INTERBUS Router

User Manual

A-IBR

Document No. D169-010
07/2026
Revision 1.0

CONTENTS

Revision History

Revision	Date	Comment
1.0	7 April 2026	Initial document

1. PREFACE

1.1. INTRODUCTION TO THE INTERBUS ROUTER

This manual describes the installation, operation, and diagnostics of the Aparian INTERBUS Router module. The INTERBUS Router, (hereafter referred to as the **module**) provides intelligent data routing between either EtherNet/IP or Modbus TCP and an INTERBUS master.

INTERBUS is a fast sensor–actuator bus for transmitting process data in industrial environments. Due to its transmission procedure and ring topology, INTERBUS features a fast, cyclic, and time-equidistant process data transmission.

Each slave device has an input and output bidirectional port allowing the ring structure with only a single cable between each device.

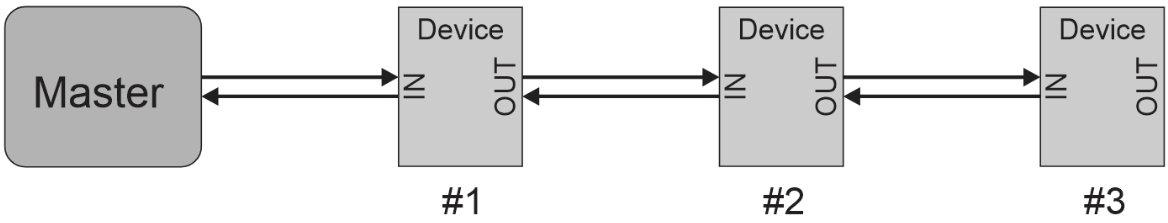


Figure 1.1. – INTERBUS System

The INTERBUS Router module can emulate up to 15 INTERBUS slave devices, and map the INTERBUS input and output data to EtherNet/IP or Modbus devices.

Each (virtual) INTERBUS device can be configured for a specific Device Class, Type, Data Direction and Data Width.

Primary Interface:
The module can use one of four Primary Interface modes:

EtherNet/IP Target
Here a remote EtherNet/IP device (e.g. a Logix controller) establishes a number of Class 1 connections to the module. INTERBUS data can be mapped into 4 separate input and output class 1 cyclic connections to the Logix controller (allowing up to 2KB input and 2KB output to be exchanged at the requested packet interval – RPI).

EtherNet/IP Originator
As an EtherNet/IP originator, the module can use one of two methods to read and write data to and from the INTERBUS master:

- **EtherNet/IP Explicit Messaging**

  This allows an INTERBUS master to exchange data with up to 10 EtherNet/IP devices. The module can use either Class 3 or Unconnected Messaging (UCMM) to Get and Set data in the remote EtherNet/IP devices.

- **Direct-To-Tag technology**

  This allows the INTERBUS master to exchange data with a Logix controller without the need to write any application code (e.g. ladder) in Studio 5000. The INTERBUS slave data is directly read from, or written to, Logix tags.

- **EtherNet/IP Class 1 connection**

  INTERBUS data can be mapped to a maximum of 15 EtherNet/IP devices using input and output class 1 cyclic connections. This will allow the INTERBUS Router to “own” the EtherNet/IP target device and exchange INTERBUS slave data using the EtherNet/IP device’s input and output assemblies.

Modbus Server
The diagnostics and INTERBUS data will be written to, or read from, the module’s internal Modbus Registers (Holding or Input Registers). These registers can be accessed by a remote Modbus Client using Modbus TCP.

Modbus Client
The diagnostics and INTERBUS data will be written to, or read from, the module’s internal Modbus Registers (Holding or Input Registers). The Modbus Auxiliary Map can then be used to configure the Modbus data exchange between multiple remote Modbus Server devices and the module’s internal Modbus registers via Modbus TCP.

The INTERBUS Router is configured using the Aparian Slate application. This program can be downloaded from www.aparian.com free of charge.

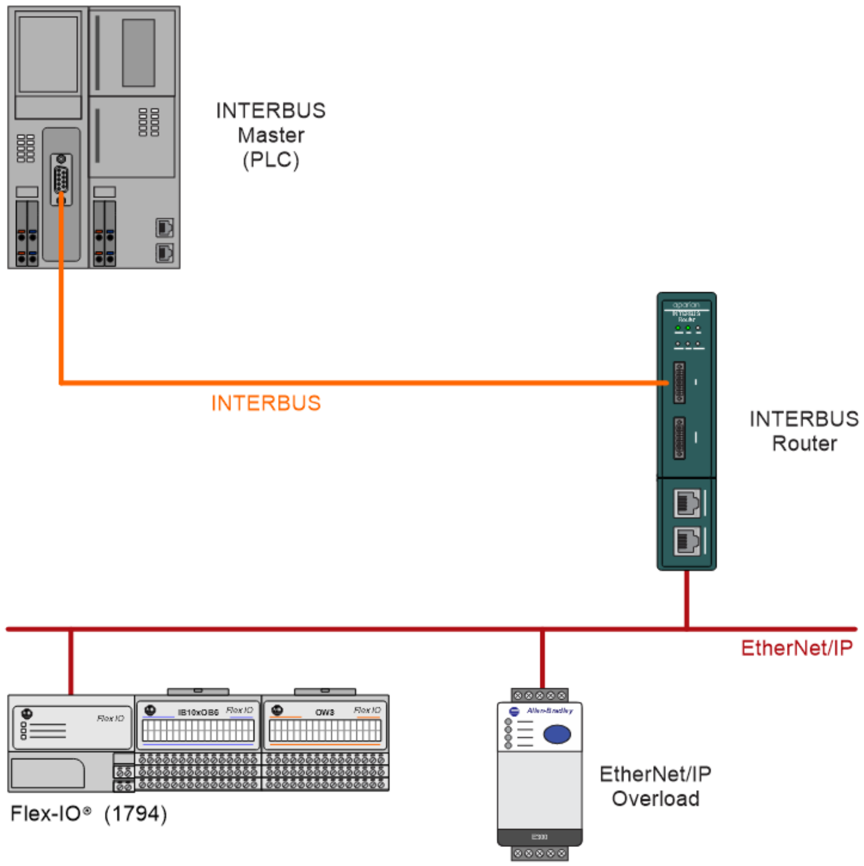


Figure 1.2. – Example of a configuration connecting INTERBUS master to EtherNet/IP I/O

The module also provides a range of statistics, Modbus packet capture functions, and internal Modbus and Data table reads to simplify the diagnostic process for remote diagnosis.

The module has two Ethernet ports and supports Device-Level-Ring (DLR) architectures.

1.2. FEATURES

- Module can emulate up to 15 INTERBUS slaves.
- Supports all INTERBUS Baud Rates (500 kb & 2 Mb).
- Module has various Primary Interfaces:
    - EtherNet/IP Target (Class 1 connection)
    - Modbus Server (TCP)
    - Modbus Client (TCP)
    - EtherNet/IP Originator (Class 1 connection with up to 15 EtherNet/IP devices and Explicit Messaging, including Direct-To-Tag Logix tag access, with up to 10 EtherNet/IP devices).
- Slate software provides a Modbus packet capture utility for better diagnosis of issues.
- Dual Ethernet ports which support Device-Level-Ring (DLR).
- Small form factor – DIN rail mounted.

1.3. ARCHITECTURE

The figures below provide an example of the typical network setup for connecting INTERBUS devices to either EtherNet/IP or Modbus TCP.

