/IP Devices* and *EtherNet/IP Map* in the Master configuration while the cyclic class 1 connections are added to the *EtherNet/IP Connections* node under the module in the PLX50CU project tree.

Note: The module supports only 32-bit header real time format as the EtherNet/IP originator, which is compatible with specific Rockwell Automation devices such as: 1794 FLEX IO, 1756 ControlLogix IO, 1734 Point IO.

3.7.4.1 EtherNet/IP Class 1 Device Connections

The module can establish up to 10 cyclic Class 1 EtherNet/IP connections to EtherNet/IP devices. This can be done by either manually entering the connection data into the *Connection Parameter* window, or by importing the configuration from one or more of the following sources:

- Online Logix Controller
- Logix Controller L5X
- EDS File
- Connection Library

3.7.4.1.1 Manual Configuration

A class 1 connection can be added to the *EtherNet/IP Connections* tree by right-clicking on the tree in PLX50CU and selecting **ADD ETHERNET/IP CONNECTION**.

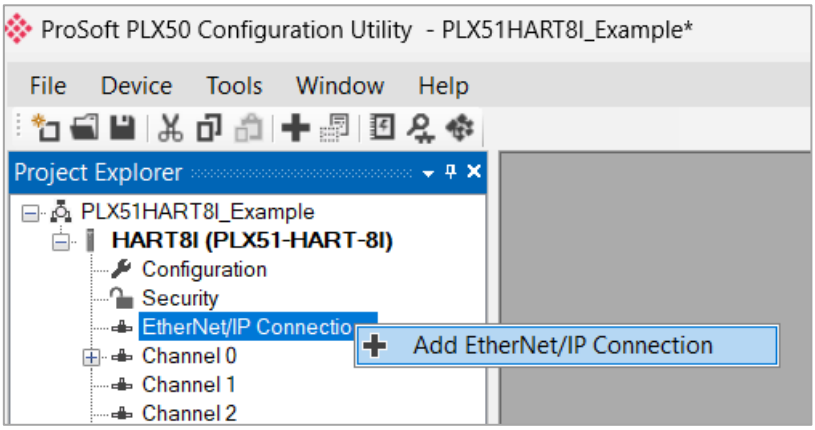


Figure 3.71 – Adding EtherNet/IP Class 1 Connection

Next the user will need to enter the connection parameters for the Class 1 connection.

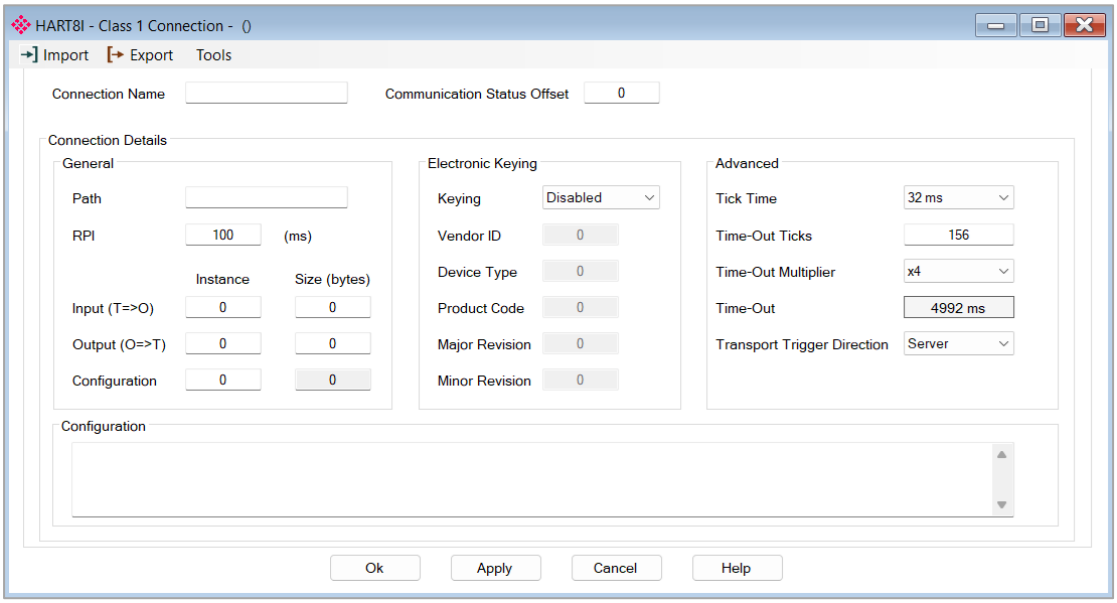


Figure 3.72 – EtherNet/IP Class 1 Connection Parameters

Important: It is recommended that the user not change the values in the *Advanced* frame of the connection parameters.

Parameter	Description
Connection Name	The instance name given to the Class 1 Connection.
Interface Fail Action	When communications to any of the HART devices have failed, the EtherNet/IP IO can be configured to either keep the connection running as is, change the connection status to program mode, or force the connection offline. This will allow the EtherNet/IP device to go into a pre-determined state when the HART device communication fails.
General	
Path	The path to the target device. If the device is an Ethernet device, then this will be the IP address of the module. If the device is a module on a backplane or via an adapter, enter the IP address of the bridge or adapter followed by the backplane port (for example '1') and the slot number of the device. Each item is separated by a comma. As an example, to connect to an Allen-Bradley Flex module (via the Flex Adapter at IP address 192.168.1.100) that is in slot 2 of the Flex backplane, the user will need to enter the following path: **192.168.1.100**,**1**,**2** (IP address, port (backplane), slot).
RPI	The requested packet interval (RPI) is the rate in milliseconds at which the data will be sent from the originator to the target and vice versa.
Input (T=>O) – Instance	The instance of the input assembly.
Input (T=>O) – Size (bytes)	The size in bytes of the input assembly.
Output (O=>T) – Instance	The instance of the output assembly.
Output (O=>T) – Size (bytes)	The size in bytes of the output assembly.
Configuration – Instance	The instance of the configuration assembly.
Configuration – Size (bytes)	The size in bytes of the configuration assembly. **Note:** This is a read-only value and will be equal to the number of bytes entered into the configuration window below.

Electronic Keying	
Keying	Electronic Keying can be used to ensure that the target device is the correct device type. **Disabled**: Keying is not enabled, and no key information will be sent in the connection establishment. **Compatible**: Keying has been enabled with compatibility enabled. This will allow devices with older firmware to also establish a connection. **Exact**: Keying has been enabled and the exact device with specific firmware revision will allow the establishment of the connection.
Vendor ID	The Vendor ID of the target device.
Device Type	The Device Type of the target device.
Product Code	The Product Code of the target device.
Major Revision	The Major Revision of the target device.
Minor Revision	The Minor Revision of the target device.
Advanced (Note: Changing these values is not recommended)	
Tick Time	For unconnected messages, this is the time for each tick to calculate the unconnected Time-Out time.
Time-Out Ticks	The number of ticks before the unconnected message is set for timeout.
Time-Out Multiplier	This is the multiplier of the RPI to define the connection timeout time.
Time-Out	The unconnected message timeout time (read-only)
Transport Trigger Direction	The Transport Trigger direction: Server or Client.
Configuration	
Data	The configuration data that is sent with the forward open connection establishment. The data will need to be entered as a space-delimited, hexadecimal string. For example: **0A 0D 12 EE** The configuration size will increase by one each time a byte is added to the configuration.

Table 3.11 – EtherNet/IP Class 1 Connection Parameters

3.7.4.1.2 Import From Online Controller

The EtherNet/IP connection parameters are imported directly from an online Logix controller.

3.7.4.1.2.1 Preparation

Before the connection information can be imported, some preparation is required using Studio5000 and a Logix controller:

1. In Studio5000 create a new project and add the required EtherNet/IP device in the IO tree. If the device's profile supports configuration, then configure the device as required.
2. Download the project to a Logix controller.

Important: When instantiating modules in Studio5000 do not make use of the "Rack Optimization" communication format.

Important: Some versions Logix (V32+) do not support the reading of the module's configuration. Where possible use an earlier version (e.g. V24).

Important: It is possible that not all the connection information will be imported as it may not be available due to the type of device and Logix version.

3.7.4.1.2.2 Import Connection Parameters

The connection parameters can be imported from the Logix controller by selecting the **IMPORT FROM ONLINE CONTROLLER** option located under the *Import* menu of the Class 1 Connection form.

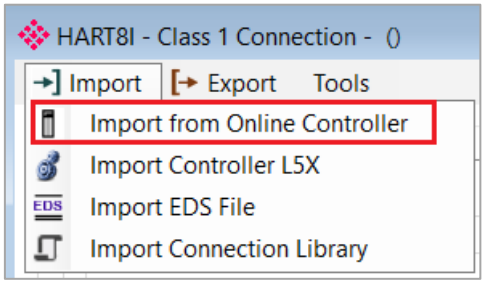


Figure 3.73 – Import from Online Controller

The *Import Connection Parameters* dialog will open.

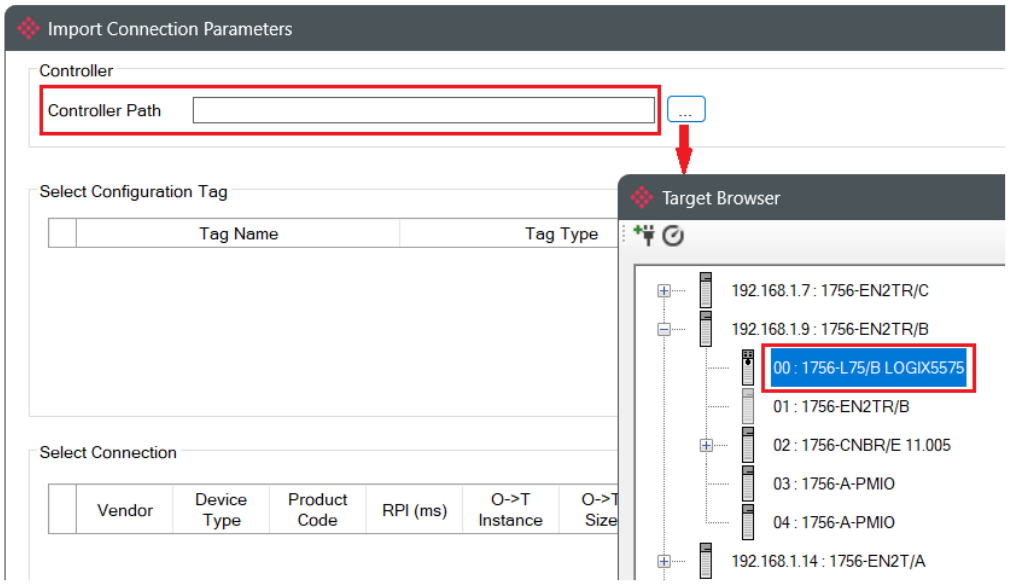


Figure 3.74 – Import Connection Parameters – Controller Path

Enter the path to the Logix controller. This can be either entered manually, or the **BROWSE** button "**…**", can be selected to launch the *Target Browser*, where the Logix controller can be selected.

Once the Logix controller path has been selected, all the device configuration tags and device connections will be read from the controller and displayed in the *Configuration Tag* grid and *Connection* grid respectively.

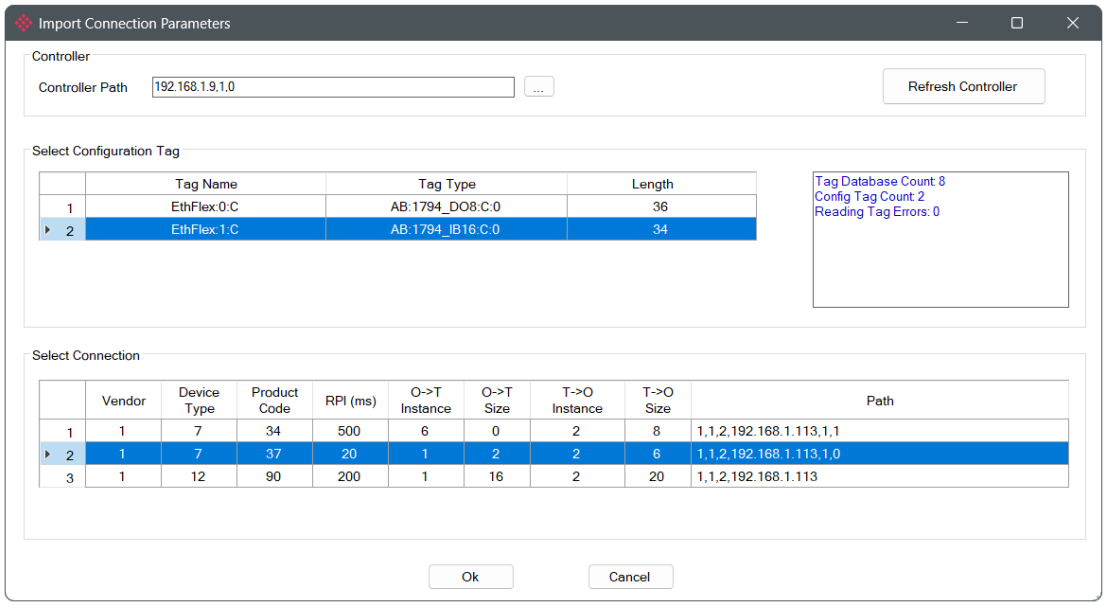


Figure 3.75 – Import Connection Parameters – Select Connection

To import all the necessary connection information, the user will need to select both the appropriate *Configuration Tag*, and the matching *Connection*.

The new connection's configuration data is derived from the selected *Configuration Tag*, when the new connection's parameters are derived from the selected *Connection*.

Once the appropriate selections have been made, press **OK**. The imported data will be populated into the *Connection* form.

The user can then modify the *Connection Name*, *Path* and *RPI* as required.

3.7.4.1.3 Import From Controller .L5X File

Here the EtherNet/IP connection parameters are imported from a Logix controller's .L5X file.

3.7.4.1.3.1 Preparation

Before the connection information can be imported some preparation is required using Studio5000:

1. In Studio5000 create a new project and add the required EtherNet/IP device in the IO tree. If the device's profile supports configuration, then configure the device as required.
2. Save the Studio5000 project as an .L5X file.

Important: When instantiating modules in Studio5000 do not make use of the "Rack Optimization" communication format.

Important: It is possible that not all the connection information will be imported as it may not be available in the .L5X file due to the type of device and Logix version.

3.7.4.1.3.2 Import .L5X File

The connection parameters can be imported from the .L5X file by selecting the **IMPORT CONTROLLER L5X** option located under the *Import* menu of the *Class 1 Connection* form.

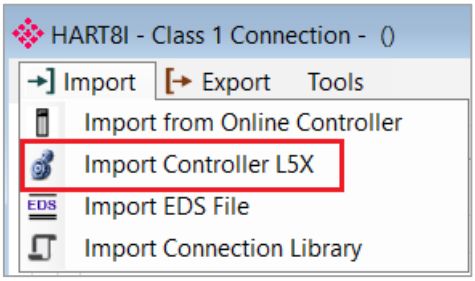


Figure 3.76 – Import from Controller L5X

The *Import L5X Device Configuration* form will open.

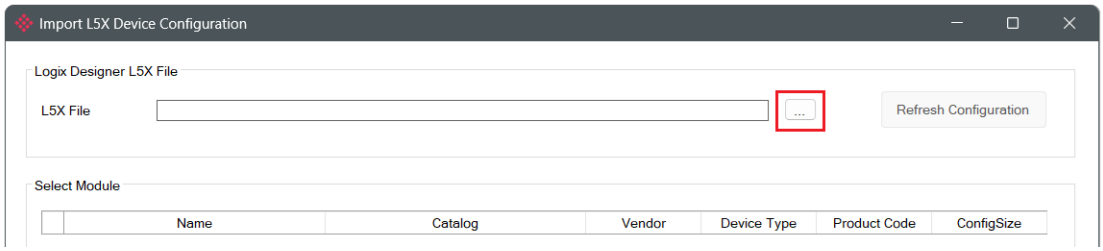


Figure 3.77 – Import L5X Device Configuration – Select L5X

Click on the **BROWSE** ("**…**") button to select the previously generated .L5X file. The modules found in the selected .L5X file will then be displayed in the Module List.

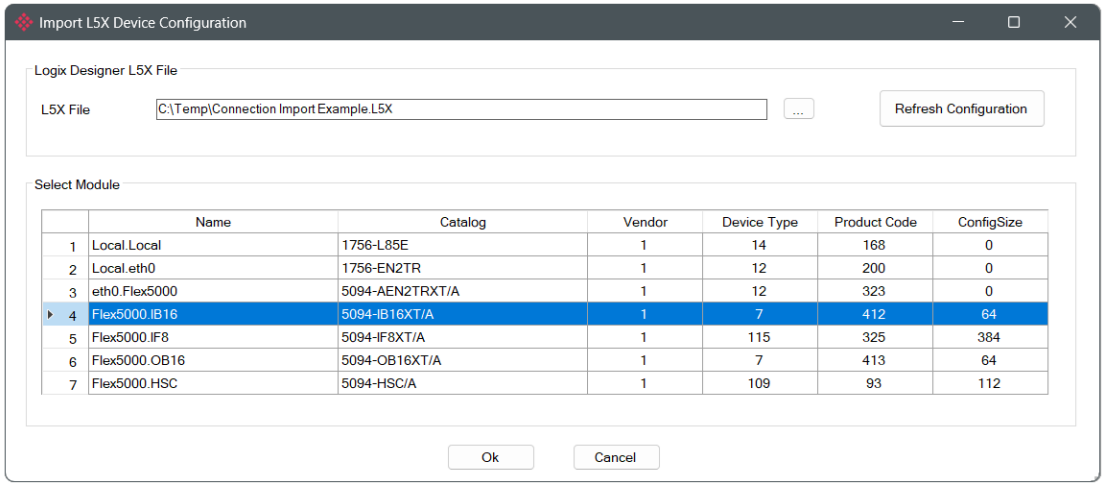


Figure 3.78 – Import L5X Device Configuration

Select the required module and click **OK**. The imported data will be populated into the *Connection* form. The user can then modify the *Connection Name*, *Path* and *RPI* as required.

3.7.4.1.4 Import EDS File

The connection parameters can be imported from a suitable EDS file. Typically, this approach is preferred for devices that do not require configuration data.

To import the connection parameters from a device EDS file, select the **IMPORT EDS FILE** option located under the *Import* menu of the *Class 1 Connection* form.

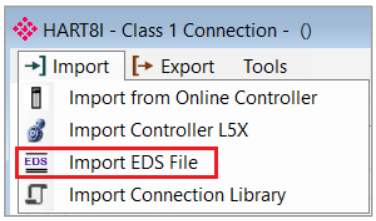


Figure 3.79 – Import EDS File

A *Select an Electronic Data Sheet* dialog will open allowing the user to select the EDS file.

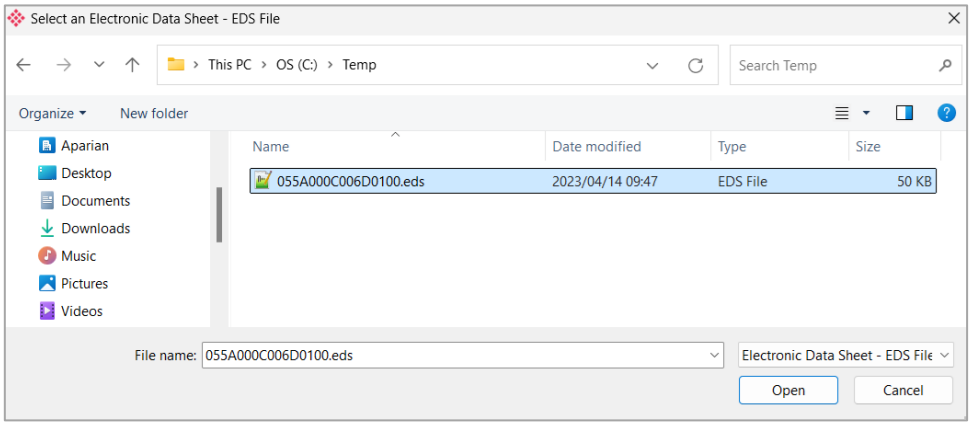


Figure 3.80 – Browse to EDS File

The selected EDS file will be imported, and a summary of the connections displayed. The user will need to select one of the IO connections.

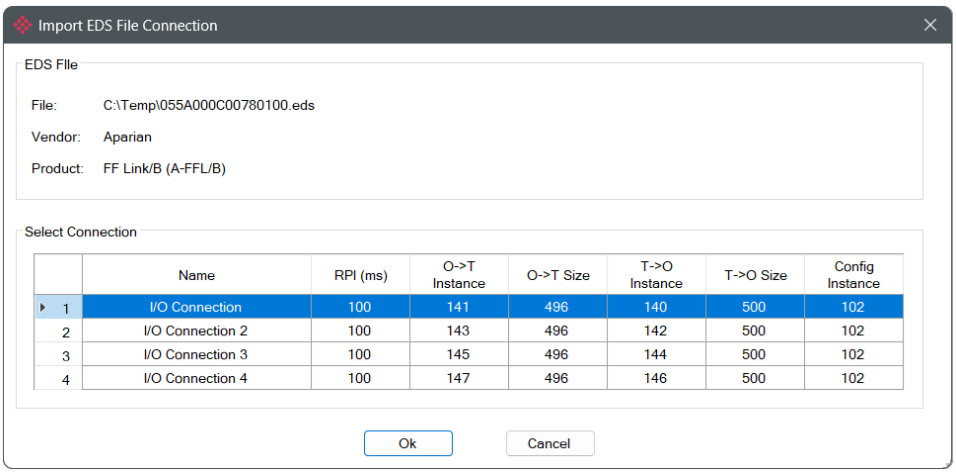


Figure 3.81 – Select Connection

The selected connection within the EDS file will be used to populate the Connection parameters. The user can then modify the *Connection Name*, *Path* and *RPI* as required.

3.7.4.1.5 Import Connection Library

The connection parameters can be imported from a previously created Connection Library (.EIPCNX) file.

Note: Please contact support to receive a bundle of the latest Connection Library files, for commonly used devices.

To import the connection parameters from a Library file, select the **IMPORT CONNECTION LIBRARY FILE** option located under the *Import* menu of the *Class 1 Connection* form.

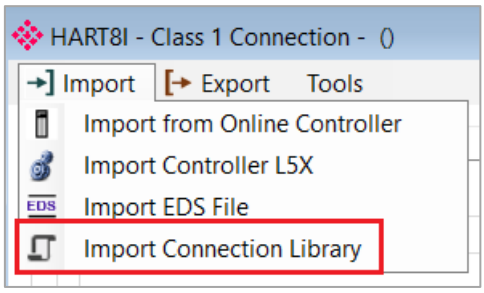


Figure 3.82 – Import Connection Library File

A *File Open* dialog will open allowing the user to select the Library (.EIPCNX) file. The selected Library file will be used to populate the Connection parameters. The user can then modify the *Connection Name*, *Path* and *RPI* as required.

3.7.4.1.6 Export Library File

To create a Library file for future use, select the **EXPORT CONNECTION LIBRARY** option located under the *Export* menu.

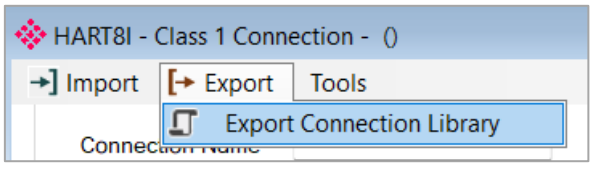


Figure 3.83 – Export Connection Library File

3.7.4.2 EtherNet/IP Explicit Message Device Connections

Up to 10 EtherNet/IP devices can be added for explicit messaging. The user will need to add each device as explained in the EtherNet/IP Devices section below. Once the EtherNet/IP devices have been added the user can then configure the required mapping for the EtherNet/IP Explicit messaging as shown in EtherNet/IP Map section below.

3.7.4.2.1 EtherNet/IP Devices

This tab is enabled when the *Primary Interface* is set to **ETHERNET/IP ORIGINATOR**.

Up to 10 EtherNet/IP devices can be configured with up to 50 EtherNet/IP mapped items allowing for either explicit EtherNet/IP Class 3 or Unconnected Messaging (UCMM) to any of the 10 configured devices. The data from each EtherNet/IP device is written to, or read from, an Internal Data Space with a size of 100Kbytes. See section *8.3.2 Explicit EtherNet/IP Messaging* for more details.

The EtherNet/IP Devices configuration tab is opened by either double-clicking on the module in the tree, or by right-clicking the module and selecting **CONFIGURATION**.

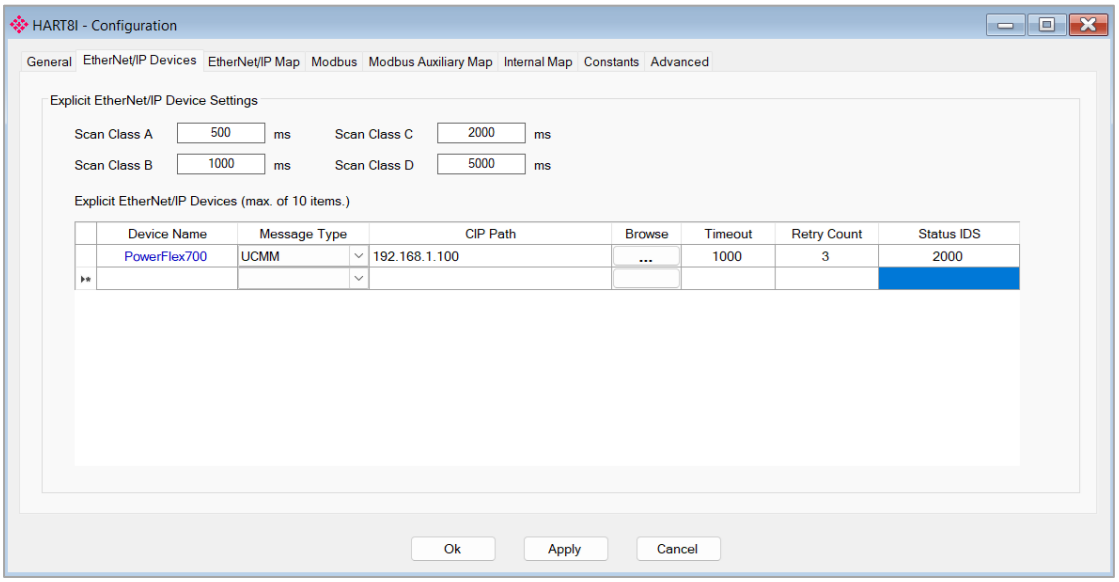


Figure 3.84 – EtherNet/IP Devices - Configuration

The EtherNet/IP Devices configuration consists of the following parameters:

Parameter	Description
Scan Class A, B, C, D	The configurable update rate (in milliseconds) for each scan class in the EtherNet/IP Map.
Device List (per device)	
Device Name	The user assigned instance name for the specific device.
Message Type	The module can use either *Class 3* or *Unconnected Messaging* when communicating to the target EtherNet/IP device.
CIP Path	The CIP Path to the target device. This can either be entered manually, or the user can browse them by clicking the **BROWSE** button. The Target Browser will open and automatically scan all available EtherNet/IP devices. If the Ethernet/IP module is a bridge module, it can be expanded by right-clicking on the module and selecting the **SCAN** option. The required EtherNet/IP device can then be chosen by selecting it and clicking the **OK** button, or by double-clicking on the target module.

Timeout	The time (in milliseconds) the module will wait for a response from the target EtherNet/IP device.
Retry Count	The number of message retries before the target EtherNet/IP device is considered offline.
Comm Status Offset	This is the offset in the Internal Data Space (used to map EtherNet/IP device data) which provides the communication status of each EtherNet/IP device. The Communication Status is as shown below: Bit 0: (1: Device Online, 0: Device Offline) Bit 1 to 7: Reserved.

Table 3.12 – EtherNet/IP Devices configuration parameters

3.7.4.2.2 EtherNet/IP Map

This tab is enabled when the *Primary Interface* is set to **ETHERNET/IP ORIGINATOR**.

Up to 50 EtherNet/IP mapped items, either explicit EtherNet/IP Class 3 or Unconnected Messaging (UCMM) to any of the 10 pre-configured devices can be configured. The data from each EtherNet/IP device is written to or read from Internal Data Space with a size of 100Kbytes. See section *8.3.2 Explicit EtherNet/IP Messaging* for more details.

The *EtherNet/IP Map* configuration tab is opened by either double-clicking on the module in the tree, or by right-clicking the module and selecting **CONFIGURATION**.

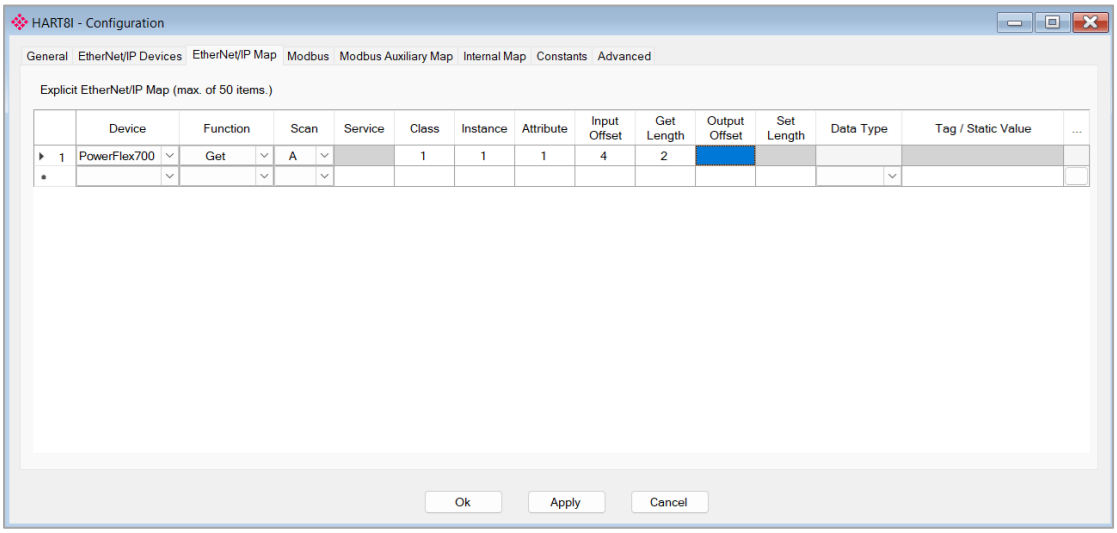


Figure 3.85 – EtherNet/IP Map configuration

The EtherNet/IP Map configuration consists of the following parameters:

Parameter	Description
Device	The device instance name configured in the previous EtherNet/IP Devices tab. The selected device will be used for executing the communication function.
Function	The user can select one of four functions. **Get**: The module will read data from the target EtherNet/IP device by using the Get Single Attribute CIP function. The received data will be placed into the Internal Data Space at the *Input Offset* location configured in this tab. **Set**: The module will write data to the target EtherNet/IP device by using the Set Single Attribute CIP function. The data to be written will be retrieved from the Internal Data Space at the *Output Offset* location configured in this tab.

	Set Static: Like the Set function above, but the data to be written will be fixed (equal to the *Static Value*) parameter in this configuration window. This function will typically be used with the single (S) Scan class which means the PLX51-HART-8I can be set up to write the fixed value only once when the target device communication has been established. **Custom**: This function allows the user to use a custom Service to write and read data in the same transaction. The user will need to see which custom services that target device supports in that device's user manual. **Read Tag**: When using a Logix controller as an EtherNet/IP Device, the PLX51-HART-8I can read a Logix tag from the target Logix controller using Class 3 or UCMM messaging. The value from the tag will be saved at the configured Input Offset. **Write Tag**: When using a Logix controller as an EtherNet/IP Device, the PLX51-HART-8I can write to Logix tag from the target Logix controller using Class 3 or UCMM messaging. The value from the tag will be read from the configured Output Offset.
Scan	The user can select Scan Class **A**, **B**, **C** or **D** (which was configured in the EtherNet/IP Devices tab). The specific mapped item will then be executed at that configured scan class rate. The user can also select the **S** class which means that the mapped item will only be executed once, when communication to the target device is established. If the target device goes offline, then the mapped items with this class will be re-armed and resent when communication is re-established.
Service	The custom CIP service/function which is only available when the ***Custom*** function has been selected.
Class, Instance, Attribute	The CIP class, instance, and attribute of the request message to be sent.
Input Offset	The location in the Internal Data Space where the received data will be written. This will only be available for *Get* and *Custom* functions.
Get Length	The length of the data to be received. If the number of bytes received is more than the *Get Length*, then the data will not be written to the Internal Data Space. **Note**: When the function is Logix Read, then the Get Length will be the number of elements of the configured data type and not the byte count. This will only be available for *Get* and *Custom* functions.
Output Offset	The location in the Internal Data Space from where the data to be written to the target device will be read. This will only be available for S*et* and *Custom* functions.
Set Length	The length of the data to be written. **Note**: When the function is Logix Write, then the Set Length will be the number of elements of the configured data type and not the byte count. This will only be available for *Set* and *Custom* functions.
Data Type	The data type of the Static Value. This will only be available for *Set Static* function.
Tag / Static Value	The value to be written to the target device when the *Set Static* function has been selected. **Note:** When using the SINT Array data type, the values must be entered as space-delimited hex values. For example: 05 34 2E A1

Table 3.13 – EtherNet/IP Map configuration parameters

3.7.4.3 Internal Data Space Mapping

When the PLX51-HART-8I is operating as an EtherNet/IP Originator, the data from the EtherNet/IP IO devices can be mapped to module using the Internal Map. The *Internal Map* configuration window is opened by either double-clicking on the module in the tree or right-clicking the module and selecting **CONFIGURATION** and selecting the *Internal Map* tab.

3.7.4.3.1 IDS Copy – EtherNet/IP Originator Source

When copying data from an EtherNet/IP IO device to the module, the *Source Type* must be set to **EIP ORIGINATOR**.

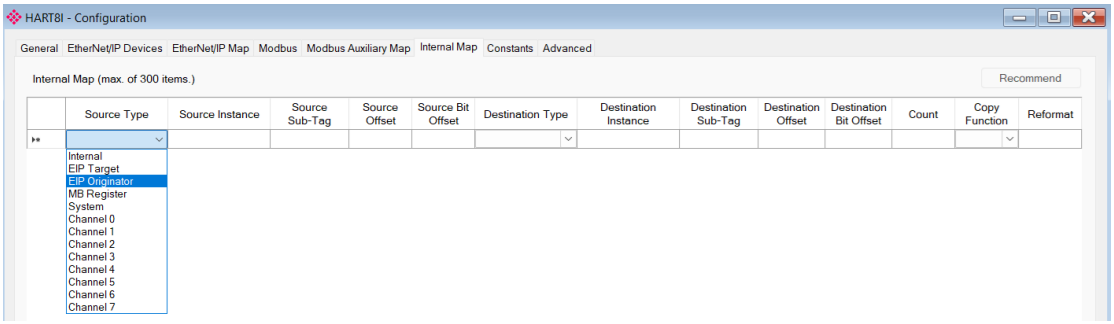


Figure 3.86 – IDS Copy – EtherNet/IP Originator Source Type

The *Source Instance* will be one of the EtherNet/IP IO devices added to the EtherNet/IP IO tree in PLX50CU.

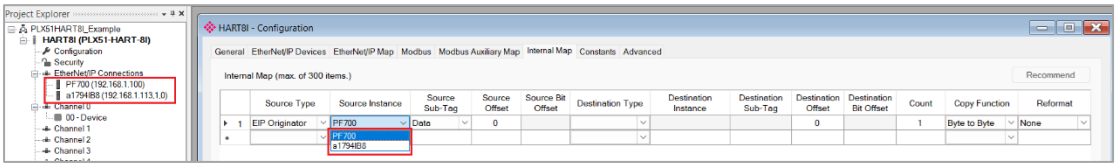


Figure 3.87 – IDS Copy – EtherNet/IP Originator Source Instance

The *Source Offset* is the offset in the selected EtherNet/IP device Class 1 Input Assembly.

The *Count* is the number of bytes that will be copied.

The user can choose to copy either the **DATA**, or **STATUS**, from the EtherNet/IP connection.

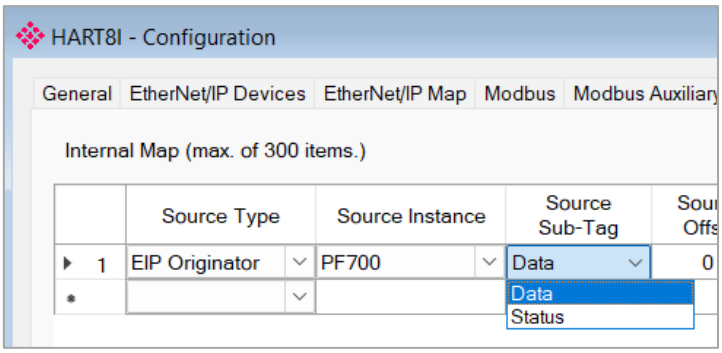


Figure 3.88 – IDS Copy – EtherNet/IP Originator Status

When selecting the *Status*, the format is shown below:

Parameter	Data Type	Description
EtherNet/IP Originator Connection Status	DINT	Bit 0 – Connection Ok

Table 3.14 – EtherNet/IP Originator Connection Status

3.7.4.3.2 IDS Copy – EtherNet/IP Target Destination

When copying data from the PLX51-HART-8I to an EtherNet/IP IO device's **Output** Assembly, the *Destination Type* must be set to **EIP ORIGINATOR**.

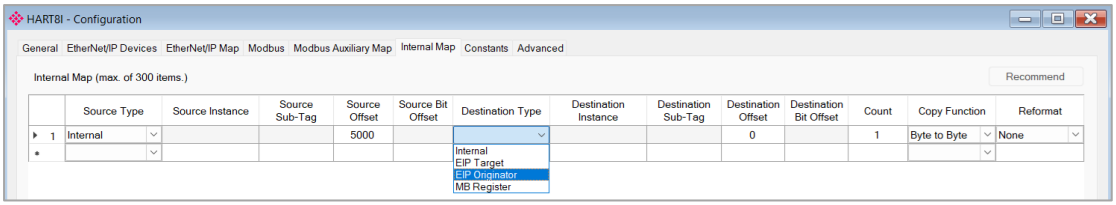


Figure 3.89 – IDS Copy – EtherNet/IP Originator Destination Type

The *Destination Instance* will be one of the EtherNet/IP IO devices added to the EtherNet/IP IO tree in PLX50CU.

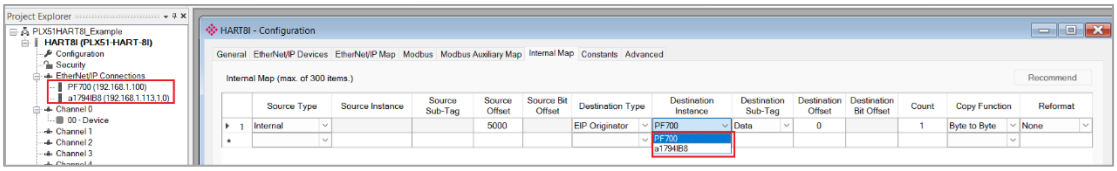


Figure 3.90 – IDS Copy – EtherNet/IP Originator Destination Instance

The *Destination Offset* is the offset in the selected EtherNet/IP device Class 1 Output Assembly.

The *Count* is the number of bytes that will be copied.

See section *3.8 Internal Data Space Map* for more information regarding the operation.

3.8 Internal Data Space Map

The internal data map is used to exchange data from/to the one interface (Ethernet, RS232, RS485, etc.) to the Analog Input Channels and HART devices. Up to 300 items can be mapped. The Internal Map configuration window is opened by either double-clicking on the module in the tree, or right-clicking the module and selecting **CONFIGURATION** and then selecting the *Internal Map* tab.

The *Count* is the number of bytes that will be copied from the source to the destination. There are four different *Copy Functions* that can be used.

Function	Description
Byte to Byte	Each byte from the source will be directly copied to each byte in the destination.
Byte to Bit	Each byte from the source will be copied to each bit in the destination. If a value greater than zero is read from the source byte then a 1 will be written to the destination bit address. If a value of zero is read from the source byte then a 0 will be written to the destination bit address. The destination offset will be the bit offset, and the destination address will be increased by one bit each time.
Bit to Bit	Each bit from the source will be directly copied to each bit in the destination.
Bit to Byte	Each bit from the source will be copied to each byte in the destination. If a value of one is read from the source bit then a 1 will be written to the destination byte address. If a value of zero is read from the source bit then a 0 will be written to the destination byte address. The source offset will be the bit offset, and the source address will be increased by one bit each time.

Table 3.15 – Internal Map Copy functions

The data in the destination source can also be reformatted. The reformat option provides five different reformat options.

Note: The reformat option is only available for *Byte to Byte* copy functions.

Function	Description
None	No reformatting applied (AA BB CC DD)
BB AA	16-bit Byte swap
BB AA DD CC	32-bit Byte Pair Swap
CC DD AA BB	Word Swap
DD CC BB AA	Word and Byte Pair Swap

Table 3.16 – Internal Map Reformat Options

3.8.1 Copy From

One of thirteen sources can be selected to copy from:
INTERNAL, **EIP TARGET**, **EIP ORIGINATOR**, **MB REGISTER**, **SYSTEM**, **CHANNEL 0** to **7**.

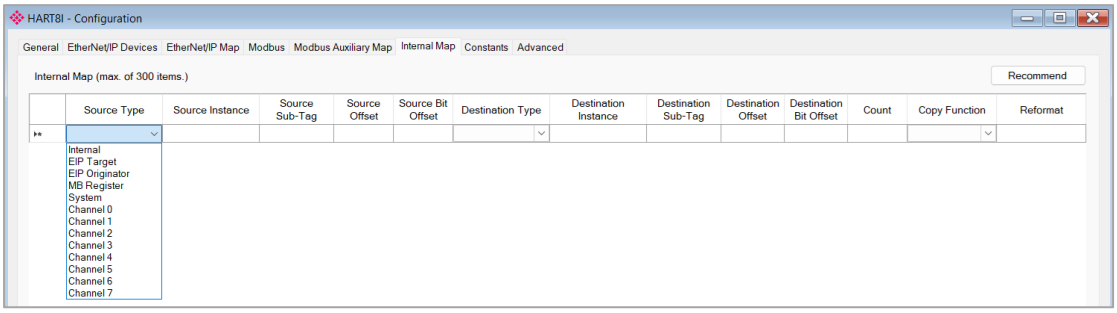


Figure 3.91 – Internal Map – Source Type

3.8.1.1 Internal

When copying data from the internal data space (IDS), the *Source Type* must be set to **INTERNAL**.

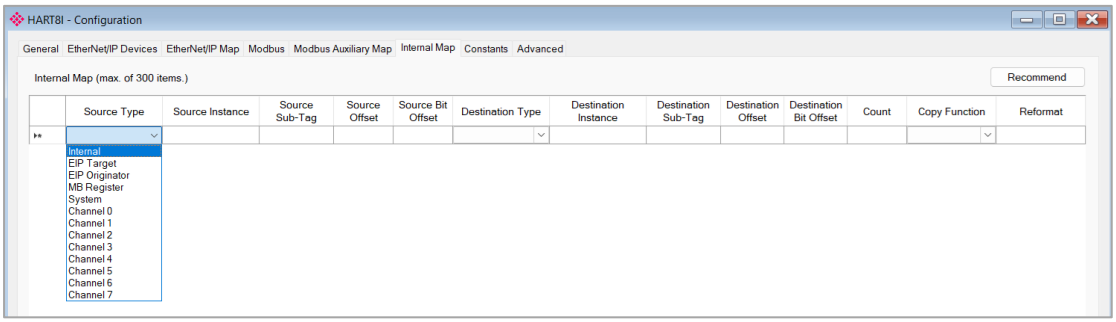


Figure 3.92 – IDS Copy – Internal Source Type

The *Source Instance* is Not Applicable for the internal data space.

The *Source Offset* is the offset in the *Internal Data Space (IDS)* which has a maximum of 100,000 bytes.

The *Count* is the number of bytes that will be copied.

3.8.1.2 EIP Target

When copying data from a connection originator (e.g. the output assembly from the Logix Controller) to the module, the *Source Type* must be set to **EIP TARGET**.