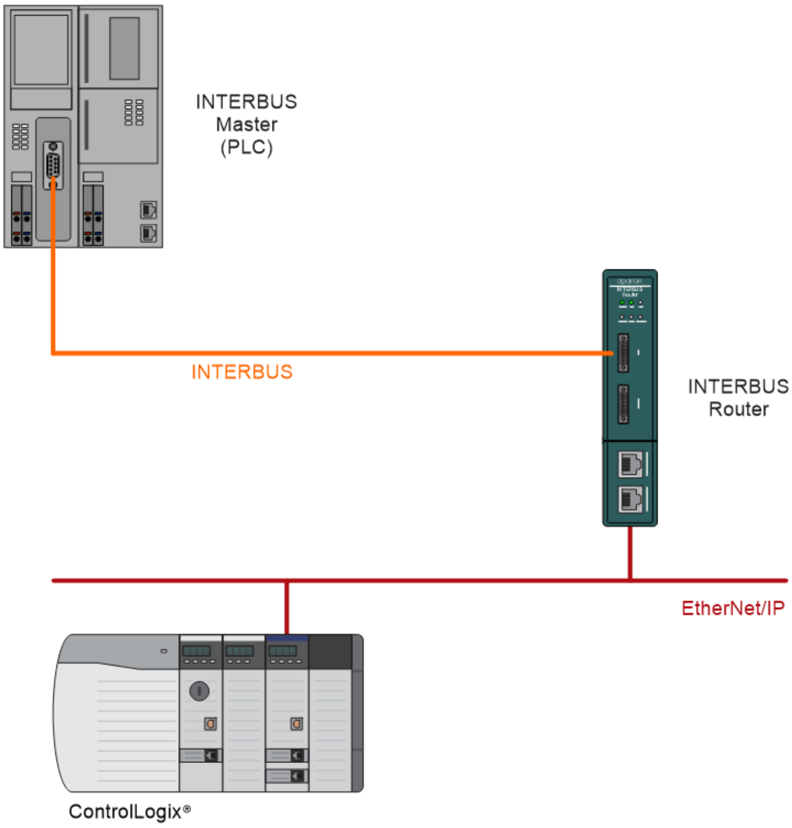


Figure 1.3. – Example of connecting to a Logix Controller

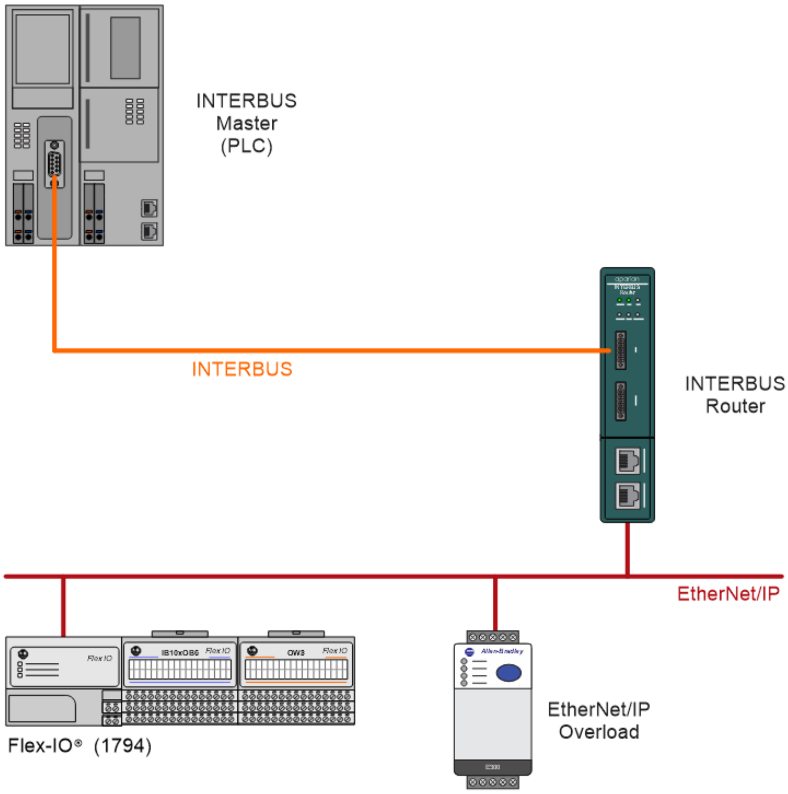


Figure 1.4. – Example of connecting EtherNet/IP I/O

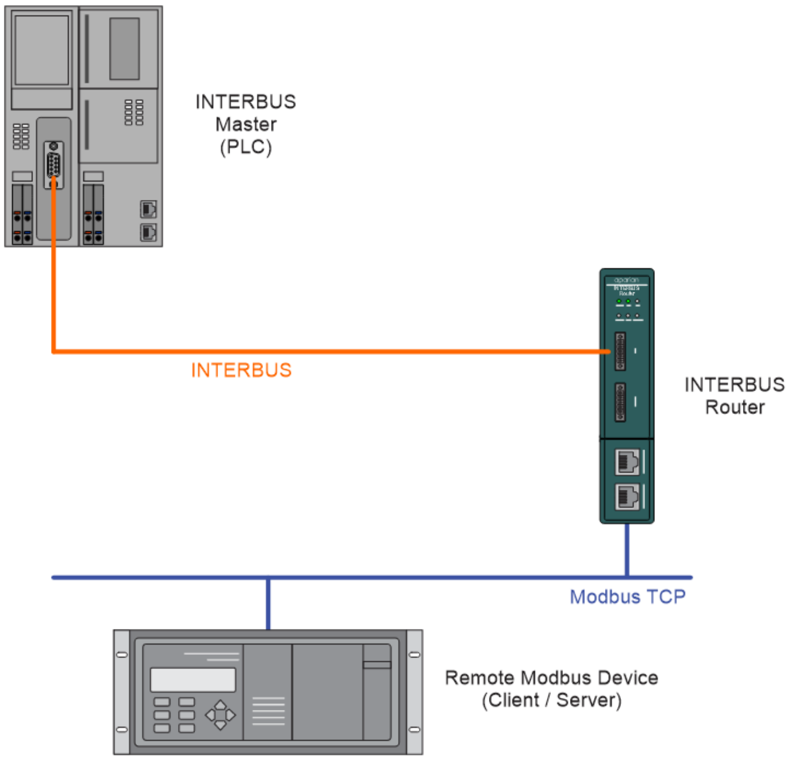


Figure 1.5. - Example of connecting to a Modbus TCP Client or Server

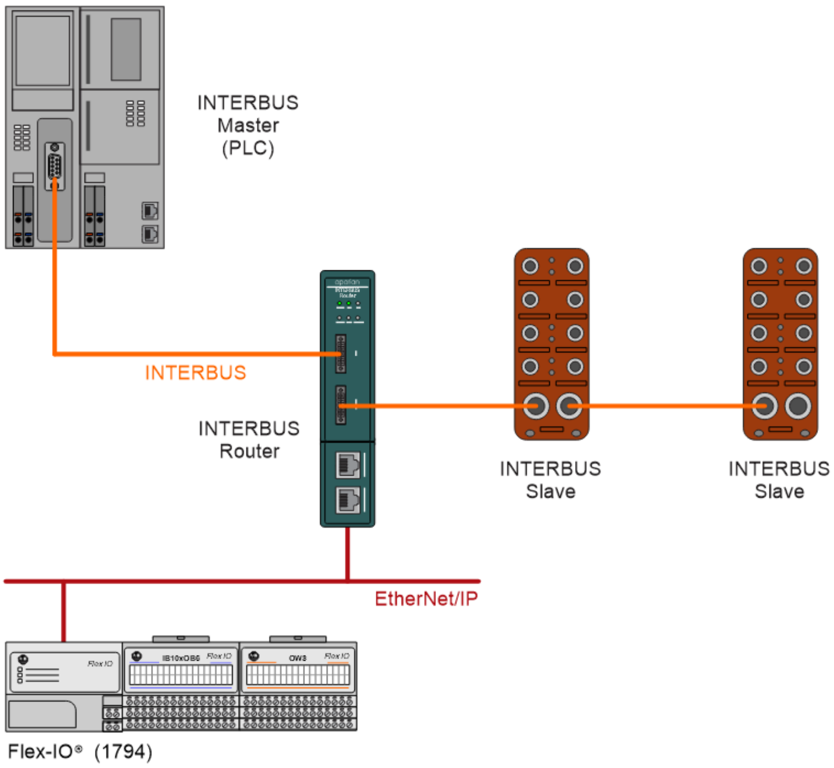


Figure 1.6. - Example of extending INTERBUS to additional INTERBUS slaves.

1.4. ADDITIONAL INFORMATION

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

Resource	Link
Slate Installation	http://www.aparian.com/software/slate
INTERBUS Router User Manual INTERBUS Router Datasheet Example Code & UDTs	https://www.aparian.com/products/INTERBUSRouter
Ethernet wiring standard	www.cisco.com/c/en/us/td/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig/Connectors.html

Table 1.1. - Additional Information

1.5. 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 web link	https://www.prosoft-technology.com/Services-Support/Customer-Support
Support email	support@prosoft-technology.com

Table 1.2. – Support Details

2. INSTALLATION

2.1. MODULE LAYOUT

The module has two INTERBUS ports (IN and OUT) on the front of the enclosure, two Ethernet ports on the angled front, and one power port at the bottom, as shown in the figure below.

The power port uses a three-way connector which is used for the DC power supply positive and negative (ground) voltage as well as the earth connection.

The Ethernet cable used for the Ethernet ports must be wired according to industry standards which can be found in the additional information section of this document.

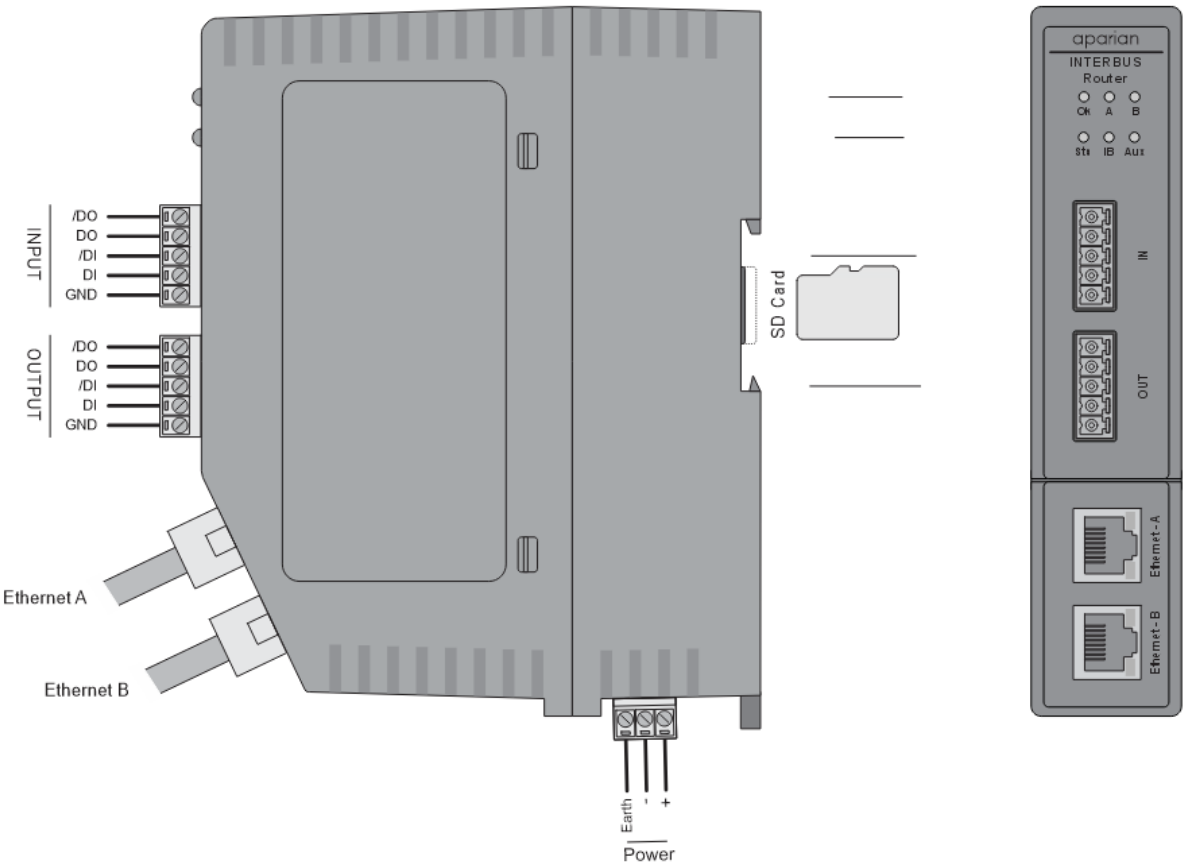


Figure 2.1 – INTERBUS Router side and front view

The module also supports an SD Card for disaster recovery which can be used to automatically update the configuration, network parameters, and/or firmware of a new module.

The module provides six diagnostic LEDs as shown in the front view figure above. These LEDs are used to provide information regarding the module system operation, the Ethernet interface, INTERBUS and the auxiliary communication.

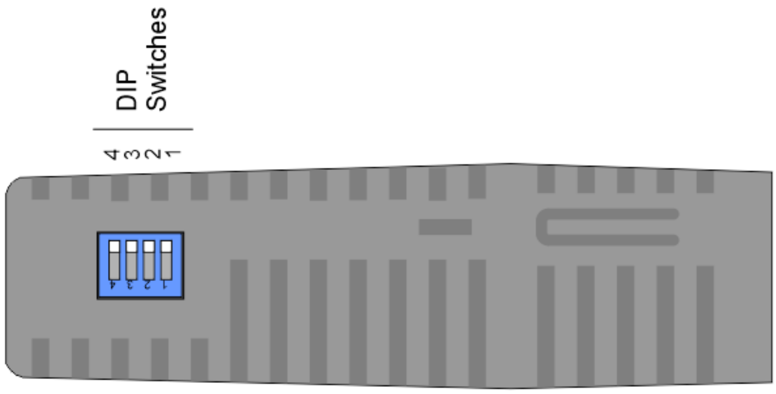


Figure 2.2 – INTERBUS Router top view

The module provides four DIP switches at the top of the enclosure as shown in the top view figure above.

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 in the rare occasion when an earlier firmware update was interrupted at a critical stage.
DIP Switch 2	This will force the module into DHCP mode which is useful when the user has forgotten the IP address of the module.
DIP Switch 3	This DIP Switch is used to lock the configuration from being overwritten by the Slate. When set Slate will not be able to download to the module.
DIP Switch 4	When this DIP Switch is 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

2.2. MODULE MOUNTING

NOTE: This module is an open-type device and is meant to be installed in an enclosure suitable for the environment such that the equipment is only accessible with the use of a tool.

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

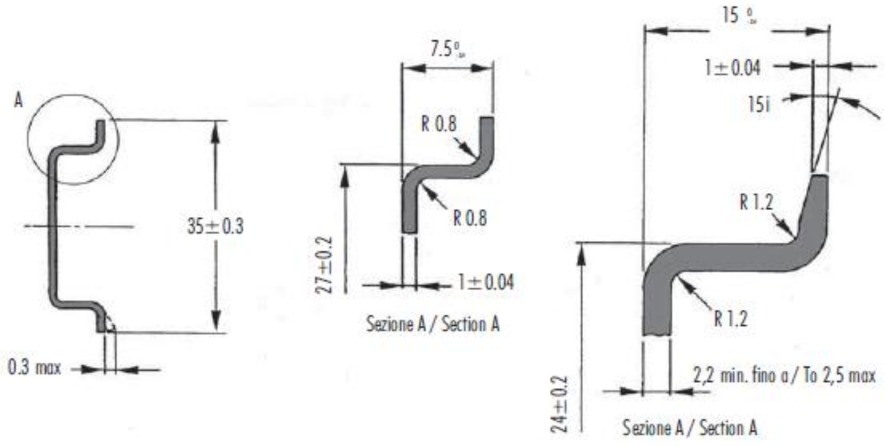


Figure 2.3 - DIN rail specification

The DIN rail clip is mounted on the bottom of the module at the back as shown in the figure below. 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.

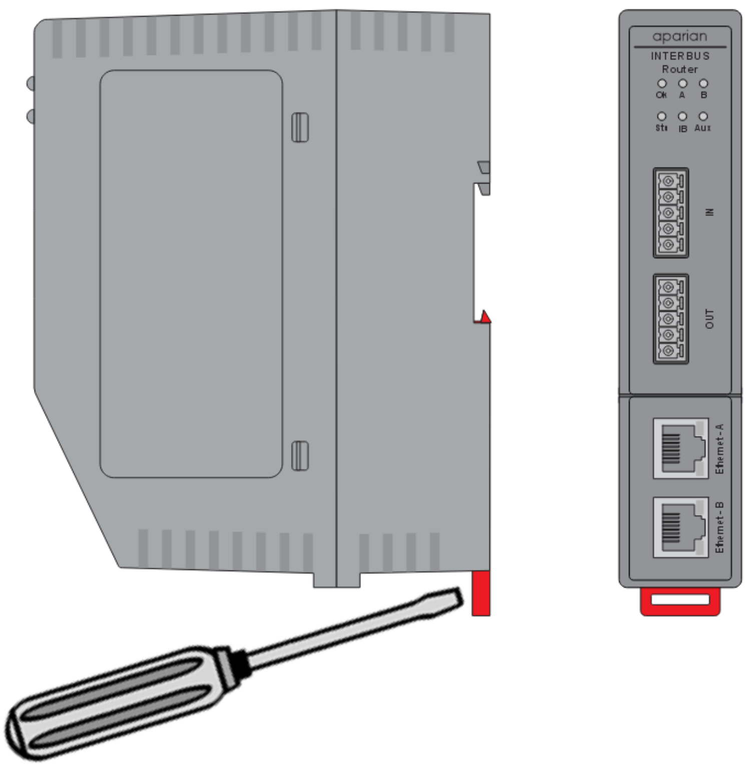


Figure 2.4 - DIN rail mounting

2.3. POWER

A three-way power connector is used to connect Power+, Power– (GND), and earth. The module requires an input voltage of 10 – 30Vdc. **Refer** to the technical specifications section in this document.

NOTE: The module allows the user to provide power on both bottom and front power connectors and can be used for power supply redundancy.

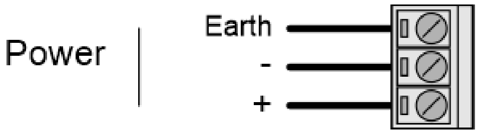


Figure 2.5 - Power connector

2.4. INTERBUS PORTS

There are two five-way INTERBUS connectors for the INPUT and OUTPUT ports respectively.

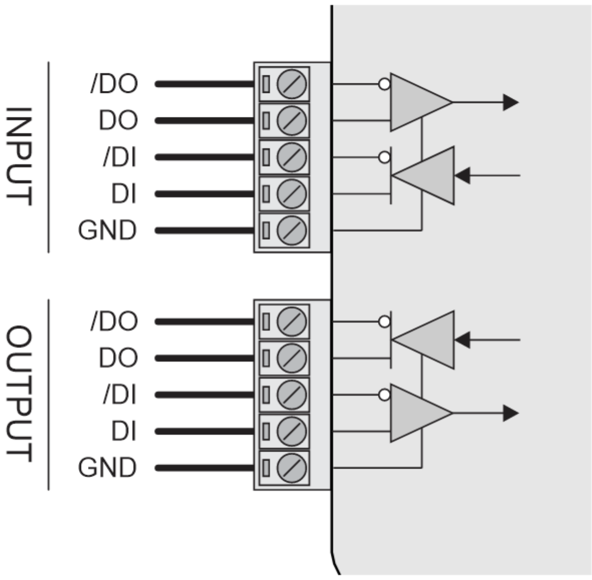


Figure 2.6 – INTERBUS IN/OUT connector

2.5. ETHERNET PORTS

The Ethernet connectors should be wired according to industry standards. **Refer** to the additional information section in this document for further details. The module has an embedded switch connecting the two Ethernet ports.

3. SETUP

3.1. INSTALL CONFIGURATION SOFTWARE

All the network setup and configuration of the module is achieved by means of the Aparian Slate device configuration environment. This software can be downloaded from http://www.aparian.com/software/slate.

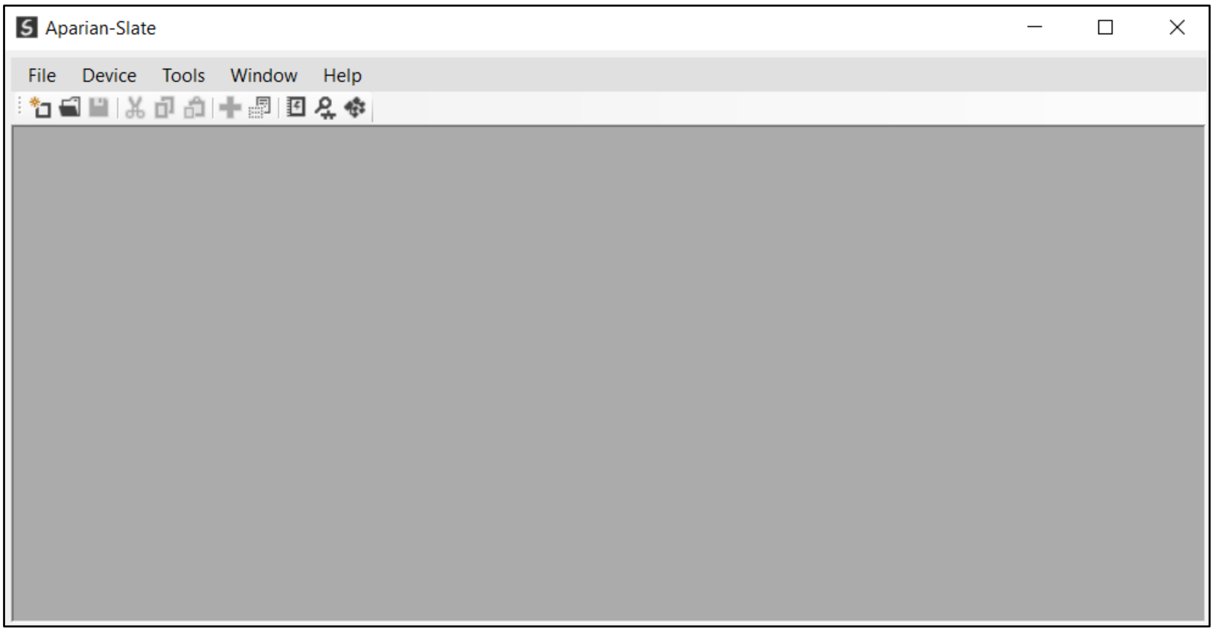


Figure 3.1. - Aparian Slate Environment

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 a number of DHCP utilities available, however it is recommended that the DHCP server in Slate be used.

Within the Slate environment, the DHCP server can be found under the Tools menu.