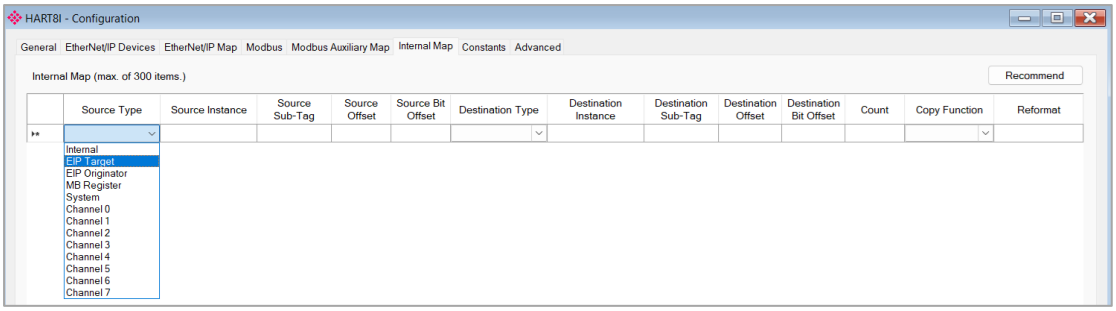


Figure 3.93 – IDS Copy – EtherNet/IP Target Source Type

The *Source Instance* will be the connection number, which can be connection 0 to 7, based on the number of connections configured.

The *Source Offset* is the offset in the EtherNet/IP output assembly from where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.8.1.3 EIP Originator

When copying data from an EtherNet/IP IO device to the module, the *Source Type* must be set to **EIP ORIGINATOR**.

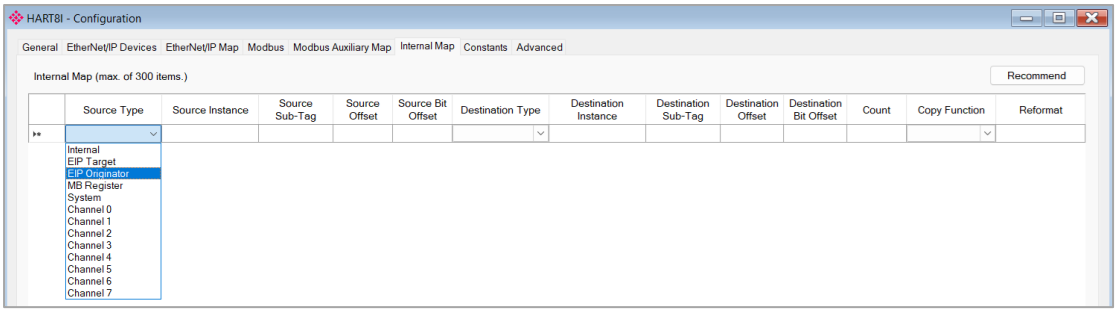


Figure 3.94 – IDS Copy – EtherNet/IP Originator Source Type

The source instance will be one of the EtherNet/IP IO devices added to the EtherNet/IP IO tree in the PLX50CU.

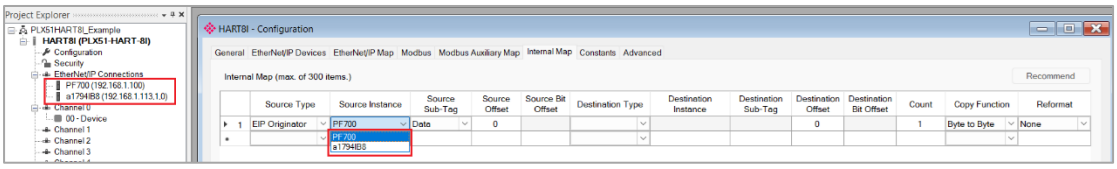


Figure 3.95 – IDS Copy – EtherNet/IP Originator Source Instance

The *Source Offset* is the offset in the selected EtherNet/IP device Class 1 Input Assembly.

The *Count* is the number of bytes that will be copied.

The user can select to copy the data from the EtherNet/IP connection or status.

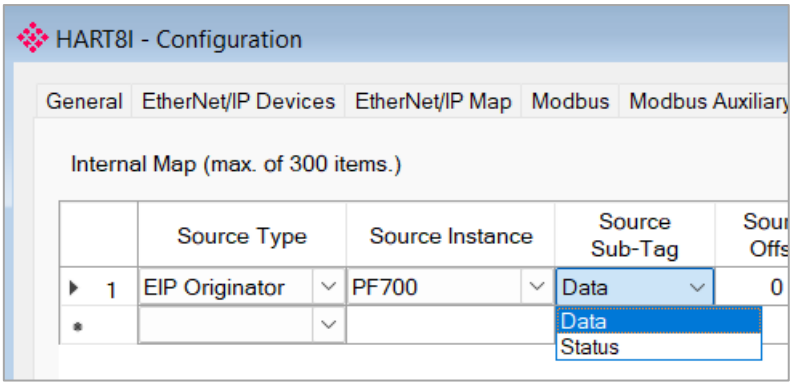


Figure 3.96 – IDS Copy – EtherNet/IP Originator Status

When selecting the status, the format of the Status information is shown below:

Parameter	Data Type	Description
EtherNet/IP Originator Connection Status	DINT	Bit 0 – Connection Ok

Table 3.17 – EtherNet/IP Originator Connection Status

3.8.1.4 Modbus Register

When copying Modbus data to the module, the *Source Type* must be set to **MB REGISTER**.

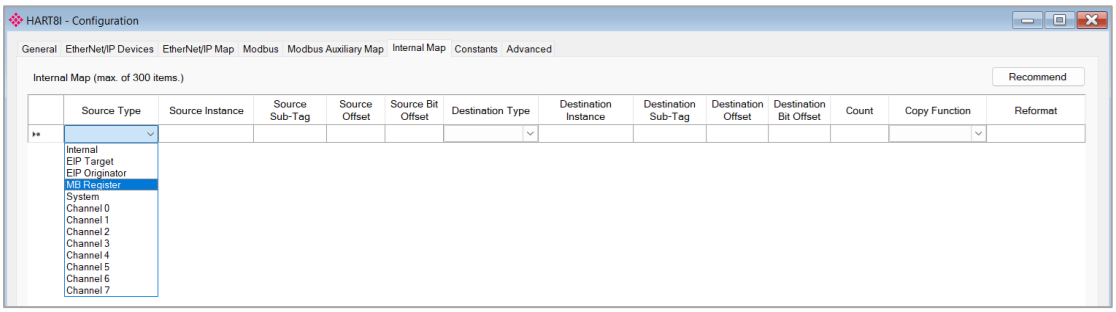


Figure 3.97 – IDS Copy - Modbus Source Type

The *Source Instance* will be the Modbus register type required.

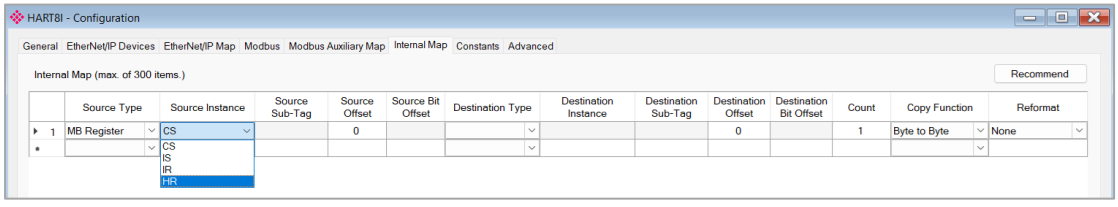


Figure 3.98 – IDS Copy - Modbus Source Instance

The *Source Offset* is the Modbus Register offset from where the data will be copied.

The *Count* is the number of bytes that will be copied.

3.8.1.5 System

When copying system information, the *Source Type* must be set to **SYSTEM**.

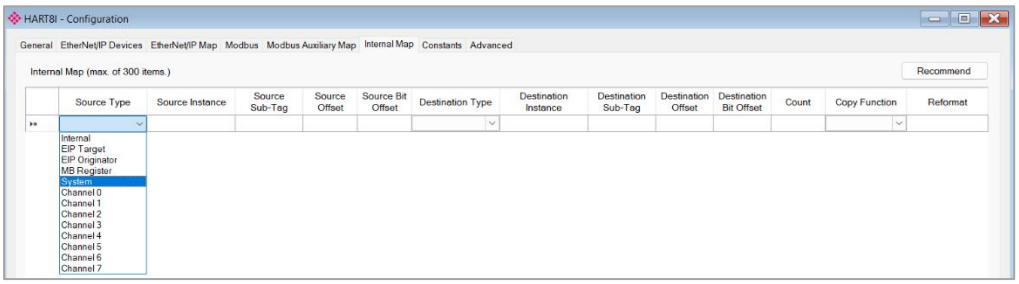


Figure 3.99 – IDS Copy – System Information

The module's System information has the following format.

Parameter	Data Type	Description
General Status	DINT	Module Status. Bit 0: Module Config Valid Bit 1: EtherNet/IP Originator Comms Ok Bit 2: Modbus Comms Ok Bit 3: EtherNet/IP Target Comms Ok Bit 4: Power 1 Ok Bit 5: Power 2 Ok Bit 6: Controller in Run Mode Bit 7: NTP Ok Bit 8: Reserved Bit 9: Real Time Clock (RTC) Ok
Config CRC	INT	The checksum associated with the current configuration.
Reserved	INT	-
Uptime	DINT	The number of seconds elapsed since the module was powered up.
Date Year	INT	Current year for the local module.
Date Month	INT	Current month for the local module.
Date Day	INT	Current day for the local module.
Time Hour	INT	Current hour for the local module.
Time Minutes	INT	Current minute for the local module.
Time Seconds	INT	Current second for the local module.
Temperature	REAL	The internal temperature of the module.
Startup DIP Switches	INT	The DIP Switch positions at module power up.
Current DIP Switches	INT	The current DIP Switch positions.
Ethernet Port 1 Status	INT	Bit 0: Link Up (1) / Link Down (0) Bit 1: Port Mirror Enabled (1) / Port Mirror Disabled (0)
Ethernet Port 2 Status	INT	Bit 0: Link Up (1) / Link Down (0) Bit 1: Port Mirror Enabled (1) / Port Mirror Disabled (0)
Ethernet Switch Mode	INT	Current mode of the embedded Ethernet switch. 0: Normal Switching. Single IP address with packet routing between ports. 1: Split Port. No packet routing between the Ethernet ports with dual IP addresses.
Device Level Ring (DLR) Status	INT	Bit 0: Enabled (1) / Disabled (0) Bit 1: Ring network (1) / Linear network (0) Bit 2: Ring Fault (1) / Ring Ok (0)
NTP Status	INT	Bit 0: Enabled (1) / Disabled (0) Bit 1: Synchronized (1) / Not Synchronized (0)
PTP Status	INT	Bit 0: Enabled (1) / Disabled (0) Bit 1: Synchronized (1) / Not Synchronized (0)
Reserved	INT[4]	-

Table 3.18 – System Information Format

3.8.1.6 Channel

When copying data from an Analog Input Channel or HART device, the *Source Type* must be set to **CHANNEL 0** to **CHANNEL 7**.

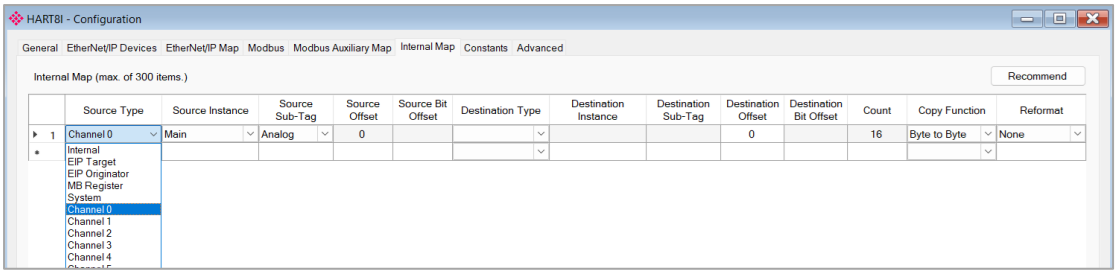


Figure 3.100 – IDS Copy – Channel Source Type

The *Source Instance* will be **MAIN** or the name of the configured HART devices for that specific Analog Input Channel.

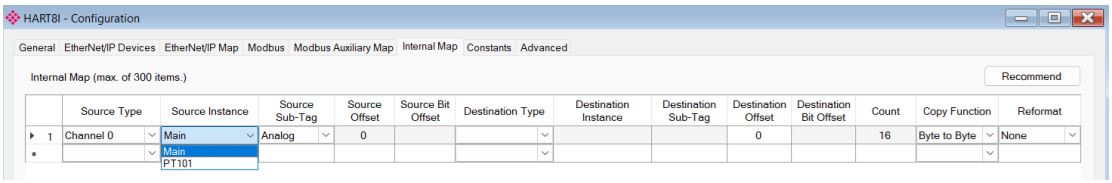


Figure 3.101 – IDS Copy – Channel Source Instance and Sub-Tag

When *Source Instance* **MAIN** is selected, the *Source Sub-Tag* can set to **ANALOG** or **STATISTICS** (which will be the HART communication statistics on that channel).

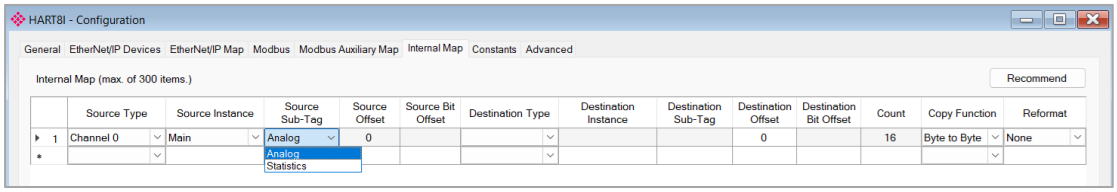


Figure 3.102 – IDS Copy – Channel Source Instance and Sub-Tag

Source Sub-Tag: **Analog**

Parameter	Data Type	Description
Channel Status	DINT	Bits to follow.
HART Comms	Bit 0	Enabled (1) / Disabled (0)
Analog Filter	Bit 1	Enabled (1) / Disabled (0)
Allow Dual HART Masters	Bit 2	Enabled (1) / Disabled (0)
Channel Analog Value Under Range	Bit 3	Under Range (1) / Ok (0)
Channel Analog Value Over Range	Bit 4	Over Range (1) / Ok (0)
Current Loop Open	Bit 5	Open Circuit (1) / Ok (0)
Current Loop Shorted	Bit 6	Short Circuit (1) / Ok (0)
HART Burst Mode	Bit 7	Enabled (1) / Disabled (0)
Relay Message Priority	Bit 8	Priority (1) / Normal (0)
Factory Calibration for Current	Bit 9	Ok (1) / Invalid (0)
Factory Calibration for Voltage	Bit 10	Ok (1) / Invalid (0)
User Calibration for Current	Bit 11	Ok (1) / Invalid (0)
User Calibration for Voltage	Bit 12	Ok (1) / Invalid (0)
Current Value	REAL	Raw Current Value (mA)
Scaled Value	REAL	Scaled Value
Voltage Value	REAL	Raw Voltage Value (V)

Table 3.4 – IDS Copy - Channel Main Analog

Source Sub-Tag: **Statistics**

Parameter	Data Type	Description
HART Tx Count	DINT	The number of HART packets sent.
HART Rx Count	DINT	The number of HART packets received.
Communication Errors	DINT	The number of communication error occurrences.
Command Errors	DINT	The number of command error occurrences.
Timeout Errors	DINT	The number of HART timeout error occurrences.
Device Offline Count	DINT	Number of times a HART device has gone offline.
Relay Message Rx Count	DINT	The number of HART packets received for relay (Class 2) messages (DTMs etc.)
Relay Message Tx Count	DINT	The number of HART packets sent via relay (Class 2) messages (DTMs etc.)
Advanced Message Rx Count	DINT	The number of Advanced Message HART responses that have been received.
Advanced Message Tx Count	DINT	The number of Advanced Message HART packets that have been sent.

Table 3.4 – IDS Copy - Channel Main Statistics

When a HART device is selected as the *Source Instance*, the *Source Sub-Tag* will be set to **DATA**.

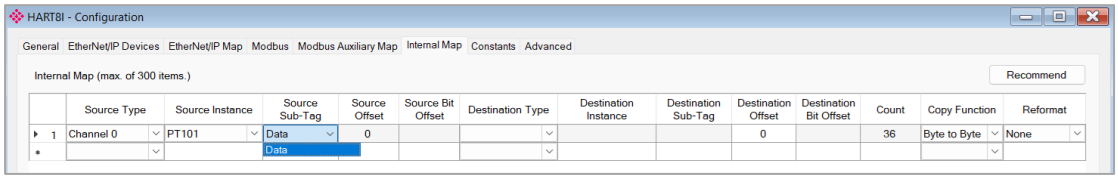


Figure 3.103 – IDS Copy – Channel Source Instance and Sub-Tag

Source Sub-Tag: **Data**

Parameter	Data Type	Description
Node Address	INT	The Short Address of the HART device
HART Status	INT	HART Status information as reported by field device. See the appendix for information regarding the HART status.
Device Status	DINT	Bits to follow.
HART Device Online	Bit 0	Online (1) / Offline (0)
Relay Messages Inhibited	Bit 1	Inhibited (1) / Normal (0)
PV	REAL	Primary Variable
SV	REAL	Secondary Variable
TV	REAL	Tertiary Variable
FV	REAL	Fourth Variable
PV Units Code	INT	Primary Variable Units Code
SV Units Code	INT	Secondary Variable Units Code
TV Units Code	INT	Tertiary Variable Units Code
FV Units Code	INT	Fourth Variable Units Code
Advanced Message Success	INT	One bit for each of the advanced messages configured for the specific HART device. For example, the status of bit 4 will match the status of the 5th Advanced HART message configured for the HART device. Succes (1) / Failed (0)

Advanced Message Activity	INT	One bit for each of the advanced messages configured for the specific HART device. Each time there is an Advanced Message being sent for the specific HART device, it will toggle the relevant bit in this activity. For example, bit 4 will change state (i.e. toggle) each time the 5th Advanced HART message configured for the HART device is executed.

Table 3.4 – IDS Copy - Channel HART Device Data

The *Source Offset* is the offset of the Channel data from where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.8.2 Copy To

One of four destinations can be selected to copy to:
INTERNAL, **EIP TARGET**, **EIP ORIGINATOR**, and **MB REGISTER**.

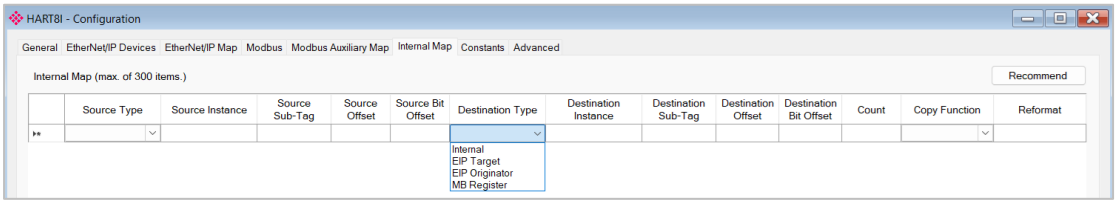


Figure 3.104 – Internal Map – Destination Type

3.8.2.1 Internal

When copying data to the internal data space (IDS), the *Destination Type* must be set to **INTERNAL**.

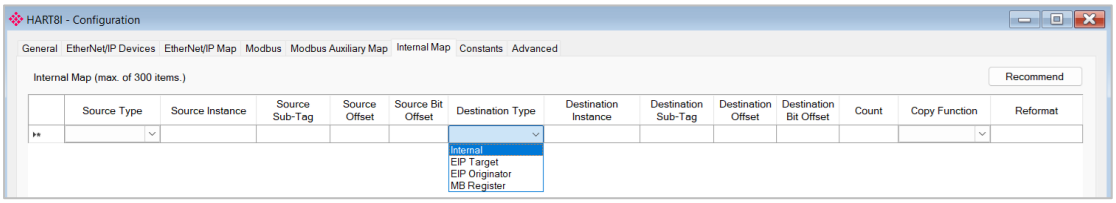


Figure 3.105 – IDS Copy – Internal Source Type

The *Destination Instance* is not applicable for the internal data space.

The *Destination Offset* is the offset in the *Internal Data Space (IDS)* which has a maximum of 100,000 bytes.

The *Count* is the number of bytes that will be copied.

3.8.2.2 EIP Target

When copying data from the PLX51-HART-8I to the EtherNet/IP Target input assembly, the *Destination Type* must be set to **EIP TARGET**.

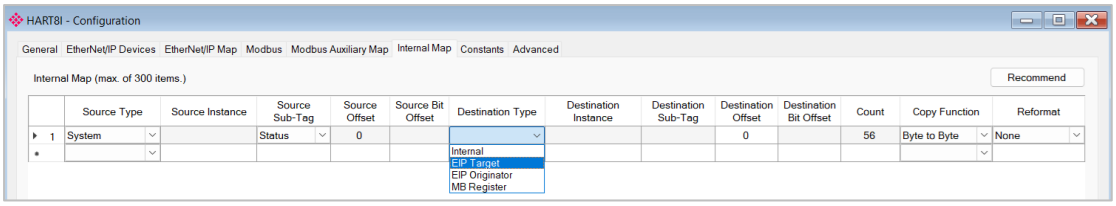


Figure 3.106 – IDS Copy – EtherNet/IP Target Destination Type

The *Destination Instance* will be the connection number, which can be connection 0 to 7, based on the number of connections configured.

The *Destination Offset* is the offset of the EtherNet/IP input assembly from where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.8.2.3 EIP Originator

When copying data from the PLX51-HART-8I to an EtherNet/IP IO device's Output Assembly, the *Destination Type* must be set to **EIP ORIGINATOR**.

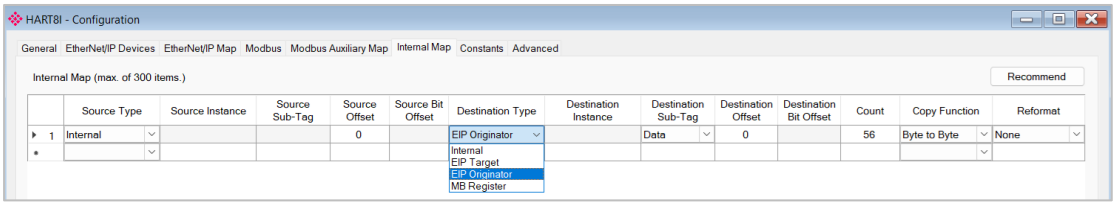


Figure 3.107 – IDS Copy – EtherNet/IP Originator Destination Type

The *Destination Instance* will be one of the EtherNet/IP IO devices added to the EtherNet/IP IO tree in the PLX50CU.

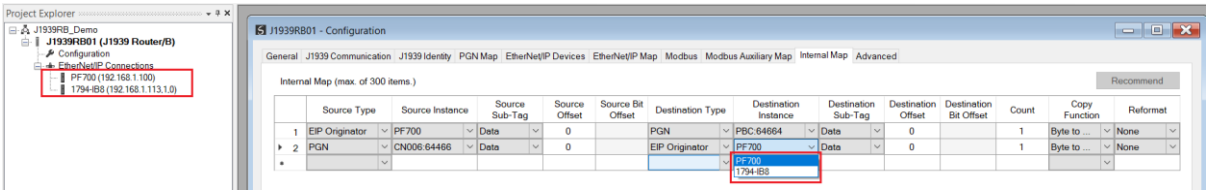


Figure 3.108 – IDS Copy – EtherNet/IP Originator Destination Instance

The *Destination Offset* is the offset in the selected EtherNet/IP device Class 1 Output Assembly.

The *Count* is the number of bytes that will be copied.

3.8.2.4 Modbus Register

When copying data from the PLX51-HART-8I to a Modbus Register, the *Destination Type* must be set to **MB REGISTER**.

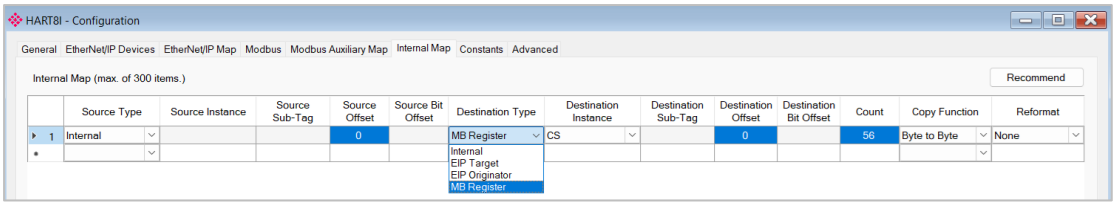


Figure 3.109 – IDS Copy - Modbus Destination Type

The *Destination Instance* will be the Modbus register type required.

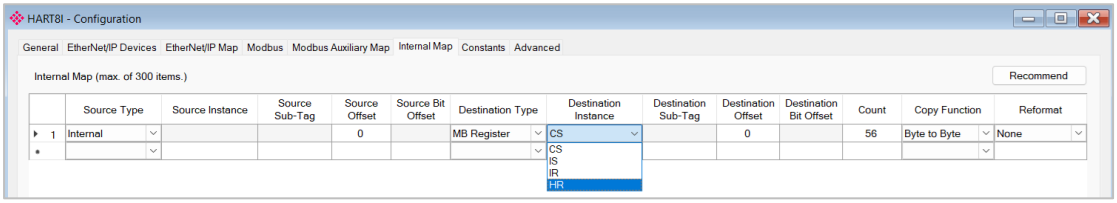


Figure 3.110 – IDS Copy - Modbus Destination Instance

The *Destination Offset* is the Modbus Register offset to where the data must be copied.

The *Count* is the number of bytes that will be copied.

3.8.3 Constants

The *Internal Data Constant* configuration provides a mechanism to load the Internal Data Space (IDS) with constant data at module start-up. This is often useful for the pre-population of configuration data for HART devices, as well as Modbus and EtherNet/IP devices.

The *Constants* configuration tab is opened by either double-clicking on the module in the tree, or by right-clicking the module and selecting **CONFIGURATION**.

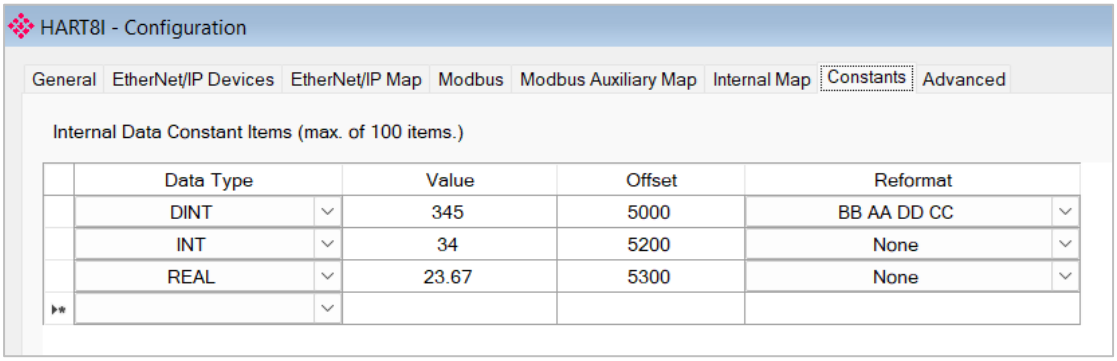


Figure 3.111 – Constants configuration

The *Constant* configuration consists of the following parameters:

Parameter	Description
Data Type	The Data Type of the constant item, either: SINT INT DINT LINT REAL USINT UINT UDINT
Value	The constant value.
Offset	The offset in the Internal Data Space where the constant value will be copied.
Reformat	Used to specify how the data is formatted before writing to Internal Data Space: **None**: No reformatting applied. (AA BB or AA BB CC DD). **BB AA**: 16bit Byte swap **BB AA DD CC**: 32bit Byte Pair Swap **CC DD AA BB**: Word Swap **DD CC BB AA**: Word and Byte Pair Swap

Table 3.19 – Constants configuration parameters

3.9 Advanced

The *Advanced* configuration tab is opened by either double-clicking on the module in the tree, or by right-clicking the module and selecting **CONFIGURATION**.

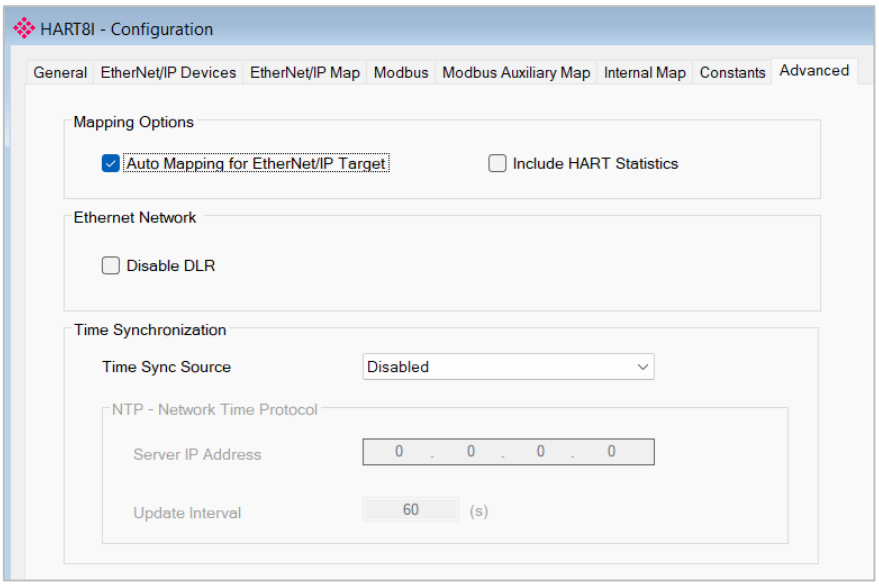


Figure 3.112 – Advanced configuration

The Advanced configuration consists of the following parameters:

Parameter	Description
Mapping Options	
Auto Mapping for EtherNet/IP Target	When selected, the **RECOMMENDED** button in the Internal Mapping will be disabled and the recommended mapping will automatically be applied. (On by default)
Include HART Statistics	When **AUTO MAPPING FOR ETHERNET/IP TARGET** is enabled, this will force the recommended mapping to include the HART statistics.
Ethernet Network	
Disable DLR	Disable the Device Level Ring (DLR) operation.
Time Synchronization	
Time Sync Source	**Disabled**: The module will not be synchronized by an external time source. **NTP**: The PLX51-HART-8I can synchronize its onboard clock to an NTP Server. **PTP**: The PLX51-HART-8I can synchronize its onboard clock to a PTP Master.
NTP Server IP Address	When the *Time Sync Source* is set to **NTP**, this setting is the IP address of the NTP Server which will be used as a time source.
NTP Update Interval	When the *Time Sync Source* is set to **NTP**, this setting is the updated interval (in seconds) that the PLX51-HART-8I will request time from the NTP Server.

Table 3.20 – Advanced configuration parameters

3.10 Module Download

Once the PLX51-HART-8I configuration is complete, it must be downloaded to the module. Before downloading, the *Connection Path* of the module should be set. This path will automatically default to the IP address of the module, as set in the module configuration. It can be modified if the module is not on a local network.

The *Connection Path* can be set by right-clicking on the module and selecting the **CONNECTION PATH** option.

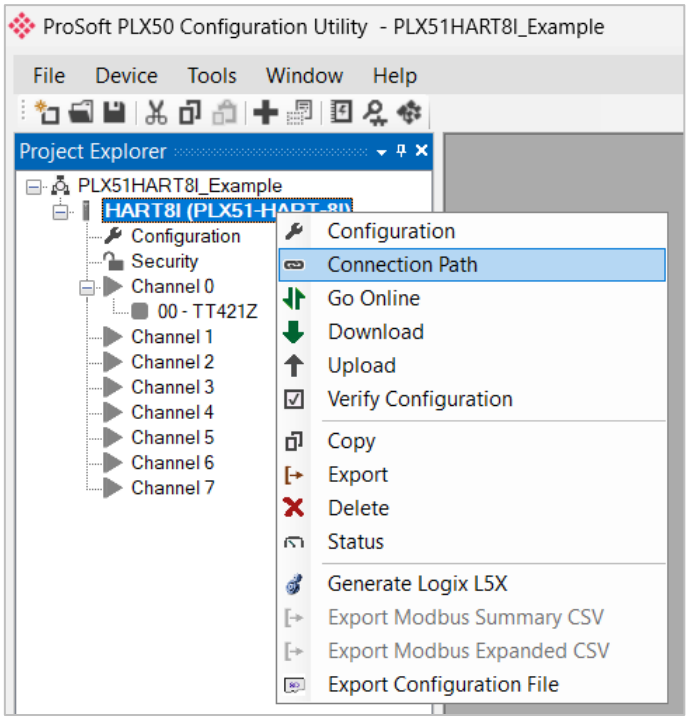


Figure 3.113 - Selecting Connection Path

The new connection path can be entered manually or selected by means of the Target Browser.

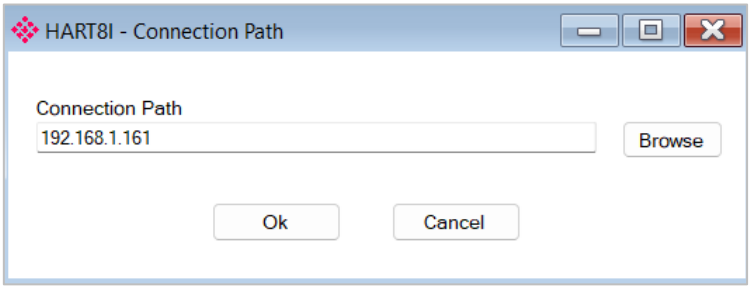


Figure 3.114 - Connection Path

To initiate the download, right-click on the module and select the **DOWNLOAD** option.

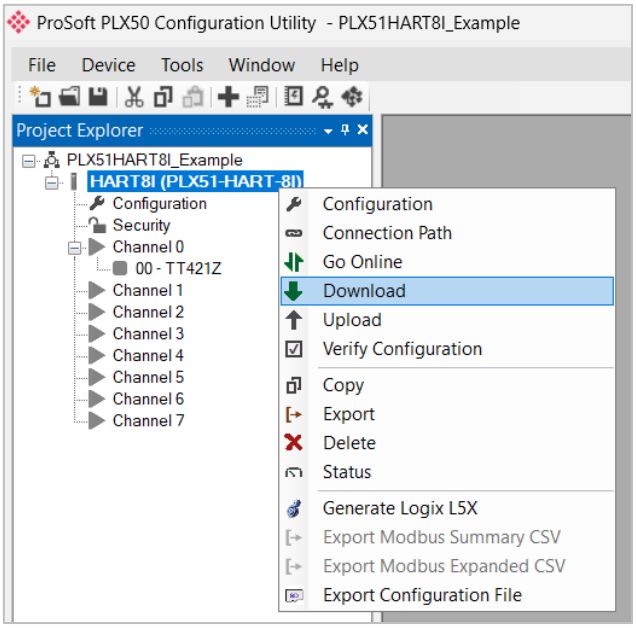


Figure 3.115 - Selecting Download

Once complete, the user will be notified that the download was successful.

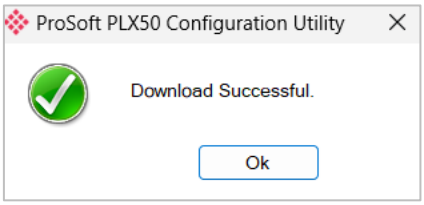


Figure 3.116 - Successful download

Within the PLX50 Configuration Utility environment the module will be in the **Online** state, indicated by the green circle around the module. The module is now configured and will immediately start operating.

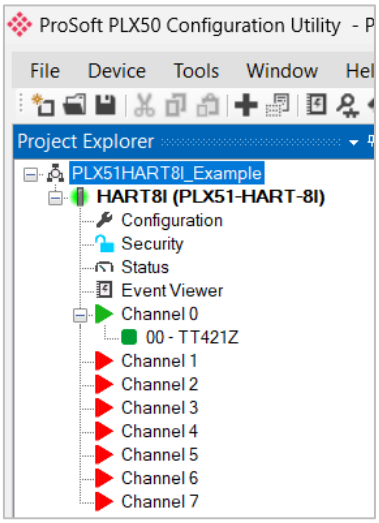


Figure 3.117 - Module online

4 Firmware Update

The PLX51-HART-8I supports in-field firmware upgrading. The latest firmware for the module can be downloaded from www.prosoft-technology.com. The firmware is digitally signed, so only approved firmware can be used.

To firmware upgrade the module:

1 From the *Tools* menu in the PLX50CU, select the **DEVICEFLASH** utility.

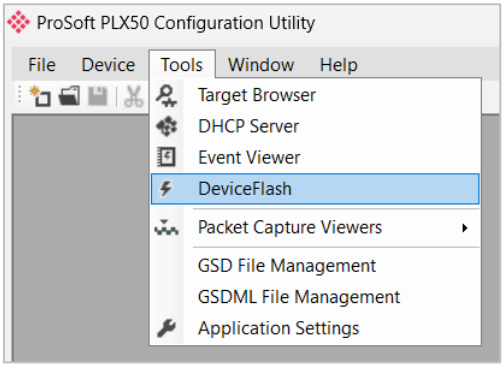


Figure 4.1 – Select DeviceFlash utility from the PLX50CU

2 When the utility opens, the user will be prompted to select the binary file to be used to firmware upgrade the module.

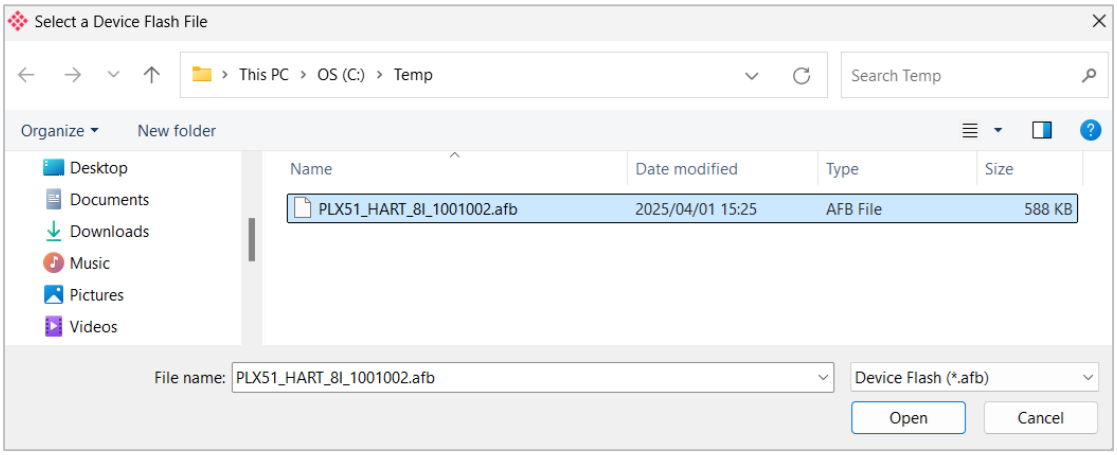


Figure 4.2 – Select the binary file

3 After selecting the file, the user will be prompted to select the device to firmware upgrade on the local network.

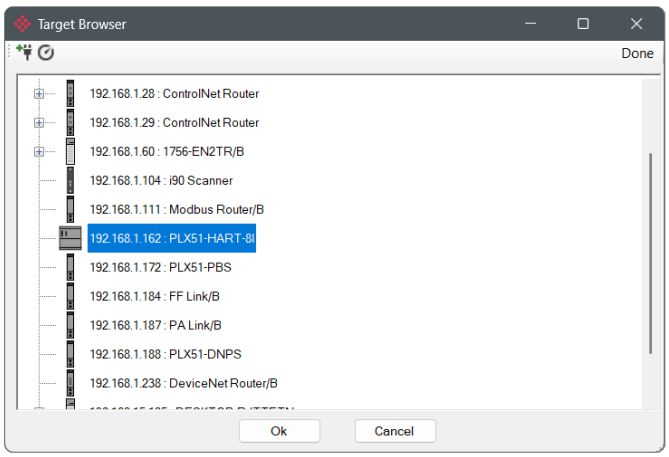


Figure 4.3 – Select the device to be updated

4 The firmware update will take less than 2 minutes to complete.

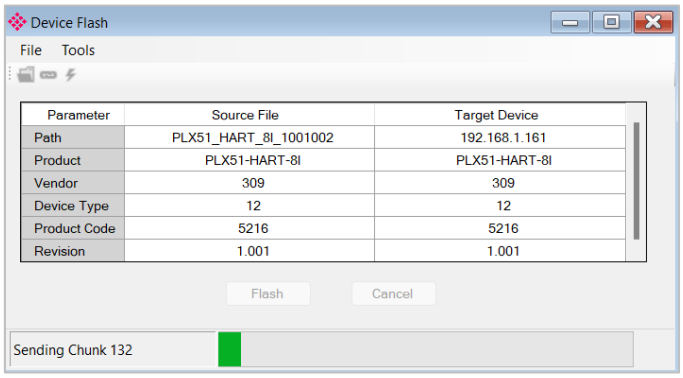


Figure 4.4 – Firmware Update Busy

5 After successful firmware update, the *Target Device* values will display green.

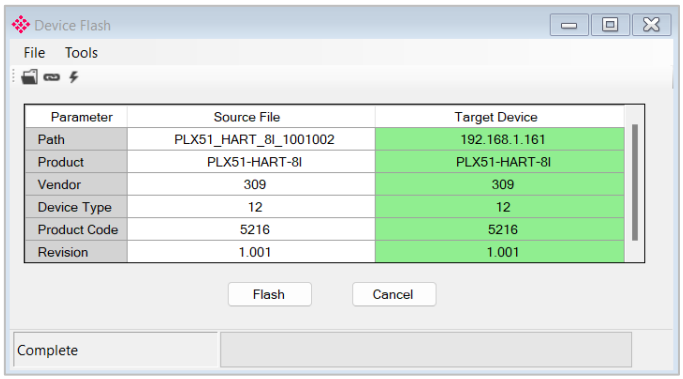


Figure 4.5 – Firmware update successfully completed.

Important: If for any reason the firmware update failed (e.g. power down during the update), then the module will revert to the bootloader. The user can then simply reflash the module again to update it to the latest application firmware.

5 SD Card Recovery

The PLX51-HART-8I supports an SD Card (see below) which can be used for disaster recovery. The SD Card can be pre-loaded with the required firmware, application configuration, and/or network parameters.

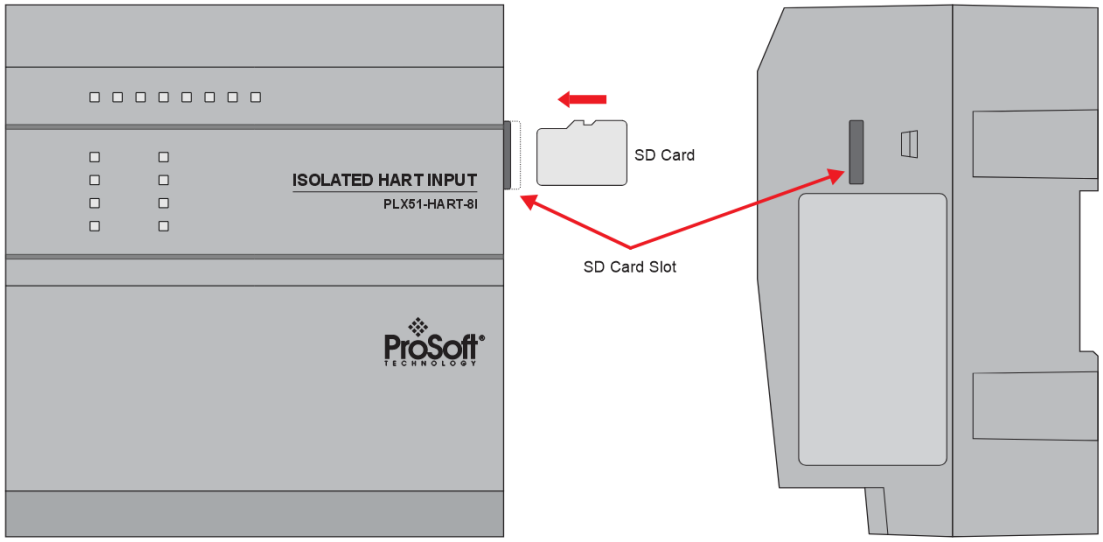


Figure 5.1 – Module Side View – SD Card Slot

Important: The user will need to ensure that the SD Card has been formatted for FAT32.

Important: All necessary files must be copied into the root directory of the SD Card. The module will not use files that are in folders.

5.1 Firmware

The user can copy the required firmware (which can be downloaded from the ProSoft website) onto the root directory of the SD Card.

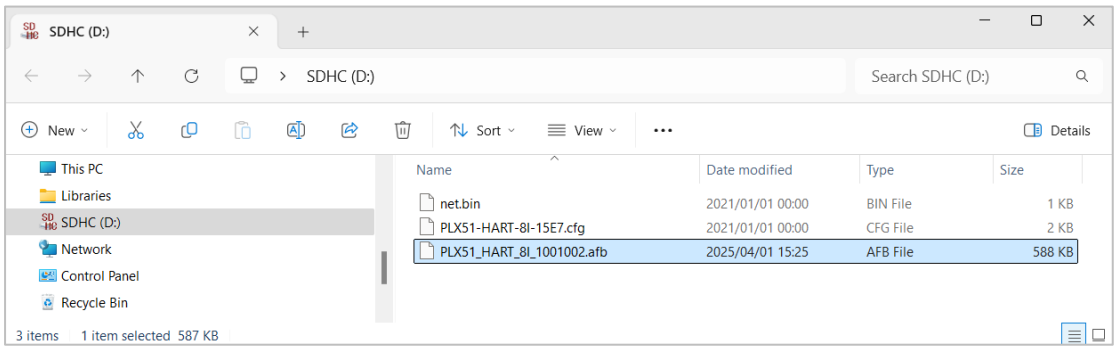


Figure 5.2 – SD Card – Firmware file

Important: The filename of the firmware file must not be changed. The specific module will use only the firmware that is valid (e.g. the PLX51-HART-8I will only use the **PLX51_HART_8I_XXX.afb** firmware file).

Important: If more than one firmware file, with different firmware revisions, of the same product is on the SD Card it can cause the module to constantly firmware upgrade the module.

If a faulty module is replaced, the user can insert the SD Card (loaded with the firmware file) into the new module. While the module is booting it will detect if the firmware on the new module is different from that on the SD Card. If different, the firmware will either be upgraded or downgraded to the firmware revision on the SD Card.

5.2 Configuration

If a PLX51-HART-8I is replaced, the user can insert the SD Card (loaded with the configuration file) into the new module. The new module will determine if the configuration on the SD Card is different than the currently loaded configuration (even when there is no configuration on the module). If different, the configuration on the SD Card will be downloaded into the module's NV memory before the module starts executing. The module OK LED will turn blue when the application configuration is being updated from the SD Card.

The user can add the PLX50CU configuration file to the SD Card root directory in one of two ways.

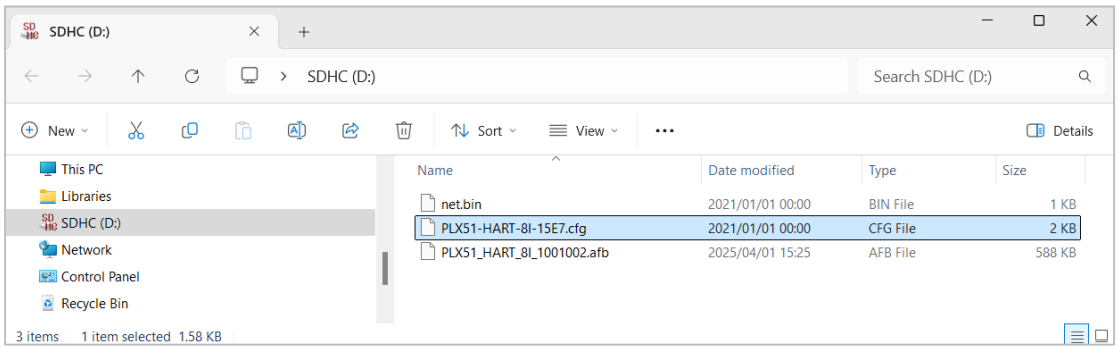


Figure 5.3 – SD Card – Configuration file

5.2.1 Manual Copy

Once the user has created the application configuration needed in the PLX50CU, the configuration can be exported to a file that can be used on the SD Card. Once the file has been created the user can copy this file into the root directory of the SD Card.

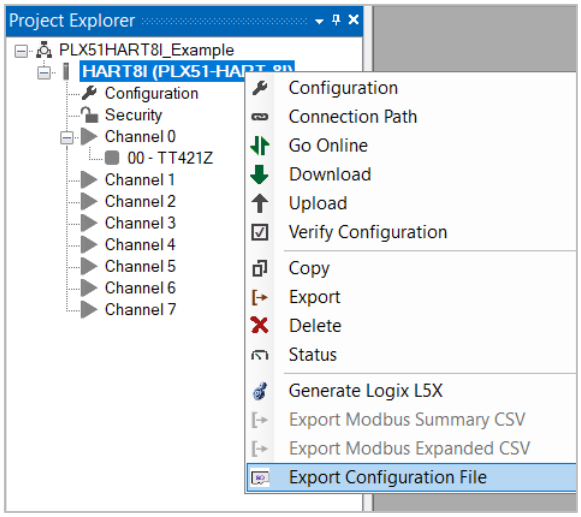


Figure 5.4 – Configuration Export for SD Card

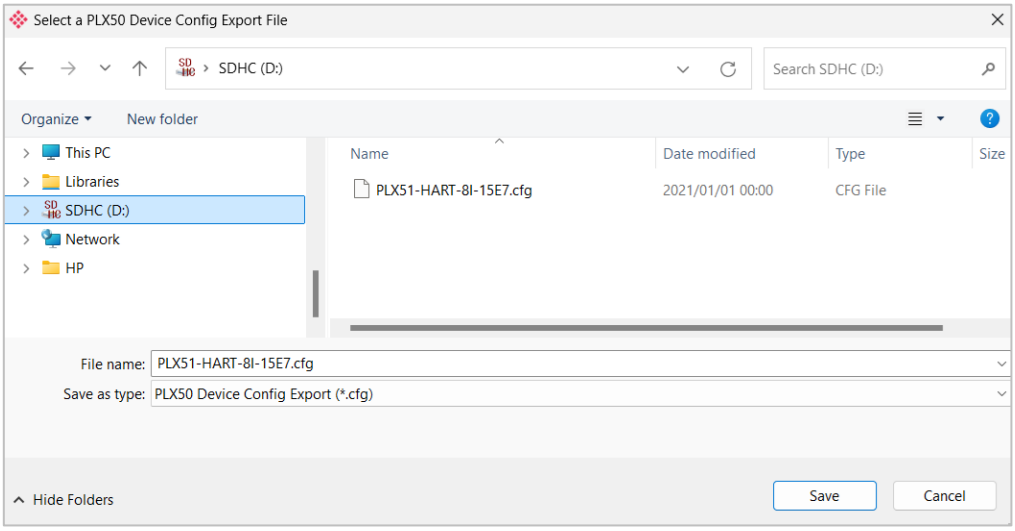


Figure 5.5 – Configuration Export for SD Card

Important: The filename of the configuration file must not be changed. The specific module will use only the configuration that is valid (e.g. the PLX51-HART-8I will only use the PLX51-HART-8I configuration file).

Important: If more than one configuration file, with different configuration signatures, of the same product is on the SD Card then only the last configuration will be used.

5.2.2 PLX50CU Triggered Upload

When the SD Card has been inserted into the PLX51-HART-8I and the user is online with the module in PLX50CU, then the user has the option to directly upload the configuration on to the SD Card using the **SAVE CONFIGURATION TO SD CARD** option. This will copy the configuration that has been downloaded to the module directly to the SD Card without the need to remove it from the module and inserted into a PC.

Important: All other configuration files in the SD Card root directory will be deleted when the upload is done.

Important: The PLX51-HART-8I must boot up with the SD Card inserted, before the **SAVE CONFIGURATION TO SD CARD** option will correctly save the configuration to the SD Card.

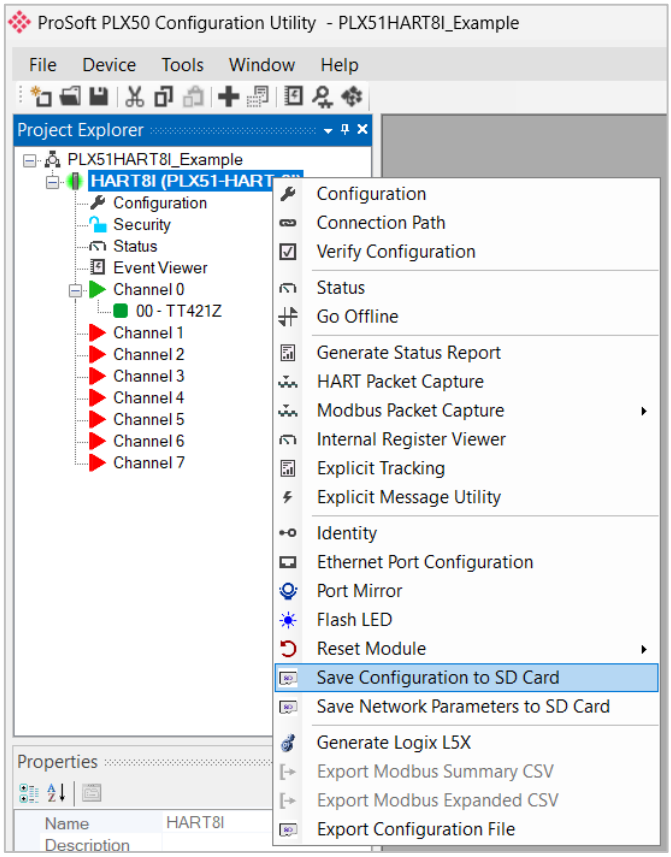


Figure 5.6 – Save Configuration to SD Card

5.3 Network Parameters

If a faulty PLX51-HART-8I is replaced, the user can insert the SD Card (loaded with the network file) into the new module. The new module will determine if the network parameter file on the SD Card is different than the current network parameters in the module. If different, the network parameters on the module will be updated with the network parameters on the SD Card.

The user can add the current module network parameters to the SD Card from the PLX50CU, when using the module. This is done by right-clicking on the module, and selecting **SAVE NETWORK PARAMETERS TO SD CARD**.

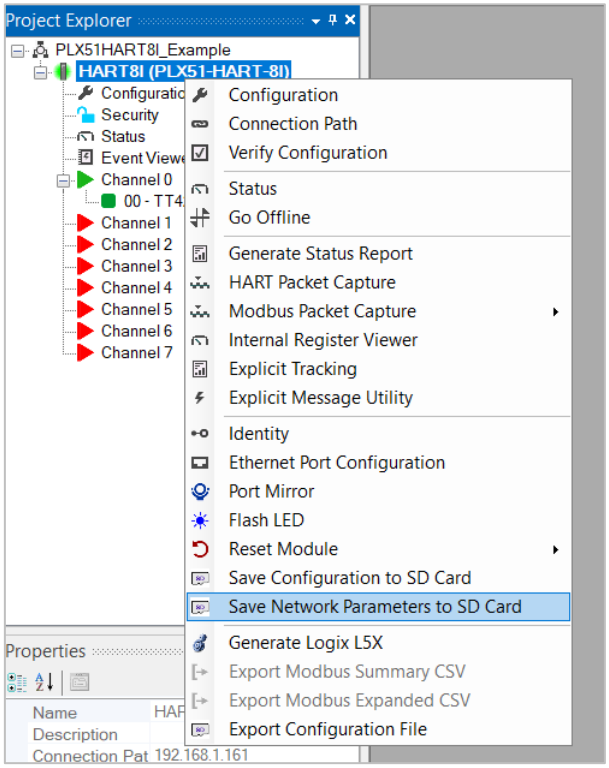


Figure 5.7 – Save Network Parameters to SD Card

6 Security Services

The PLX51-HART-8I supports security services allowing the user to configure various levels of module security.

When security is enabled all EtherNet/IP communication between the PLX50CU and the module is encrypted preventing information from being intercepted by a third party.

Security of the module is configured and downloaded separately to the module's primary (application) configuration and can thus be configured online without affecting the running process.

The security services provide the following features:

- Configurable level of security
- Encrypted EtherNet/IP communication
- Fixed User Roles and Custom Users
- Configurable Password rules
- Login Expiry
- Failed Login Cool-off and Account Disable options
- Configurable Global Services and Custom Ports
- Optional IP Address Access Control List
- Optional MAC Access Control List
- Restrictions on Reset command
- Restrictions on Device Flash options
- Security Audit trail in Event Log

Optional user authentication can be enabled, requiring users to login to the module when connecting. In addition to the fixed role users, (viz. Administrator, Engineer, Operator, Auditor and Viewer) up to 5 custom users can be configured. Each custom user is assigned one of the fixed roles.

Once user authentication has been initialized, only users with Administrator privileges are able to change the security configuration and reset passwords etc.

The allowed privileges for each role are tabulated below:

Privileges / Roles	Admin	Engineer	Operator	Auditor	Viewer	None
System						
Identity Object	✓	✓	✓	✓	✓	✓
Device Flash (Firmware Upgrade)	✓	-	-	-	-	-
Reset Module	✓	✓	-	-	-	-
Change Ethernet Interface Settings	✓	✓	-	-	-	-
Application						
Download/Upload Configuration	✓	✓	-	-	-	-
View Status and Statistics	✓	✓	✓	✓	✓	-
Clear Statistics	✓	✓	✓	-	-	-
Packet Capture	✓	✓	✓	✓	-	-
View Event Log	✓	✓	✓	✓	✓	-
Clear Event Log	✓	-	-	-	-	-
Generate Status Report	✓	✓	✓	✓	-	-
Modbus Pass Through Functions	✓	✓	-	-	-	-
Internal Register Viewer	✓	✓	-	-	-	-
Security						
Download/Upload Security Configuration	✓	-	-	-	-	-
Clear All Security	✓	-	-	-	-	-
View Security Status and Statistics	✓	✓	-	✓	-	-
Clear Security Statistics	✓	-	-	-	-	-
Change Own Password	✓	✓	✓	✓	✓	-
Change Another User's Password	✓	-	-	-	-	-

Table 6.1 – User Role Privileges.

6.1 Securing Process

The process to secure a module involves the following basic steps:

- Set up Security configuration
- Download Security Configuration to the module
- Initialize User Authentication

6.1.1 Configuration

The *Security Configuration* is accessed by right-clicking on the **SECURITY** item in the device tree and selecting the **SECURITY CONFIGURATION** option.

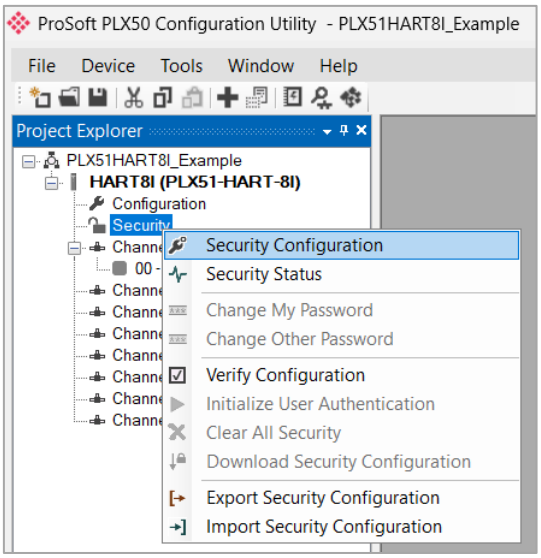


Figure 6.1 – Selecting Security Configuration.

The configuration form will open and display multiple configuration tabs.

6.1.1.1 General Configuration

The *General* configuration tab is shown below.

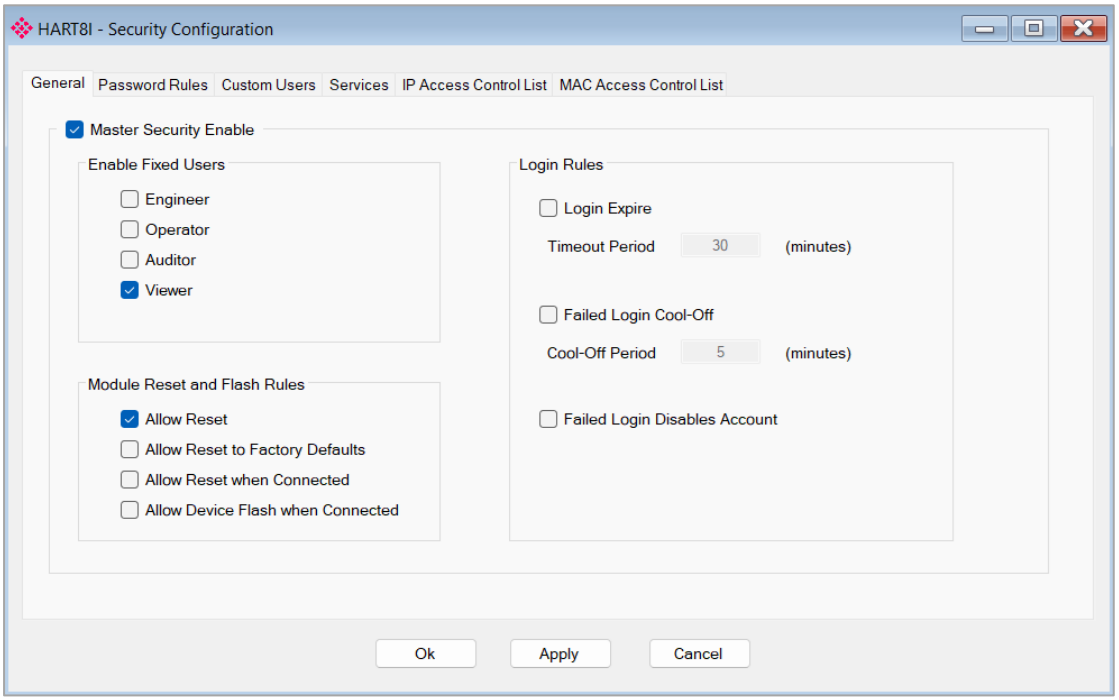


Figure 6.2 – Security Configuration – General.

The *General* configuration tab comprises the following parameters:

Parameter	Description
Master Security Enable	Used to enable or disable the master security. **Note**: If this option is disabled then all Security measures are disabled.
Enable Fixed Users Engineer Operator Auditor Viewer	Allows each of the fixed users to be enabled or disabled. **Note**: The fixed *Administrator* user cannot be disabled.
Module Reset and Device Flash Rules	
Allow Reset	Must be checked to allow any type of Reset via EtherNet/IP.
Allow Reset to Factory Defaults	Must be checked to allow Reset to Factory Defaults (including Reset to Factory Defaults except Communication settings).
Allow Reset when Connected	Must be checked to allow any type of Reset when the module is connected, where connected implies an EtherNet/IP Class 1 connection.
Allow Device Flash when Connected	Must be checked to allow Device Flash when the module is connected, where connected implies an EtherNet/IP Class 1 connection.
Login Rules	
Login Expire	Selecting this option causes all users to be automatically logged-out after the *Login Expire Timeout Period*.
Login Expire Timeout Period	The duration, in minutes, after which all users will be automatically logged-out. **Min**: 1 minute **Max**: 1440 minutes (24 hours)
Failed Login Cool-Off	Selecting this option initiates a Cool-off period after a user has entered an incorrect password 3 times in succession. During the cool off period the user will not be able to login.

	Note: This option, and the *Failed Login Disable Account* option, cannot be simultaneously selected.
Failed Login Cool-Off Period	The Cool-Off duration, in minutes. Once a user has entered an incorrect password 3 times in succession, they would need to wait for this period before they can login again. **Min**: 1 minute **Max**: 1440 minutes (24 hours)
Failed Login Disables Account	Selecting this option causes the user's account to be disabled if they enter an incorrect password 3 times in succession. **Note**: Once the user's account has been disabled, an Administrator would need to reset their password. **Note**: This option, and the Failed Login Cool-Off option, cannot be simultaneously selected. **Note**: This option will not be applicable for the Administrator user account.

Table 6.2 – Security Configuration – General.

6.1.1.2 Password Rule Configuration

The *Password Rules* tab is shown below.

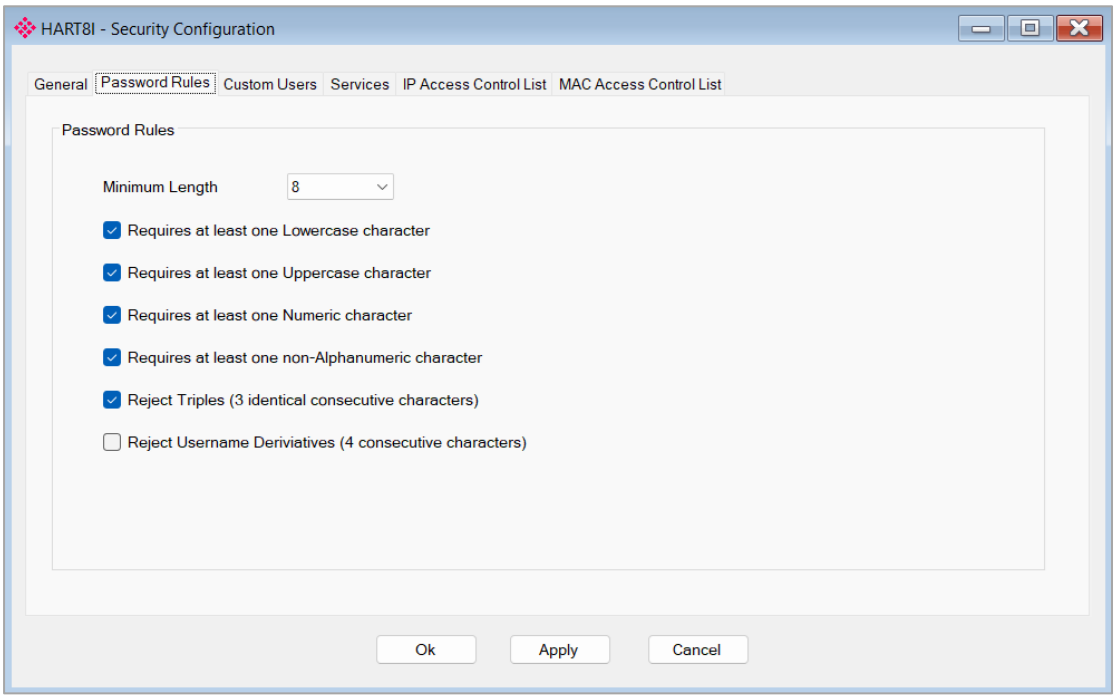


Figure 6.3 – Security Configuration – Password Rules.

The *Password Rules* tab comprises the following parameters:

Parameter	Description
Minimum Length	The minimum number of characters the password must contain. **Min**: 1 **Max**: 32
Requires at least one **Lowercase** character	When selected, all passwords will require at least one lowercase character. e.g. a b c d
Requires at least one **Uppercase** character	When selected, all passwords will require at least one uppercase character. e.g. A B C D
Requires at least one **Numeric** character	When selected, all passwords will require at least one non-alphanumeric character. e.g. 1 2 3 4
Requires at least one **Non-Alphanumeric** character	When selected, all passwords will require at least one non-alphanumeric character. e.g. ! @ # $ %
Reject **Triples**	When selected, all passwords may not contain 3 identical (case-insensitive) consecutive characters. e.g. MyDDDog, strangecCcat.
Reject Username Derivative	When selected, all passwords may not contain any derivative of the respective username. A derivative is defined as any 4 consecutive characters of the password case-insensitive-matching any 4 consecutive characters of the username.

Table 6.3 – Security Configuration – Password Rules

6.1.1.3 Custom Users Configuration

The *Custom Users* configuration tab is shown below.

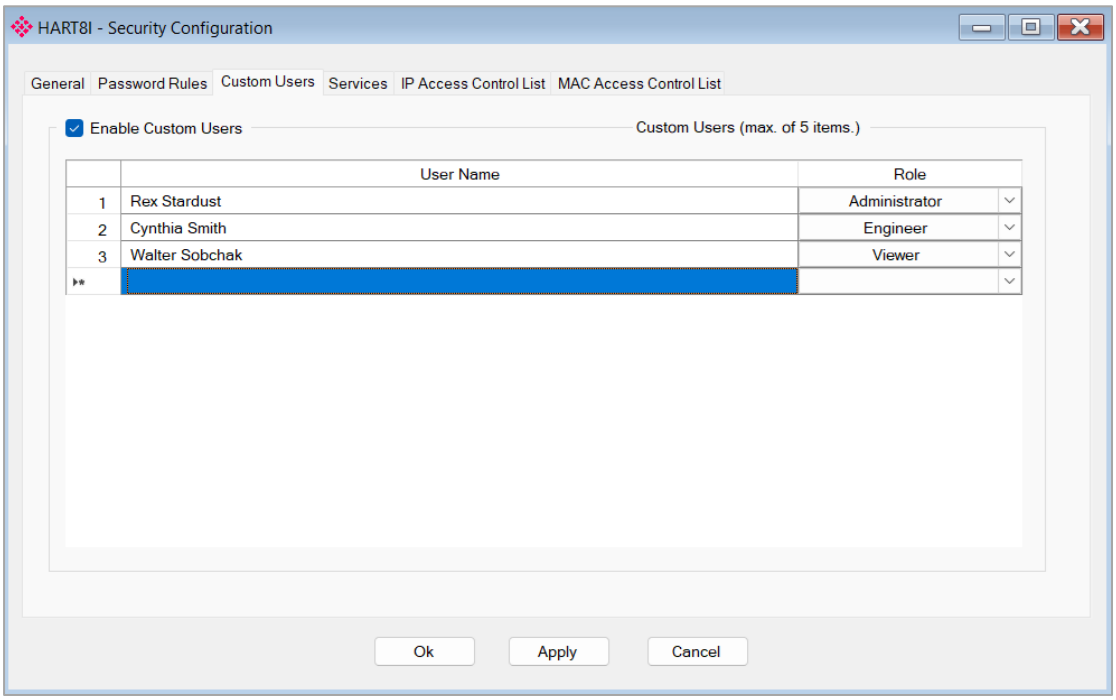


Figure 6.4 – Security Configuration – Custom Users.

The *Custom Users* configuration tab comprises the following parameters:

Parameter	Description
Enable Custom Users	Global Enable / Disable for all Custom Users
User Name	User Name of the Custom User. **Note**: The User Name cannot exceed 32 characters. **Note**: The User Name cannot be the same as any of the fixed roles. (Administrator, Engineer etc.)
Role	The role allocated to this user. Select one of the following: **Administrator** **Engineer** **Operator** **Auditor** **Viewer**

Table 6.4 – Security Configuration – Custom Users.

6.1.1.4 Services Configuration

The *Services* configuration tab is shown below.

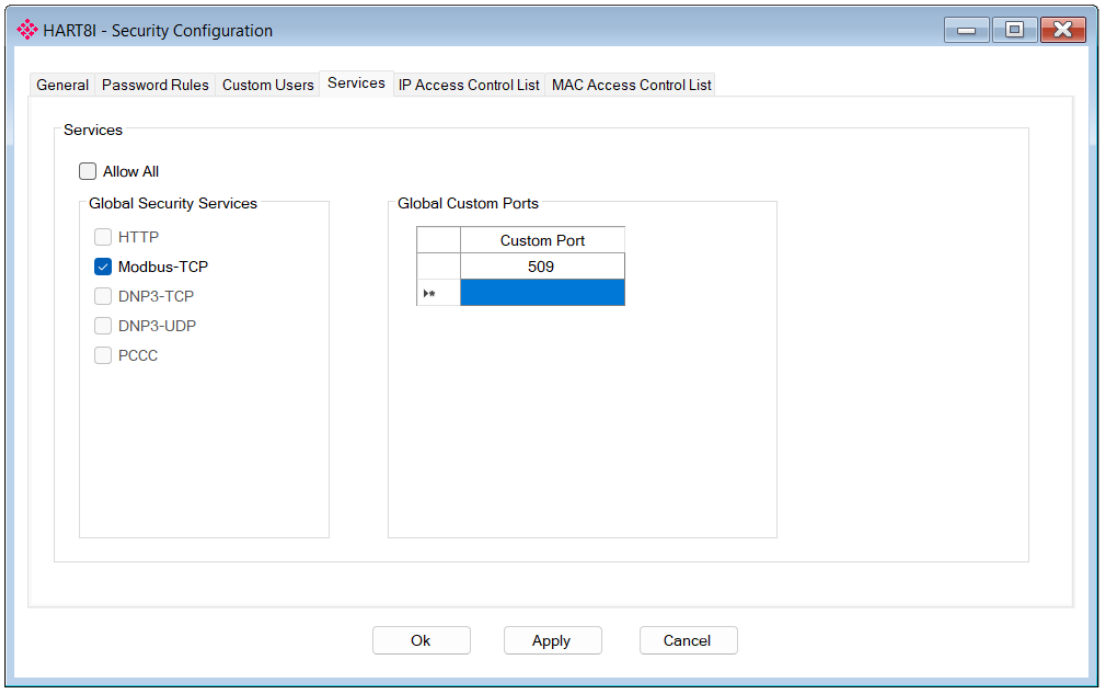


Figure 6.5 – Security Configuration – Services.

The *Services* configuration tab comprises the following parameters:

Parameter	Description
Allow All	When selected all services are allowed by default.
Modbus-TCP	Allow Modbus-TCP connections to be accepted.
Custom Ports	Up to 4 custom (TCP / UDP) ports can be added to the allowed list. **Note:** When the application is using non-standard ports for communication services (e.g. Modbus TCP) then these ports will need to be added to the *Custom Ports* list.

Table 6.5 – Security Configuration – Services

6.1.1.5 IP Access Control List Configuration

Enabling the *IP Access Control List* will block all communication from PCs (and other devices) unless their IP addresses are explicitly included in the list with the allowed services.

The *IP Access Control List* configuration tab is shown below.

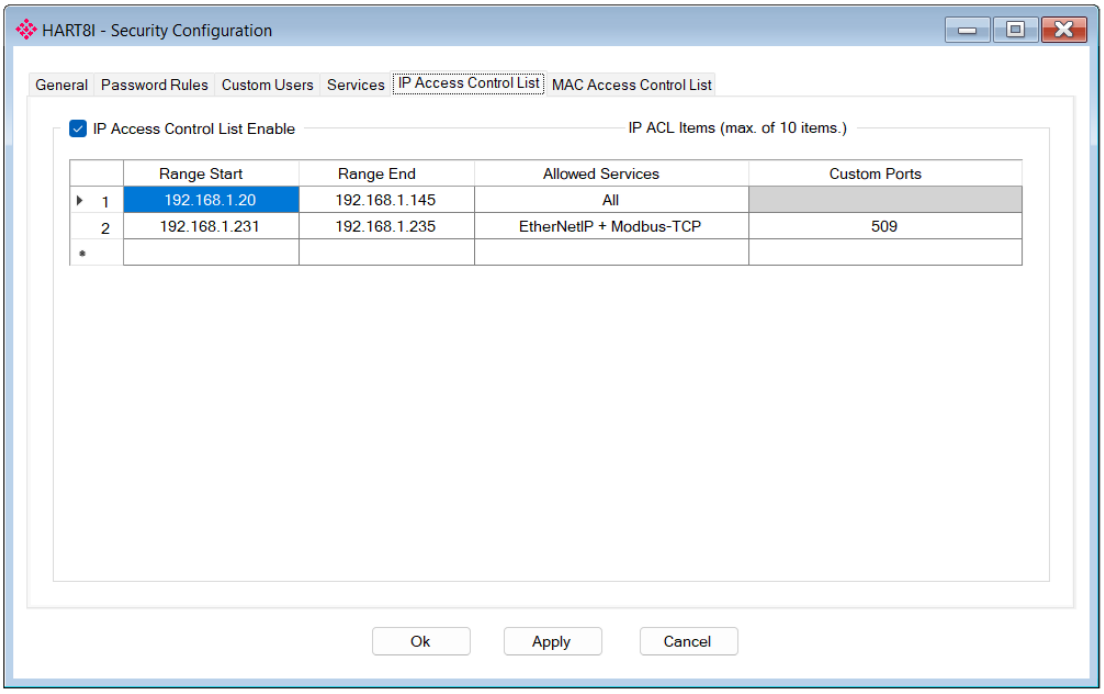


Figure 6.6 – Security Configuration – IP Access Control List.

The *IP Access Control List* configuration tab comprises the following parameters:

Parameter	Description
IP Access Control List Enable	Enable / Disable for all *IP Access Control List*
IP Access Control List	
Range Start	First IP address in the range.
Range End	Last IP address in the range.
Allowed Services	The services allowed for this IP range.
Custom Ports	Additional custom ports allowed for this IP range.

Table 6.6 – Security Configuration – IP Access Control List.

To modify the *Allowed Services* the user can either click on the specific **ALLOWED SERVICE** cell, or right-click on the specific row and select the **EDIT SERVICES** option.

The *Service Selection* form will open allowing the user to select each service's checkbox.

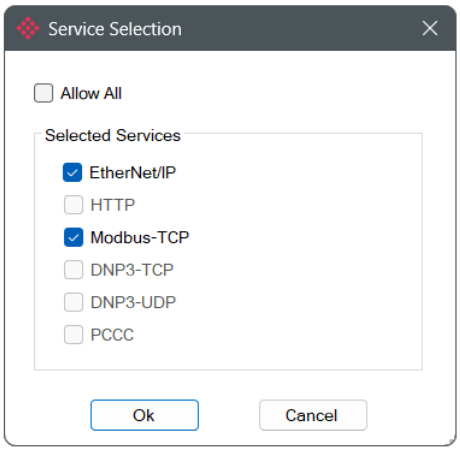


Figure 6.7 – Security Configuration – Service Selection.

To modify the *Custom Ports* the user can either click on the specific **CUSTOM PORTS** cell, or right-click on the specific row and select the **EDIT CUSTOM PORTS** option.

Note: The *Custom Ports* option is not available if the *Allow All* option has been selected in the *Allowed Services*.

The *Custom Ports Selection* form will open allowing the user to modify the *Custom Ports*.

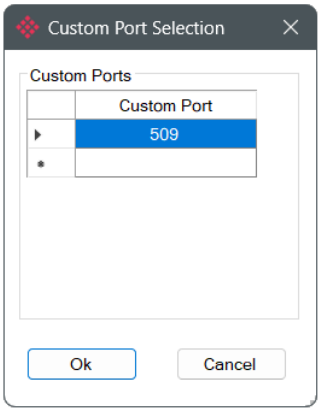


Figure 6.8 – Security Configuration – Custom Ports.

6.1.1.6 MAC Access Control List Configuration

Enabling the *MAC Access Control List* will block all communication from PCs (and other devices) unless their MAC addresses are explicitly added to the list.

Important: Incorrectly configuring the MAC Access Control List may result in the module no longer being able to communicate with the PLX50CU.

The *MAC Access Control List* configuration tab is shown below.

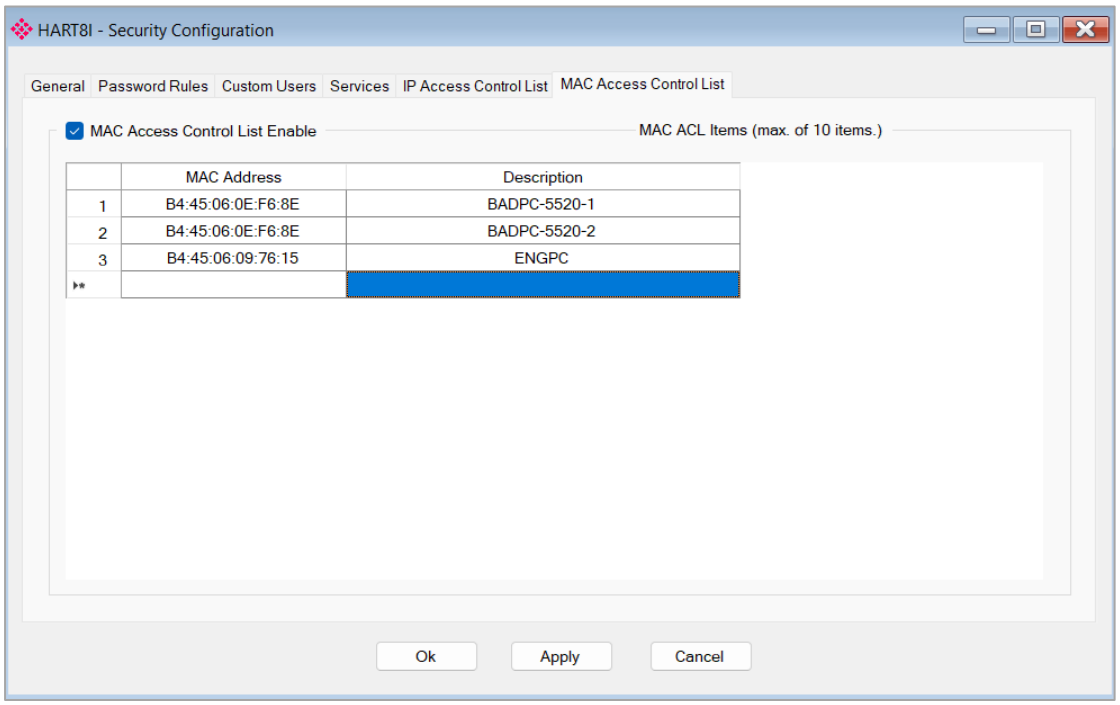


Figure 6.9 – Security Configuration – MAC Access Control List.

The *MAC Access Control List* configuration tab comprises the following parameters:

Parameter	Description
MAC Access Control List Enable	Enable / Disable for all MAC Access Control List
MAC Access Control List	
MAC Address	The MAC address which will be allowed to communicate with the module.
Description	An optional description for the Device with the matching MAC address.

Table 6.7 – Security Configuration – MAC Access Control List.

The MAC addresses can be entered manually, or the user can right-click and select the **BROWSE** option.

This will open the *Network Interface Browser* displaying all the network interfaces and their corresponding MAC addresses found on the local PC. The user can then select which MAC addresses to be added to the *MAC Access Control List*.

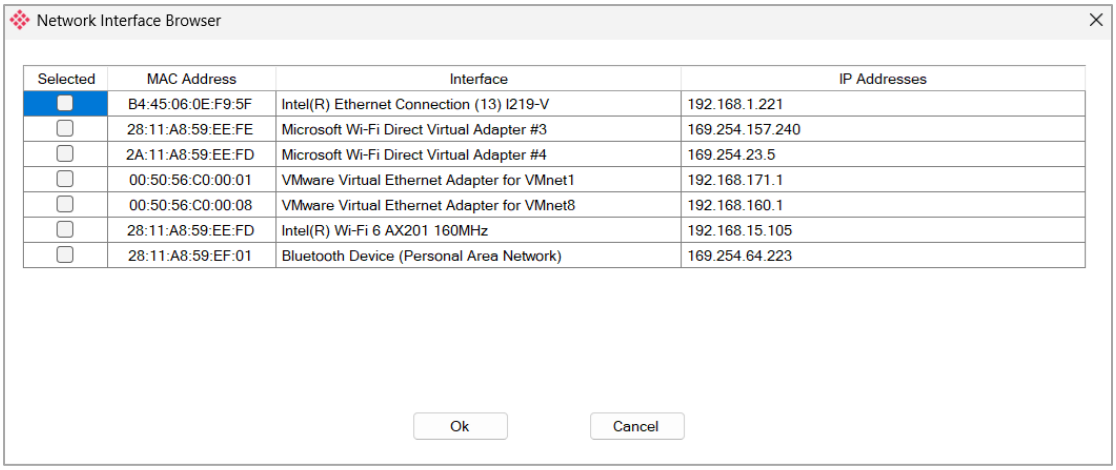


Figure 6.10 – Security Configuration – Network Interface Browser.

6.1.2 Download Security Configuration

Once the security configuration has been completed it must be downloaded to the module.

When online with the module, the current state of the security will be indicated by the icon of the Security node in the project tree as follows:

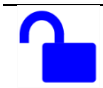
Icon	Description
	Module Offline – Master Security Disabled
	Module Offline – Master Security Enabled
	Module Online – No Security Configuration Downloaded
	Module Online – Master Security Disabled
	Module Online – Master Security Enabled, User Authentication Uninitialized
	Module Online - Secured

Table 6.8 – Security Status Icons.

To download the security configuration right-click on the Security item in the project tree and select the **DOWNLOAD SECURITY CONFIGURATION** item.

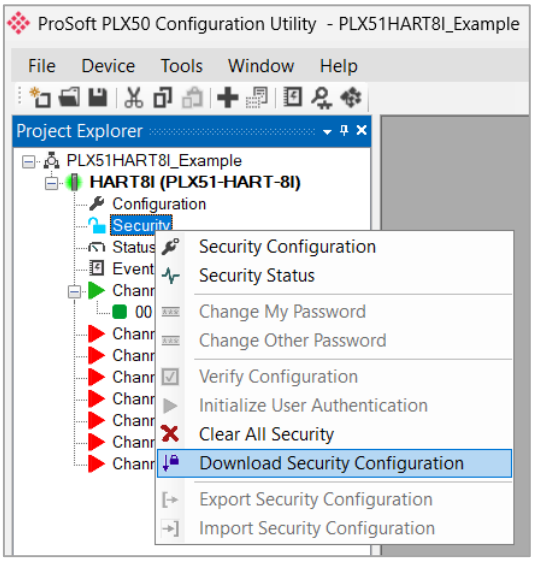


Figure 6.11 – Download Security Configuration

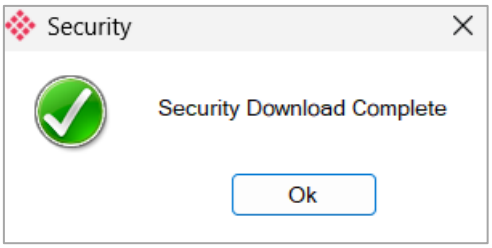


Figure 6.12 – Download Security Configuration Complete

6.1.3 Initialize User Authentication

The final step in securing the module is to initialize user authentication. This involves creating an Administrator password as well as setting the Default password to be used by all other users for their initial login.

Right-click on the **SECURITY** node in the project tree and select the **INITIALIZE USER AUTHENTICATION** option.

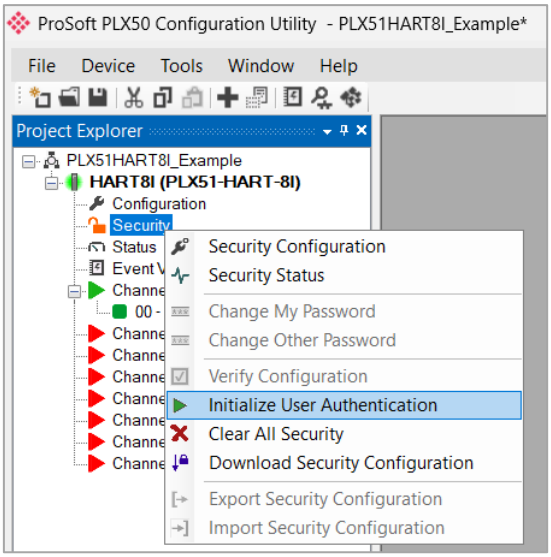


Figure 6.13 – Initialize User Authentication.

The user (now deemed to be the Administrator) will need to configure a password for the fixed *Administrator* user.

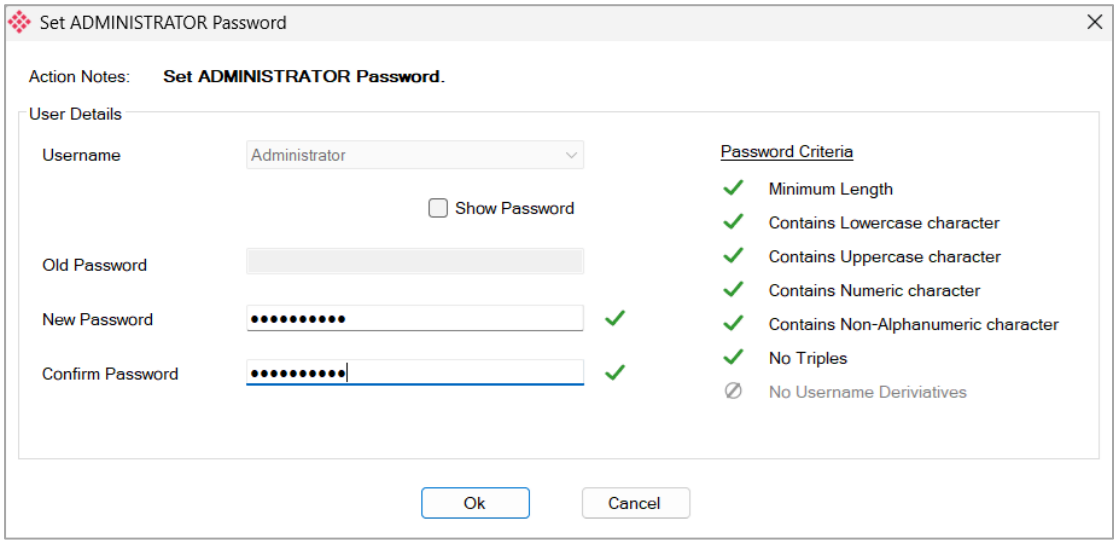


Figure 6.14 – Set Administrator Password.