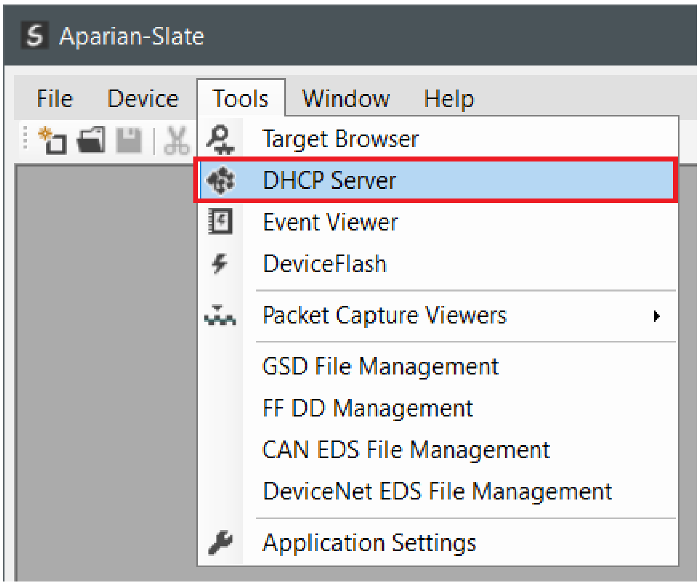


Figure 3.2. - Selecting DHCP Server

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

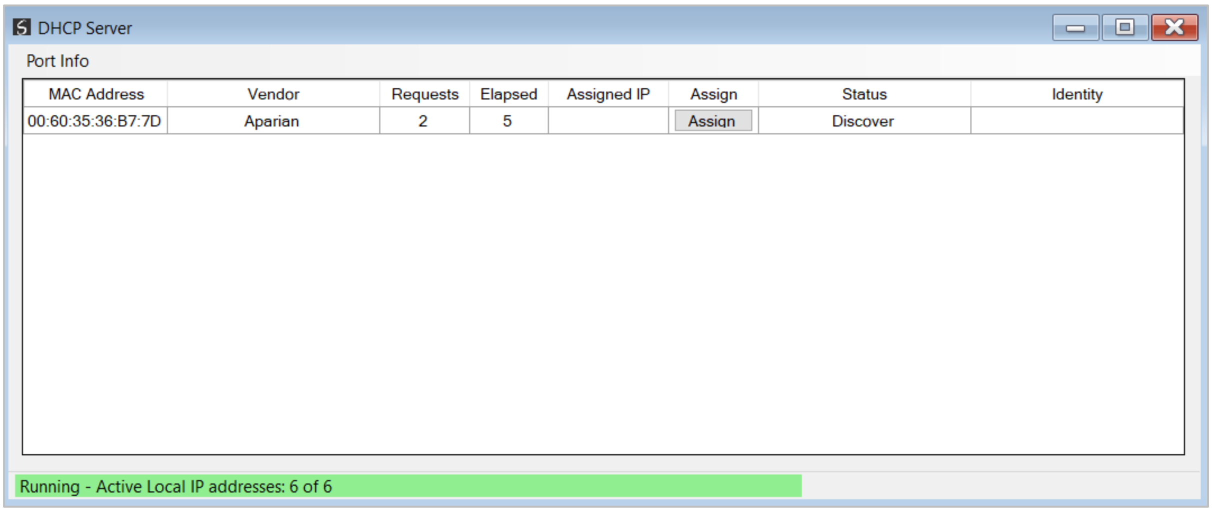


Figure 3.3. - DHCP Server

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. The IP Address Assignment window will open.

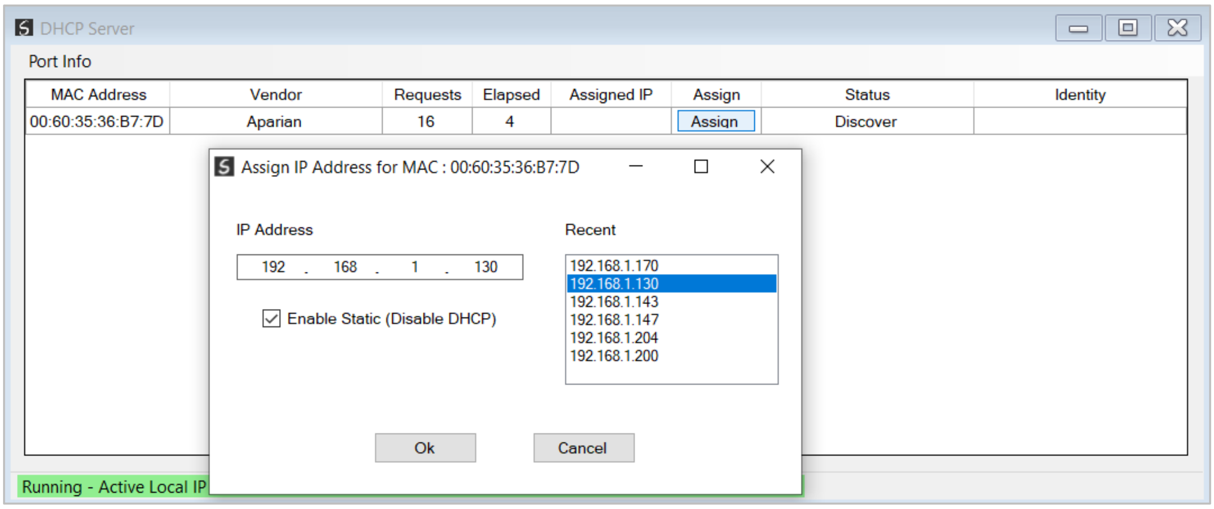


Figure 3.4. - Assigning IP Address

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.

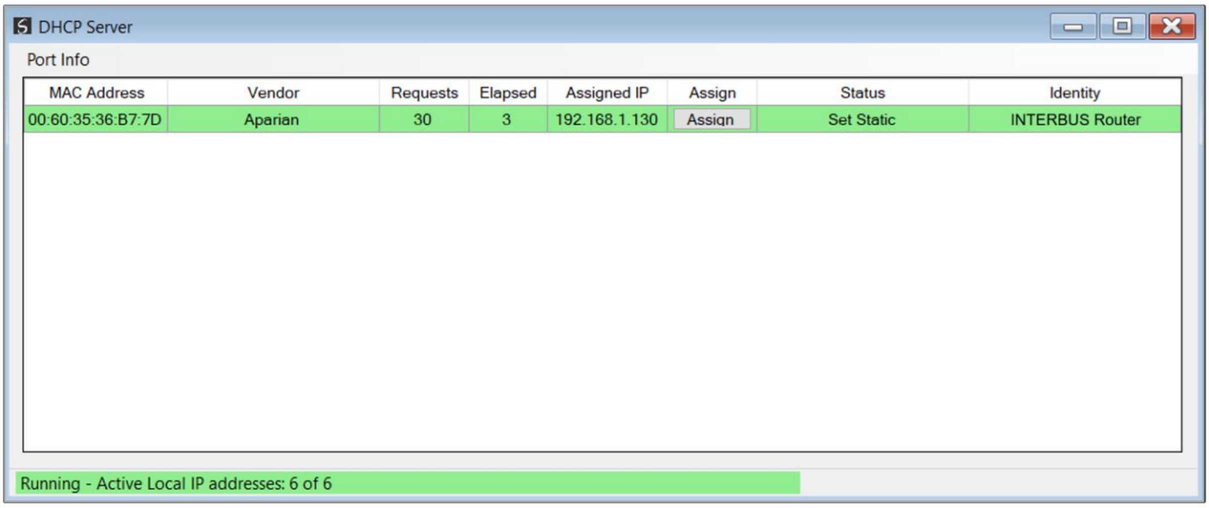


Figure 3.5. - Successful IP address assignment

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.

NOTE: 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.

If the module's DIP switch 2 is in the On position during the address assignment, the user will be warned by the following message.

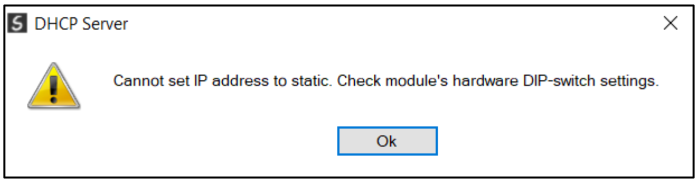


Figure 3.6. - Force DHCP warning

In addition to the setting the IP address, a number of other network parameters can be set during the DHCP process. These settings can be viewed and edited in Slate'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.

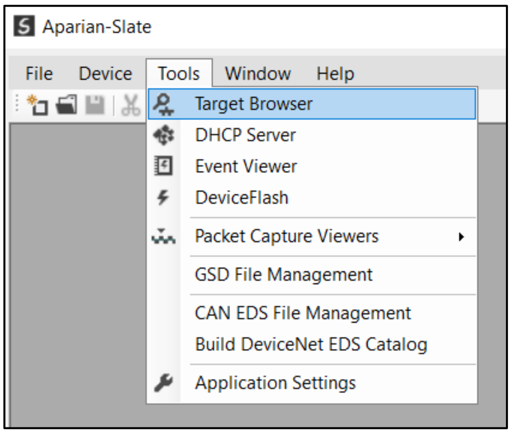


Figure 3.7. - Selecting the Target Browser

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

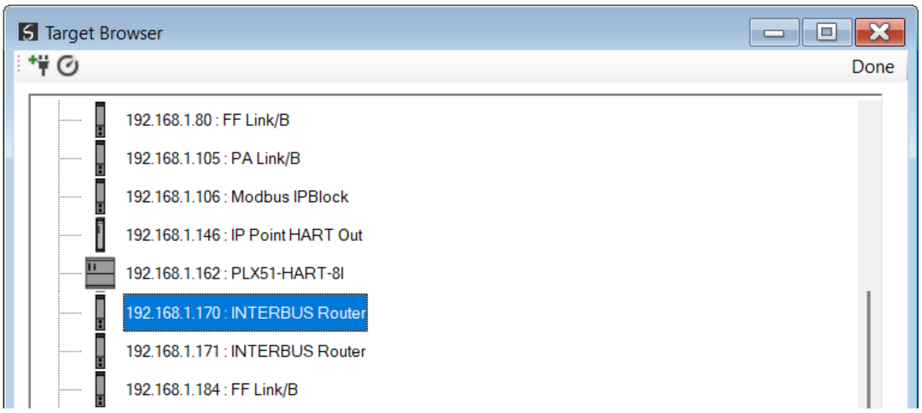


Figure 3.8. - Target Browser

Right-clicking on a device, reveals the context menu, including the Port Configuration option.