As the new password is entered, it will be checked against the configured password rules. The icons adjacent to each password rule will indicate if the criteria are fulfilled or not, or not applicable, as shown below:

Icon	Description
	Criteria Not Applicable
	Failed Criteria
	Passed Criteria

Table 6.9 – Password Rule Status Icons.

A green tick icon will be displayed to the right of the *New Password* once it meets all the password criteria. A green tick adjacent to the *Confirm Password* will indicate that it matches the *New Password*.

The entered passwords can either be displayed or masked by clicking on the **SHOW PASSWORD** check box.

Once the Administrator password has been set, then the *Default* password must be set.

The *Default* password is the password to be used by all other users for their initial login.

The *Default* password is configured in similar manner and must also comply with the configured password rules.

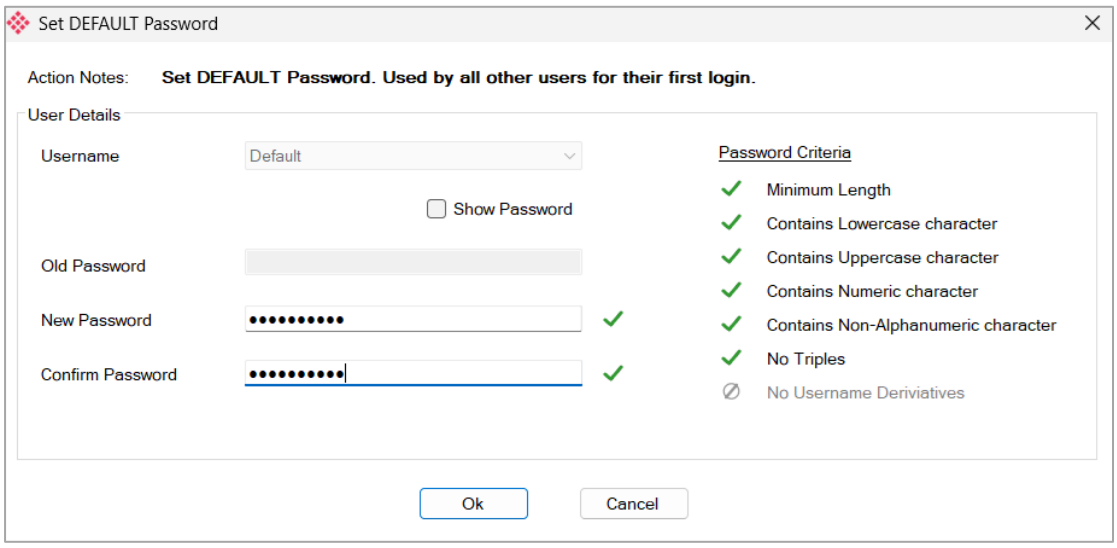


Figure 6.15 – Set Default Password.

Note: If required, the Administrator can change the default password individually for each user, by using the **CHANGE OTHER PASSWORD** option.

On completion of the *User Authentication Initialization* step, the module will be secured indicated by the green locked icon.

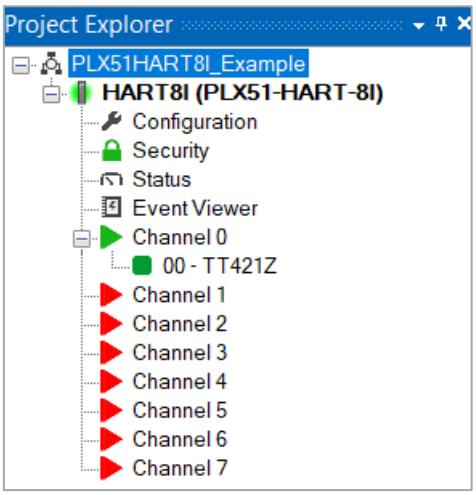


Figure 6.16 – Secured Module.

6.2 Operation

To interact with a secure and user initialized module, each user will need to log in.

6.2.1 Initial User Login

Similar, to an unsecured module, a user would open the existing PLX50CU project, right-click on the module, and select **GO ONLINE**.

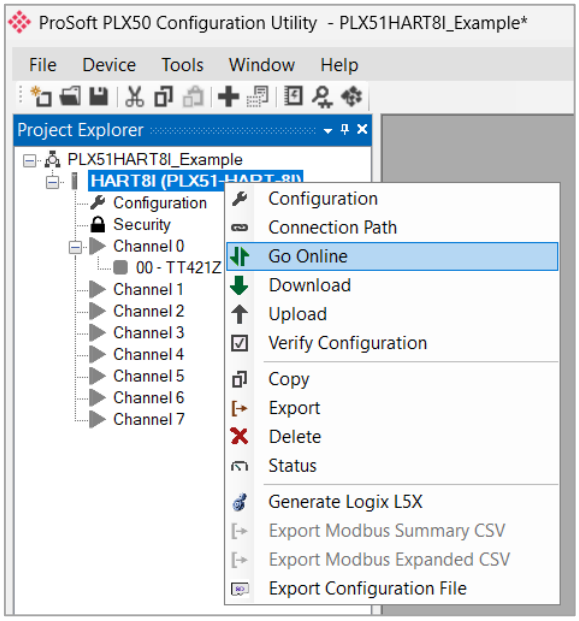


Figure 6.17 – Go Online.

Since the module has been secured, it will then prompt the user to login.

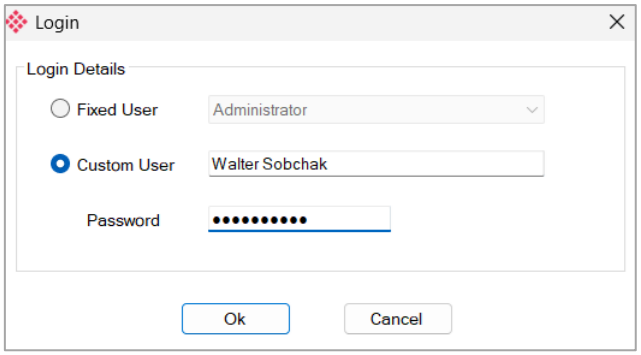


Figure 6.18 – Custom User Login.

The user will need to select either one of the **FIXED USERS** or select the **CUSTOM USER** option and then enter the Custom Username.

The user will then need to enter their password.

Should this be the initial login with the Default password, or if the Administrator has reset the password and selected the option for the user to change the password, then the Set Password form will open. The user will then need to set an appropriate password before continuing.

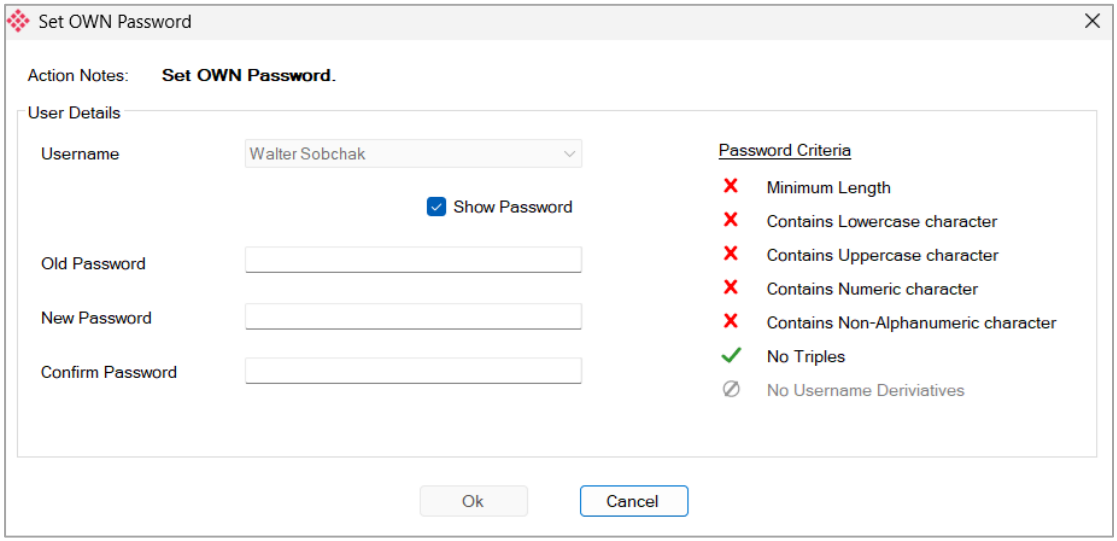


Figure 6.19 – Change Own Password

Note: The *Old Password* that needs to be entered on the Initial User Login, will be the same password that was used to login.

All users are permitted to change their password at any time by right-clicking on the **SECURITY** node in the project tree and selecting the **CHANGE MY PASSWORD** option.

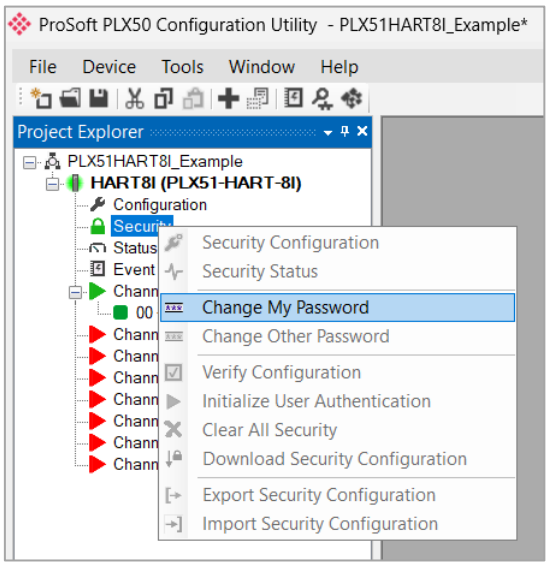


Figure 6.20 – Select Change My Password

6.2.2 Role Specific Operations

Users with *Administrator*, *Engineer* and *Auditor* roles are permitted to access additional functions not available by other users.

6.2.2.1 Security Status

The *Security Status* can be viewed by right-clicking on the **SECURITY** node in the project tree and selecting the **SECURITY STATUS** option.

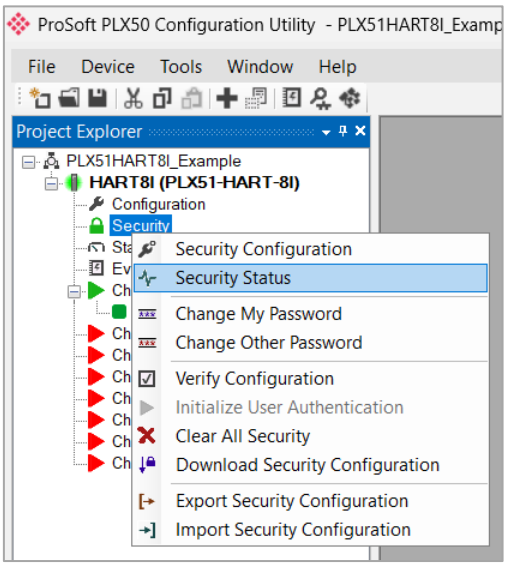


Figure 6.21 – Select Security Status.

The *Security Status* window will open displaying various statistics regarding the security services.

The *General* tab displays an overview of the security status.

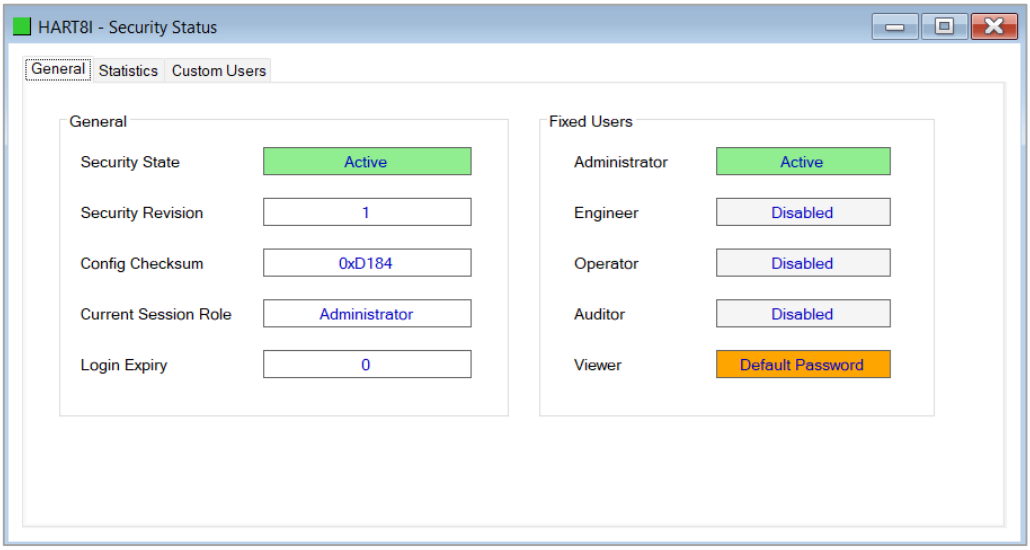


Figure 6.22 – Security Status – General.

The *General* status tab displays the following:

Parameter	Description
General	
Security State	The status of the security services. **No Config**: No security configuration has been downloaded to the module. **Disabled**: Security configuration has been downloaded to the module, but the master *Enable Security* option in the configuration has been disabled. **Uninitialized**: The security configuration has been downloaded and enabled, but the *Initialize User Authentication* step has not yet been completed. **Active**: The module has been successfully secured.
Security Revision	The revision of the security services currently running on the module. This is a function of the module's firmware revision.
Config Checksum	The checksum of the current security configuration.
Current Session Role	The role assigned to the user that is currently logged in.
Login Expiry	The time (seconds) until the user is automatically logged out. Only applicable if the **LOGIN EXPIRE** option has been enabled in the security configuration.
Fixed Users	
Fixed Users Status Administrator Engineer Operator Auditor Viewer	The status of each fixed user. **Disabled**: The user has not been enabled in the security configuration. **Default Password**: The user has not changed from their Default assigned password, or from when an Administrator reset their password. **No Password**: No password exists for the user. This would typically occur when a fixed user is enabled after the *User Authentication Initialization* step has taken place. An Administrator would need to reset the password for this specific user. **Active**: The user is enabled and has a valid password configured.

Table 6.10 – Security Status – General

The *Statistics* tab displays several security service statistics.

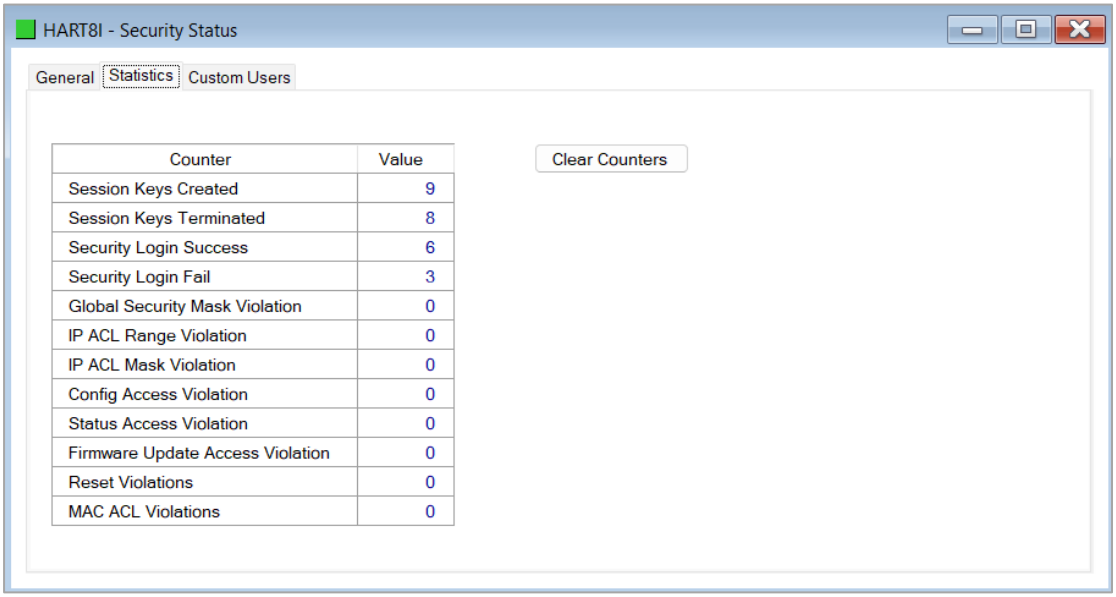


Figure 6.23 – Security Status – Statistics.

Note: Only an Administrator is permitted to select the **CLEAR COUNTERS** option.

Parameter	Description
Session Keys Created	The number of security session keys created between the configuration software and the module. Each time a user connects to the module with the configuration software, and the module has been secured, a new session key will be created.
Session Keys Terminated	The number of times when either the connection from the configuration software has been terminated or there was an error in the connection decryption. In both these cases the session keys will be deleted.
Security Login Success	The number of successful logins.
Security Login Fail	The number of failed login attempts.
Global Security Mask Violation	The number of times a connection request is received from another device on the Ethernet network, which has not been enabled in the module's global security mask configuration.
IP ACL Range Violation	Each time a request or packet is received from a device that has an IP address outside the IP ACL range, this number will be incremented.
IP ACL Mask Violation	Each time a request or packet is received from a device that has an IP address outside the Subnet ACL range, this number will be incremented.
Config Access Violation	The number of times a connection with the incorrect role privileges tried to access the module security configuration.
Status Access Violation	The number of times a connection with the incorrect role privileges tried to access the module security status.
Firmware Update Access Violation	The number of times an attempt to flash upgrade the module in an incorrect state (e.g., while running a class 1 EtherNet/IP connection).
Reset Violations	The number of times an attempt to reset the module in an incorrect state (e.g., while running a class 1 EtherNet/IP connection).
MAC ACL Violations	Each time a request or packet is received from a device that does not have a matching MAC address to those in the MAC ACL list, this number will increase.

Table 6.11 – Security Status – Statistics

The *Custom Users* status tab displays the following:

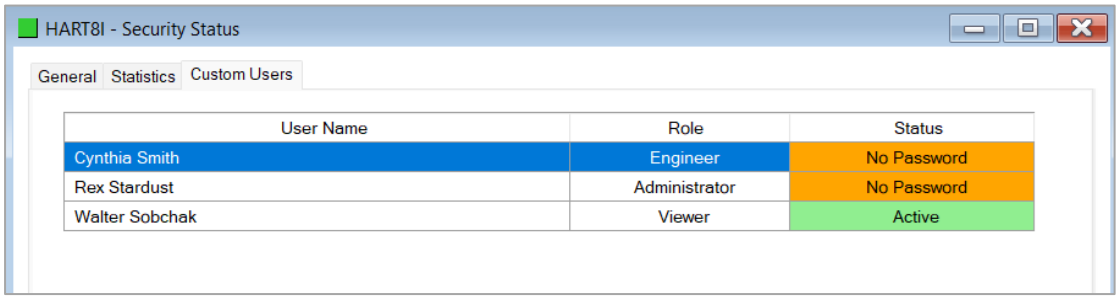


Figure 6.24 – Security Status – Custom Users

Parameter	Description
User Name	The configured user name.
Role	The configured role for this specific user.
Status	The status of the specific user: **Default Password**: The user has not changed from their Default assigned password, or from when an Administrator reset their password. **No Password**: No password exists for the user. This would typically occur when a user is added after the User Authentication Initialization has taken place. An Administrator would need to reset the password for this specific user. **Active**: The user is enabled and has a valid password configured.

Table 6.12 – Security Status – General

6.2.3 Change Other Password

An Administrator can change (or reset) any user's password by right-clicking on the **SECURITY** node in the project tree and selecting the **CHANGE OTHER PASSWORD** option.

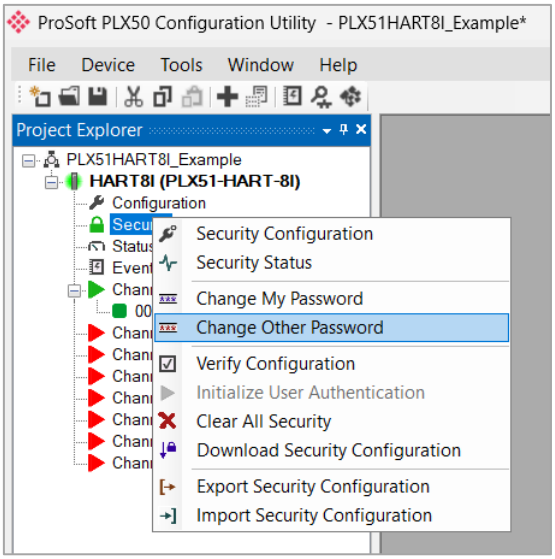


Figure 6.25 – Select Change Other Password.

The *Set Password* form will open, and the Administrator can then select the User's password to change. The Administrator will need to re-enter their password as well as the new password for the user.

The **REQUIRE USER TO CHANGE PASSWORD** option requires that user to change the password the next time they login.

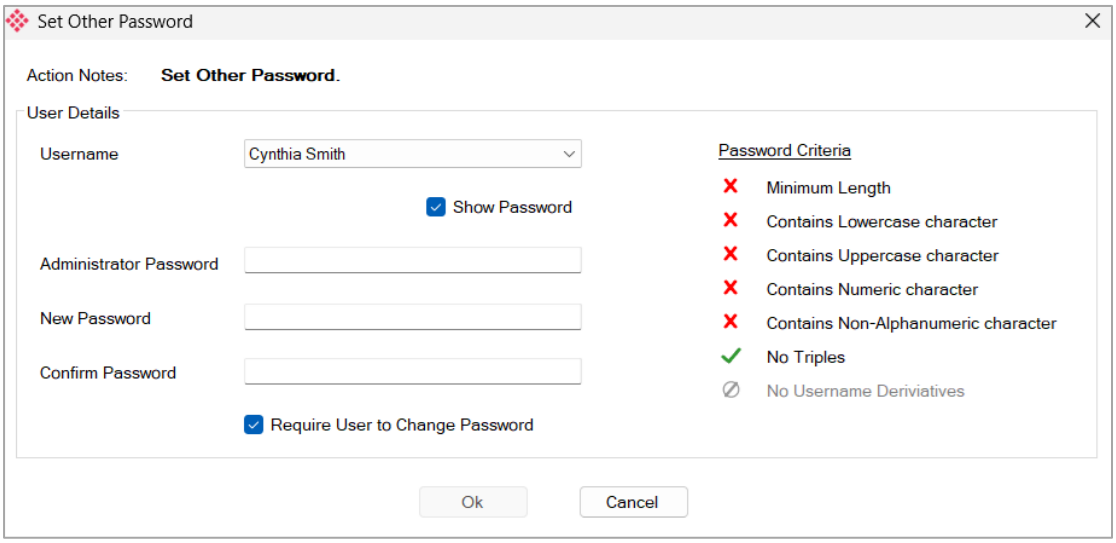


Figure 6.26 – Set Other Password.

6.2.4 Clear All Security

An Administrator can remove all the security from a module and return it to an unsecured state. This is done by right-clicking on the **SECURITY** node in the project tree and selecting the **CLEAR ALL SECURITY** option.

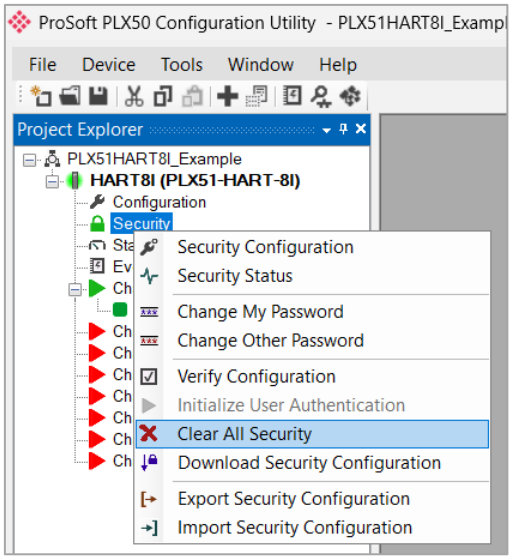


Figure 6.27 – Select Clear All Security.

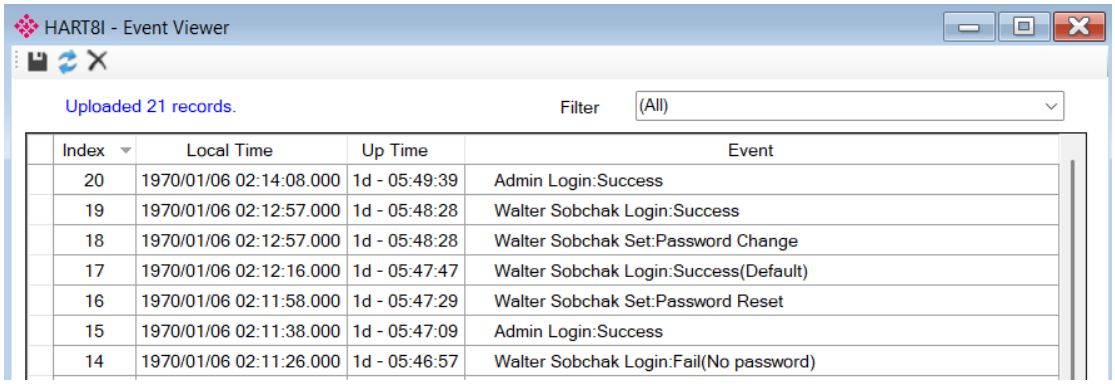
This action will require the Administrator to enter their password. The security configuration and all passwords will be removed with this action.

Important: This process will remove all module security configuration including all passwords.

6.3 Event Log

All security related events are added to the module's event log.

Note: Only an Administrator is permitted to select the *Clear* the event log option.



Index	Local Time	Up Time	Event
20	1970/01/06 02:14:08.000	1d - 05:49:39	Admin Login:Success
19	1970/01/06 02:12:57.000	1d - 05:48:28	Walter Sobchak Login:Success
18	1970/01/06 02:12:57.000	1d - 05:48:28	Walter Sobchak Set:Password Change
17	1970/01/06 02:12:16.000	1d - 05:47:47	Walter Sobchak Login:Success(Default)
16	1970/01/06 02:11:58.000	1d - 05:47:29	Walter Sobchak Set:Password Reset
15	1970/01/06 02:11:38.000	1d - 05:47:09	Admin Login:Success
14	1970/01/06 02:11:26.000	1d - 05:46:57	Walter Sobchak Login:Fail(No password)

Figure 6.28 – Event Log.

6.4 Reset Security Configuration

The PLX51-HART-8I's security configuration can be reset (cleared) by powering-up the module with DIP switches 2, 3, and 4 set to the **ON** position.

Important: This process will remove all module application configuration and security configuration including all passwords.

Note: Once the module has booted-up, the DIP switches should be returned to normal (all OFF). New security configuration cannot be downloaded with the Reset DIP switch combination active.

7 Device Type Manager (DTM)

The PLX51-HART-8I supports FDT / DTM technology, allowing the user to configure any HART device using its DTM (Device Type Manager) in any standard FDT Frame (Field Device Tool).

To use a device DTM with the PLX51-HART-8I, the *Prosoft Technology PLX51 ILX56 HART and Profibus DTM pack* must first be installed. It can be downloaded from www.prosoft-technology.com.

7.1 Installation

Installation of the DTM pack is achieved by executing the following installer:
Prosoft Technology PLX51 ILX56 HART and Profibus DTM Pack1.009 Setup.msi

The installation wizard will guide the user through the installation process.

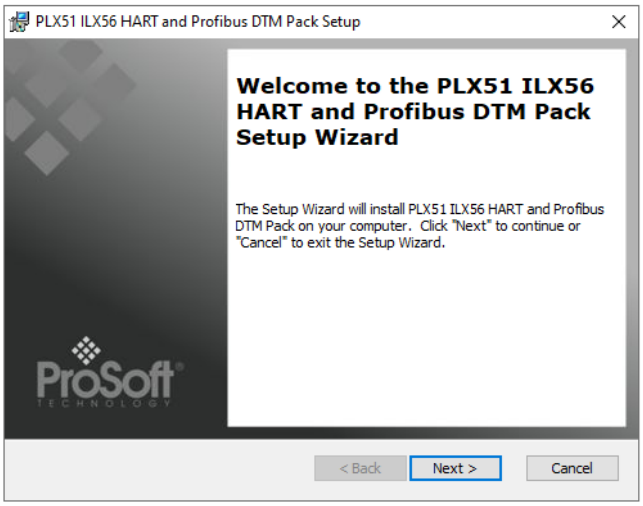


Figure 7.1 – DTM Pack Installation

7.2 Configuration

Once the DTM pack is installed, the selected FDT Frame will need its DTM Catalogue updated. The steps required for this action are slightly different for each FDT frame. Typically, one selects the **DTM CATALOGUE** or **DEVICE CATALOGUE** and then selects **REFRESH** or **REBUILD**.

After the catalogue has been updated, a new project can be created using the PLX51-HART-8I DTM.

7.2.1 PLX51-HART-8I DTM

To use the PLX51-HART-8I DTM in a new project, select the **ADD DEVICE** function and then select the **PLX51-HART-8I DTM**. The example below makes use of PACTware FDT frame.

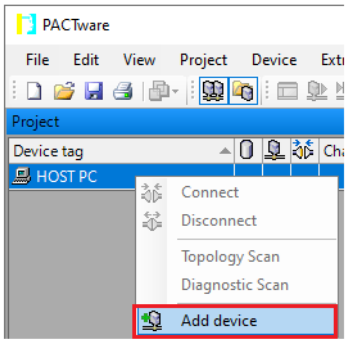


Figure 7.2 – Adding new device

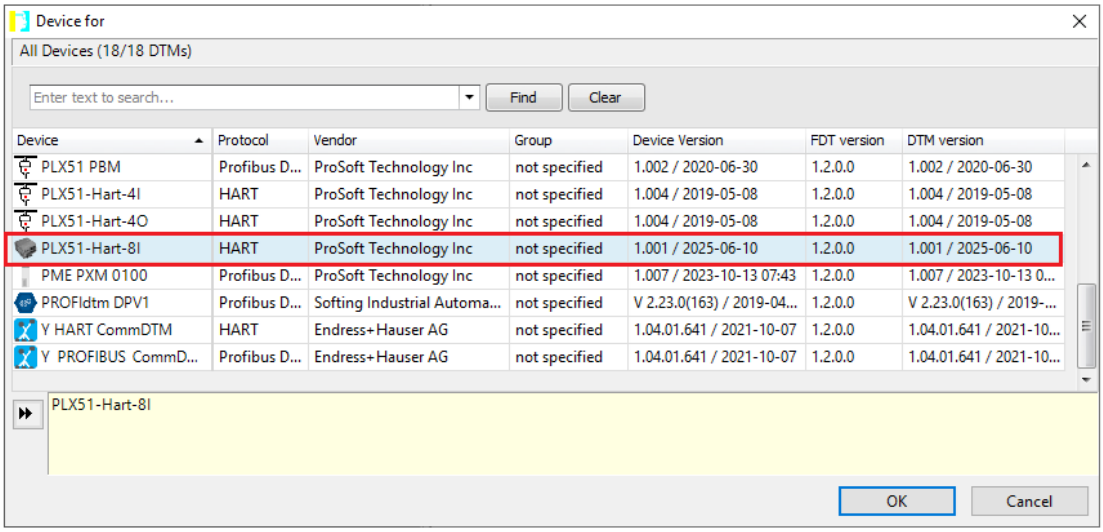


Figure 7.3 – Selecting PLX51-HART-8I DTM

After installing the PLX51-HART-8I DTM, select the **PARAMETER** option.

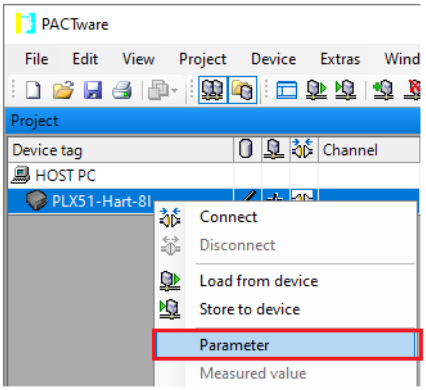


Figure 7.4 – Select Parameter option

The PLX51-HART-8I DTM's configuration allows the CIP Path to the PLX51-HART-8I to be configured. This is typically the IP address of the PLX51-HART-8I, but can include a more complex CIP path when, for example, routing through a ControlLogix chassis is required.

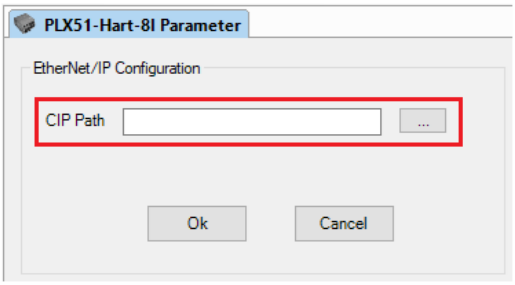


Figure 7.5 – PLX51-HART-8I CIP Path

The path can either be entered manually or the **BROWSE** "**…**" button can be used to open the *Target Browser* to select the PLX51-HART-8I.

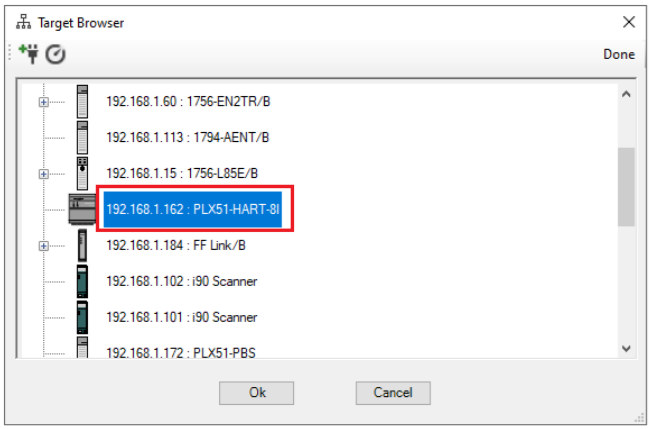


Figure 7.6 – Target Browser

The PLX51-HART-8I DTM is now ready for device DTMs to be added under it.

7.2.2 Adding Device DTMs

After the PLX51-HART-8I DTM has been configured, the child Device DTMs can be added by right-clicking on the PLX51-HART-8I DTM and selecting **ADD DEVICE**.

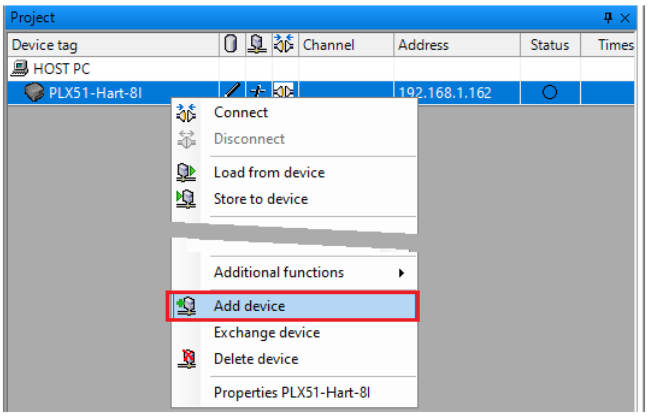


Figure 7.7 – Add child device

The user can then select the matching device DTM.

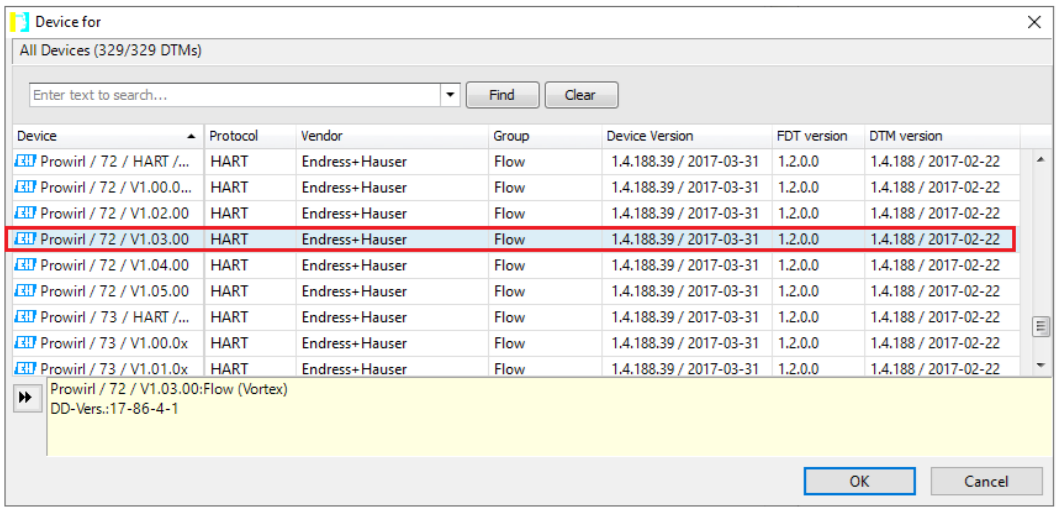


Figure 7.8 – Device DTM Selection

Once the child device has been selected, the user must select the channel (Ch 0-7) under which the device will be added.

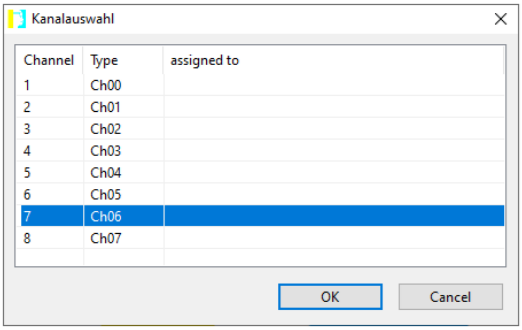


Figure 7.9 – Device DTM Select Channel

Once the child Device DTM has been added, a configuration window opens to set the *Node Address*.

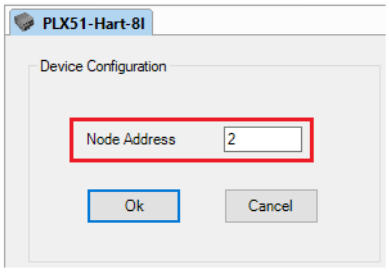


Figure 7.10 – Device DTM Node Address

7.3 Operation

After the FDT project has been configured, the DTMs can be placed online by selecting the **CONNECT** option.

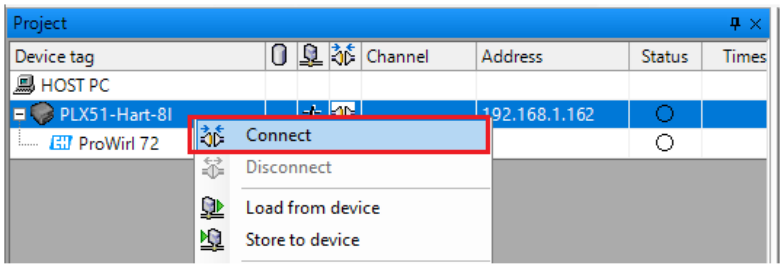


Figure 7.11 – DTM Connect

Once the PLX51-HART-8I DTM is online (connected) several diagnostic pages can be opened by selecting the **MEASURED VALUE** option.

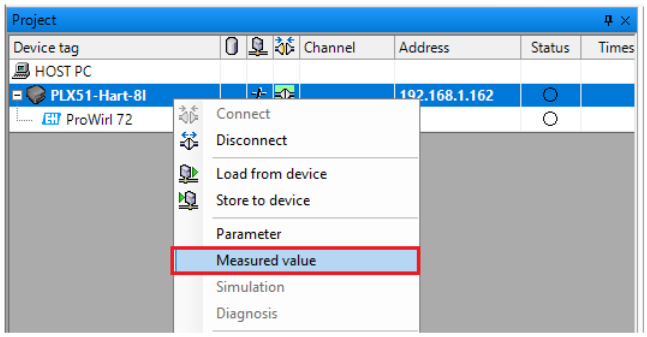


Figure 7.12 – Select Measured Value

The *General* page provides basic status information for the PLX51-HART-8I.

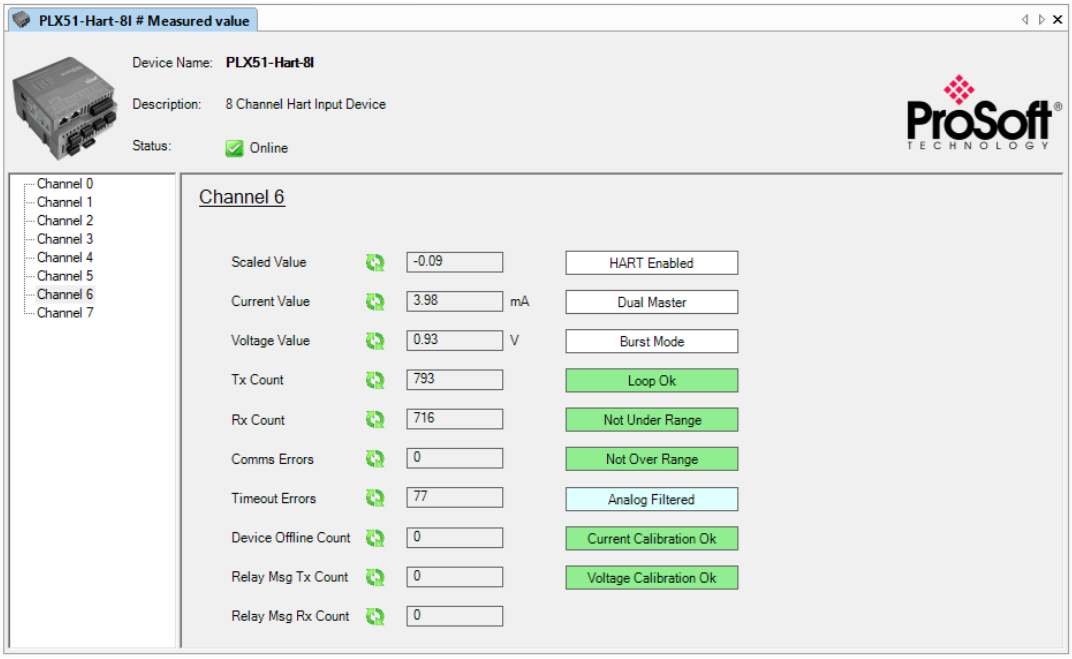


Figure 7.13 – PLX51-HART-8I DTM - General Status Page

A field Device DTM under the PLX51-HART-8I DTM can also be brought online by selecting the **CONNECT** option.

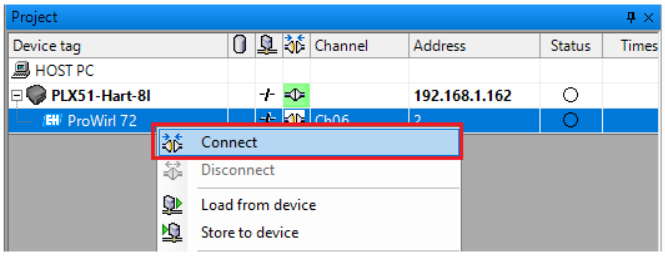


Figure 7.14 – Field Device DTM Connect

Depending on the device DTM, several function windows, for example, online parameters, diagnostics and measure variables, can be displayed. These items are accessed by right-clicking on the device DTM and selecting the required function.

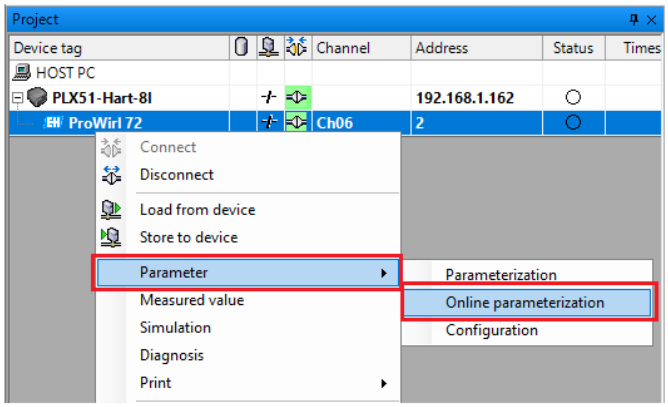


Figure 7.15 – Device DTM - Selecting Online Parameterization

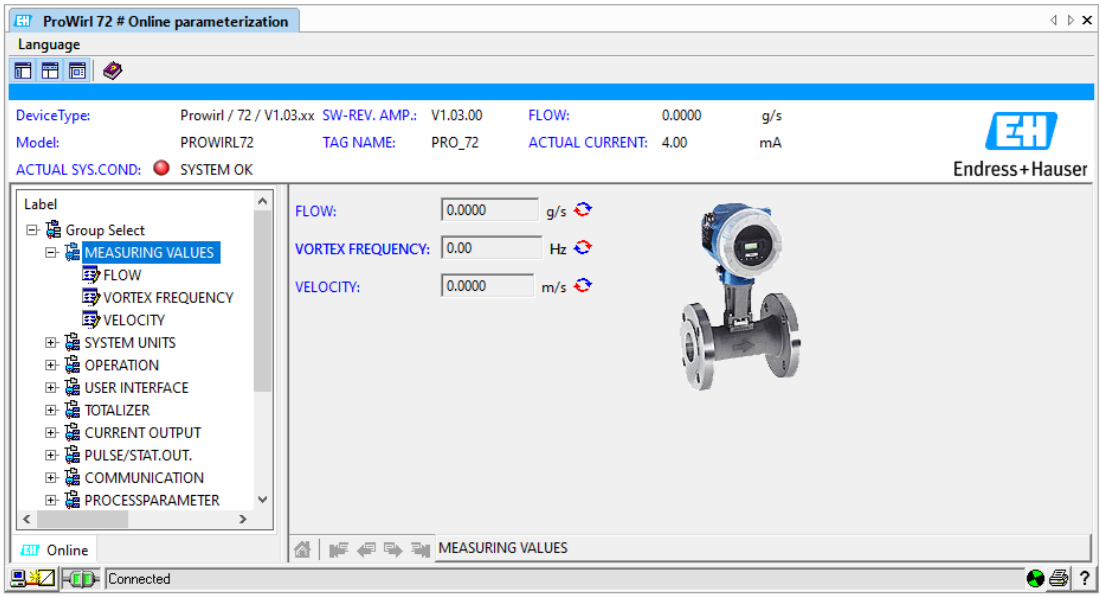


Figure 7.16 – Device DTM - Online Parameterization

8 Operation

This chapter provides additional information about the operation of the various module interfaces.

8.1 HART Devices

The PLX51-HART-8I supports up to 8 x HART devices per Analog Input Channel. Each HART device on the channel will get equal bandwidth if needed. The update rate for each HART device can be configured as well as the update rate for each Advanced Message for a specific HART device.

Important: Due to the limited bandwidth of HART (1200 bps), it is important to ensure the HART communications on a specific channel does not exceed the available bandwidth. See section *3.5 Channel Configuration* for more information.

The PLX51-HART-8I will first read all the HART device information once communication to a HART device is established. The module will then proceed to update the HART device process variables at the configured update rate in the PLX50CU channel configuration.

8.1.1 Process Variables

The HART device process variables will be updated at the configured *PV Update Rate* in the PLX50CU configuration. These requests will, by default, have the same priority as all other HART messages to be sent (Advanced Messages and Explicit Messages requested from Ethernet – e.g., DTM requests). If there are other HART messages configured, then it will slow down the update rate of the HART process variables for that specific device.

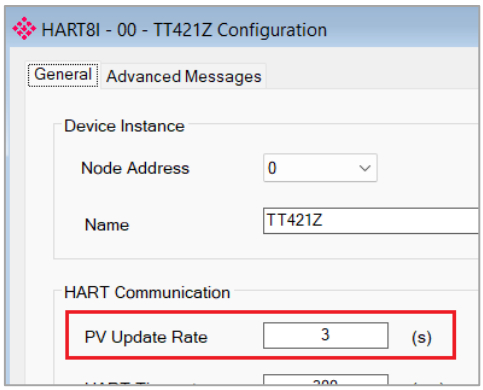


Figure 8.1 – PV Update Rate

If the PV Priority has been selected in the PLX50CU configuration, then it will prioritize the update of the HART process variables (PVs), to ensure that the HART PVs are updated as close as possible to the configured update rate for that specific HART device.

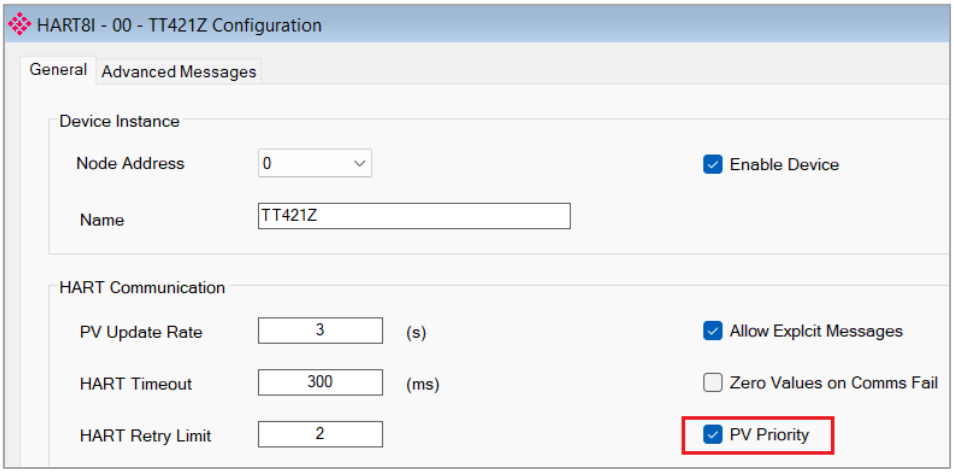


Figure 8.2 – PV Priority

Important: With multiple HART devices configured per channel, the limited HART communication bandwidth will be shared between all of them, potentially slowing the HART PV updates per HART device.

8.1.2 Advanced Messages

Up to 16 Advanced Messages can be configured per HART device. This will allow the user to read/write HART messages to the device that does not require a fast update rate (unlike Process Variables).

Note: The Advanced Messages are intended for non-critical background information or parameter updates. If the *Process Variable* or *Relay Message Priorities* have not been set, then the Advanced Messages will have the same priority as all other requests, slowing the update rate of *Process Variables* or *Relay Messages*.

8.1.3 Multi-device HART Channel

The PLX51-HART-8I will provide equal opportunity for each HART device to have a HART request sent. For example, the PLX51-HART-8I will check if any message is required to send to the first HART device on a channel. If not, it will check the second, and so on until the last HART device is reached, in which case it will start with the first HART device again. If a message is required to be sent, then that transaction will be executed. Once completed, the next HART device be checked.

The update rates of the various messages (e.g., Process Variables, Advanced Messages, etc.) determine how often a device is required to send a request.

8.1.4 Explicit HART Messaging

Explicit HART Messaging (or Relay Messaging) allows the PLX51-HART-8I to receive external requests (over Ethernet) and relay those to a specific HART device. This will allow Asset Management Software (e.g., E+H Fieldcare) to parameterize and diagnose HART devices. See chapter *7 Device Type Manager (DTM)* for more information regarding Asset Management.

When a device has already been added to the PLX51-HART-8I in the PLX50CU and the device is online, the normal explicit message service can be used. Only the HART device short number is required (like the Node Address configured in PLX50CU for the HART device).

Important: This message service cannot message HART devices that have not been added to the PLX51-HART-8I.

8.1.4.1 PLX50CU Explicit Message Utility

Explicit HART Messaging can be executed from the PLX50CU for a specific channel. This is launched by right-clicking on an Analog Channel when online in the PLX50CU and selecting **EXPLICIT MESSAGE UTILITY**.

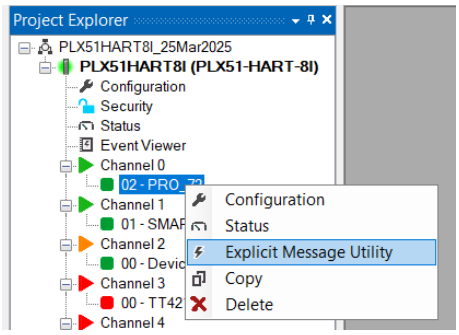


Figure 8.3 – Launching HART Explicit Messaging Utility

Once the utility is launched the user can send ad-hoc HART messages or requests.

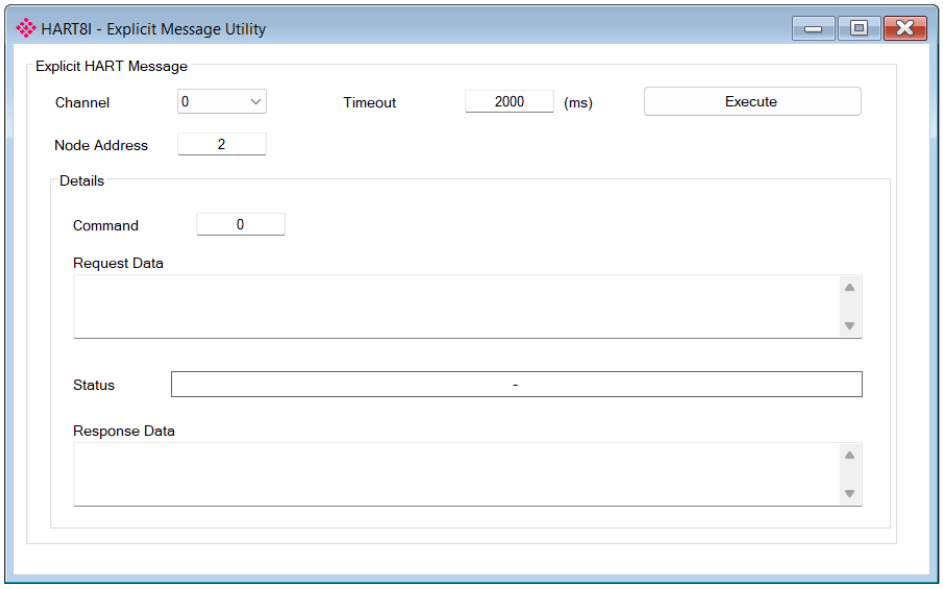


Figure 8.4 – HART Explicit Messaging Utility

Parameter	Description
Channel	The Channel on which the request will be sent
Node Address	The HART short address of the destination device.
Timeout	The maximum number of milliseconds for the transaction, before it is marked as failed.
Execute	The button is used to trigger the HART message transaction.
Details	
Command	The HART Command to be sent.
Request Data	If required, HART data can be added to the HART request. The data will need to be entered as a space-delimited, hexadecimal string. Example: 40 80 00 00 01 3F 81 B7 7F 20 41 CD 8E 30
Status	The status of the HART response.
Response Data	The HART data returned in the HART Response (if any). The data will be formatted as a space-delimited, hexadecimal string. Example: 40 80 00 00 01 3F 81 B7 7F 20 41 CD 8E 30

Table 8.1 - HART Explicit Messaging Utility parameters

Once the relevant parameters and data have been populated, then the user can press the **EXECUTE** button to send the HART request to the specific channel and HART device.

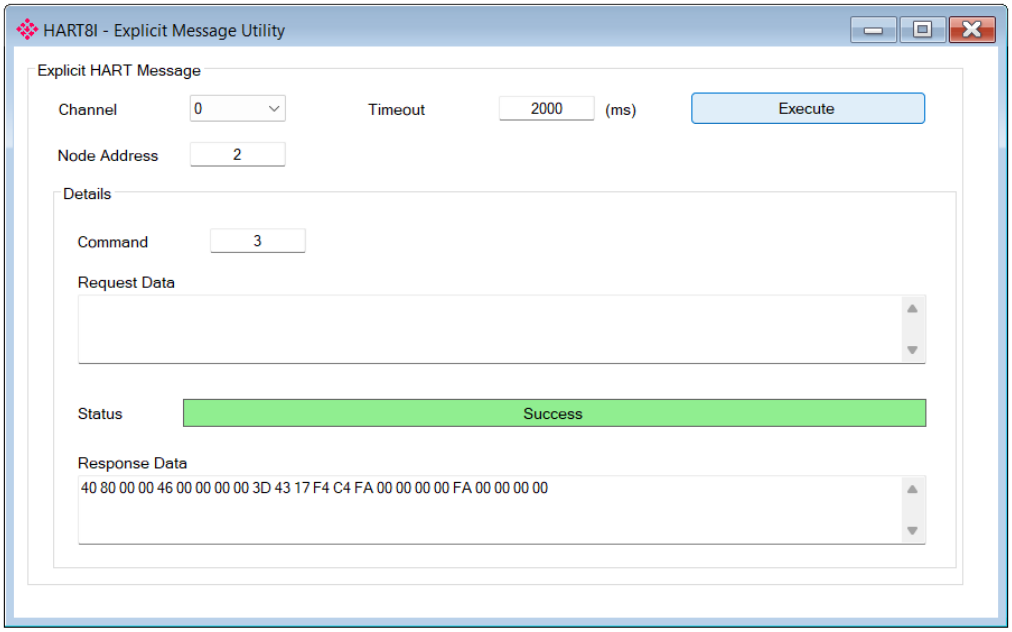


Figure 8.5 – HART Explicit Messaging Utility Executed Successfully

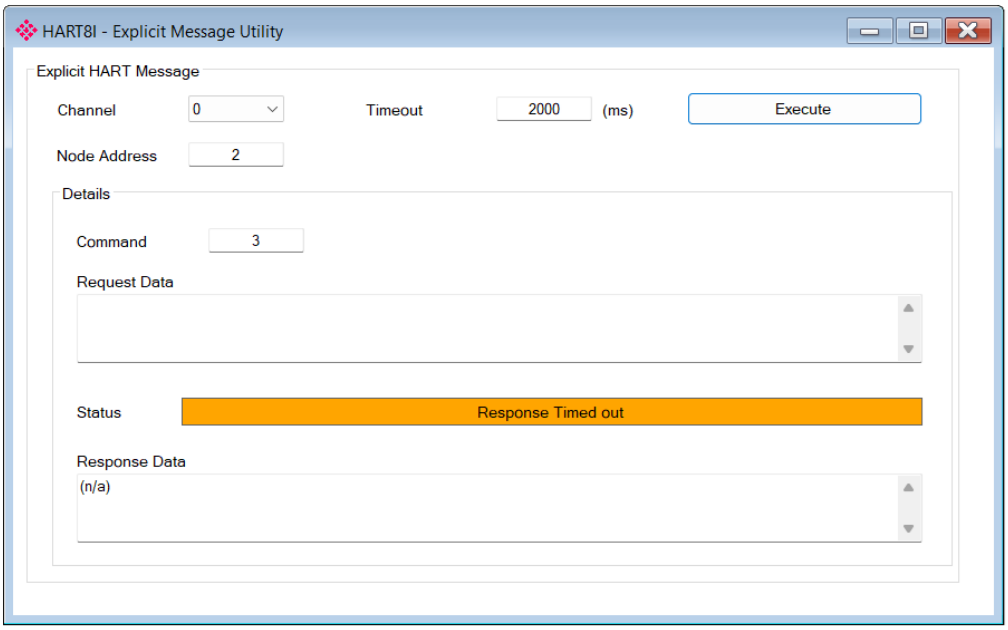


Figure 8.6 – HART Explicit Messaging Utility Execution Failed

8.1.4.2 Logix Message Instruction

See section *8.2.2 Explicit Messaging* for more information.

8.2 EtherNet/IP Target

A controller (e.g. Logix controller) can own the PLX51-HART-8I over EtherNet/IP using up to eight (8) Class 1 EtherNet/IP connections when the PLX51-HART-8I is operating as an EtherNet/IP Target. This will allow the PLX51-HART-8I to exchange data with the controller using the input and output assembly of the Class 1 EtherNet/IP connection.

Note: When using EtherNet/IP Target, it is recommended to use the *Recommend* mapping in the Internal Map configuration. This will automatically map and reformat all the required data in the Internal Map.

8.2.1 Class 1 Assembly Mapping

When the PLX51-HART-8I operates in a Logix “owned” mode the Logix controller will establish a class 1 cyclic communication connection to the module. Up to 8 input and output assemblies are exchanged at a fix interval (RPI).

Note: The module input and output assembly of each connection will be an undecorated array of bytes. The imported Logix routine (generated by PLX50 Configuration Utility) will copy this data to the input and output assemblies.

Once the generated .L5X file has been imported (which will match the Internal Mapping in the configuration), the user will be able to use the tags generated for the specific PLX51-HART-8I application.

The PLX51-HART-8I System tag is shown below:

Name	Value	Style	Data Type	Description
HART8IIn.Status	{...}		PSH8SystemStatus	
HART8IIn.Status.ConfigValid	0	Decimal	BOOL	Configuration Valid (0=Invalid, 1=Valid)
HART8IIn.Status.EIPOriginatorCommsOk	0	Decimal	BOOL	EtherNet/IP Originator (0=Fail,1=Ok)
HART8IIn.Status.ModbusOnline	0	Decimal	BOOL	Modbus Status (0=Offline,1=Online)
HART8IIn.Status.EIPOwned	0	Decimal	BOOL	EtherNet/IP Target: (0=Not-Owned, 1=Owned)
HART8IIn.Status.Power1Ok	0	Decimal	BOOL	Power Input 1 (0=Off, 1=On)
HART8IIn.Status.Power2Ok	0	Decimal	BOOL	Power Input 2 (0=Off, 1=On)
HART8IIn.Status.ControllerRunMode	0	Decimal	BOOL	Controller Mode (0=Program, 1=Run)
HART8IIn.Status.NTPOK	0	Decimal	BOOL	NTP Status (0=Fail, 1=Ok)
HART8IIn.Status.CANBusOk	0	Decimal	BOOL	CAN Bus Status (0=Fail, 1=Ok)
HART8IIn.Status.RTCValid	0	Decimal	BOOL	Real-Time Clock Status (0=Fail, 1=Ok)
HART8IIn.Status.ConfigCRC	16#0000	Hex	INT	Configuration Checksum
HART8IIn.Status.CurrentCANBaud	0	Decimal	INT	Current CAN bus BAUD (0=10k,1=20k,2=50k,3=125...
HART8IIn.Status.Uptime	0	Decimal	DINT	Uptime
HART8IIn.Status.FreeRunCounter	0	Decimal	DINT	Free Running Counter
HART8IIn.Status.DateYear	0	Decimal	INT	Date Year
HART8IIn.Status.DateMonth	0	Decimal	INT	Date Month
HART8IIn.Status.DateDay	0	Decimal	INT	Date Day
HART8IIn.Status.TimeHour	0	Decimal	INT	Time Hour
HART8IIn.Status.TimeMinute	0	Decimal	INT	Time Minute
HART8IIn.Status.TimeSecond	0	Decimal	INT	Time Second
HART8IIn.Status.DeviceTemperature	0.0	Float	REAL	Device Temperature (Degrees Celsius)
HART8IIn.Status.DIPSwitchesAtStartup	0	Decimal	INT	DIP Switches at startup
HART8IIn.Status.DIPSwitchesCurrent	0	Decimal	INT	DIP Switches current
HART8IIn.Status.EthPort1Status	0	Decimal	INT	Ethernet Port 1 Status (Bit0: 0=LinkDown, 1=LinkUp...
HART8IIn.Status.EthPort2Status	0	Decimal	INT	Ethernet Port 2 Status (Bit0: 0=LinkDown, 1=LinkUp...
HART8IIn.Status.EthSwitchMode	0	Decimal	INT	Ethernet Switch Mode (0=Switch, 1=Split)
HART8IIn.Status.DLRStatus	0	Decimal	INT	Device Level Ring Status (Bit0: 0=Disable,1=Enabl...
HART8IIn.Status.NTPStatus	0	Decimal	INT	NTP Status (Bit0: 0=Disabled,1=Enabled; Bit1: 0=N...
HART8IIn.Status.PTPStatus	0	Decimal	INT	PTP Status (Bit0: 0=Disabled,1=Enabled; Bit1: 0=N...

Figure 8.7 – Logix System Status Tag

The Channel tag will provide analog input data as well as any HART device connected to that specific analog input channel.

Name	Value	Style	Data Type	Description
HART8IIn	{...}		HART8IInxE801	
HART8IIn.Status	{...}		PSH8SystemStatus	
HART8IIn.Ch0	{...}		HART8ICh0x9AA3	
HART8IIn.Ch0.Analog	{...}		PSH8ChannelAna...	
HART8IIn.Ch0.Analog.HARTEnabled	0	Decimal	BOOL	HART Communication (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.AnalogFilter	0	Decimal	BOOL	Analog Filter (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.EnableDUALMasters	0	Decimal	BOOL	Dual Master Support (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.UnderRange	0	Decimal	BOOL	Channel UnderRange (0=Ok, 1=UnderRange)
HART8IIn.Ch0.Analog.OverRange	0	Decimal	BOOL	Channel OverRange (0=Ok, 1=OverRange)
HART8IIn.Ch0.Analog.LoopOpen	0	Decimal	BOOL	Loop Open (0=Ok, 1=Open Circuit)
HART8IIn.Ch0.Analog.LoopShorted	0	Decimal	BOOL	Loop Shorted (0=Ok, 1=Short Circuit)
HART8IIn.Ch0.Analog.BurstModeActive	0	Decimal	BOOL	Burst Mode (0=Disabled, 1=Enabled)
HART8IIn.Ch0.Analog.RelayMsgPriority	0	Decimal	BOOL	Relay Message (0=Normal, 1=Priority)
HART8IIn.Ch0.Analog.CalibrationFactoryCurrentOk	0	Decimal	BOOL	Factory Current Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CalibrationFactoryVoltageOk	0	Decimal	BOOL	Factory Voltage Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CalibrationUserCurrentOk	0	Decimal	BOOL	User Current Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CalibrationUserVoltageOk	0	Decimal	BOOL	User Voltage Calibration (0=Invalid, 1=Ok)
HART8IIn.Ch0.Analog.CurrentValue	0.0	Float	REAL	Raw Current Value (mA)
HART8IIn.Ch0.Analog.ScaledValue	0.0	Float	REAL	Scaled Value
HART8IIn.Ch0.Analog.VoltageValue	0.0	Float	REAL	Raw Voltage Value (V)

Figure 8.8 – Analog Input Channel Specific tags

Name	Value	Style	Data Type	Description
HART8IIn	{...}		HART8IInxE801	
HART8IIn.Status	{...}		PSH8SystemStatus	
HART8IIn.Ch0	{...}		HART8ICh0x9AA3	
HART8IIn.Ch0.Analog	{...}		PSH8ChannelAna...	
HART8IIn.Ch0.Device	{...}		PSH8HARTDevice	
HART8IIn.Ch0.Device.NodeAddress	0	Decimal	INT	Node Address
HART8IIn.Ch0.Device.HARTStatus	16#0000	Hex	INT	HART Status
HART8IIn.Ch0.Device.DeviceOnline	0	Decimal	BOOL	Device Online (0=Offline, 1=Online)
HART8IIn.Ch0.Device.RelayMessageInhibited	0	Decimal	BOOL	Relay Message Control (0=Normal,1=Inhibited)
HART8IIn.Ch0.Device.PV	0.0	Float	REAL	Primary Variable
HART8IIn.Ch0.Device.SV	0.0	Float	REAL	Secondary Variable
HART8IIn.Ch0.Device.TV	0.0	Float	REAL	Tertiary Variable
HART8IIn.Ch0.Device.FV	0.0	Float	REAL	Fourth Variable
HART8IIn.Ch0.Device.PVUnitsCode	0	Decimal	INT	Primary Variable Units Code
HART8IIn.Ch0.Device.SVUnitsCode	0	Decimal	INT	Secondary Variable Units Code
HART8IIn.Ch0.Device.TVUnitsCode	0	Decimal	INT	Tertiary Variable Units Code
HART8IIn.Ch0.Device.FVUnitsCode	0	Decimal	INT	Fourth Variable Units Code
HART8IIn.Ch0.Device.AdvMsgSuccess	2#0000_0000_0000_0000	Binary	INT	Advanced Message Success (1 bit per Adv Msg Ite...
HART8IIn.Ch0.Device.AdvMsgActivity	2#0000_0000_0000_0000	Binary	INT	Advanced Message Activity (1 bit per Adv Msg Ite...

Figure 8.9 – Analog Input Channel – HART Device Specific tags

8.2.2 Explicit Messaging

The Explicit HART Message can also be sent from a Logix Controller using a Logix MSG instruction.

Below is an example and parameter structure required to execute this Explicit HART Message from Logix.

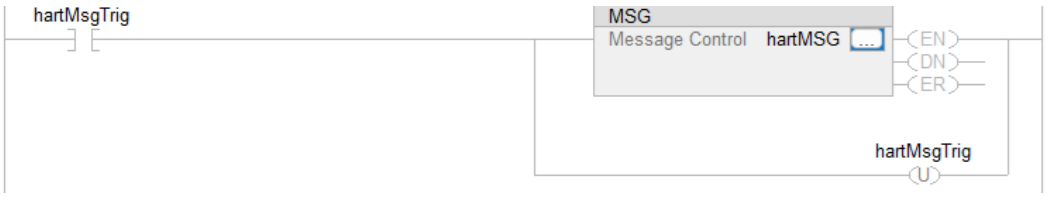


Figure 8.10 – Relay HART Message

The required attributes for the message instruction are as follows:

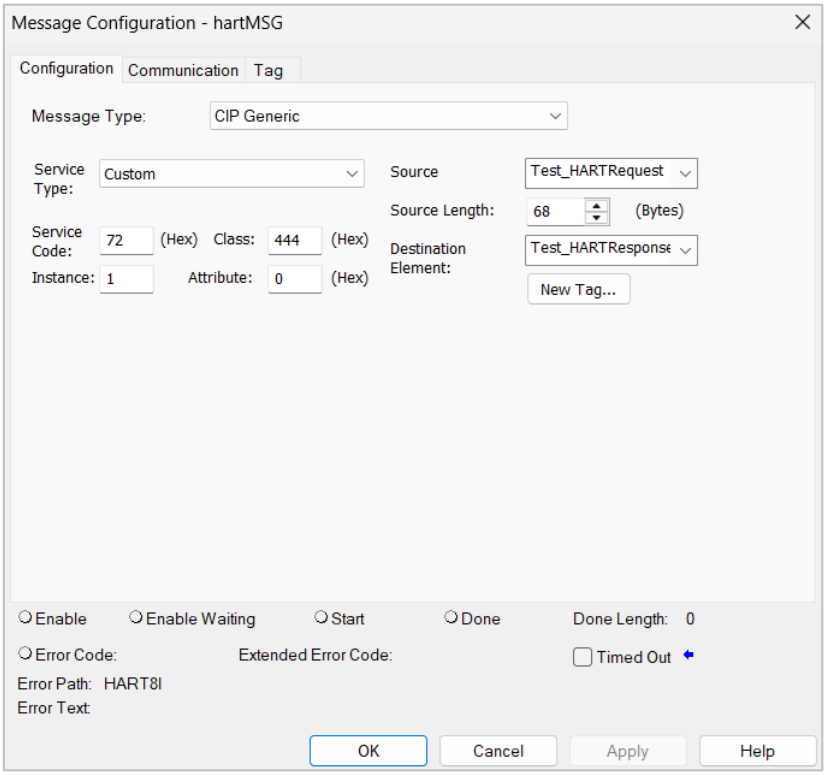


Figure 8.11 – Relay HART Message Configuration

Parameter	Value / Description
Message Type	CIP Generic
Service Type	Custom
Service Code	72 Hex (Relay HART Message service)
Class	444 Hex
Instance	Channel value + 1 1 for Channel 0 2 for Channel 1 3 for Channel 2 4 for Channel 3 5 for Channel 4 6 for Channel 5 7 for Channel 6 8 for Channel 7
Attribute	0
Source Element	Tag of type PSHExplicitHARTRequest
Source Length	68
Destination Element	Tag of type PSHExplicitHARTResponse

Table 8.2 – Relay HART Message Parameters

The required Request and Response HART Command structures are defined as follows:

HART Command Request		
Byte Offset	**Data Type**	**Description**
0	SINT	Bit 7: Priority Bit 6 to 0: Node Address
1	SINT	HART Command
2	SINT	Timeout (x 100ms)
3	SINT	Data Length of data to be sent with the request
4	SINT[64]	Request Data with max length of 64 bytes

Table 8.3 – Relay HART Message Response Structure

HART Command Response		
Byte Offset	**Data Type**	**Description**
0	SINT	Response Status: 0: Success 1: Response timed out 2: Device not online 3: Request not sent before timeout 4: Request buffer overflow 5: Response checksum error 6: Response command error 7: Dual Master error
1	SINT	Data Length received in the response.
2	INT	HART Status (see section *11.2 HART Response Status*)
4	SINT	Response Data with max length of 64 bytes.

Table 8.4 – Relay HART Message Request Structure

8.3 EtherNet/IP Originator

The PLX51-HART-8I can operate as an EtherNet/IP originator. In this mode the module can exchange data from the analog channels and HART devices with EtherNet/IP devices using either the input and output assemblies of the Class 1 EtherNet/IP connection to the device or using explicit (Class 3 or UCMM) EtherNet/IP messages.

8.3.1 EtherNet/IP Class 1 Connections

In the example below, the PLX51-HART-8I is exchanging data with HART devices while also owning two EtherNet/IP IO modules. The HART device data is being exchanged with the EtherNet/IP IO modules.

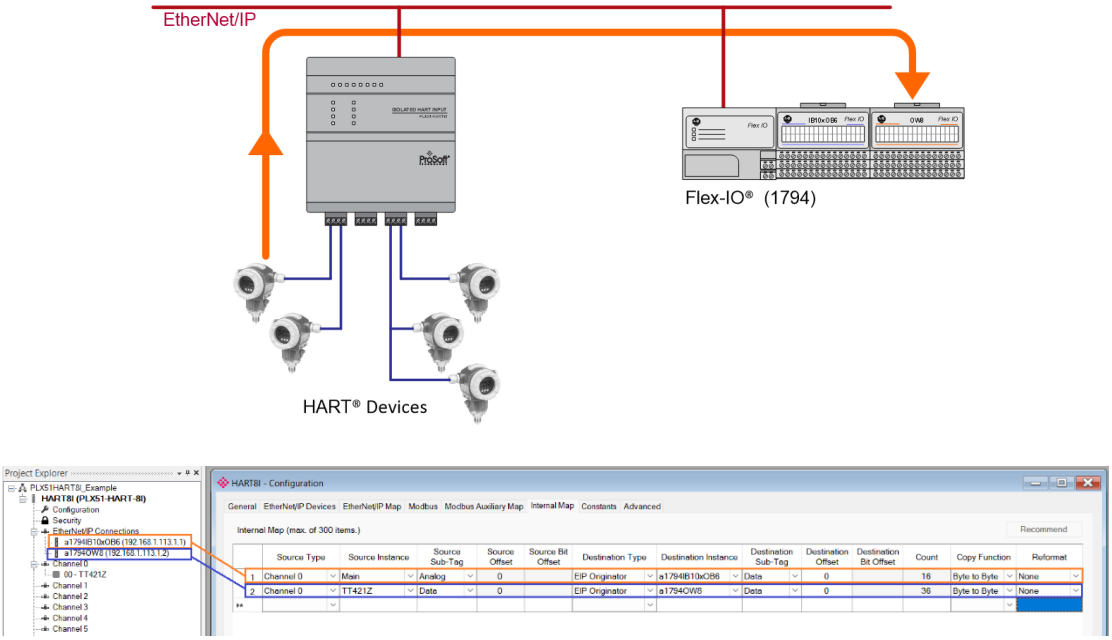


Figure 8.12 – Internal Mapping from Analog Channel and HART Device to EtherNet/IP Originator

8.3.2 Explicit EtherNet/IP Messaging

When using EtherNet/IP Explicit Messaging, the user can configure up to 10 EtherNet/IP devices which will be used for Explicit Messaging. This configuration is accessed in the *EtherNet/IP Devices* tab. Following this, the EtherNet/IP Map of explicit messages needs to be configured. The Explicit Messaging uses the internal data space (IDS) where data can be written to and read from for exchanges between the HART devices and the explicit EtherNet/IP devices.

The Input and Output IDS Offset is where the Explicit EtherNet/IP device data will be read from or written to. The data in the IDS can then be copied to or from the Analog channels or HART devices using internal mapping.

In the example below, the HART device data being received is copied to the Internal Data Space (IDS) at offset **3000** in the Internal Map configuration. The data at IDS offset **3000** is then written to a Logix tag using the Explicit messaging EtherNet/IP Map.

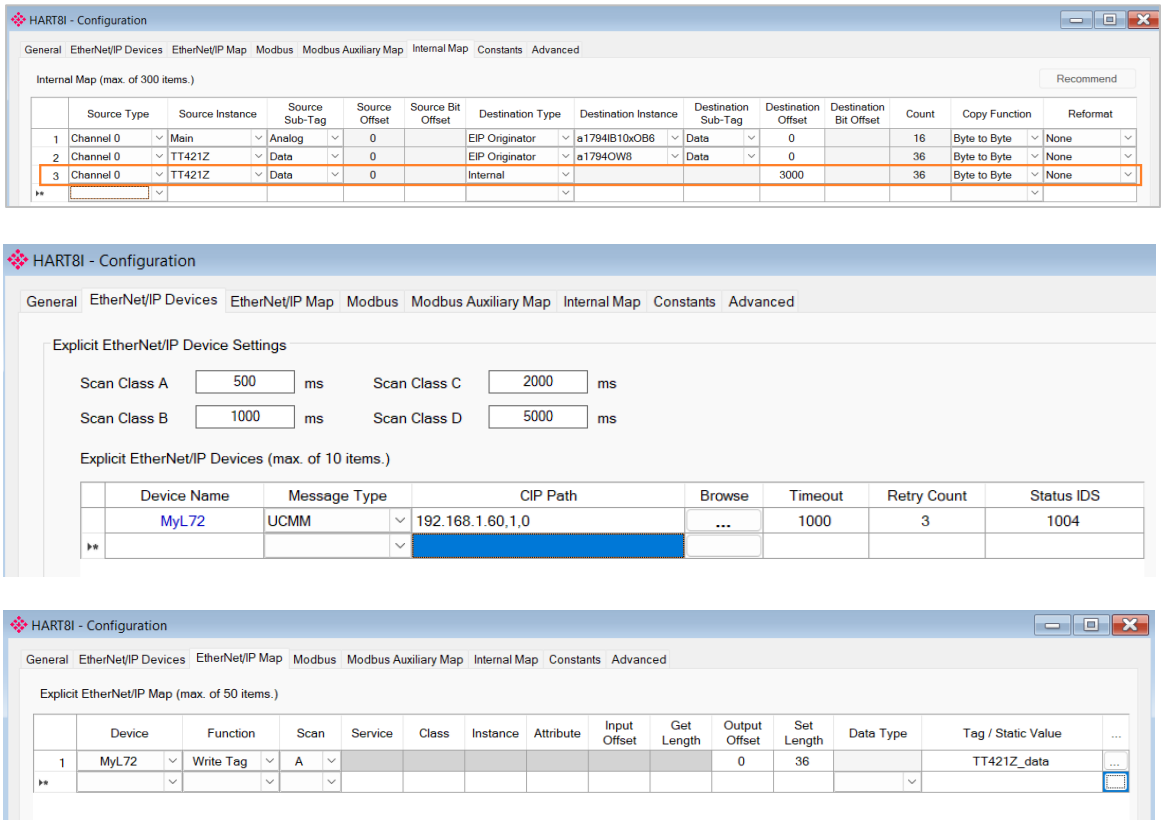


Figure 8.13 – Received HART device data to Explicit Logix Tag

8.4 Modbus Client

When the PLX51-HART-8I has the *Primary Interface* set to **MODBUS CLIENT**, then Analog Input and HART device data can be exchanged with one or more remote Modbus servers.

The internal Modbus Registers are asynchronously exchanged with Modbus devices as configured in the *Modbus Auxiliary Map*. In this mapping the user can exchange (read or write) data between the internal Modbus Registers and a remote Modbus device on Modbus TCP, RTU232, or RTU485.

In the example below, the PLX51-HART-8I, with the *Primary Interface* set to **MODBUS CLIENT**, will read data from a HART device and write this to a Modbus Holding Register of a Modbus Server.

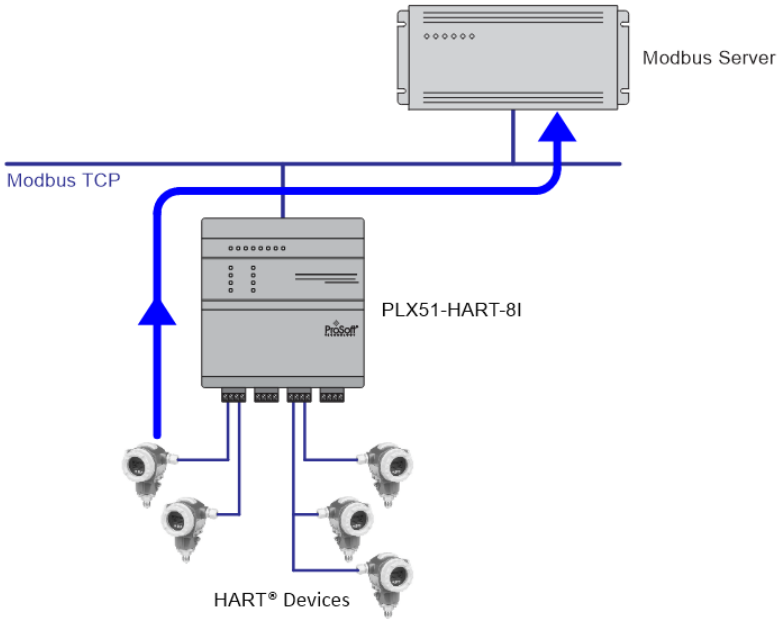


Figure 8.14 – Modbus Client to HART device operation

The data from the HART device is copied to the internal Modbus Holding Register at the desired offset (in this example **1030**).

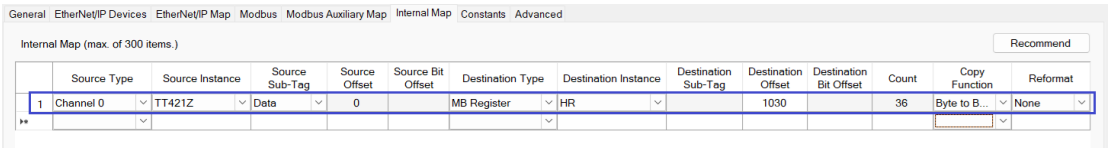


Figure 8.15 – Copy HART device data to internal Modbus HR

Next, the *Modbus Auxiliary Map* is configured to write Holding Register **1030-1047** to the remote Modbus server at IP address **192.168.1.55** from the internal Modbus Holding Register **1030-1033**.

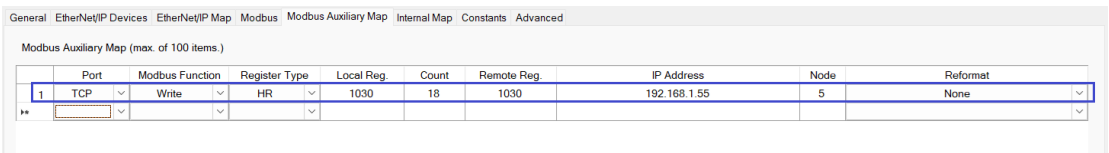


Figure 8.16 – Modbus Client Auxiliary Mapping

8.5 Modbus Server

When the PLX51-HART-8I has the *Primary Interface* set to **MODBUS SERVER**, then the Analog Input and HART data can be mapped to configurable internal Modbus Registers and offsets using the Internal Map.

The internal Modbus Registers can then be asynchronously exchanged with one or more remote Modbus Clients on Modbus TCP, RTU232, or RTU485.

In the example below the PLX51-HART-8I with the *Primary Interface* set to **MODBUS SERVER**, receives data from the HART device and makes it available to remote Modbus Clients.

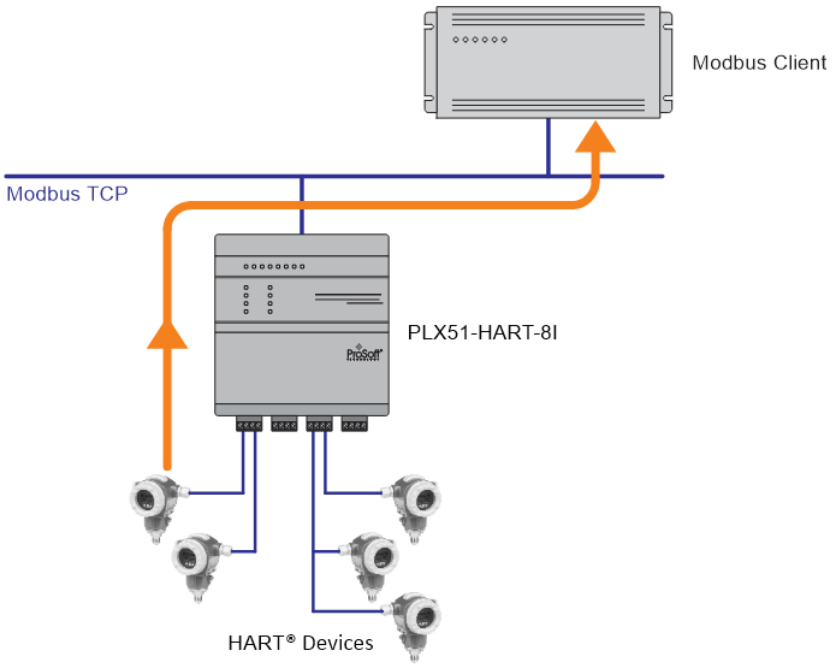


Figure 8.17 – HART device to Modbus TCP Client

In the Internal Mapping configuration, the HART device data is mapped to internal Modbus Holding Register **1024-1041**.

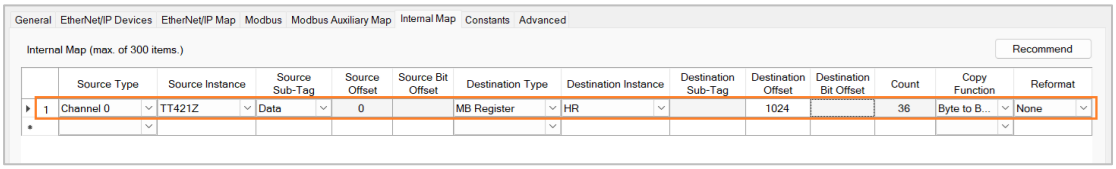


Figure 8.18 – Modbus Server –Internal Mapping

Note: The user will need to ensure that when writing to the PLX51-HART-8I Modbus Holding Registers, the registers holding data from the device are not inadvertently overwritten.

9 Diagnostics

9.1 LEDs

The PLX51-HART-8I provides 16 LEDs for diagnostics purposes.

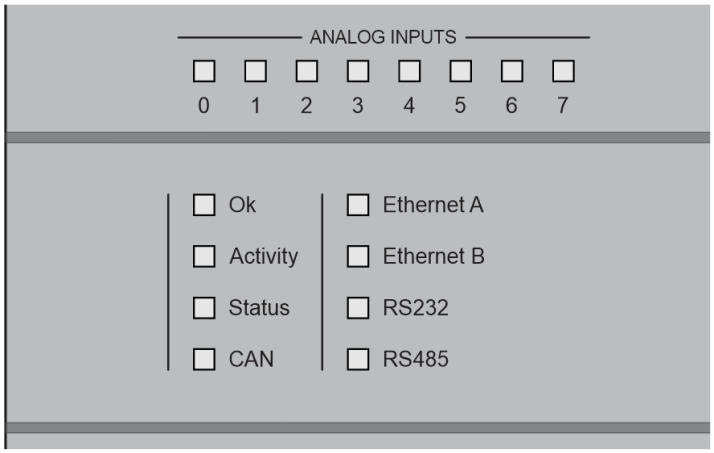


Figure 9.1 - Module front view

LED	Description
Ok	Indicates the system-level operation of the module. **Red**: The module is not operating correctly. For example, if the module application firmware has been corrupted or there is a hardware fault the module will have a red Module LED. **Green (flashing)**: The module has booted and is running correctly without any application configuration loaded. **Green (solid)**: The module has booted and is running correctly with application configuration loaded. **Blue (solid)**: The module is busy updating the application configuration from the SD Card during startup.
Activity	Indicates the activity on the primary interface (EtherNet/IP Target, Modbus Server, Modbus Client, or EtherNet/IP Originator). **Blinking Green**: A successful transaction was completed on the primary interface. **Blinking Red**: The transaction failed on the primary interface (e.g., invalid request).
Status	Indicates the status from the primary interface (EtherNet/IP Target, Modbus Server, Modbus Client, or EtherNet/IP Originator). **EtherNet/IP Target** **Solid Green**: The module is connected (with the correct number of connections) to the Logix Controller, and the Logix Controller is in RUN mode. **Flashing Green**: The module is connected (with the correct number of connections) to the Logix Controller, and the Logix Controller is in PROG/FAIL mode. **Solid Red**: The module is not connected to a Logix Controller or it is connected, but the actual number of connections does not match the configured number of connections.