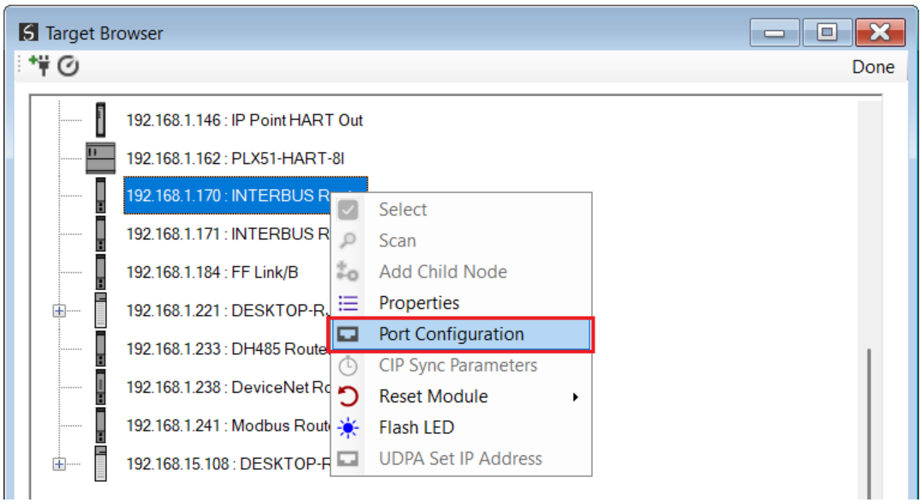


Figure 3.9. - Selecting Port Configuration

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

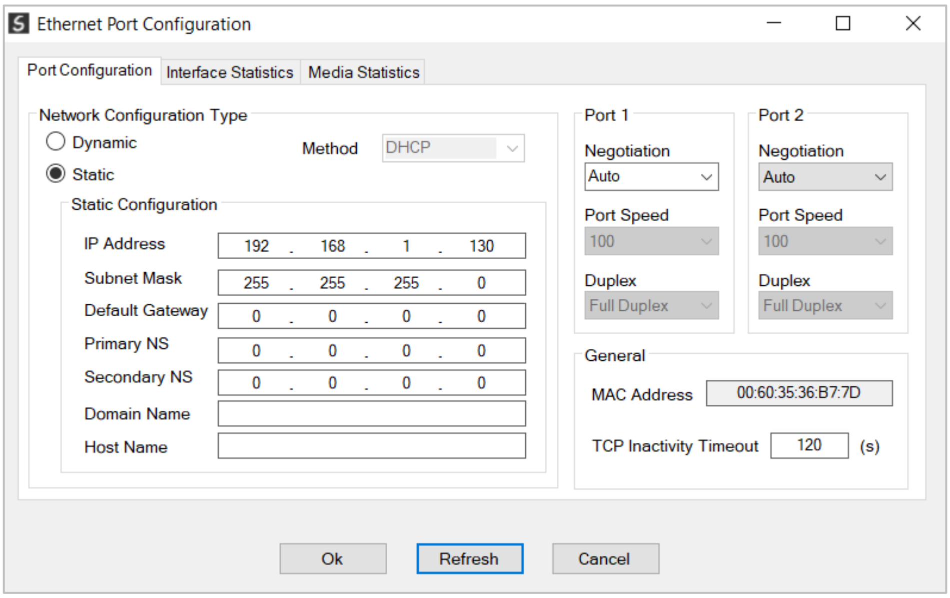


Figure 3.10. - Port Configuration

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 Slate project must be created. Under the File menu, select New.

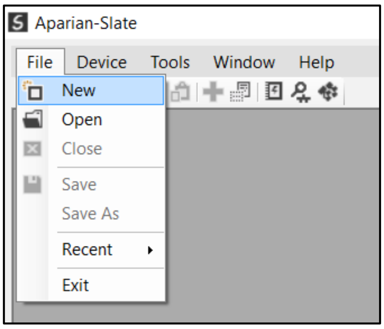


Figure 3.11. - Creating a new project

A Slate 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.

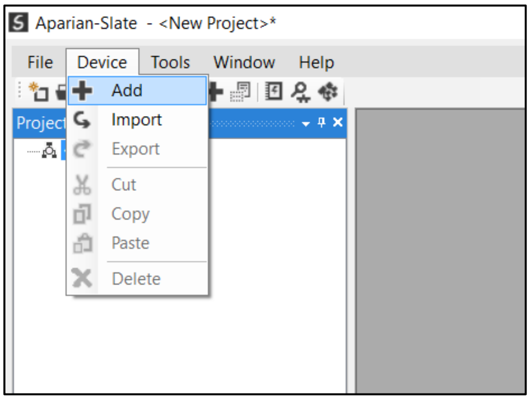


Figure 3.12. - Adding a new device

In the Add New Device window select the INTERBUS Router and click the Ok button.

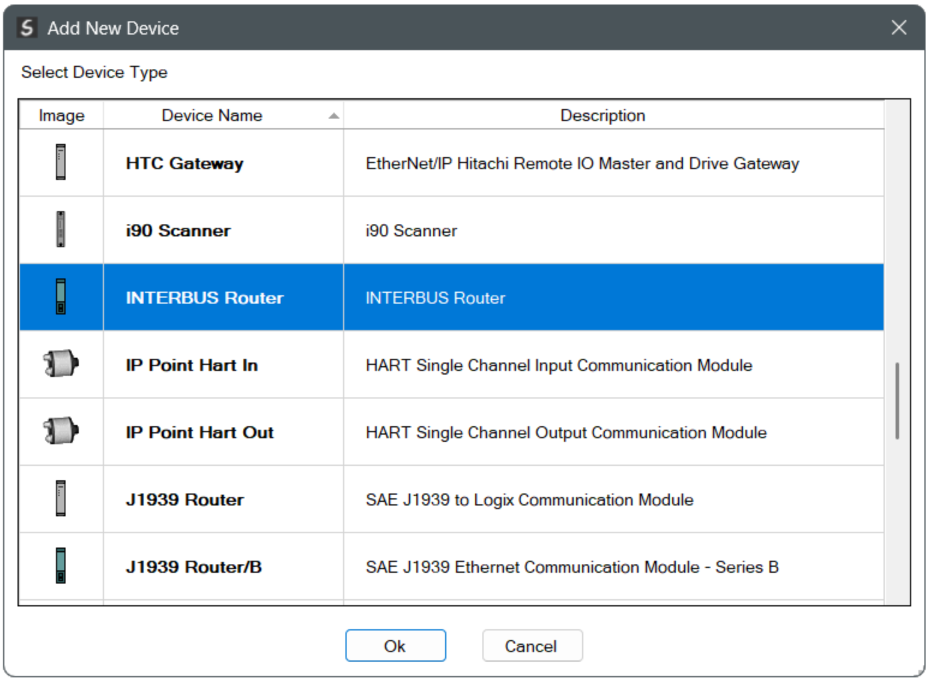


Figure 3.13 – Selecting a new INTERBUS Router

The device will appear in the Project Explorer tree as shown below, and its configuration window opened. 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***.

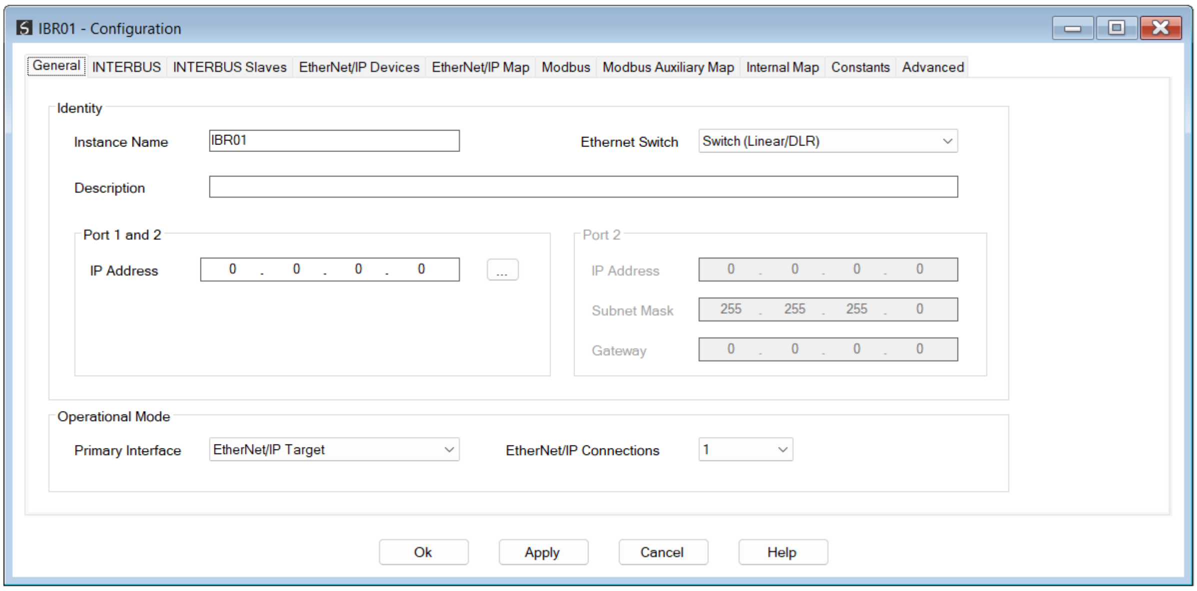


Figure 3.14. – INTERBUS Router configuration

Refer to the additional information section in this document for Slate's installation and operation documentation.

3.4. GENERAL PARAMETERS

The INTERBUS parameters will be configured by Slate. When downloading this configuration into the module it will be saved in non-volatile memory that persists when the module is powered down.

NOTE: When a firmware upgrade is performed the module will clear all the module configuration stored in non-volatile storage.

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

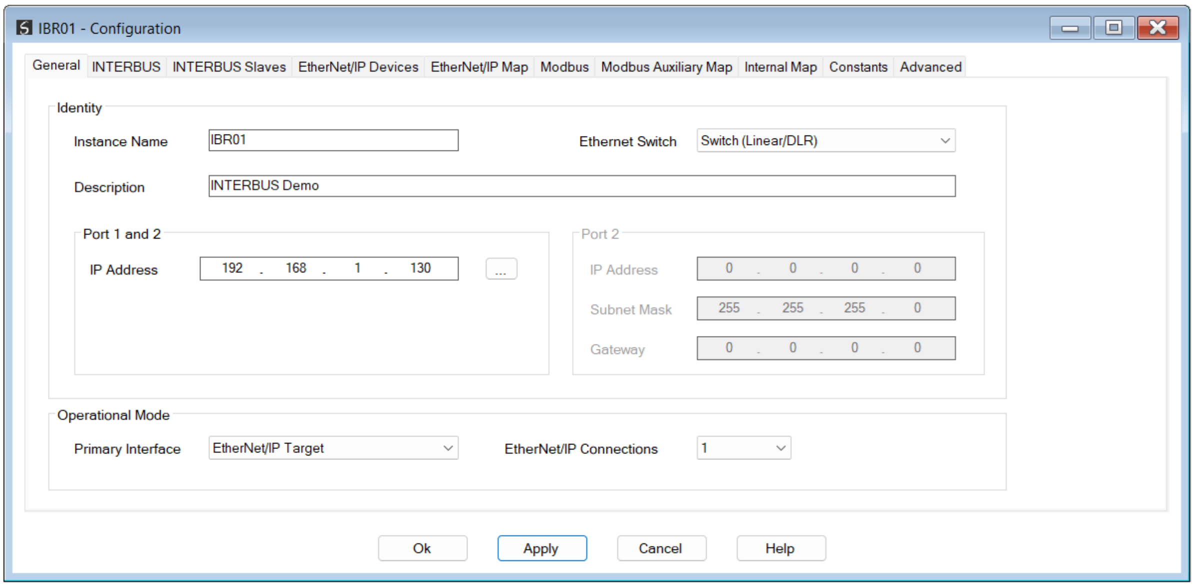


Figure 3.15 - General Configuration

The general configuration consists of the following parameters:

Parameter	Description
Instance Name	This parameter is a user defined name to identify between various INTERBUS Routers.
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 (foreign) 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 on one port is <u>not</u> transmitted to the other. <u>Port 1:</u> 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. <u>Port 2:</u> The IP address is the one contained within the configuration below (Port 2).

	EtherNet/IP requests and connections will <u>not</u> be processed. Modbus TCP requests will be processed.
Port 1 IP Address	The primary configured IP address of the module.
Port 2 IP Address	**THIS IS RELEVANT ONLY IN SPLIT (DUAL-IP) ETHERNET SWITCH MODE** The IP address used on Port 2.
Port 2 Subnet Mask	**THIS IS RELEVANT ONLY IN SPLIT (DUAL-IP) ETHERNET SWITCH MODE** The Subnet Mask used on Port 2.
Port 2 Gateway	**THIS IS RELEVANT ONLY IN SPLIT (DUAL-IP) ETHERNET SWITCH MODE** The Default Gateway address used on Port 2. **NOTE**: If the IP address ranges for Port 1 and Port 2 overlap, then only one Port's Gateway address can be non-zero.
Primary Interface	**EtherNet/IP Target** A Logix controller can own the INTERBUS Router over EtherNet/IP using up to 4 class 1 connections. **Modbus Server** A Modbus Client can read and write data to the module which can then be mapped to one or more INTERBUS slaves. The module can operate as a Modbus Server on Ethernet TCP. **Modbus Client** A module can read and write data from various Modbus devices which can then be mapped to one or more INTERBUS slaves. The module can operate as a Modbus Client on Ethernet TCP. **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): *<u>EtherNet/IP Class 1 Connection</u>* The INTERBUS Router can own EtherNet/IP IO by using the Slate software to configure the IO connections. *<u>EtherNet/IP Explicit Messaging</u>* The INTERBUS Router can exchange data with up to 10 EtherNet/IP devices using explicit messaging.
EtherNet/IP Connections	The number of connections the module will use when operating as an EtherNet/IP target.

Table 3.1 - General configuration parameters

3.5. INTERBUS CONFIGURATION

3.5.1. COMMUNICATION

The INTERBUS Communication 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 ***INTERBUS Communication*** tab.

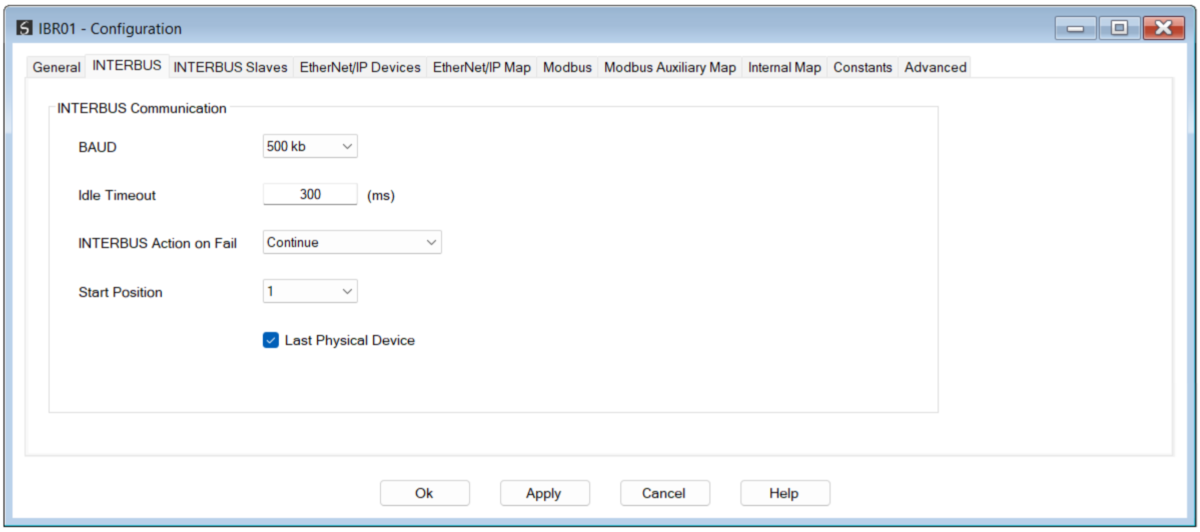


Figure 3.16 – INTERBUS Communication Configuration

The **INTERBUS Communication** configuration consists of the following parameters:

Parameter	Description
BAUD Rate	The INTERBUS bus BAUD rate. The following options are available: • 500 kbps • 2 Mbps
Idle Timeout	Should no master frames be received within this time (in milliseconds) the module will deem the INTERBUS master to be offline.
Start Position	The physical position of the first virtual INTERBUS slave represented by the module. This is the same as the number of other INTERBUS slave devices placed between the master and the module.
INTERBUS Acton on Fail	This describes the behavior of the INTERBUS communication following failure of the primary interface, when configured for either Modbus (Client or Server) or EtherNet/IP target. The following options are available: **Continue** INTERBUS communication continues, and the INPUT data exchanged with the INTERBUS Master remains unchanged (i.e. last value).

	Zero Data INTERBUS communication continues, and the INPUT data exchanged with the INTERBUS Master is set to zero. **Offline** INTERBUS communication stops, causing the INTERBUS master to fault. **Note:** When the primary interface is set to EtherNet/IP Originator, then this behavior is configured for each EtherNet/IP Originator connection.
Last Physical Device	Enable this option if the module is the last physical device in the INTERBUS ring. When this parameter is checked, there should not be any other device connected on the module's INTERBUS OUT port.

Table 3.2 - INTERBUS Communication configuration parameters

3.5.2. INTERBUS Slave Configuration

The INTERBUS Slave 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 ***INTERBUS Slaves*** tab.

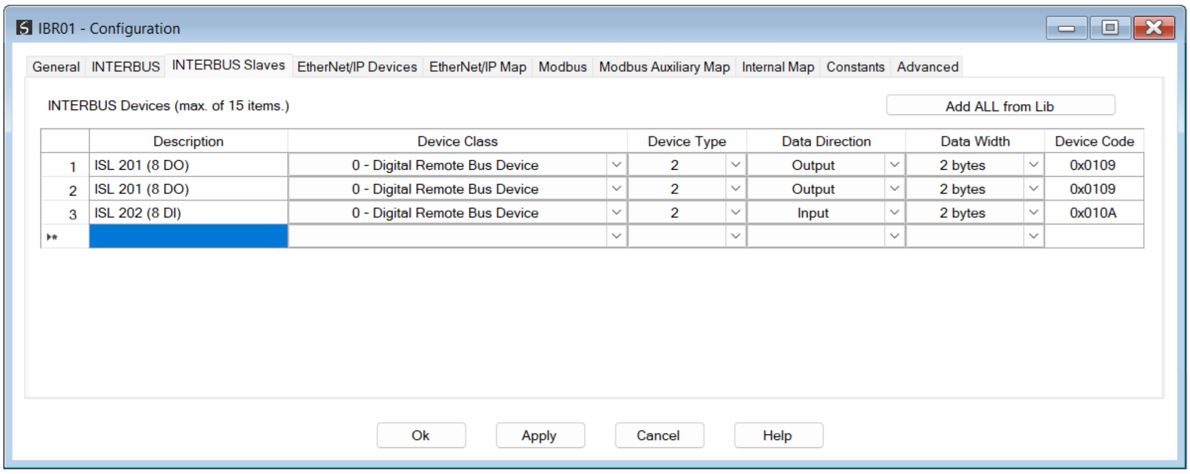


Figure 3.17 – INTERBUS Slave Configuration

The **INTERBUS Identity** configuration consists of the following parameters:

Parameter	**Description**
Description	A user defined description for the slave device.
Device Class	The slave device's Device Class, select one of the following: • 0 - Digital Remote Bus Device • 2 - Digital Remote Bus Device • 3 - Analog Remote Bus Device • 4 - Analog Local Bus Device

	• 5 - Analog Local Bus Device • 6 - Analog Local Bus Device • 7 - Analog Local Bus Device • 8 - Digital Local Bus Device • 9 - Digital Local Bus Device • 10 - Digital Local Bus Device • 11 - Digital Local Bus Device
Device Type	The Device Type sets up the lower 2 bits of the Device Class, either 0, 1, 2 or 3.
Data Direction	The direction of the data, either: • No Data - Placeholder / bus coupler • Input – Input Data Only • Output – Output Data Only • Input Output – Input and Output Data
Data Width	The (input/output) data width: • None • 2 bytes • 4 bytes • 6 bytes • 8 bytes • 10 bytes • 16 bytes • 18 bytes • 4 bits • 1 byte • 12 bits • 3 bytes • 1 bit • 2 bits • 12 bytes • 14 bytes • 52 bytes • 32 bytes • 48 bytes • 64 bytes • 20 bytes • 24 bytes • 28 bytes
Device Code	The Device Code is identifier for the device and is compiled using the Device's Class, Type, Data Direction and Data Width. This is a read-only field.

Table 3.3 – INTERBUS Slave parameters

3.6. PRIMARY INTERFACE

The INTERBUS Router module supports four different modes for the Primary Interface.

3.6.1. ETHERNET/IP TARGET

A controller (e.g. Logix controller) can own the INTERBUS Router over EtherNet/IP using up to 4 Class 1 EtherNet/IP connections when the Primary Interface is set to EtherNet/IP target. This will allow the INTERBUS Router to exchange data with the controller using the input and output assembly of the Class 1 EtherNet/IP connections. Data from the virtual INTERBUS slaves can be mapped to the Logix controller over EtherNet/IP.

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

3.6.1.1. STUDIO / LOGIX 5000 CONFIGURATION

A. ADD MODULE TO ETHERNET/IP I/O CONFIGURATION

The INTERBUS Router 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).

NOTE: Logix version 21 and newer supports EDS AOPs.

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.