	EtherNet/IP Originator **Solid Green**: The module is connected and successfully exchanging messages with all the configurated EtherNet/IP devices (Class 1 and Explicit). **Solid Red**: The module is not connected with either the Class1 or Explicit message devices, or the Explicit messages are failing. **Modbus Client** **Solid Green**: All the Modbus requests configured in the Modbus Auxiliary map are successfully executing. **Solid Red**: One or more of the Modbus requests configured in the Modbus Auxiliary map are failing. **Modbus Server** **Solid Green**: The module has received a Modbus request within the Modbus Slave Timeout configuration. **Solid Red**: The module has **not** received a Modbus request within the Modbus Slave Timeout configuration.
CAN	*This is currently not used.*
Ethernet A / B	The Ethernet LED will illuminate when an Ethernet link has been detected (by plugging in a connected Ethernet cable). The LED will flash when traffic is detected. This module has two Ethernet ports A and B. Each LED represents each port.
RS232	Indicates if there was activity on the RS232 port as well as the status of the activity. The Modbus transaction was successfully received when **blinking green** or there was a checksum error when **blinking red**.
RS485	Indicates if there was activity on the RS485 port as well as the status of the activity. The Modbus transaction was successfully received when **blinking green** or there was a checksum error when **blinking red**.
Analog Inputs (0-7)	Each channel LED represents the status of that specific analog channel. **Solid Green**: The loop current is within the acceptable range (3.8 to 20.5 mA) and HART communication is **successful** with the field device(s). **Flashing Green**: The loop current is within the acceptable range (3.8 to 20.5 mA) and HART communication has **failed** to the field device(s). **Solid Yellow/Orange**: The loop current is within the over range (20.5 to 21 mA) or under range (3.6 to 3.8mA) limits and HART communication is **successful** with the field device(s). **Flashing Yellow/Orange**: The loop current is within the over range (20.5 to 21 mA) or under range (3.6 to 3.8mA) limits and HART communication has **failed** to the field device(s). **Solid Red**: The loop current is either open circuit (less than 3.6mA) or short circuit (greater than 21mA) and HART communication is **successful** with the field device(s). **Flashing Red**: The loop current is either open circuit (less than 3.6mA) or short circuit (greater than 21mA) and HART communication has **failed** to the field device(s).

Table 9.1 - Module LED operation

9.2 Module Status Monitoring in PLX50 Configuration Utility

The PLX51-HART-8I provides various statistics to assist with module operation, maintenance, and fault finding. The statistics can be accessed in full by PLX50CU.

To view the module's status in the PLX50CU environment, the module must be online. If the module is not already Online (following a recent configuration download), then right-click on the module and select the **GO ONLINE** option.

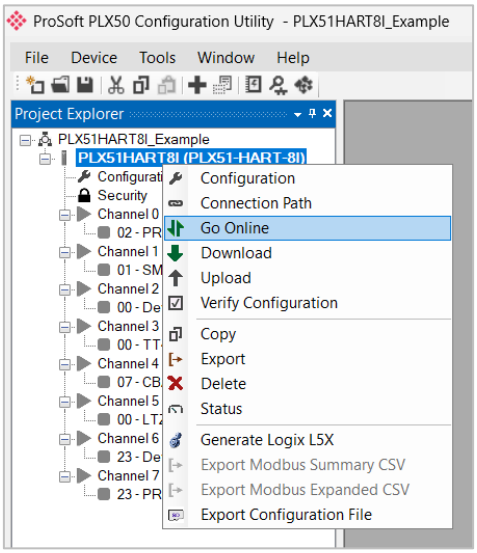


Figure 9.2 - Selecting to Go Online

The *Online* mode is indicated by the green circle behind the module in the Project Explorer tree.

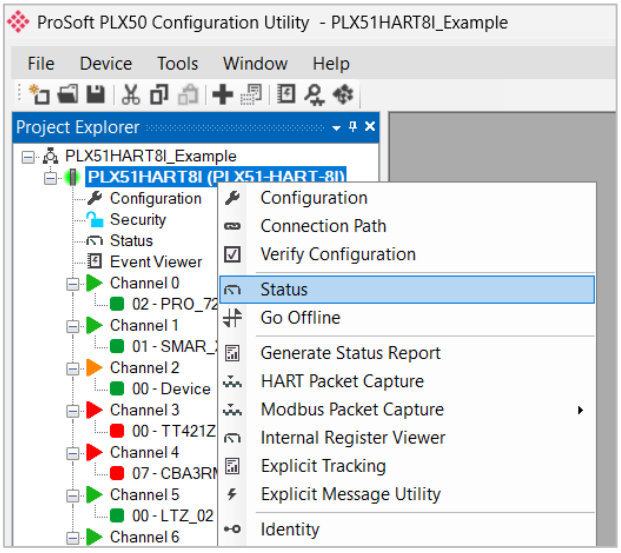


Figure 9.3 - Selecting online Status

The Status monitoring window can be opened by either double-clicking on the **STATUS** item in the Project Explorer tree, or by right-clicking on the module and selecting **STATUS**. The status window contains multiple tabs to display the status of the module.

9.2.1 General

The *General* tab displays the general status for the PLX51-HART-8I.

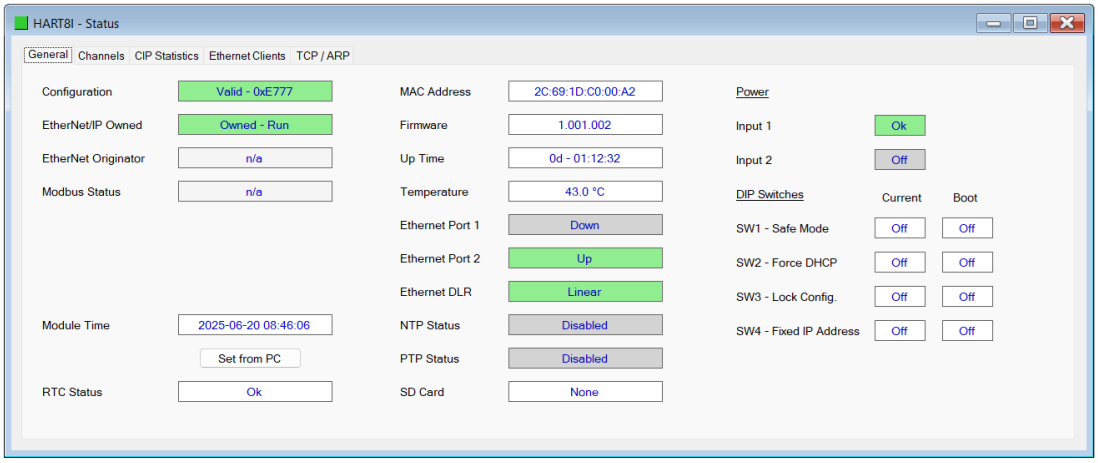


Figure 9.4 - Status monitoring – General

Parameter	Description
Configuration	Indicates whether the module's configuration is valid and provides the configuration's CRC checksum.
EtherNet/IP Owned	When the module is configured as an EtherNet/IP Target, this will indicate if the module is owned by an EtherNet/IP connection originator, as well as the Run/Program state of the controller.
EtherNet/IP Originator	When the module is configured as an EtherNet/IP Originator, this will show if all the Class 1 and Explicit Message connections to EtherNet/IP target devices are established and returning valid data.
Modbus Status	When the module is operating as a Modbus Server, this parameter will indicate that the module has received a valid Modbus request within the Modbus *Inactivity Timeout* time. When the module is operating as a Modbus Client, this parameter will indicate that all the mapping items in the Modbus Auxiliary Map are executing correctly.
Module Time	The current date and time in the module. This can either be updated manually or automatically via NTP or PTP. When powered down, the time also persists for a couple of days by using a backup Real Time Clock (RTC).
RTC Status	The status of the on-board Real Time Clock (RTC). **Ok**: The RTC has valid time. **Invalid**: The RTC no longer has valid time. This is typically due to the module been unpowered for more than 7 days.
MAC Address	Displays the module's unique Ethernet MAC address.
Firmware	The version of the module's firmware.
Up Time	Indicates the elapsed time since the module was powered-up.
Temperature	The internal temperature of the module.
Ethernet Port 1/2	This is the status of each Ethernet port. **Down**: The Ethernet connector has not been successfully connected to an Ethernet network. **Up**: The Ethernet connector has successfully connected to an Ethernet network. **Mirror Enabled**: The Ethernet port is mirroring the traffic on the other Ethernet port.

Ethernet DLR (Device Level Ring)	The status of the Ethernet DLR. **Disabled**: Device Level Ring functionality has been disabled. **Linear**: The DLR functionality has been enabled, and the Ethernet network architecture is linear. **Ring: Fault**: The DLR functionality has been enabled, and the Ethernet network architecture is ring, but there is a fault with the network. **Ring: Ok**: The DLR functionality has been enabled, and the Ethernet network architecture is ring and is operating as expected.
NTP Status	The status of the local NTP Client. **Disabled**: The NTP time synchronization has been disabled. **Locked**: NTP time synchronization has been enabled, and the module has locked onto the target time server. **Not Locked**: NTP time synchronization has been enabled, and the module has not locked onto the target time server.
PTP Status	The status of the PTP Synchronization. **Disabled**: The PTP time synchronization has been disabled. **Locked**: PTP time synchronization has been enabled, and the module is synchronized with a PTP Master **Not Locked**: PTP time synchronization has been enabled, but the module is not synchronized to a PTP Master.
SD Card	Indicates if a SD Card is present or not.
Power	Indication from which port the module is receiving power.
DIP Switch Position	The status of the DIP switches when the module booted. **Note**: This status will not change if the DIP switches are altered when the module is running.

Table 9.2 - Parameters displayed in the Status Monitoring – General Tab

9.2.2 Channels

The *Channels* tab displays an overview of the Analog Input Channels.

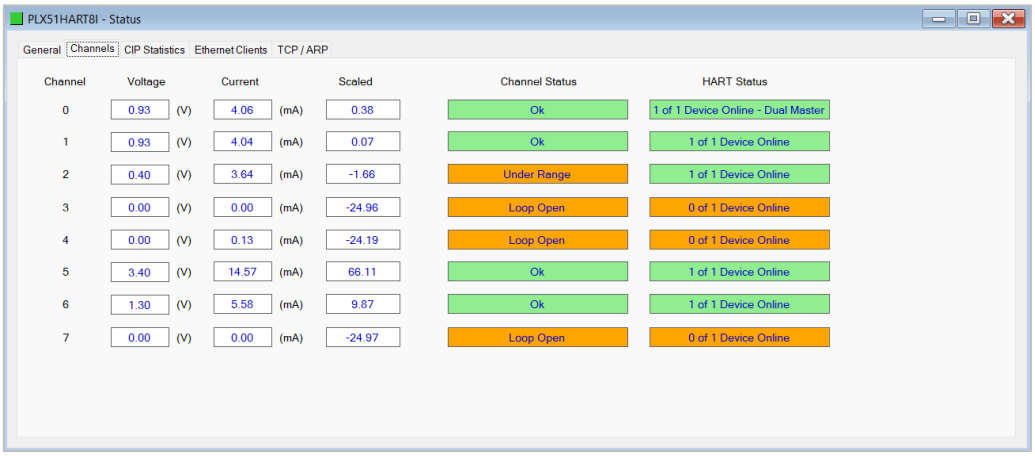


Figure 9.5 - Status monitoring – Channel Overview

Statistic	Description
Voltage	The input voltage reading for the specific channel (V).
Current	The input current reading for the specific channel (mA).
Scaled	The scaled value for the specific channel.
Channel Status	The status of the specific channel. **Disabled**: The channel is disabled. **OK**: The loop current is within the acceptable range (3.8 to 20.5 mA). **Loop Open**: The loop current is open circuit (less than 3.6mA). **Under Range**: The loop current is within the under range (3.6 to 3.8 mA) limit. **Over Range**: The loop current is within the over range (20.5 to 21 mA) limit. **Loop Shorted**: The loop current is short circuit (greater than 21mA). **Cal. Fail**: The calibration has failed or is no longer valid.
HART Status	The status of the HART communication for the specific channel. **Disabled**: HART has been disabled for this channel. **No Devices Configured**: No HART devices have been configured or enabled for this channel. **# of # Device Online**: Showing the number of HART devices online when compared to the number of HART devices configured for the specific channel. **- Dual Master** (suffix): The Dual Master configuration option has been enabled. **- Burst** (suffix): The channel is configured for Burst mode.

Table 9.3 – Analog Input Channel overview

9.2.3 EtherNet/IP Explicit

The EtherNet/IP Explicit Statistics tab displays the statistics associated with EtherNet/IP Device explicit mapping.

Note: This tab is only applicable when the module has the *Primary Interface* set to **ETHERNET/IP ORIGINATOR**.

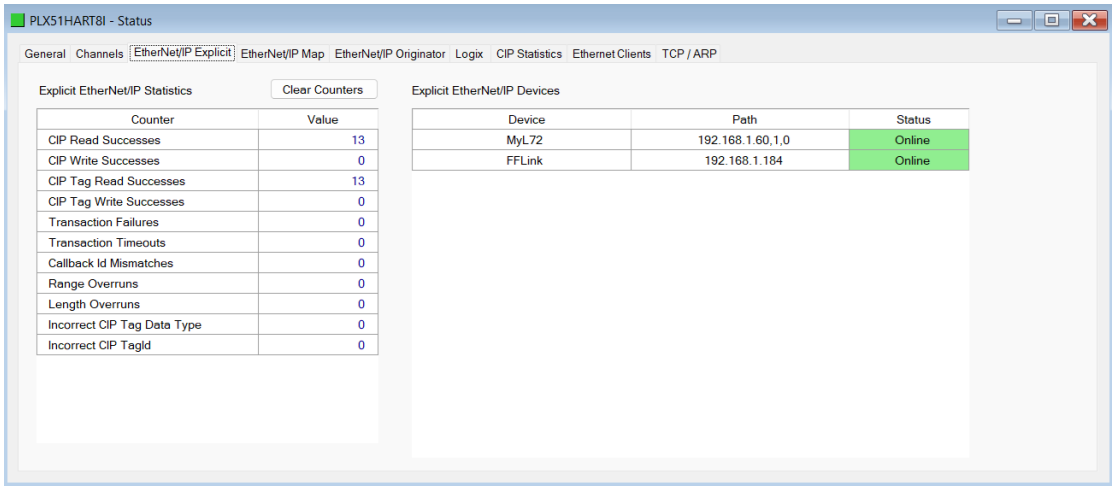


Figure 9.6 - Status monitoring – EtherNet/IP Explicit

Statistic	Description
Read Successes	The number of successful reads from the target EtherNet/IP device.
Write Successes	The number of successful writes to the target EtherNet/IP device.
Transaction Failures	The number of failed reads/writes to the target EtherNet/IP device (e.g. error response).
Transaction Timeouts	The number of times the target EtherNet/IP device failed to respond.
Callback Id Mismatches	The EtherNet/IP UCMM or Class 3 response does not match the request.
Range Overruns	The number of times the returned data amount runs over the maximum Internal Data Space.
Length Overruns	The number of times the returned data is greater than the configured get length.
Incorrect CIP Data Type	When the Explicit Message Function is a Tag Read/Write, this statistic will increase when the incorrect CIP data type was returned in the response.
Incorrect CIP Tag Id	When the Explicit Message Function is a Tag Read/Write, this statistic will increase when the incorrect CIP UDT tag ID was returned in the response.
CIP Tag Read Successes	When the Explicit Message Function is a Tag Read, this statistic will increase when there was a successful Logix Tag Read.
CIP Tag Write Successes	When the Explicit Message Function is a Tag Write, this statistic will increase when there was a successful Logix Tag Write.

Table 9.4 – EtherNet/IP Explicit Statistics

9.2.4 EtherNet/IP Map

The EtherNet/IP Map tab displays the success counts for each EtherNet/IP device mapped item.

Note: This tab is only applicable when the module has the *Primary Interface* set to **ETHERNET/IP ORIGINATOR**.

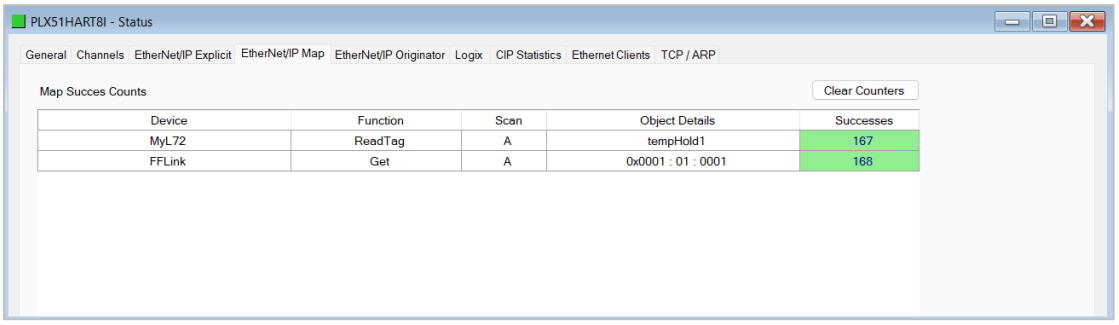


Figure 9.7 - Status monitoring – EtherNet/IP Map

Each time a mapped item is executed successfully its associated count will increase. The count cell will momentarily be highlighted green following a successful transaction.

9.2.5 EtherNet/IP Originator

The *EtherNet/IP Originator* tab displays the EtherNet/IP Class 1 connection status and statistics for each configured EtherNet/IP device.

Note: This tab is only applicable when the module has the *Primary Interface* set to **ETHERNET/IP ORIGINATOR**.

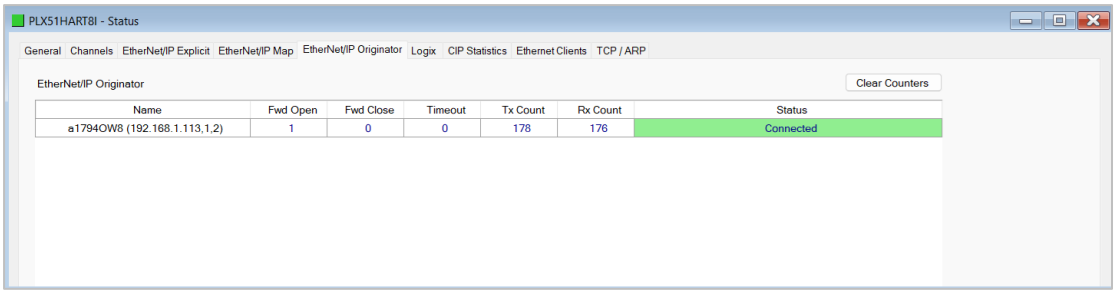


Figure 9.8 - Status monitoring – EtherNet/IP Originator

Statistic	Description
Status	The current connection status of the module. **Connected**: The device is connected and exchanging data using Class 1 cyclic communication. **Offline**: The device is offline and not connected **Various response faults**: If the connection parameters entered are not correct, then generally the target device will reply with the specific reason for the connection reject, for example: Ownership Conflict Connection In Use Or Duplicate Forward Open
Class 1 Originator Statistics	
Forward Open Count	The number of Class 1 Forward Open (connection establishment) messages sent to this device.
Forward Close Count	The number of Class 1 Forward Close (connection termination) messages sent or received from this device.
Connection Timeouts	The number of this connection was closed due to timeouts.
Tx Count	Number of Class 1 messages sent to the specific target device.
Rx Count	Number of Class 1 messages received from the specific target device.

Table 9.5 – EtherNet/IP Class 1 status and statistics

9.2.6 Logix

The *Logix* tab displays the Logix statistics for the explicit EtherNet/IP Tag Read/Write message instructions.

Note: This tab is only relevant when the module has the *Primary Interface* set to **ETHERNET/IP ORIGINATOR** and Logix Tag Read/Write functions are being used in the EtherNet/IP Explicit Message Map.

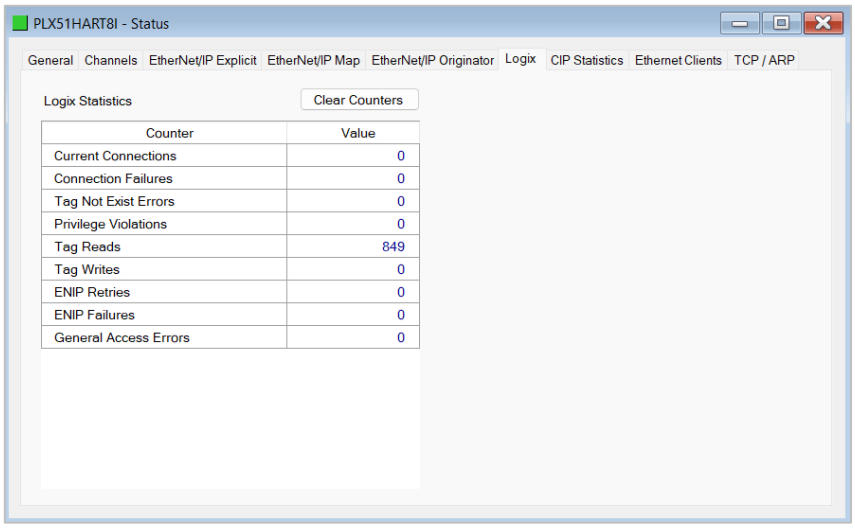


Figure 9.9 - Status monitoring – Logix Statistics

Parameter	Description
Current Connections	The number of current open class 3 connections.
Connection Failures	The number of failed attempts at establishing a class 3 connection with a Logix controller.
Tag Not Exist Errors	The number of tag read and tag write transactions that failed due to the destination tag not existing.
Privilege Violations	The number of tag read and tag write transactions that failed due to a privilege violation error. **Note:** This may be caused by the *External Access* property of the Logix tag being set to either **NONE** or **READ ONLY**.
Tag Reads	The number of tag read transactions executed by the PLX51-HART-8I.
Tag Writes	The number of tag write transactions executed by the PLX51-HART-8I.
ENIP Retries	This count increases when no response is received from the Logix Controller within the ENIP timeout.
ENIP Failures	This count increases when the ENIP Retry Limit is reached, and no response has been received from the Logix Controller.
Access General Error	This count increases when a tag cannot be accessed for any other reason not reported above.

Table 9.6 – Logix Statistics Tab

9.2.7 Modbus

The *Modbus* tab displays the Modbus statistics for the Modbus Read and Write Message Exchanges when the module is a Modbus Server or Modbus Client.

Note: The *Modbus Statistics* tab is displayed only if the module has the primary interface set to **MODBUS CLIENT** or **MODBUS SERVER**.

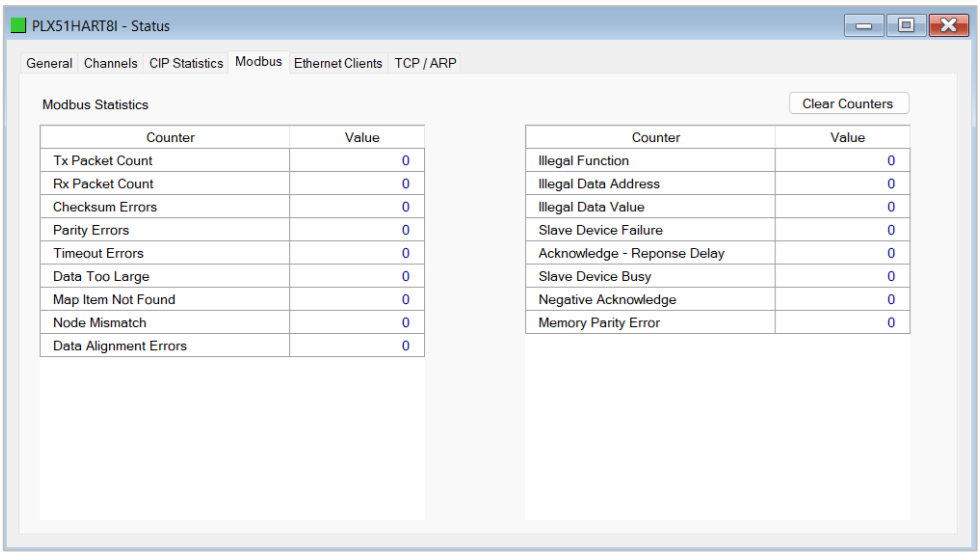


Figure 9.10. - Status monitoring – Modbus Statistics

Statistic	Description
Tx Packet Count	The number of Modbus packets sent by the module.
Rx Packet Count	The number of Modbus packets received by the module.
Checksum errors	The number of corrupted Modbus packets received by the module.
Parity errors	The number of bytes with parity errors received by the module.
Timeout Errors	The number of message response timeouts the module has encountered.
Data Too Large	The number of Modbus requests or responses where the data was too large to process.
Map Item Not Found	The number of Modbus requests did not match any mapped items.
Node Mismatch	The received Modbus request did not match the module's Modbus node address.
Data Alignment Errors	The Modbus request and associated mapped item is not byte aligned with the destination Logix tag.
Illegal Function	The number of times the Modbus device responded with an Illegal Function exception.
Illegal Data Address	The number of times the Modbus device responded with an Illegal Data Address exception.
Illegal Data Value	The number of times the Modbus device responded with an Illegal Data Value exception.
Slave Device Failure	The number of times the Modbus device responded with a Device Failure exception.
Acknowledge – Response Delay	The number of times the Modbus device responded with an Acknowledge exception.
Slave Device Busy	The number of times the Modbus device responded with a Slave Busy exception.
Negative Acknowledge	The number of times the Modbus device responded with a Negative Acknowledge exception.
Memory Parity Error	The number of times the Modbus device responded with a Memory Parity exception.

Table 9.7 - Modbus Statistics Tab

9.2.8 CIP Statistics

The *CIP Statistics* tab displays the Ethernet CIP statistics.

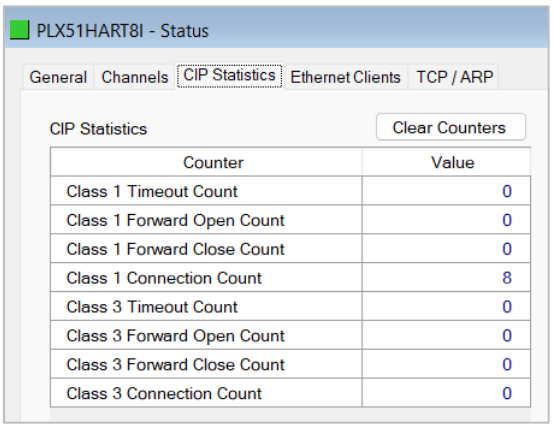


Figure 9.11 - Status monitoring – CIP Statistics

Statistic	Description
Class 1 Timeout Count	The number of Class 1 connections closed due to Timeouts.
Class 3 Timeout Count	The number of Class 3 connections closed due to Timeouts.
Class 1 Forward Open Count	The number of Class 1 Forward Open (connection establishment) messages sent.
Class 3 Forward Open Count	The number of Class 3 Forward Open (connection establishment) messages sent.
Class 1 Forward Close Count	The number of Class 1 Forward Close (connection termination) messages sent.
Class 3 Forward Close Count	The number of Class 3 Forward Close (connection termination) messages sent.
Class 1 Connection Count	The current number of active Class 1 connections.
Class 3 Connection Count	The current number of active Class 3 connections.

Table 9.8 – Mapped Item statistics

9.2.9 Ethernet Clients

The *Ethernet Clients* tab displays details of the Ethernet and EtherNet/IP clients connected to the PLX51-HART-8I.

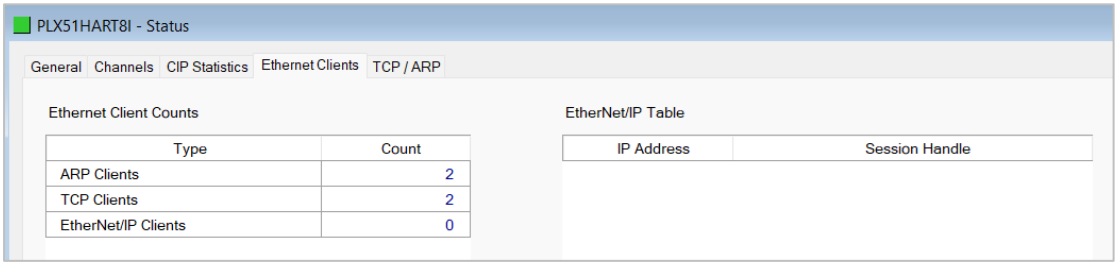


Figure 9.12 –Status monitoring – Ethernet Client Statistics

9.2.10 TCP/ARP

The *TCP/ARP* tab displays details of the internal Ethernet ARP and TCP lists of the PLX51-HART-8I.

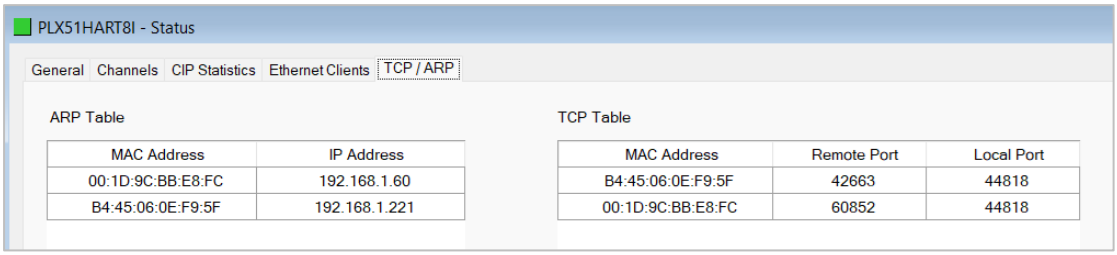


Figure 9.13 – Status monitoring – Ethernet TCP / ARP Statistics

9.3 Channel 0 - 7

The PLX51-HART-8I provides statistics and status information for each of the Analog Input channels.

The *Channel Status* window can be opened by right-clicking on the specific Channel and selecting **STATUS** (when online in the PLX50CU). The *Channel Status* window contains multiple tabs to display the status of the specific Channel.

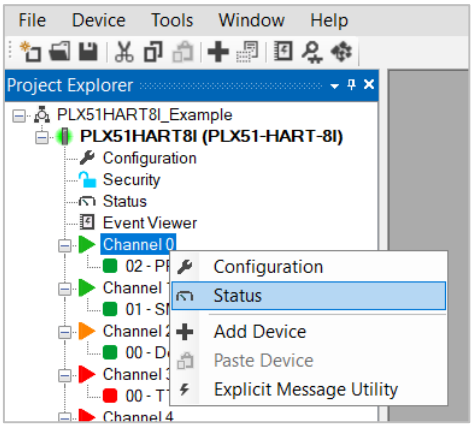


Figure 9.14 – Channel Status monitoring

9.3.1 General

The *General* tab displays the general status for a specific HART channel for the PLX51-HART-8I.

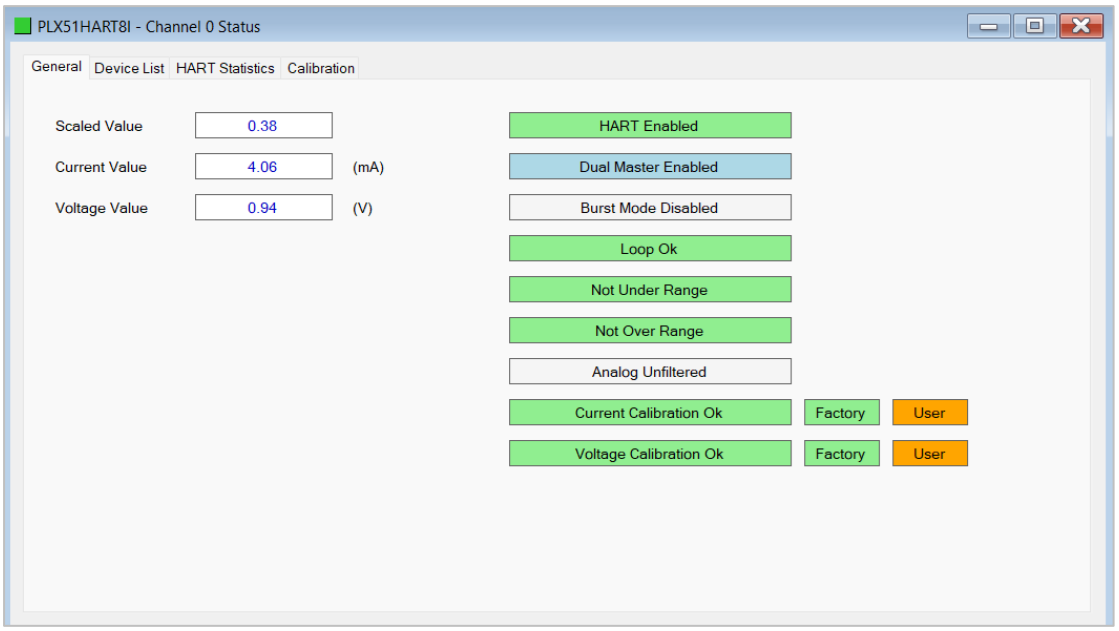


Figure 9.15 – Channel Status monitoring – General

Statistic	Description
Scaled Value	The input voltage reading for the specific channel (V).
Current Value	The input current reading for the specific channel (mA).
Voltage Value	The scaled value for the specific channel.

Table 9.9 – Analog Input Channel - General

9.3.2 Device List

See section *3.5.1.2 Device List Scanning* for more information.

9.3.3 HART Statistics

The *HART Statistics* tab displays the statistics for the HART communication for the selected Analog Input Channel.

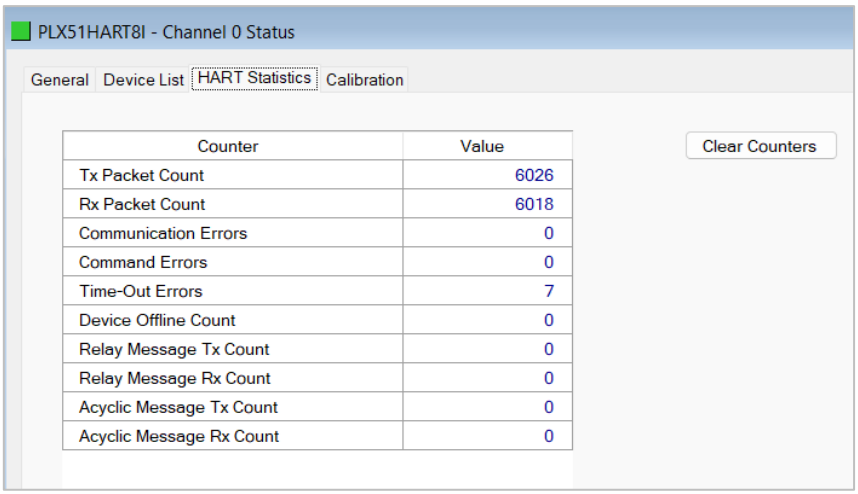


Figure 9.16 - Channel Status monitoring – HART Statistics

Statistic	Description
Tx Packet Count	The number of HART packets sent.
Rx Packet Count	The number of HART packets received.
Communication Errors	The number of communication errors experienced.
Command Errors	The number of command errors experienced.
Time-Out Errors	The number of HART timeout errors experienced.
Relay Message Tx Count	The number of HART packets sent via relay messages (DTMs etc.)
Relay Message Rx Count	The number of HART packets received for relay messages (DTMs etc.)
Acyclic Message Tx Count	The number of HART packets sent from the Advanced Messages configuration list.
Acyclic Message Rx Count	The number of HART packets received for the Advanced Messages configuration list.

Table 9.10 – Analog Input Channel overview

9.3.4 Calibration

See section *3.6 Channel Calibration* for more information.

9.4 HART Devices

The PLX51-HART-8I provides individual statistics and status information for each HART Device connected to a specific Analog Input Channel.

The HART Device *Status* monitoring window can be opened by right-clicking on the specific HART Device and selecting **STATUS** (when online in the PLX50CU). The HART Device *Status* window contains multiple tabs to display the status of the specific HART Device.

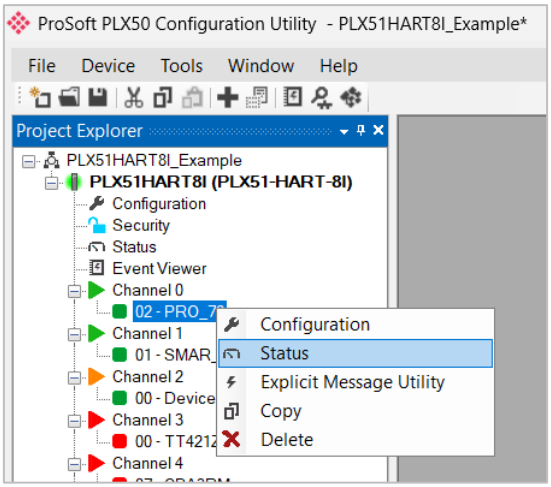


Figure 9.17 – HART Device Status monitoring

9.4.1 General

The *General* tab displays the general status for a specific HART device for the PLX51-HART-8I.

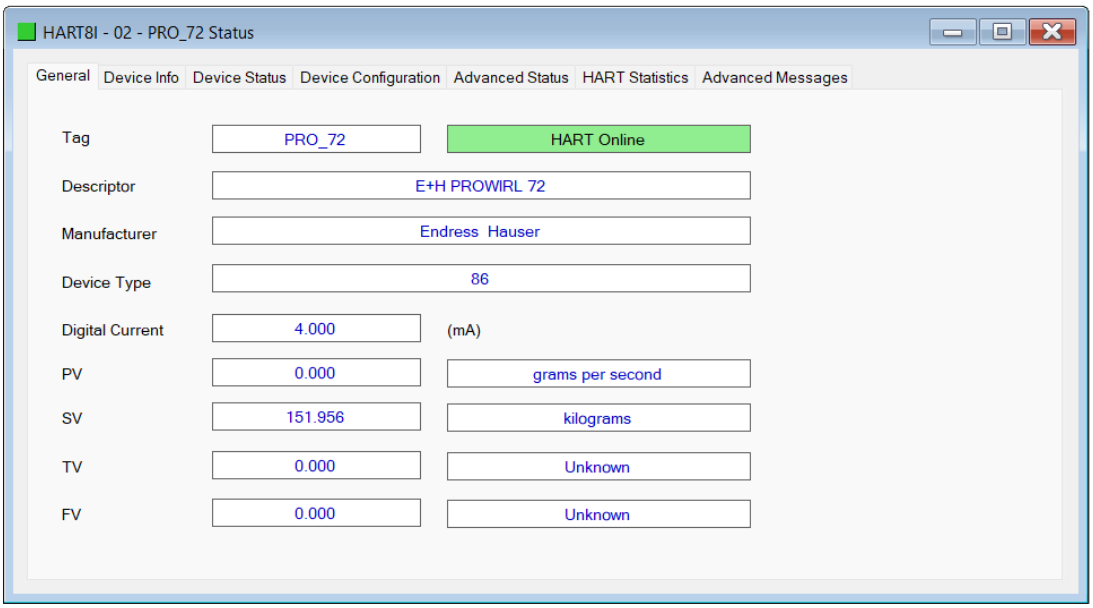


Figure 9.18 - HART Device Status monitoring – General

Statistic	Description
Tag	The user tag name configured in the field device. (8 characters)
Status	The status of the HART communication.
Descriptor	The user descriptor configured in the field device. (16 characters)
Manufacturer	The field device manufacturer.
Device Type	The device type code assigned by the manufacturer.
PV (and Units)	The primary variable displayed in engineering units, with the engineering unit enumeration.
SV (and Units)	The secondary variable displayed in engineering units, with the engineering unit enumeration.
TV (and Units)	The third variable displayed in engineering units, with the engineering unit enumeration.
FV (and Units)	The fourth variable displayed in engineering units, with the engineering unit enumeration.

Table 9.11 – HART Device Status monitoring – General

9.4.2 Device Info

The *Device Info* tab displays additional information of the HART device.

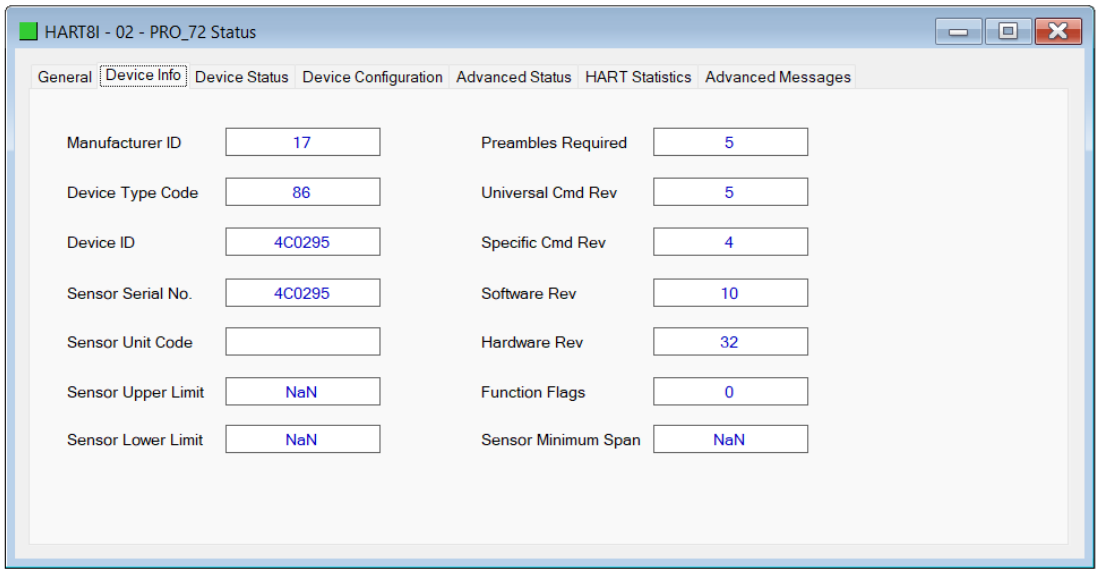


Figure 9.19 - HART Device Status monitoring – Device Info

Statistic	Description
Manufacturer ID	The field device manufacturer's unique identification code.
Device Type Code	The device type code assigned by the manufacturer.
Device ID	The device identification code assigned by the manufacturer.
Sensor Serial Number	The serial number of the field device sensor.
Sensor Unit Code	The engineering unit code used for the sensor limits.
Sensor Upper Limit	The upper limit of the sensor in engineering units.
Sensor Lower Limit	The lower limit of the sensor in engineering units.
Preambles Required	The minimum number of preambles required by the field device to process a HART request.
Universal Command Revision	The universal command revision supported by the field device.
Specific Command Revision	The specific command revision supported by the field device.
Software Revision	The software revision of the field device.
Hardware Revision	The hardware revision of the field device electronics.
Function Flags	The Device Function Flags as reported by the field device.
Sensor Minimum Span	The minimum span allowed by the sensor.

Table 9.12 – HART Device Status monitoring – Device Info

9.4.3 Device Status

The *Device Status* tab displays the status of the HART Device as well as the status returned by the HART device in the last response.

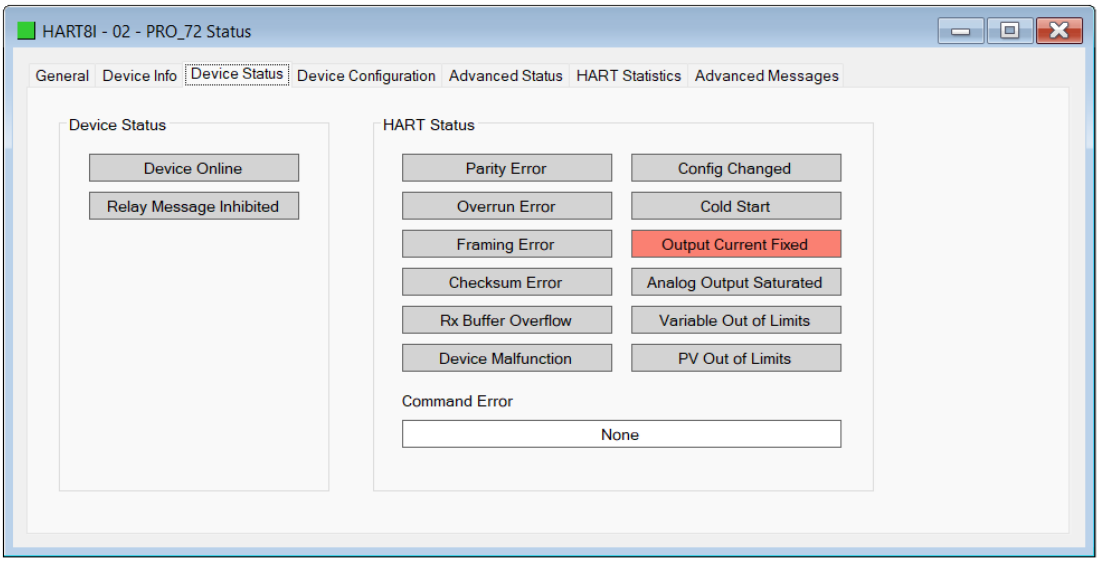


Figure 9.20 - HART Device Status monitoring – Device Status

Statistic	Description
Device Online	This will indicate if the specific HART Device is online or offline.
Relay Message Inhibit	Flagged when Class 2 HART relay messages have been disabled in the configuration.
Parity Error	Flagged if the field device received a message with a parity error
Overrun Error	Flagged if the field device received buffer is overrun.
Framing Error	Flagged if the field device receives a message with an invalid stop delimiter.
Checksum Error	Flagged if the field device receives a message with an invalid checksum.
Rx Buffer Overflow	Flagged if the field device receives a message too long for the receive buffer.
Device Malfunction	Flagged if the field device has detected an error or suffered some hardware failure.
Config Changed	Flagged if an operation resulted in the configuration changing.
Cold Start	Flagged if the field device has experienced a power failure or reset.
Output Current Fixed	Flagged if the loop current is set at a fixed value and is not responding to process variations
Analog Output Saturated	Flagged if the Loop Current has reached its upper or lower limit
Variable Out of Limits	Flagged if a variable other than the PV is beyond its operating limits.
PV Out of Limits	Flagged if the PV is beyond its operating limits.
Command Error	An enumerated error in response to the last command issued.

Table 9.13 – HART Device Status monitoring – Device Status

9.4.4 Device Configuration

The *Device Configuration* tab provides the facility to display and modify common HART parameters in the specific HART device.

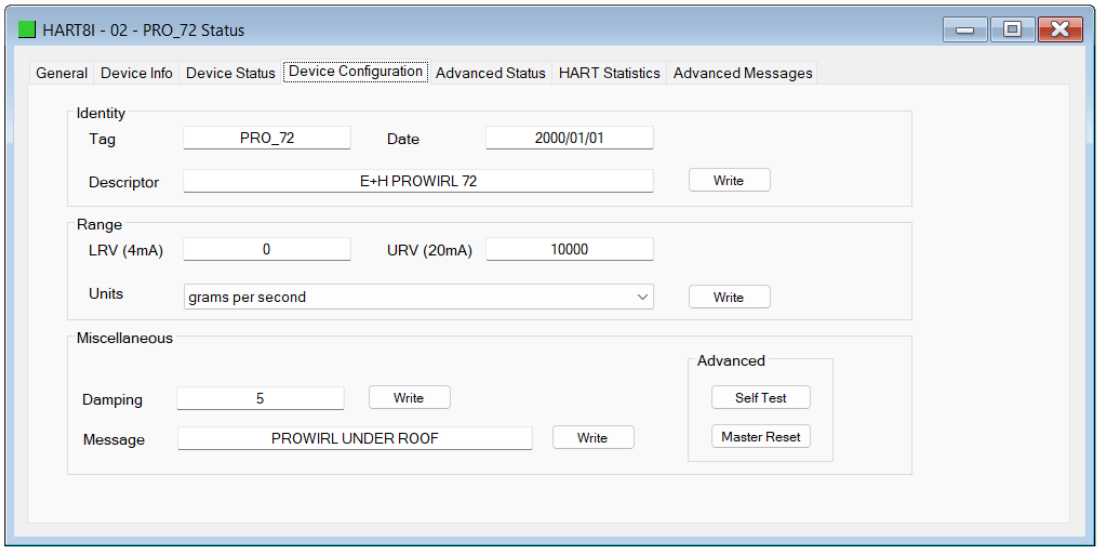


Figure 9.21 - Status monitoring – HART Device Status monitoring – Device Configuration

Statistic	Description
Tag	The user tag name configured in the field device. (8 characters). **Note**: The Tag, Descriptor and Date are updated together.
Descriptor	The user descriptor configured in the field device. (16 characters). **Note**: The Tag, Descriptor and Date are updated together.
Date	The date when the tag and descriptor configuration was last modified. **Note**: The Tag, Descriptor and Date are updated together.
LRV	The Lower Range Value in engineering units represented by the 4-mA analog signal. **Note**: The LRV, URV and Range Units are updated together.
URV	The Upper Range Value in engineering units represented by the 20-mA analog signal. **Note**: The LRV, URV and Range Units are updated together.
Range Units	The engineering units in which the LRV and URV values are specified. **Note**: The LRV, URV and Range Units are updated together.
Damping	The damping value, specified in seconds. Damping refers to the digital filtering of process variables to remove transient and potentially erroneous deviations from the actual measure variable.
Message	A user defined 32-character message stored in the field device.
Master Reset	Resets the field device

Table 9.14 – HART Device Status monitoring – Device Configuration

A parameter can be modified by entering the new value into the appropriate text box and clicking the adjacent **UPDATE** button. When the parameter is pending, that is, edited but not yet committed, then the text box will be shaded yellow. Once the value has been written (updated) the value will be written to the field device and then re-read from the field device, after which the parameter background will return to normal.

9.4.5 Advanced Status

The *Advanced Status* tab displays the advanced and device specific status information of the field device. Due to the manufacturer's specific encoding of these parameters, consult the field device manufacturer's documentation for more information.

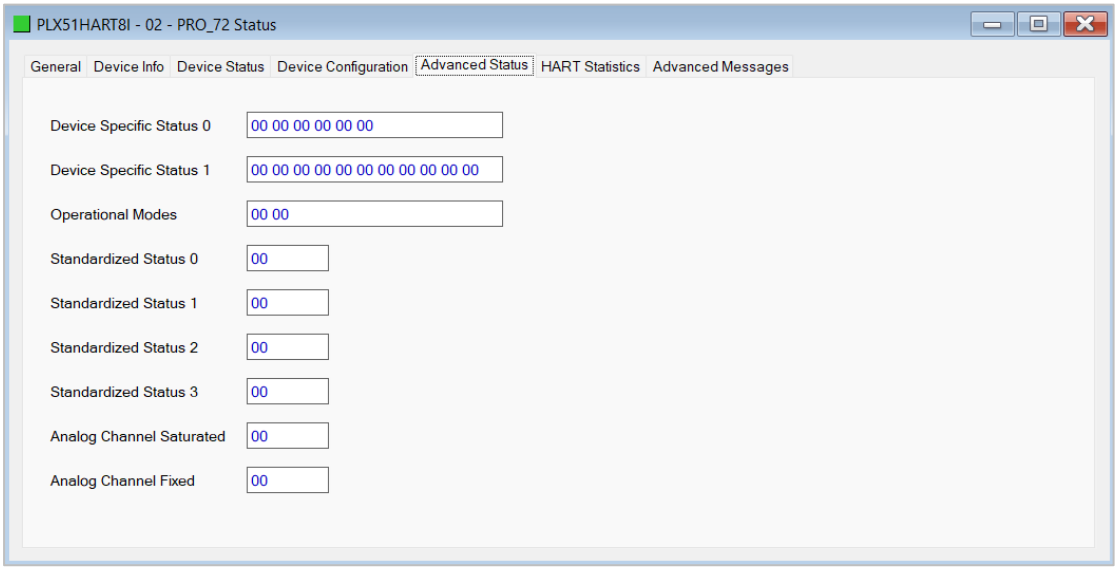


Figure 9.22 - HART Device Status monitoring – Advanced Status

9.4.6 HART Statistics

The *HART Statistics* tab displays the HART communication statistics for the specific HART Device.

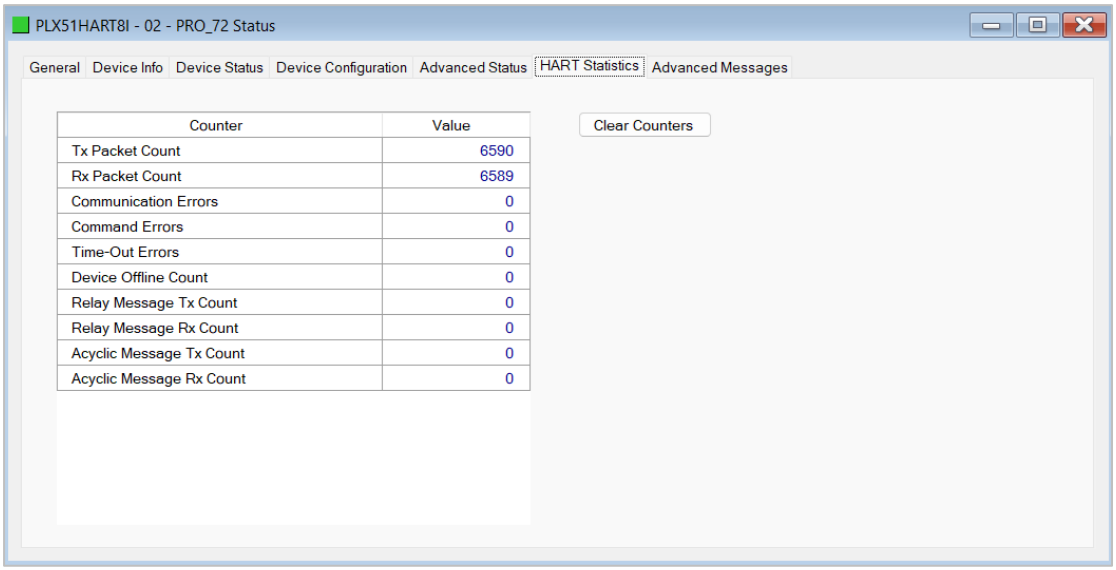


Figure 9.23 - HART Device Status monitoring – HART Statistics

Statistic	Description
Tx Packet Count	The number of HART packets sent.
Rx Packet Count	The number of HART packets received.
Communication Errors	The number of communication errors experienced.
Command Errors	The number of command errors experienced.
Time-Out Errors	The number of HART timeout errors experienced.
Relay Message Tx Count	The number of HART packets sent via relay messages (DTMs etc.)
Relay Message Rx Count	The number of HART packets received for relay messages (DTMs etc.)
Acyclic Message Tx Count	The number of HART packets sent from the Advanced Messages configuration list.
Acyclic Message Rx Count	The number of HART packets received for the Advanced Messages configuration list.

Table 9.15 – HART Device Status monitoring – HART Statistics

9.4.7 Advanced Messages

The *Advanced Messages* tab displays an overview of all the Advanced Messages configured for the specific HART Device.

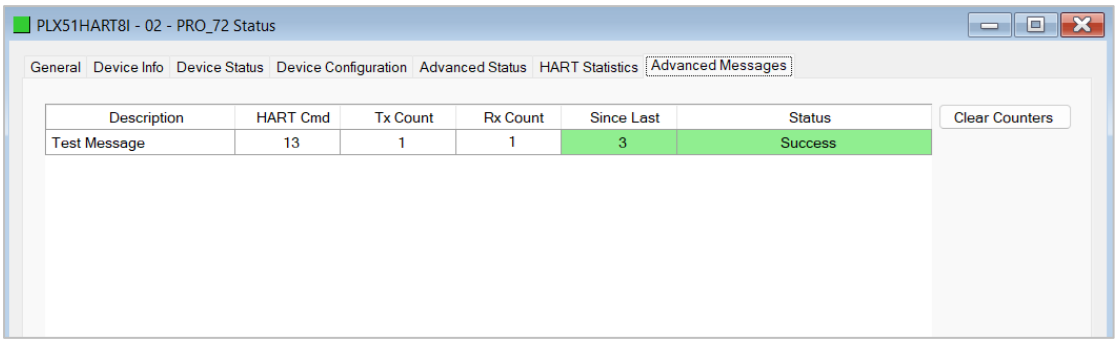


Figure 9.24 - HART Device Status monitoring – Advanced Messages

Statistic	Description
Description	The configured description for the Advanced Message
HART Cmd	The configured HART command that will be sent for the Advanced Message.
Tx Count	The number of times the Advanced Message request has been sent.
Rx Count	The number of times the Advanced Message request received a response.
Since Last	The number of seconds since the last time the specific Advanced Message was sent.
Status	The status of the last Advanced Message transaction.

Table 9.16 – HART Device Status monitoring – Advanced Messages

9.5 Target Device Status Monitoring in the PLX50 Configuration Utility

The PLX51-HART-8I provides individual statistics and status for each of the EtherNet/IP Class 1 or explicit message devices when the *Primary Interface* is set to **ETHERNET/IP ORIGINATOR**.

9.5.1 EtherNet/IP

When online with the PLX51-HART-8I in PLX50CU, right-click on the desired EtherNet/IP device under the *EtherNet/IP Connections* tree in PLX50CU and select **STATUS**.

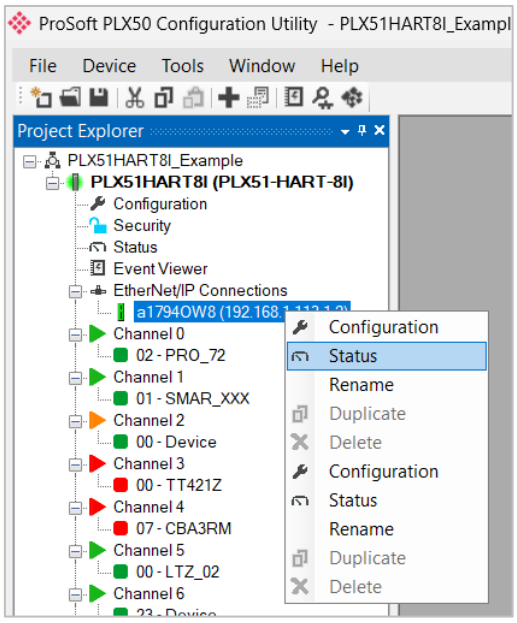


Figure 9.25 – EtherNet/IP Device Status – Status selection

9.5.1.1 General

The *General Status* for the EtherNet/IP device shows the connection statistics and parameters associated with the EtherNet/IP Class 1 connection.

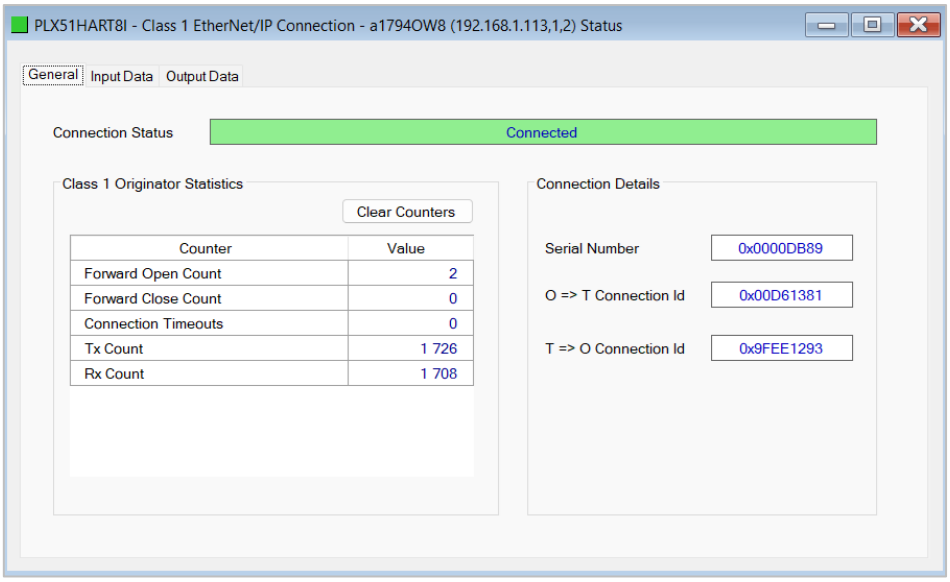


Figure 9.26 – EtherNet/IP Device Status – General Status

Statistic	Description
Connection Status	The current connection status of the module. **Connected**: The device is connected and exchanging data using Class 1 cyclic communication. **Offline**: The device is offline and not connected Various response faults If the connection parameters entered are not correct, the target device will usually reply with the specific reason for the connection rejection, for example: Connection Status: Invalid Originator To Target Size
Class 1 Originator Statistics	
Forward Open Count	The number of Class 1 Forward Open (connection establishment) messages sent to this device.
Forward Close Count	The number of Class 1 Forward Close (connection termination) messages sent or received from this device.
Connection Timeouts	The number of this connection was closed due to timeouts.
Tx Count	Number of Class 1 messages sent to the specific target device.
Rx Count	Number of Class 1 messages received from the specific target device.
Connection Details	
Serial Number	The active connection's serial number.
O -> T Connection Id	The active connection Originator to Target Connection Id.
T -> O Connection Id	The active connection Target to Originator Connection Id.

Table 9.17 – EtherNet/IP Class 1 Device status and statistics

9.5.1.2 Input Data

The *Input Data* for the EtherNet/IP device shows the Input Assembly associated with the EtherNet/IP Class 1 connection.

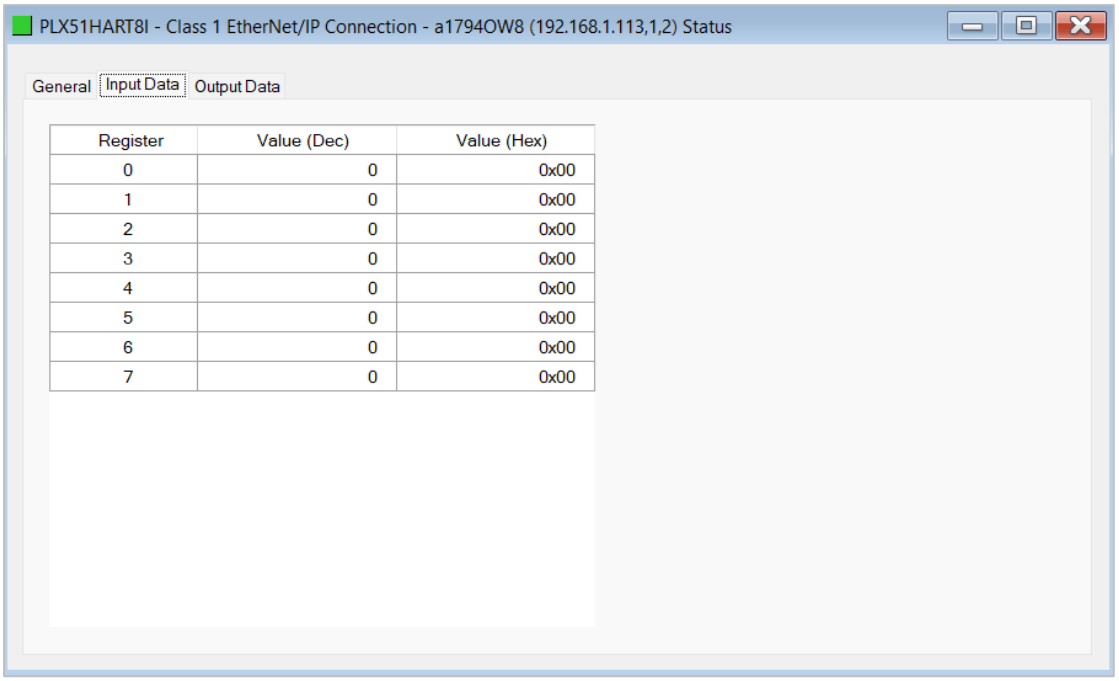


Figure 9.27 – EtherNet/IP Device Status – Input Data

9.5.1.3 Output Data

The *Output Data* for the EtherNet/IP device shows the Output Assembly associated with the EtherNet/IP Class 1 connection.

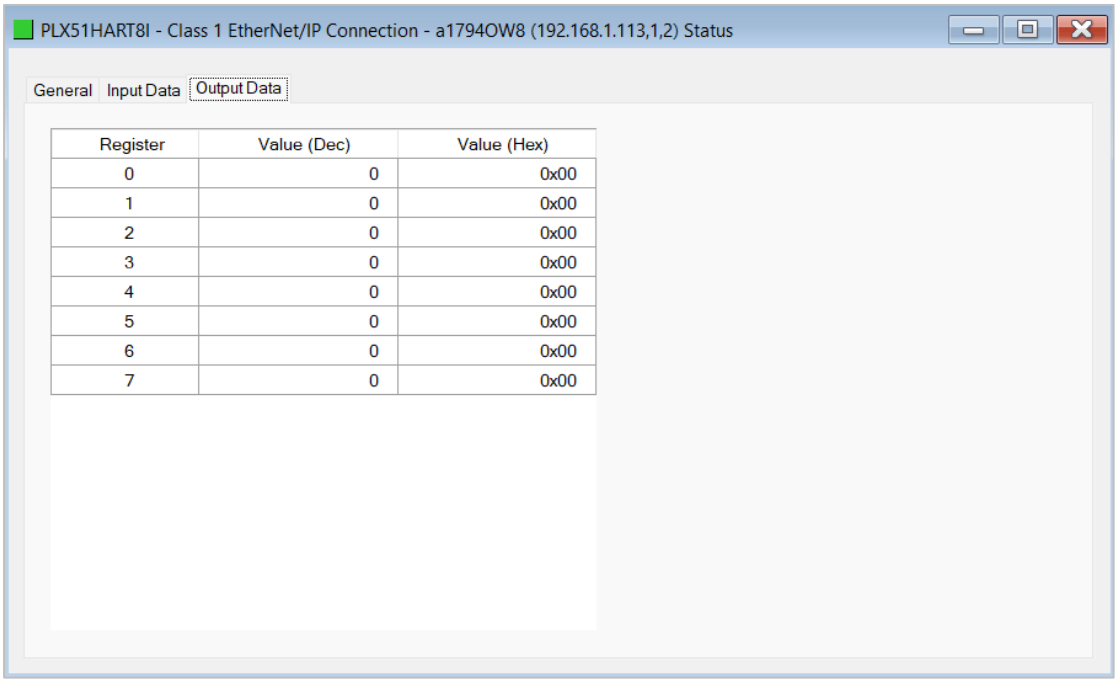


Figure 9.28 – EtherNet/IP Device Status – Output Data

9.6 Module Event Log

The PLX51-HART-8I logs various diagnostic records to an internal event log. These logs are stored in non-volatile memory and can be displayed using PLX50CU or via the web interface. To view them in PLX50CU, select the **EVENT VIEWER** option in the Project Explorer tree.

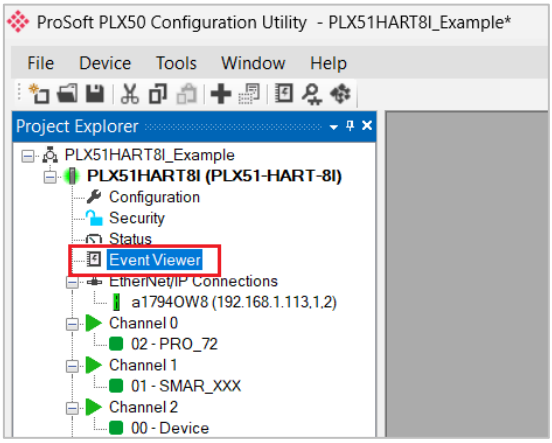
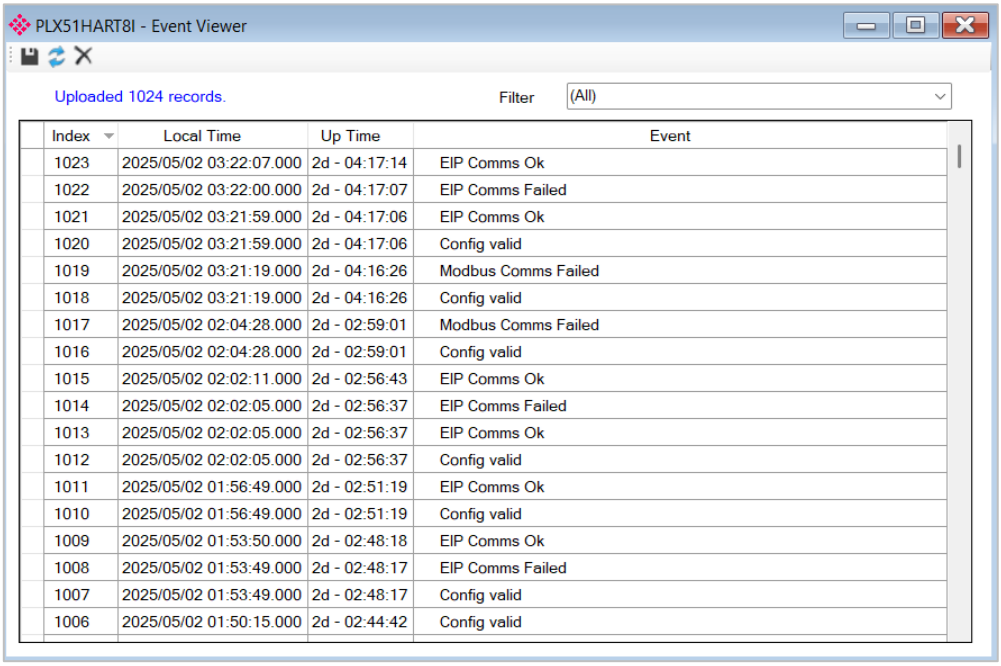


Figure 9.29 - Selecting the module Event Log

The *Event Log* window will open and automatically read all the events from the module. The log entries are sorted to have the latest record at the top. Custom sorting is achieved by double-clicking on the column headings.



Index	Local Time	Up Time	Event
1023	2025/05/02 03:22:07.000	2d - 04:17:14	EIP Comms Ok
1022	2025/05/02 03:22:00.000	2d - 04:17:07	EIP Comms Failed
1021	2025/05/02 03:21:59.000	2d - 04:17:06	EIP Comms Ok
1020	2025/05/02 03:21:59.000	2d - 04:17:06	Config valid
1019	2025/05/02 03:21:19.000	2d - 04:16:26	Modbus Comms Failed
1018	2025/05/02 03:21:19.000	2d - 04:16:26	Config valid
1017	2025/05/02 02:04:28.000	2d - 02:59:01	Modbus Comms Failed
1016	2025/05/02 02:04:28.000	2d - 02:59:01	Config valid
1015	2025/05/02 02:02:11.000	2d - 02:56:43	EIP Comms Ok
1014	2025/05/02 02:02:05.000	2d - 02:56:37	EIP Comms Failed
1013	2025/05/02 02:02:05.000	2d - 02:56:37	EIP Comms Ok
1012	2025/05/02 02:02:05.000	2d - 02:56:37	Config valid
1011	2025/05/02 01:56:49.000	2d - 02:51:19	EIP Comms Ok
1010	2025/05/02 01:56:49.000	2d - 02:51:19	Config valid
1009	2025/05/02 01:53:50.000	2d - 02:48:18	EIP Comms Ok
1008	2025/05/02 01:53:49.000	2d - 02:48:17	EIP Comms Failed
1007	2025/05/02 01:53:49.000	2d - 02:48:17	Config valid
1006	2025/05/02 01:50:15.000	2d - 02:44:42	Config valid

Figure 9.30 - Module Event Log

The log can also be stored to a file for future analysis, by selecting the **SAVE** button in the tool menu. To view previously saved files, use the **EVENT LOG VIEWER** option under the *Tools* menu.

9.7 HART Packet Capture

The PLX51-HART-8I provides the capability to capture the HART traffic on each Analog Input Channel for analysis. This will allow the user and a remote support team to resolve any possible issues on site. To invoke the capture of the module, double-click on the **HART PACKET CAPTURE** item in the Project Explorer tree.

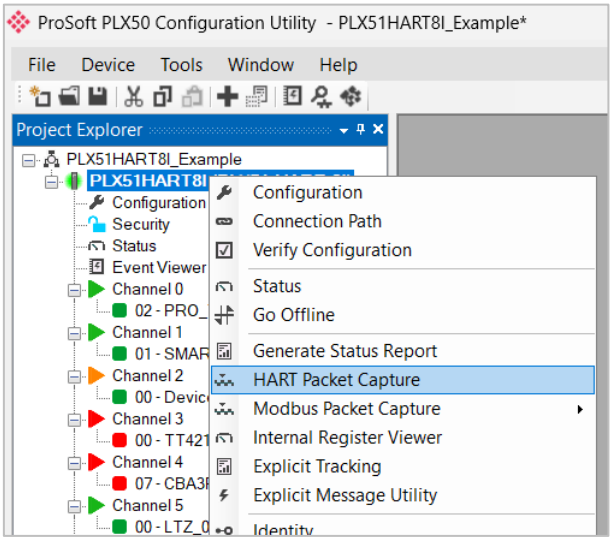


Figure 9.31 - Selecting HART Packet Capture

The *HART Packet Capture* window will open and automatically start capturing all HART packets.

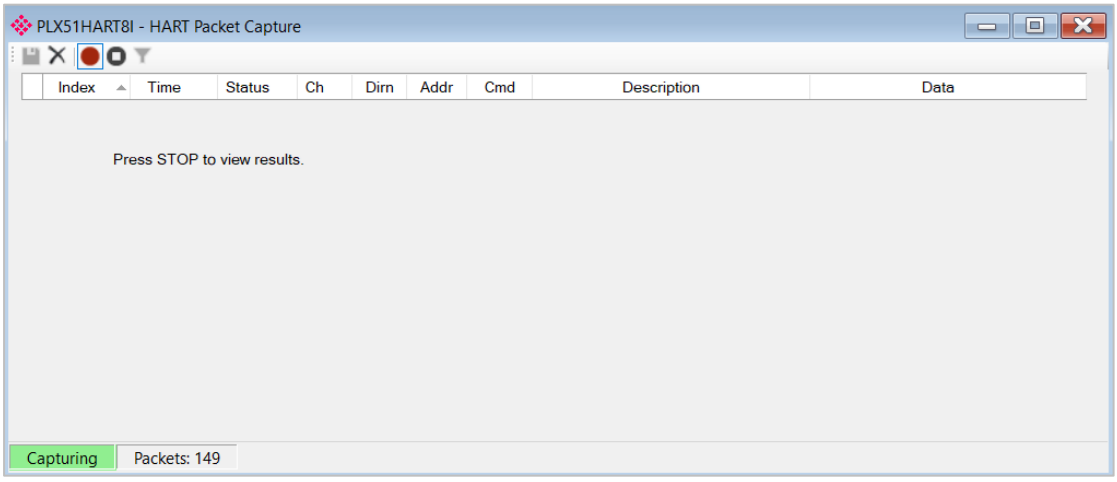


Figure 9.32 – HART packet capture

To display the captured HART packets, the capture process must first be stopped, by pressing the **STOP** button.

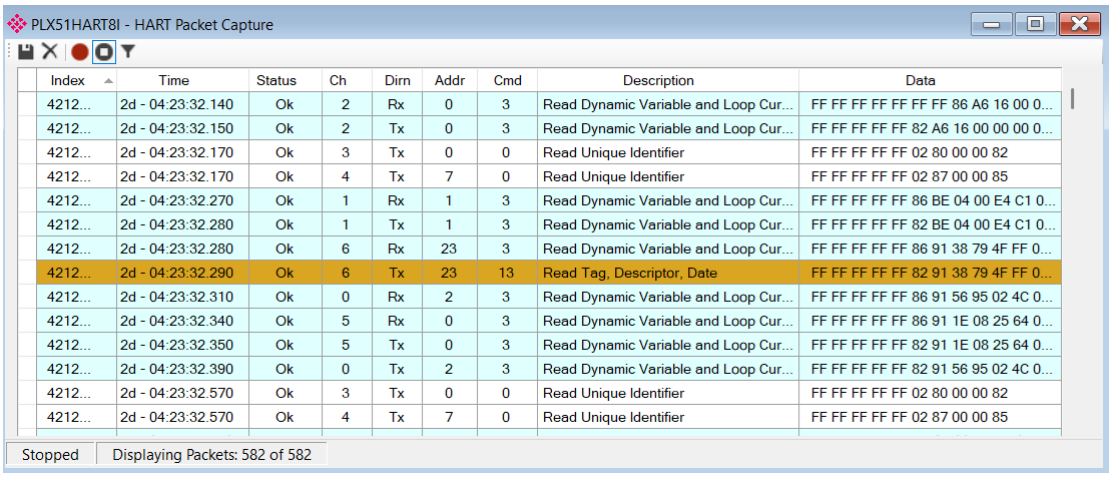


Figure 9.33 – HART Packet Capture complete

The capture HART packets can be filtered based on criteria for the following parameters:

- Channel
- Node Address
- HART Commands

To open the *Filter Options* select the **FILTER** icon in the toolbar.

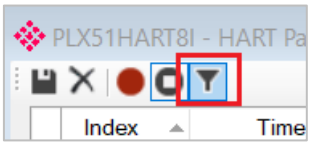


Figure 9.34 – HART Capture Filter

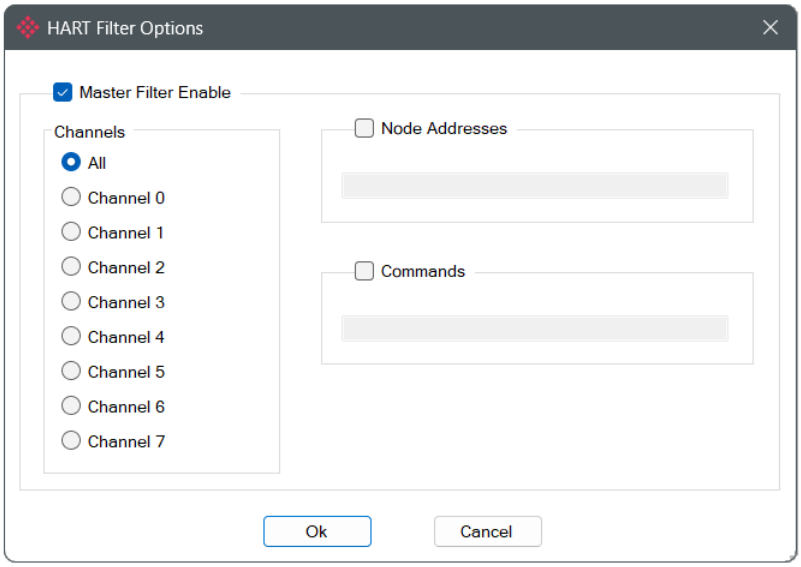


Figure 9.35 – HART Capture Filter Options

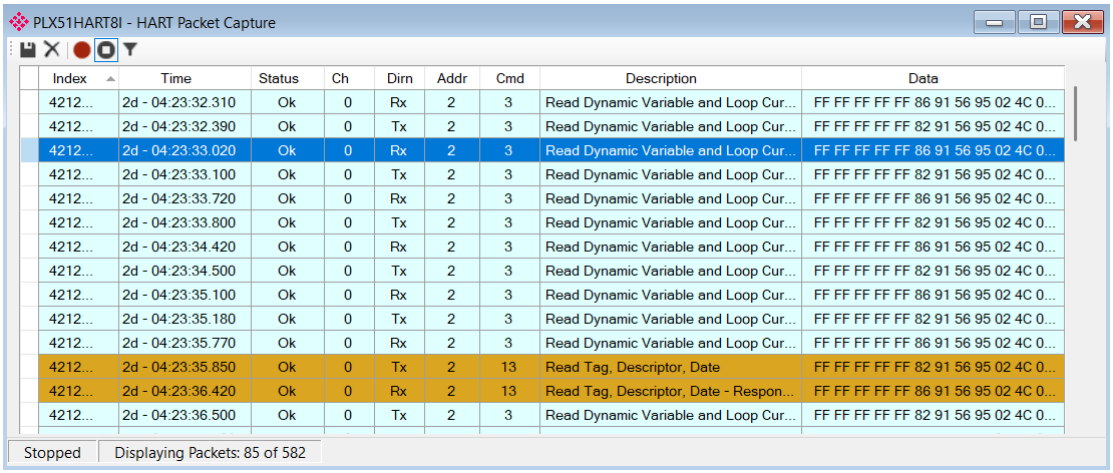


Figure 9.36 – Filtered HART Packet Capture

The captured HART packets are tabulated as follows:

Statistic	Description
Index	The packet index, incremented for each packet sent or received.
Time	The elapsed time since the module powered up.
Status	The status of the packet. Received packets are checked for valid HART constructions and valid checksums.
Ch	The HART channel where the packet was captured.
Dirn	The direction of the packet, either transmitted (Tx) or received (Rx).
Addr	The HART slave device short address.
Cmd	The HART command sent or received
Description	A basic description of the captured packet. If the user double-clicks on the description, it will provide a more detailed description.
Data	The raw HART data.

Table 9.18 – HART Packet Capture fields

The packet capture can be saved to a file for further analysis, by selecting the **SAVE** button on the toolbar. Previously saved HART Packet Capture files can be viewed by selecting the **HART PACKET CAPTURE VIEWER** option in the *Tools* menu.

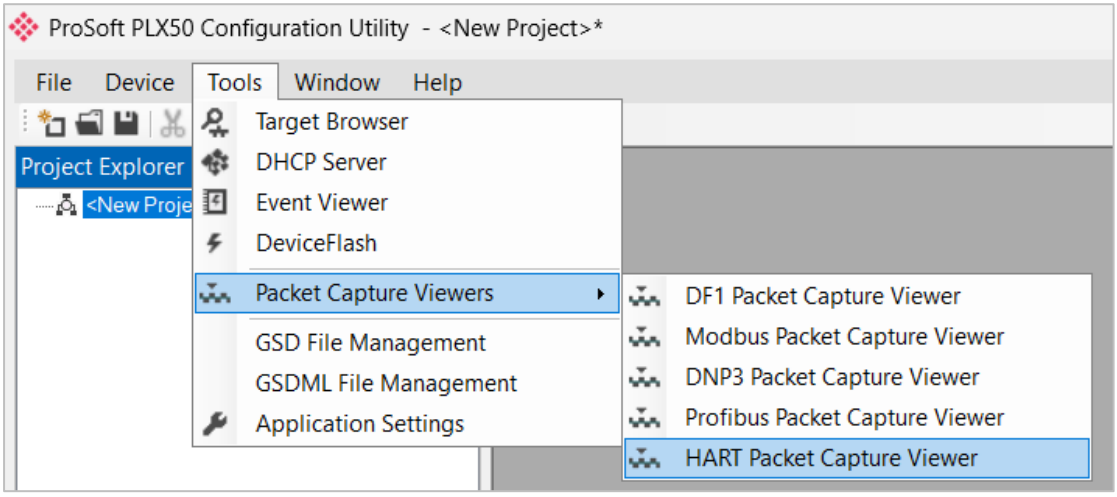


Figure 9.37 - Selecting the HART Packet Capture Viewer

9.8 Modbus Packet Capture

The module provides the capability to capture the Modbus traffic for analysis. This will allow the user and a remote support team to resolve any possible issues on site. To invoke the capture of the module, double-click on the **MODBUS PACKET CAPTURE** item in the Project Explorer tree.

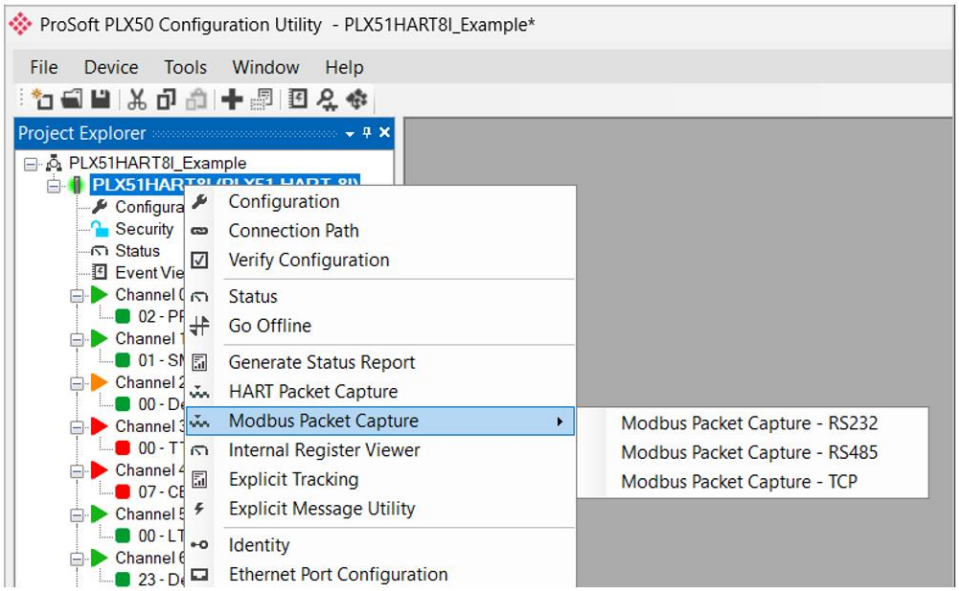


Figure 9.38 - Selecting Modbus Packet Capture

The *Modbus Packet Capture* window will open and automatically start capturing all Modbus packets.

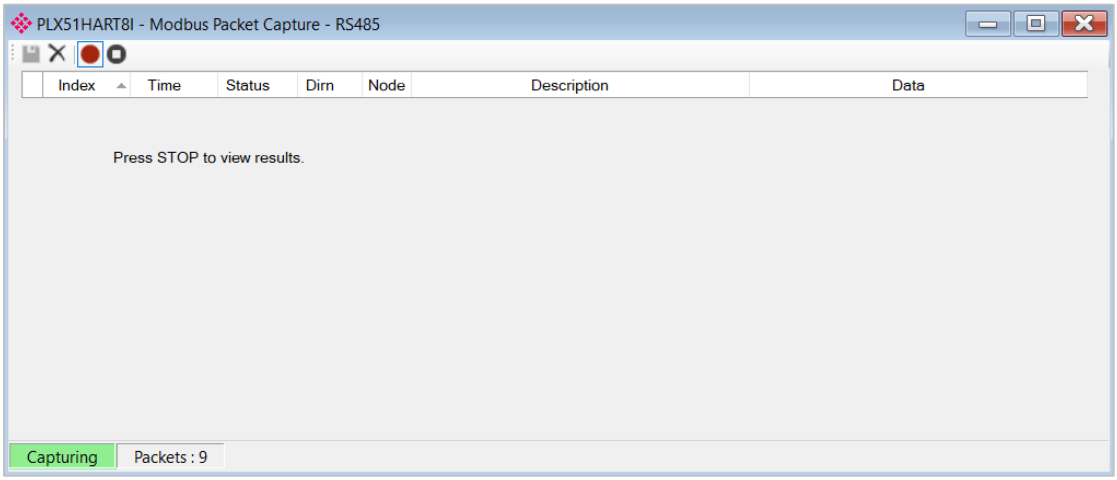


Figure 9.39 – Modbus packet capture

To display the captured Modbus packets, the capture process must first be stopped, by pressing the **STOP** button.

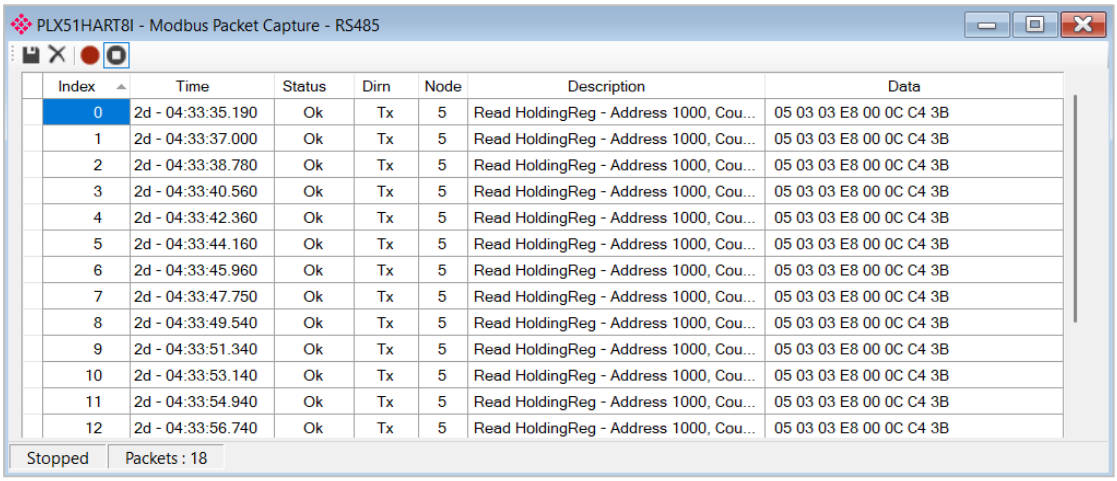


Figure 9.40 – Modbus Packet Capture complete

The captured Modbus packets are tabulated as follows:

Statistic	Description
Index	The packet index, incremented for each packet sent or received.
Time	The elapsed time since the module powered up.
Status	The status of the packet. Received packets are checked for valid Modbus constructs and valid checksums.
Port	Port on where the data was sent or received (TCP, RTU232, RTU485)
Dirn	The direction of the packet, either transmitted (Tx) or received (Rx).
Node	The Source Node address for the packet
Description	Description of the packet that was received.
Data	The raw packet data.