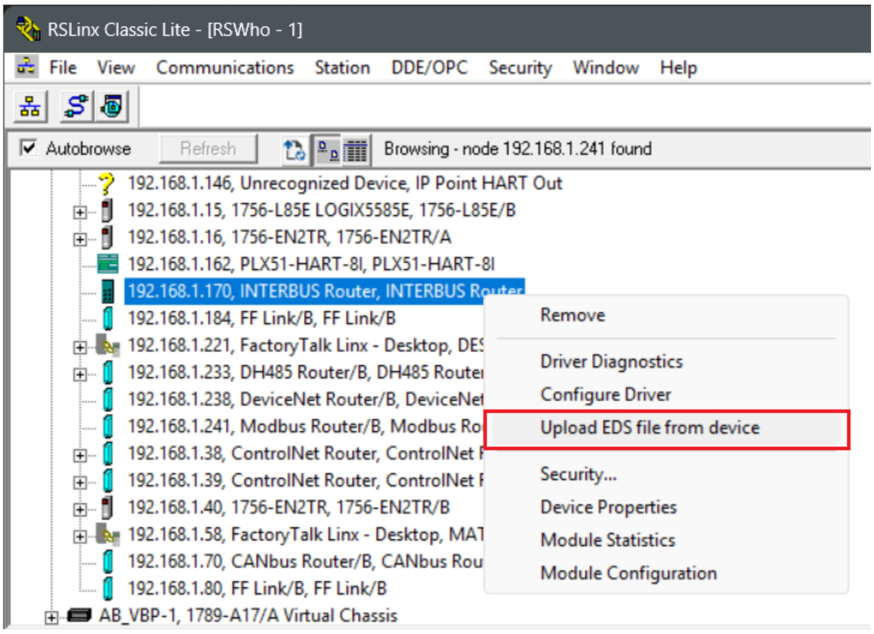


Figure 3.18 – EDS file upload from INTERBUS Router

Alternatively, the EDS file can be downloaded from the product web page at www.aparian.com and registered manually using the ***EDS Hardware Installation Tool*** shortcut under the ***Tools*** menu in Studio 5000.

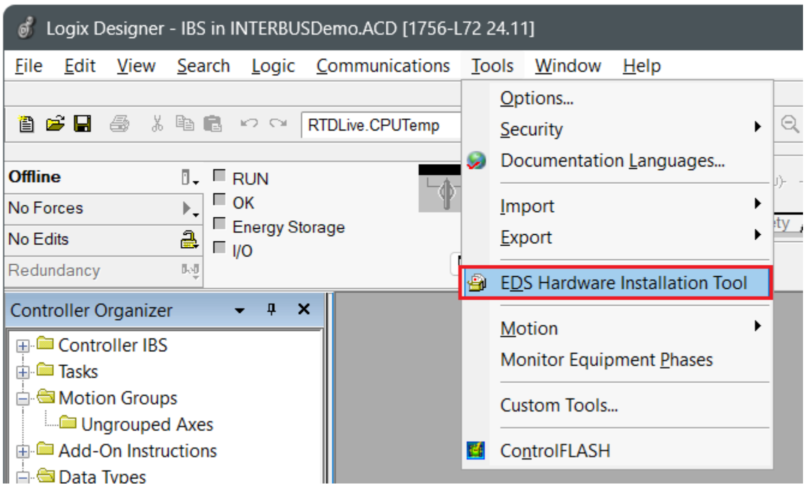


Figure 3.19 - EDS Hardware Installation Utility

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.

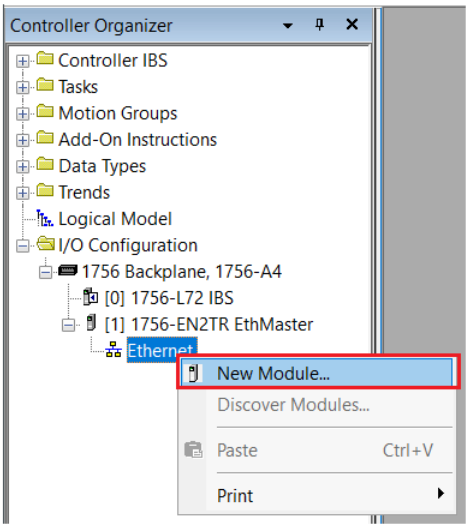


Figure 3.20 – Adding a module

The module selection dialog will open. To find the module more easily, use the Vendor filter to select only the Aparian modules as shown in the figure below.

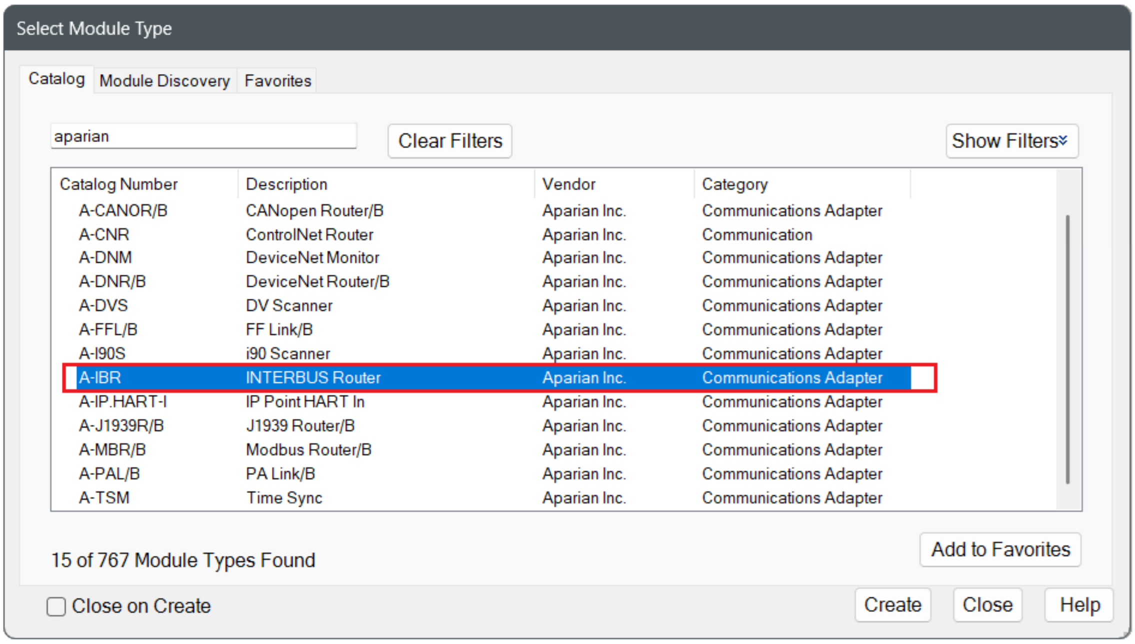


Figure 3.21 – Selecting the module

Locate and select the INTERBUS Router 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.

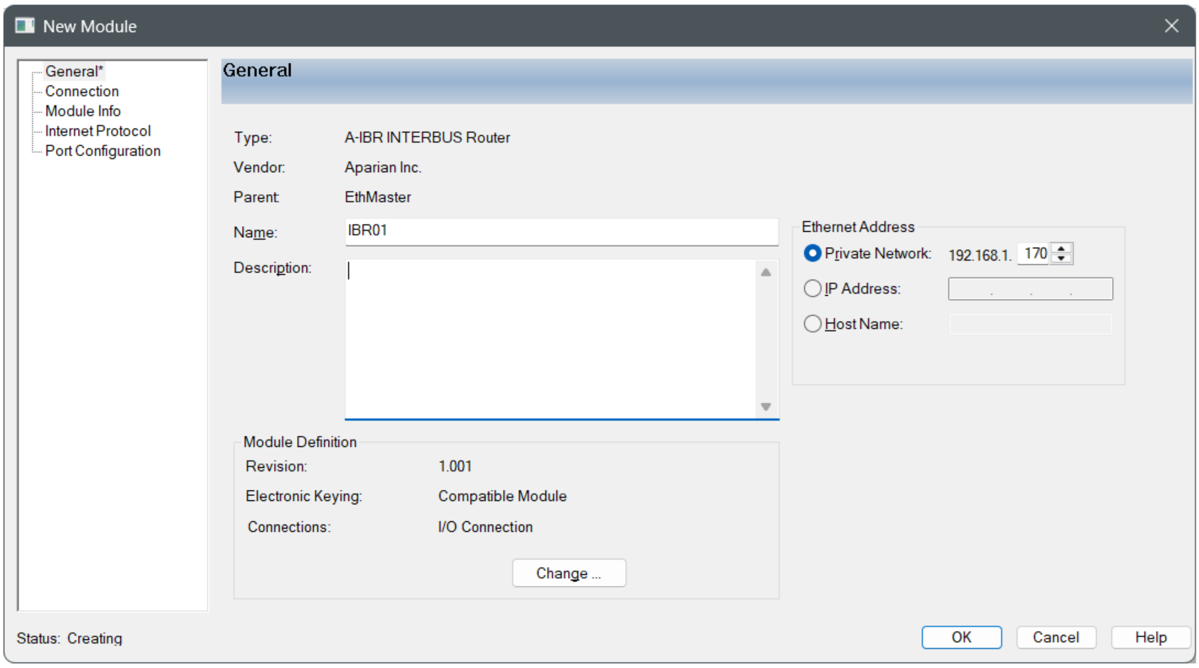


Figure 3.22 – Module instantiation

The INTERBUS Router supports up to 4 class 1 EtherNet/IP connections. The user will need to **ensure that the number of connections configured in the General tab of the module configuration (Slate) matches the selected connection count in Logix (Studio 5000)**.

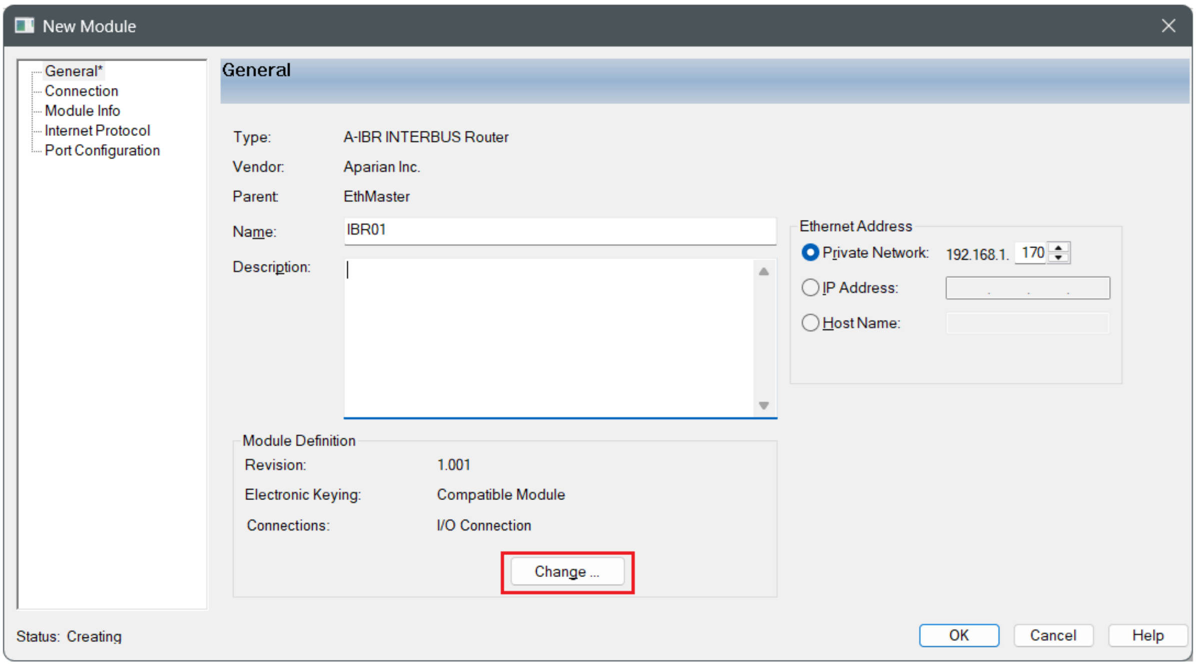


Figure 3.23 – Change number of IO Connections

Next the user will need to select the number of connections required.