Table 9.19 – Modbus Packet Capture fields

The packet capture can be saved to a file for further analysis, by selecting the **SAVE** button on the toolbar. Previously saved Modbus Packet Capture files can be viewed by selecting the **MODBUS PACKET CAPTURE VIEWER** option in the *Tools* menu.

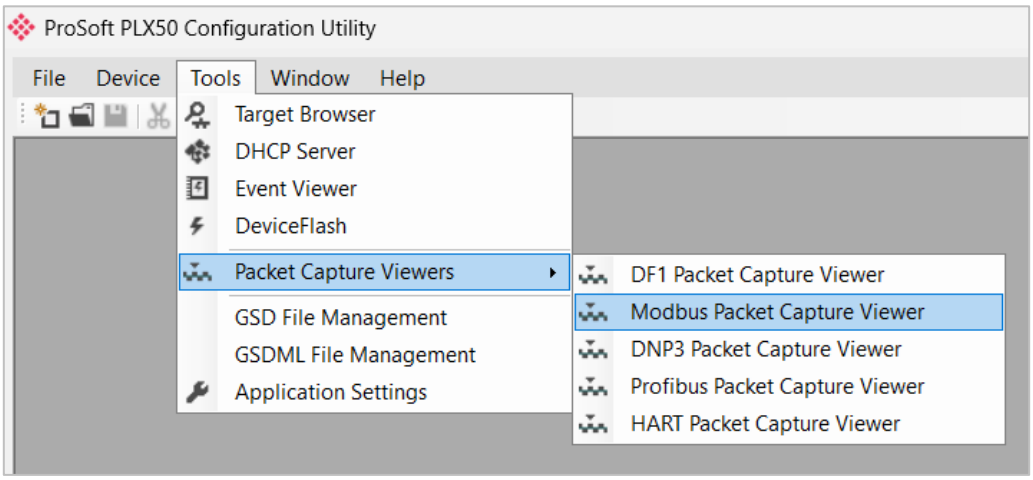


Figure 9.41 - Selecting the Modbus Packet Capture Viewer

9.9 Module Status Report

For assisting with support, the PLX50CU can generate a status report for the PLX51-HART-8I which is a Microsoft Word compatible document that can be emailed to support. To generate this report the user can right-click on the module (when online in PLX50CU) and select **GENERATE STATUS REPORT**.

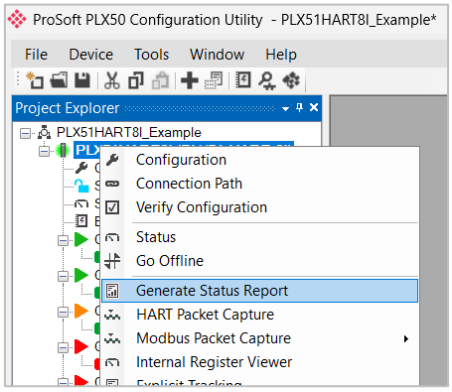


Figure 9.42 – Module Status Report

9.10 Modbus Summary CSV

PLX50CU can provide a summary of the Modbus registers being used in the form of a CSV file. This will assist the user to better understand where what data is being mapped (based on the PLX51-HART-8I configuration). To generate the Modbus Summary CSV, right-click on the module (when online in PLX50CU), and select **EXPORT MODBUS SUMMARY CSV**.

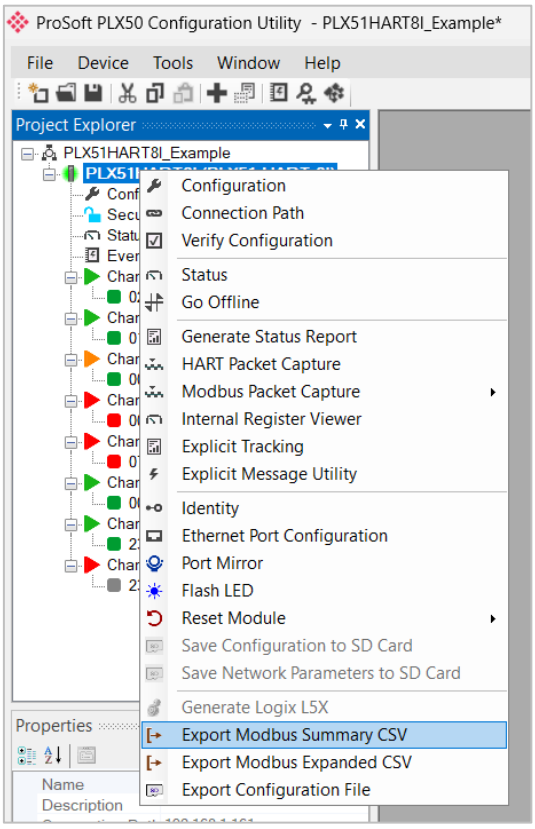


Figure 9.43 – Modbus Summary Report Generation

	A	B	C	D	E	F
1	Reg Type	Modbus Function	Start Address	End Address	Element Count	Description
2	HR	Read	1000	1023	24	System.Status
3	HR	Read	1024	1024	1	Internal.Data - N4Tempertaure.Data
4	HR	Read	1025	1026	2	Internal.Data - N4Tempertaure.Count
5	HR	Read	1027	1028	2	Internal.Data - N4Pressure.Data
6	HR	Read	1029	1030	2	Internal.Data - N4Pressure.Count
7	HR	Read	1031	1034	4	Internal.Data - DashKeys.Data
8	HR	Read	1035	1036	2	Internal.Data - DashKeys.Count
9	HR	Write	1037	1038	2	Internal.Data - E1Config.Data
10	HR	Write	1039	1040	2	Internal.Data - E1Config.Trigger
11	HR	Read	1041	1042	2	Internal.Data - E1Config.Count
12	HR	Write	1043	1045	3	Internal.Data - E2Preset.Data
13	HR	Read	1046	1047	2	Internal.Data - E2Preset.Count
14	HR	Write	1048	1051	4	Internal.Data - DashLED.Data
15	HR	Write	1052	1053	2	Internal.Data - DashLED.Trigger
16	HR	Read	1054	1055	2	Internal.Data - DashLED.Count
17	(End)					

Figure 9.44 – Modbus Summary CSV

9.11 Modbus Expanded CSV

The PLX50CU can provide a detailed version of the Modbus registers being used in the form of a CSV file. This will assist the user to better understand where what data is being mapped (based on the PLX51-HART-8I configuration). To generate the Modbus Expanded CSV, right-click on the module (when online in PLX50CU), and select **EXPORT MODBUS EXPANDED CSV**.

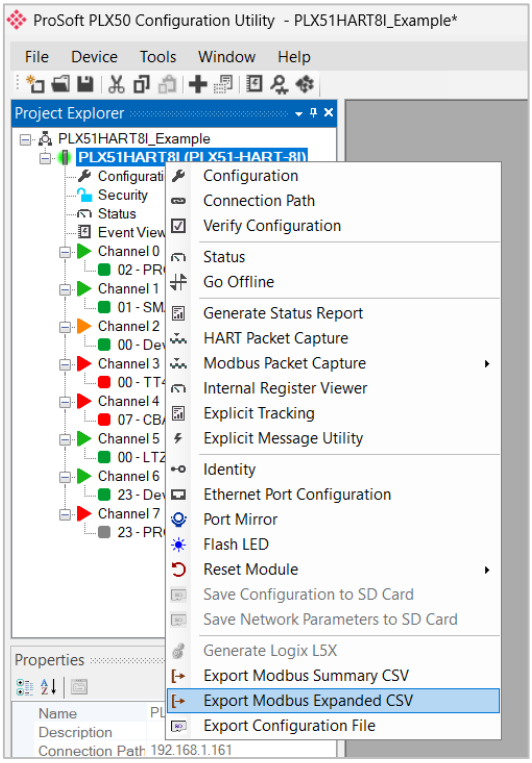


Figure 9.45 – Modbus Expanded Report Generation

	A	B	C	D	E	F
1	Reg Type	Modbus Function	Start Address	End Address	Element Count	Description
2	HR	Read	1000	1001	2	RouterStatus.GeneralStatus
3	HR	Read	1002	1002	1	RouterStatus.ConfigCRC
4	HR	Read	1003	1003	1	RouterStatus.TransactionRate
5	HR	Read	1004	1004	1	RouterStatus.CurrentBaudRate
6	HR	Read	1006	1007	2	RouterStatus.Temperature
7	HR	Read	1008	1009	2	RouterStatus.RxCanPacketCount
8	HR	Read	1010	1011	2	RouterStatus.TxCanPacketCount
9	HR	Read	1012	1013	2	RouterStatus.CANCRCErrors
10	HR	Read	1014	1015	2	RouterStatus.CANBitErrors
11	HR	Read	1016	1017	2	RouterStatus.CanStuffErrors
12	HR	Read	1018	1019	2	RouterStatus.BusOffCount
13	HR	Read	1020	1021	2	RouterStatus.CANAckErrors
14	HR	Read	1022	1023	2	RouterStatus.CANFormatErrors
15	HR	Read	1024	1024	1	Internal.Data - N4Tempertaure.Data
16	HR	Read	1025	1026	2	Internal.Data - N4Tempertaure.Count
17	HR	Read	1027	1028	2	Internal.Data - N4Pressure.Data
18	HR	Read	1029	1030	2	Internal.Data - N4Pressure.Count
19	HR	Read	1031	1034	4	Internal.Data - DashKeys.Data
20	HR	Read	1035	1036	2	Internal.Data - DashKeys.Count
21	HR	Write	1037	1038	2	Internal.Data - E1Config.Data
22	HR	Write	1039	1040	2	Internal.Data - E1Config.Trigger
23	HR	Read	1041	1042	2	Internal.Data - E1Config.Count
24	HR	Write	1043	1045	3	Internal.Data - E2Preset.Data
25	HR	Read	1046	1047	2	Internal.Data - E2Preset.Count
26	HR	Write	1048	1051	4	Internal.Data - DashLED.Data
27	HR	Write	1052	1053	2	Internal.Data - DashLED.Trigger
28	HR	Read	1054	1055	2	Internal.Data - DashLED.Count
29	(End)					

Figure 9.46 – Modbus Expanded CSV

9.12 Port Mirror

The PLX51-HART-8I can enable the one Ethernet port to mirror the traffic on the other Ethernet port. This allows the user to capture the traffic between the PLX51-HART-8I and another device without the need for an additional switch. Wireshark is the most popular tool used to capture Ethernet traffic.

To enable port mirroring, the *Port Mirror* option must be selected by right-clicking on the PLX51-HART-8I (when online in PLX50CU) and selecting **PORT MIRROR**.

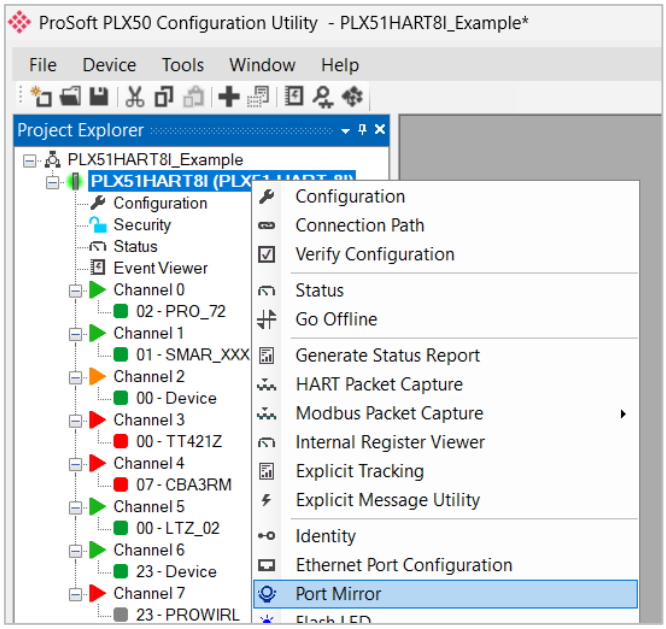


Figure 9.47 – Select Port Mirror Option

The Port Mirror *Mode* and *Port* can then be selected using the *Port Mirror Control*.

Important: The *Port Mirror* setting is volatile and will be disabled (by default) once the module is reset.

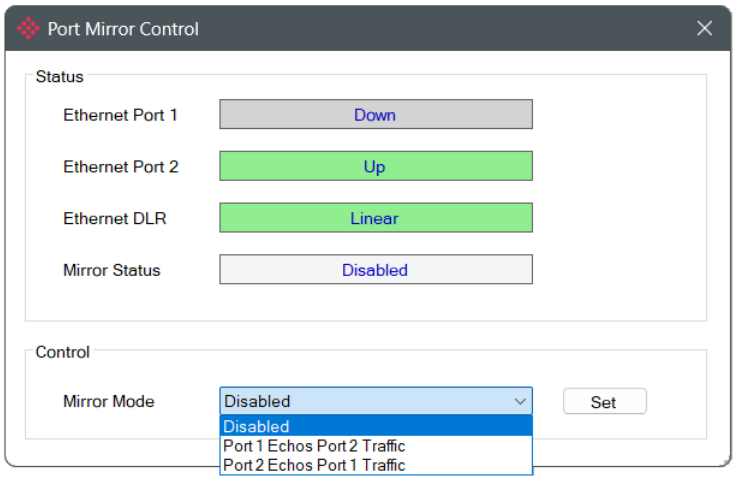


Figure 9.48 – Port Mirror Options

9.13 Flash LED

The PLX51-HART-8I can be requested to flash its OK LED to assist with finding which module has which IP Address. Once the Flash LED request has been sent, the PLX51-HART-8I will rapidly flash the OK LED between green, red, and blue for approximately five seconds. The OK LED will return to normal operation once the flashing time has elapsed.

Note: Requesting the Flash LED will not affect any operation of the module other than flashing the OK LED.

To send a Flash LED request, the **FLASH LED** option must be selected by right-clicking on the PLX51-HART-8I (when online in PLX50CU) and selecting **FLASH LED**.

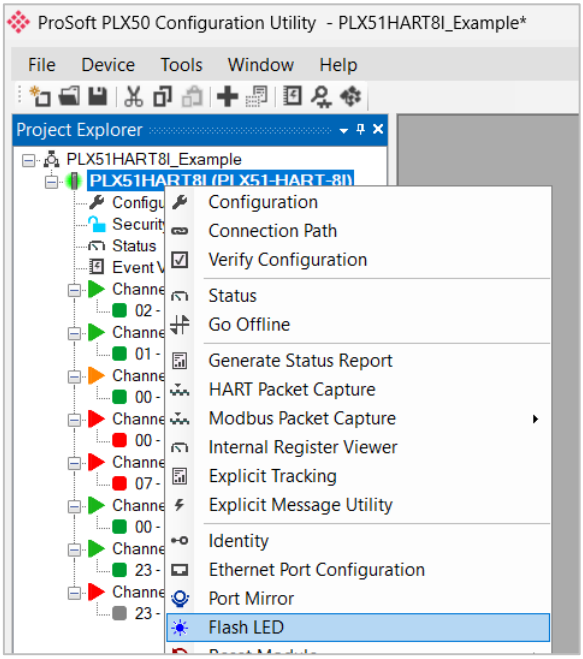


Figure 9.49 – Flash Module LED

10 Technical Specifications

10.1 Dimensions

Below are the enclosure dimensions as well as the required DIN rail dimensions. All dimensions are in millimeters.

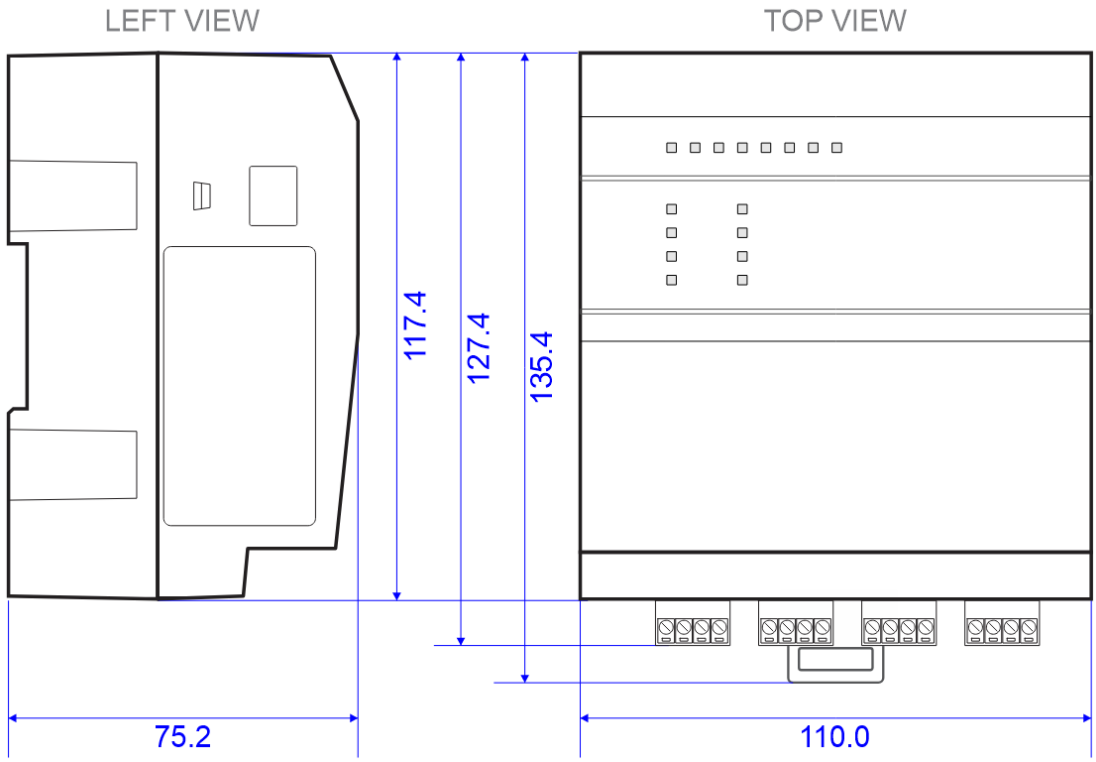


Figure 10.1 – PLX51-HART-8I enclosure dimensions.

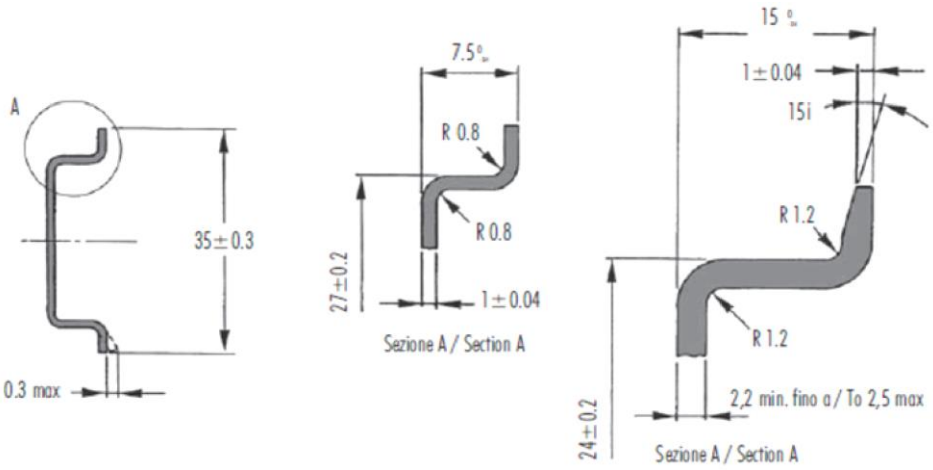


Figure 10.2 - Required DIN dimensions.

10.2 Electrical

Specification	Rating
Power requirements	Input: 10 – 32V DC, (200 mA @ 24 VDC)
Voltage Fluctuations	Voltage fluctuations < ±10% Transient Over-voltages up to the levels of OVERVOLTAGE CATEGORY I
Power consumption	5.1 W 470 mA maximum
Connector	3-way terminal
Conductors	24 – 18 AWG
Earth connection	Yes, terminal based
Emissions	IEC61000-6-4
ESD Immunity	EN 61000-4-2
Radiated RF Immunity	IEC 61000-4-3
EFT/B Immunity	EFT: IEC 61000-4-4
Surge Immunity	Surge: IEC 61000-4-5
Conducted RF Immunity	IEC 61000-4-6

Table 10.1 - Electrical specification.

10.3 Environmental

Specification	Rating
Enclosure rating	IP20, NEMA/UL Open Type Indoor use only
Temperature	-20°C to 65°C
Relative Humidity	5% to 90% - No condensation
Pollution Degree	2
Altitude	< 2000 m

Table 10.2 - Environmental specification.

10.4 Ethernet

Specification	Rating
Connector	RJ45
Conductors	CAT5 STP/UTP
ARP connections	Max 200
TCP connections	Max 100
CIP connections	Max 20
Communication rate	10/100Mbps
Duplex mode	Full/Half
Auto-MDIX support	Yes
Embedded switch	Yes, 2 x Ethernet ports Also supports Dual IP port split
Device Level Ring (DLR)	Supported
Network Time Protocol (NTP)	Supported
1588 Precision Time Protocol (PTP)	Supported

Table 10.3 - Ethernet specification.

10.5 Serial Port (RS232)

Specification	Rating
RS232 Connector	9-way terminal (shared with RS485)
RS232 Conductor	24 – 18 AWG
Electrical Isolation	1000 Vdc
BAUD	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Parity	None, Even, Odd
Data bits	8
Stop bits	1

Table 10.4 – RS232 Serial Port specification.

10.6 Serial Port (RS485)

Specification	Rating
RS485 Connector	9-way terminal (shared with RS485)
RS485 Conductor	24 – 18 AWG
Electrical Isolation	1500 Vrms for 1 minute.
BAUD	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Parity	None, Even, Odd
Data bits	8
Stop bits	1

Table 10.5 – RS485 Serial Port specification.

10.7 Analog Input Channel

Specification	Rating
Number of channels	8
ADC resolution	12 bit
Input impedance	250 Ω
Accuracy (calibrated 25°C)	< 0.15 %
Accuracy (uncalibrated)	< 0.30 %
Current Range	0 – 22 mA
Current limit	34 mA
Voltage Range	0 – 10 Vdc
Voltage Limit	11 Vdc
Isolated	Yes
Input Filter	Supported
Input Types Supported	Voltage Current 0-20mA Current 4-20mA Current 0-20mA (with external Resistor) Current 4-20mA (with external Resistor)
Analog Scaling	Supported

Table 10.6 – Analog Input Channel specification.

10.8 HART

Specification	Rating
HART Devices per Channel	Max 8 (total of 64 HART devices per PLX51-HART-8I module)
Configurable Update Rate	Supported
Configurable HART requests	Supported
Burst Mode	Supported
Pass-through requests	Supported
Device Type Manager (DTM)	Supported

Table 10.7 – HART specification.

10.9 Modbus Client

Specification	Rating
Modes Supported	Modbus TCP, Modbus RTU232, Modbus RTU485
Modbus RTU485 Termination	125 Ω - Software Enabled
Max. Modbus Server Devices	50
Max. Modbus Mapping	300
Mapping Ranges	Holding Register 0 to 65535 Input Register 0 to 65535 Input Status 0 to 65535 Coil Status 0 to 65535
Base Offset	Modbus (Base 0) PLC (Base 1)
Configurable Modbus TCP Port	Yes
Data Reformatting Supported	BB AA BB AA DD CC CC DD AA BB DD CC BB AA

Table 10.8 – Modbus Client specification

10.10 Modbus Server

Specification	Rating
Modes Supported	Modbus TCP, Modbus RTU232, Modbus RTU485 (simultaneous)
Modbus RTU485 Termination	Software set
Mapping Ranges	Holding Register 0 to 65535 Input Register 0 to 65535 Input Status 0 to 65535 Coil Status 0 to 65535
Base Offset	Modbus (Base 0) PLC (Base 1)
Configurable Modbus TCP Port	Yes

Table 10.9 – Modbus Server specification.

10.11 EtherNet/IP Target

Specification	Rating
Class 1 Cyclic Connection Count	8

Table 10.10 – EtherNet/IP Target specification.

10.12 EtherNet/IP Originator

Specification	Rating
Class 1 Cyclic Connections Supported	Yes
Class 3 / UCMM Connections Supported	Yes
Class 1 Connection Count	10
Class 3 / UCMM Target Device Count	10
Class 3 / UCMM Mapping Count	50
Logix Direct-to-Tag Supported	Yes

Table 10.11 – EtherNet/IP Originator specification.

10.13 Certifications

Please visit our website: www.prosoft-technology.com.

11 What is HART?

11.1 Introduction to HART

HART is an acronym for Highway Addressable Remote Transducer. HART can transfer digital information across a standard 4-20 mA loop, by superimposing the digital data on the analog signal using Frequency Shift Keying (FSK). As the name implies FSK changes the frequency of the carrier to represent the binary data 0 or 1. A frequency of 1200 Hz represents a logical 1 and a frequency of 2200 Hz represents a logic 0. Therefore, HART has a maximum transfer rate of 1200 bits per second (bps).

The amplitude of the FSK modulation is typically 1mA. Due to the relatively high frequency in comparison to changes of the analog signal, a low pass filter can be employed to prevent the modulation from affecting the analog signal.

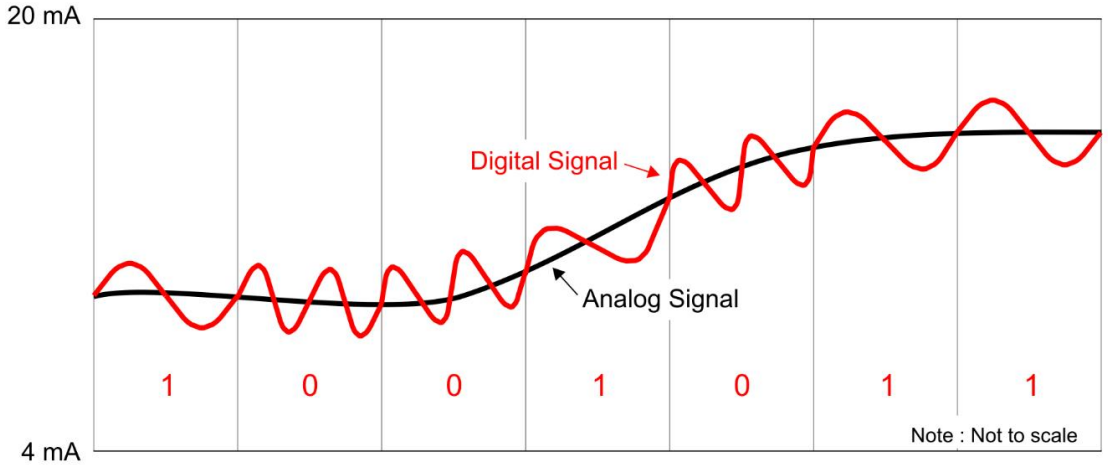


Figure 11.1 – HART FSK Modulation

11.2 HART Response Status

If Byte 0 Bit 7 = 0 then:	
First Byte: Command Errors	
Value	**Description**
0	No error
1	(Undefined)
2	Invalid selection
3	Passed parameter too large
4	Passed parameter too small
5	Too few data bytes received
6	Transmitter specific error
7	In write-protect mode
8-15	Command specific error
16	Access restricted
32	Device is busy
64	Command not implemented
Second Byte: Device Status	
Bit	**Description**
0	PV out of limits
1	Variable (non-PV) out of limits
2	Analog output saturated
3	Output current fixed
4	(Undefined)
5	Cold Start
6	Configuration Changed

Table 11.1 - Status Decoding (when first byte bit 7 = 0)

If Byte 0 Bit 7 = 1 then:	
First Byte: Communication Errors	
Bit	**Description**
0	(Undefined)
1	Rx buffer overflow
2	(Undefined)
3	Checksum error
4	Framing error
5	Overrun error
6	Parity error
Second Byte: Not defined	
Value	**Description**

Table 11.2 - Status Decoding (when first byte bit 7 = 1)

12 Security

This chapter contains security recommendations for the PLX51-HART-8I. It covers the following lifecycle phases:

- Secure installation
- Secure commissioning
- Secure administration and operation
- Secure maintenance
- Secure decommissioning

A secure device can help maintain the security and availability of the network.

12.1 Scope

This chapter covers the recommended device security measures throughout the lifecycle of the device. These recommendations include:

- How to achieve defense in depth for the device
- How to harden the device
- How a specifically configured device can help achieve defense in depth for the system
- How a specifically configured device can help harden the system

A network device is part of a superordinate system. Therefore, the device and the system are interdependent. The system lifecycle and the requirements of the system for defense in depth are outside the scope of this document. References to the system lifecycle are made only if necessary, and only for informational purposes.

For the network, additional planning and implementation steps may be necessary. For example, in a HART network, procedures may be required to control the connection of portable HART communicators to prevent unauthorized access to device configuration functions.

12.2 Defense in Depth

Defense in depth is a strategy that employs various independent security measures to guard an asset under consideration against specific attacks.

A system that employs defense in depth first confronts an attacker with a particular barrier. If an attacker overcomes this barrier, the system presents another barrier of a different type. A minimum of 2 barriers of different types shall guard any system asset under consideration. This layered security approach is considered best practice. It potentially demoralizes an attacker while taking the imperfection of real-world security barriers into account.

12.2.1 Defense in Depth vs. Hardening

In comparison to hardening, defense in depth is a more selective and structured approach. Defense in depth employs a specific subset of all conceivable security measures.

Hardening can be characterized as defense in broad. It aims at closing as many weaknesses in any barriers as reasonably possible. A strategy for hardening may include the concepts "least necessary functions" for the device and "least necessary privileges" for user accounts.

Develop a strategy for defense in depth first, then complement it by hardening.

For more information about secure installation recommendations, see section *12.4.1 Secure Installation Location*.

12.2.2 Responsibilities

Defense in depth as well as hardening need planning, implementation and maintenance. It is the responsibility of the system operator to perform these steps.

It is recommended to consider all security measures given in this document, and to select those that are most relevant for the actual situation.

12.2.3 Example

ID	Barrier	Description
	System Level	
1	Internet Firewall	An attacker must overcome the internet firewall to gain access to the company Intranet.
2	Industrial Firewall	An attacker must overcome the industrial firewall to gain access to the industrial network. The industrial firewall separates the industrial network from the company Intranet.
3	Dedicated device management VLAN	An attacker must overcome VLAN restrictions to snoop packets like unknown unicast frames of device management traffic.
	Device Level	
4	Secure management protocols	An attacker must overcome encryption to snoop packet contents.
5	Non-default user account names[1]	An attacker must guess or discover the actual user account names.
6	Non-default passwords	An attacker must guess or discover the actual passwords.
7	Specific, restricted account privileges	An attacker must guess or discover the administrator account credentials to read privileged data or manipulate device settings.

[1] Dedicated user account names can be device-specific and can be deliberately chosen to be non-descriptive.

12.3 Impact of the System Lifecycle to the Device Lifecycle

A network device is a component in a superordinate system. The system lifecycle determines parts of the device lifecycle. A system lifecycle involves a planning phase. The decisions taken in the planning phase affect the device lifecycle directly or indirectly.

Typical decisions during system planning include:

- The physical position of the device, for example, its installation location and environment
- The logical position of the device, for example, the security zone
- The requirements of the system for defense in depth

12.4 Impact of Device Requirements on System Planning

Some requirements of the device have an impact on the system lifecycle phases and system planning.

Topics of this interdependence include:

- A secure installation location, including the following aspects:
  - Device availability: Power supply, power budget, and data link redundancy
  - Device and port LEDs
- The detailed physical device security requirements
- The user account policy parameters the device offers:
  - For the login policy
  - For the password policy
  - For the username and access role policy

12.4.1 Secure Installation Location

Select a location that offers appropriate device security by restricting physical access:

- Install the device in a room that can be locked and where only authorized personnel have access.
- Install the device in a cabinet to which only authorized personnel have access.
- Install the device in a cabinet with an opaque door.

12.4.1.1 Device Availability

Device availability can be an important base for the security of the superordinate system. Check that the following device availability requirements are met as needed:

- Provide redundant power supply
- Provide an adequate power budget
- Provide data link redundancy

12.4.1.2 Device and Port LEDs

The device and port LEDs show important information about the device state and the port states.

To prevent information leakage, consider the following security aspects as needed in addition to the secure installation location:

- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

12.4.2 Dedicated User Account Login Policy

The device allows for the configuration of a login policy for the user accounts. The login policy applies to all user accounts.

Configure the following requirements for the user login:

- User
- Password
- Role

Note: It is recommended to plan an overarching user account login policy and apply it to each device.

12.4.3 Dedicated User Account Password Policy

The device allows for the configuration of a password policy for the user accounts. Configure the following requirements for the password:

- Minimum password length
- Whether it requires at least one Uppercase character
- Whether it requires at least one Lowercase character
- Whether it requires at least one non-alphanumeric character
- Whether it rejects triples (3 identical consecutive characters)

Note: The default password must be changed on the first login. It is recommended to plan an overarching user account password policy and apply it to each device. To deter attackers, consider planning different passwords on different devices.

12.4.4 Dedicated User Account Name and Access Role Policy for Device Management

Configure dedicated user accounts as needed:

- Assign the login and password policies.
- Create user accounts with:
  - Dedicated names
  - Chosen access roles that offer only the least necessary privileges
- Assign user accounts strong, individual passwords and apply the password policy check.
- Remove user accounts with standard names.

Note: It is recommended to plan an overarching user account and access role policy and apply it to each device. To deter attackers, consider planning different user account names and different passwords on different devices.

13 Device Security

This chapter covers the device security throughout the lifecycle phases of the PLX51-HART-8I.

13.1 Prerequisites

It is assumed that the following system planning steps have been addressed, including:

- Suitable physical location for the devices
- Creating a dedicated user account login policy
- Creating a dedicated user account password policy
- Creating a dedicated user account and access role policy for device management

13.2 Recommended Installation Sequence

The device security lifecycle phases in a practical order are:

- Choice of a secure installation location
- Initial software update
- Initial security configuration
- Possible hardware modification for security
- Initial device installation
- Operation
- Maintenance
- Decommissioning

Note: Depending on needs of the system, the work steps can be performed in a different sequence.

13.2.1 Reasons for the Recommended Installation Sequence

Performing the initial configuration and the initial software update before the initial device installation can have the following benefits:

- The required resources, for example, prepared configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps like software updates can be performed in parallel.
- Associated devices, for example, devices participating in a ring redundancy, can be configured contiguously.
- The remaining work steps in the field require less time.

13.2.2 Recommended Preparation for Installation

The following recommendations can help reduce the initial effort and save time:

- Decide which device software release run on the devices.
- Download the selected software files.
- Prepare device configuration files based on the network plan.
- Prepare device labels.

Note: It is recommended to use the latest available release of the device software.

13.3 Choice of a Secure Installation Location

Select an installation location that in addition offers appropriate device security by restricting physical access.

Check that the following device security requirements are fulfilled if needed:

- Install the device in a room that can be locked and where only authorized personnel have access.
- Install the device in a cabinet to which only authorized personnel have access.
- Install the device in a cabinet with an opaque door.

13.3.1 Device Availability Requirements

Device availability can be an important base for the security of the superordinate system. Also consider implementing measures that increase device availability.

Check that the following device availability requirements are fulfilled if needed:

- Provide redundant power supply.
- Provide an adequate power budget.

13.3.1.1 Power Supply Redundancy Requirements

Check that the power supply redundancy requirements are fulfilled if needed:

- The device is powered by 2 redundant power sources.
- The power supply cables to the device run along different paths as far as possible.
- The power supplies are powered in a redundant way, for example, by 2 separate mains cables.
- The mains cables to the redundant power supplies run along different paths.

13.3.1.2 Power Supply Power Budget Requirements

Refer to chapter *10 Technical Specifications* for the power requirements of the device. Check that the power requirements are fulfilled if needed:

- One single power supply can deliver power for all the connected devices.

13.4 Software Update

The following description applies to:

- The initial software update for a device out-of-the-box.
- A software update as part of operation or maintenance.

Check if an updated release of the device software is available at: www.prosoft-technology.com.

If the device software is to be updated:

1. Back up the device configuration.
2. Update the device software.
3. Reboot the device for the new software to take effect.

Note: It is recommended to regularly check for device software updates and use the latest available release. A new release of the device software can provide security improvements or benefits like new security-related device functions.

13.5 Security Configuration

The following description applies to:

- The initial security configuration for a device out-of-the-box.
- Changes in the security configuration as part of operation or maintenance.

To save time and effort, perform the following security configuration steps by loading a prepared configuration file into the device.

At the first login with the default password, the device requires the password to be changed. Use a dedicated password according to the password policy.

Perform the following steps as needed:

- Enable the *Master Security Enable* parameter
- Configure the fixed user groups
- Configure the Reset and Flash Rules
- Configure the Login Rules
- Configure the Password Rules
- Configure the Custom User Accounts
- Configure whether to restrict access to HTTP and DTM
- Configure the custom port access
- Configure the IP Access Control List (ACL) to restrict access to authorized IP addresses.
- Configure the MAC Access Control List for access restriction
- Configure the MAC Access Control List to restrict access based on MAC addresses.

When the device configuration is complete, create a backup copy of the configuration.

13.5.1 Assign a Static IP Address for the Device Management

Note: At the first login with the default password, the device requires the password to be changed. Use a dedicated password according to the password policy.

The device offers the following options of assigning a management IP address: **Static** and **DHCP** (default). Selecting *Static* helps make the device more immune to potential attacks via the DHCP protocol.

13.5.2 Disable Insecure Management Protocols

Disable insecure protocols, such as DTM, if not required by the application.

13.5.3 Configure Management IP Access Restrictions

The device allows restricting the management access to the device to a source IP or MAC address range. Use the Security/IP Access Control List to set the address range by providing an IP address and a netmask.
Refer to the Security/MAC Access Control List to set the address range by providing a list of MAC addresses.

Configure the management access restrictions individually for each protocol or for a group of protocols as follows. If the protocol is required for the application, make sure to implement security measures to restrict unauthorized access to the network.

Protocol	Recommendation for Production	Delivery State
DTM	Disabled	Enabled

13.5.4 Configure Dedicated User Account Names and Access Roles for Device Management

Note: It is assumed that a dedicated user account name and access role policy has been created.

Configure dedicated user accounts as needed:

- Assign the device login policy.
- Assign the device password policy.
- Create user accounts. For each new user account, perform the following steps:
  - Create a user account with a dedicated name.
  - Assign the new user account to an access role that offers only the least necessary privileges.
  - Assign the new user account a strong, individual password.
  - Apply the password policy check to the new user account.
- Remove user accounts with standard names.

Note: To deter attackers, consider using different user account names and different passwords on different devices.

13.5.5 Create a Backup of Device-Specific Data

When the device configuration is complete:

- Consider creating a backup copy of the configuration. For example, place the backup file in a device-specific folder.
- Include other device-specific data. For example, copy device-specific private keys or certificates to the same device-specific folder.
- Keep the backup files separate from the device in a secure location.

This minimizes effort to replace a device should the hardware become inoperable.

13.6 Possible Hardware Modifications for Security

The following descriptions apply to:

- The possible hardware modifications for a device out-of-the-box.
- Possible hardware modifications as part of operation or maintenance.

Perform the following hardware modification steps, like covering or obstructing a slot or a port, as needed:

- Restrict physical (visual) access to the device and port LEDs.

13.6.1 Restrict Physical Access to Network Ports

If there are high security requirements and certain network ports are not needed, consider covering or obstructing these network ports.

13.6.2 Restrict Physical (Visual) Access to the Device and Port LEDs

For high security requirements, perform the following steps as needed:

- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

13.7 Device Installation

The following description applies to:

- The installation of a device in a new system.
- Changes to the device as part of operation or maintenance.

13.8 Operation

In the operation phase of the device, it is assumed the appropriate physical and logical steps to set up the device and operate properly regarding the functional and security aspects of the device are observed. This reduces the required security steps during the operation phase to the considerations already described in this document.

13.8.1 Environmental Conditions

Obey the environmental conditions given section *10.3 Environmental*. For more information, please see: www.prosoft-technology.com. Do not open the device.

13.8.2 Connectivity

Obey instructions for connecting the Ethernet ports.

13.9 Maintenance

13.9.1 Software Update

If necessary, perform a software update:

- For the security aspects.
- For the detailed steps, see section *13.4 Software Update*

13.9.2 Hardware Enhancement

Typical application cases include:

- Connecting a new end device to an existing Ethernet port.
- Using redundant power supplies.
- Planning the power supply for worst case device power budget, in case one of the redundant power supplies fails.
- Providing redundant data uplinks.

13.9.3 Hardware Replacement

Note: Do not open the device.

Perform the following steps:

- Perform an initial software update.
- Perform the software configuration, for example, by transferring the existing configuration of the old device to the new device.

13.9.4 Hardware Repair

Should the device need repair, consider the following recommendations:

- Do not open the device.
- Send the device to the manufacturer for repair.
- Keep a backup copy of the device configuration.

If necessary and possible, delete the configuration and other confidential data.

13.10 Decommissioning

For high security requirements, consider physical destruction. Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping redundant.

Note: If the device is to be used in the future, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

13.10.1 Destruction of Confidential Data

Note: Resetting the device to the default state performs normal file deletion operations on the device and the external memory which may leave some of the file contents or blocks in the flash memory intact.

If there are high security requirements, consider the physical destruction of the device and the external memory.

13.10.1.1 Reset to the Delivery State

For the deletion of data, perform the following steps as needed:

- Reset the device to the default state. This performs the following operations:
  - Deletes the configuration profile in the device.
  - Resets the security parameters.

Note: The audit trail persists after a reset to the delivery state.

13.10.2 Secure Physical Destruction of Device and Components

For the secure physical destruction of physical components, perform the following steps as needed:

- Physically destroy the external memory. This addresses:
  - The configuration profiles on the external memory.
  - The software files on the external memory.
  - Any other files on the external memory.
- Physically destroy the device, including the flash memory chips. This addresses:
  - The HTTPS certificate in the device.
  - The SSH host key pair in the device.
  - The configuration profiles in the device.
  - Any other files in the device.

14 Support, Service & Warranty

14.1 Contacting Technical Support

ProSoft Technology, Inc. is committed to providing the most efficient and effective support possible. Before calling, please gather the following information to assist in expediting this process:

1. Product Version Number
2. System architecture
3. Network details

If the issue is hardware related, we will also need information regarding:

1. Module configuration and associated ladder files, if any
2. Module operation and any unusual behavior
3. Configuration/Debug status information
4. LED patterns
5. Details about the interfaced serial, Ethernet or Fieldbus devices

North America (Corporate Location)	Europe / Middle East / Africa Regional Office
Phone: +1 661-716-5100 ps.orders@belden.com Languages spoken: English, Spanish REGIONAL TECH SUPPORT ps.support@belden.com	Phone: +33.(0)5.34.36.87.20 ps.europe@belden.com Languages spoken: English, French, Hindi, Italian REGIONAL TECH SUPPORT ps.support.emea@belden.com
Latin America Regional Office	**Asia Pacific Regional Office**
Phone: +52.222.264.1814 ps.latinam@belden.com Languages spoken: English, Spanish, Portuguese REGIONAL TECH SUPPORT ps.support.la@belden.com	Phone: +60.3.2247.1898 ps.asiapc@belden.com Languages spoken: Bahasa, Chinese, English, Hindi, Japanese, Korean, Malay REGIONAL TECH SUPPORT ps.support.ap@belden.com

For additional ProSoft Technology contacts in your area, please see:
www.prosoft-technology.com/About-Us/Contact-Us

14.2 Warranty Information

For details regarding ProSoft Technology's legal terms and conditions, please see:
www.prosoft-technology.com/ProSoft-Technology-Legal-Terms-and-Conditions

For Return Material Authorization information, please see:
www.prosoft-technology.com/Services-Support/Return-Material-Instructions