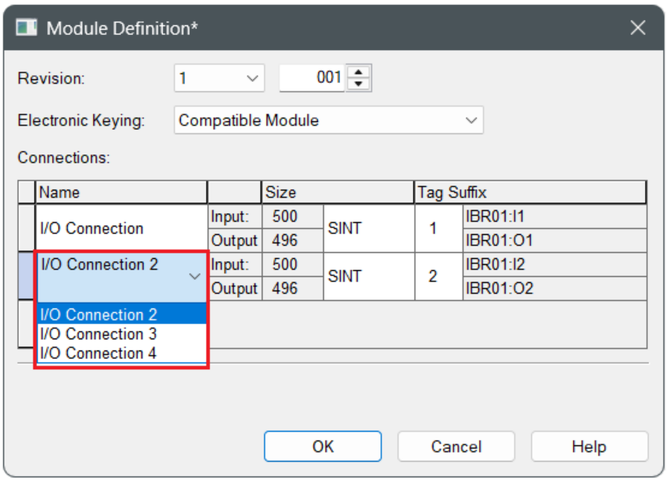


Figure 3.24 – Selection of IO Connections

Now the INTERBUS Router module will be in the Logix IO tree.

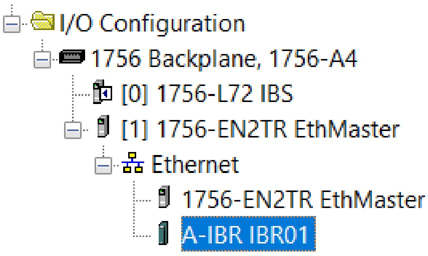


Figure 3.25 – Logix IO tree

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

B. LOGIX MAPPING

Slate will generate the required UDTs and Routines (based on the Internal Map) to map the required INTERBUS slave data. The user will need to select the ***Recommend*** button in the Internal Mapping to auto populate the Internal Mapping which can then be used to generate the L5X file for Logix mapping, routines, and UDTs

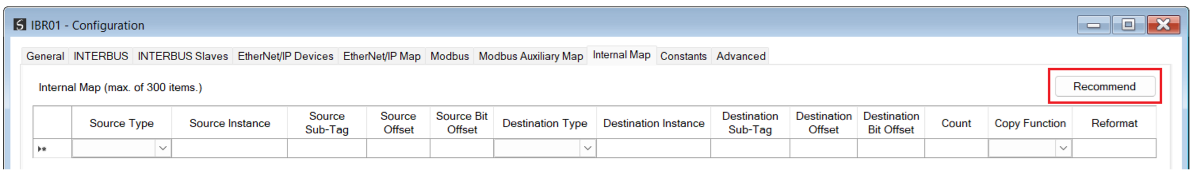


Figure 3.26 – Internal Mapping Recommend

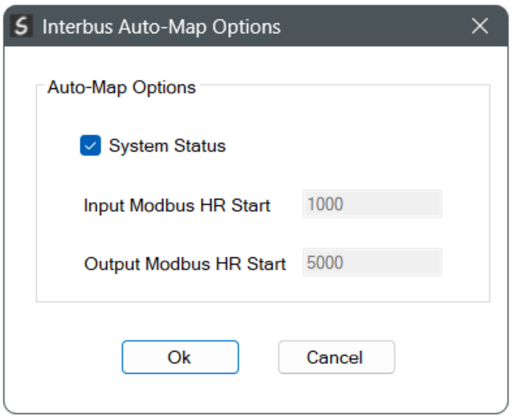
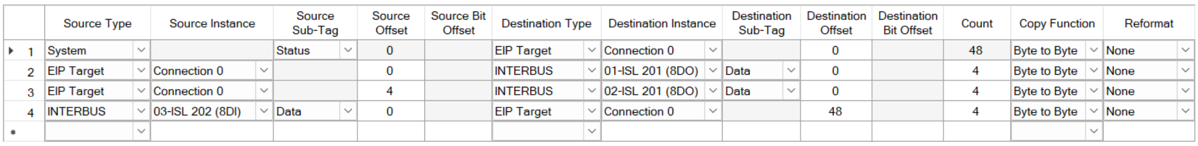


Figure 3.27 – Auto-Map Options popup



	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count	Copy Function	Reformat
1	System		Status	0		EIP Target	Connection 0		0		48	Byte to Byte	None
2	EIP Target	Connection 0		0		INTERBUS	01-ISL 201 (8DO)	Data	0		4	Byte to Byte	None
3	EIP Target	Connection 0		4		INTERBUS	02-ISL 201 (8DO)	Data	0		4	Byte to Byte	None
4	INTERBUS	03-ISL 202 (8DI)	Data	0		EIP Target	Connection 0		48		4	Byte to Byte	None
*													

Figure 3.28 – Internal Mapping Auto Populated

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

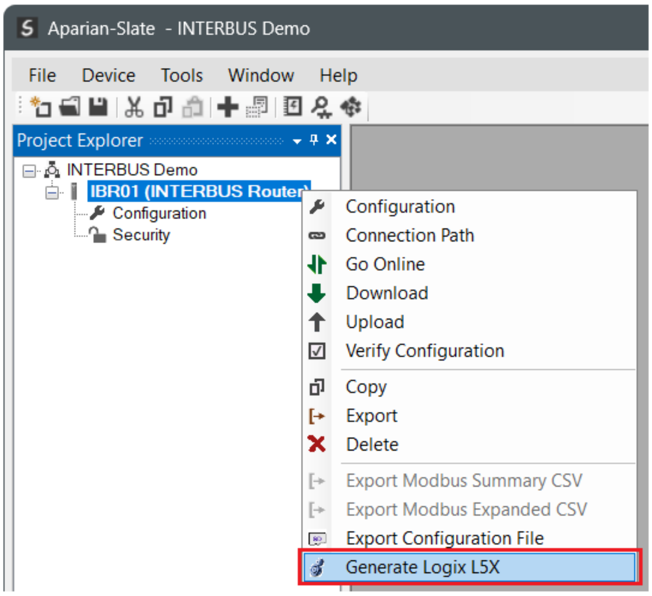


Figure 3.29 – Selecting Generate Logix L5X

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

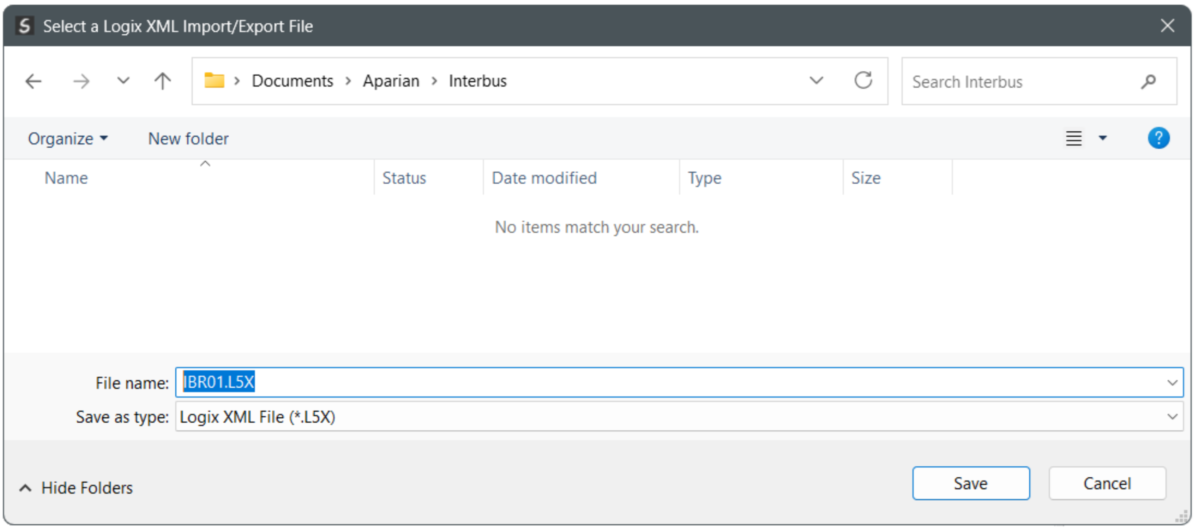


Figure 3.30 – Selecting the Logix L5X file name

This L5X file can now be imported into the Studio 5000 project by right-clicking on a suitable ***Program*** and selecting ***Add***, and then ***Import Routine***.

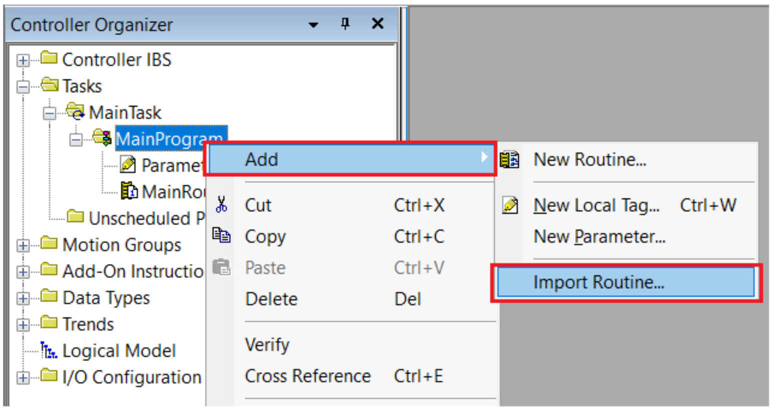


Figure 3.31 – Importing the L5X file into Studio 5000

In the file open dialog 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.

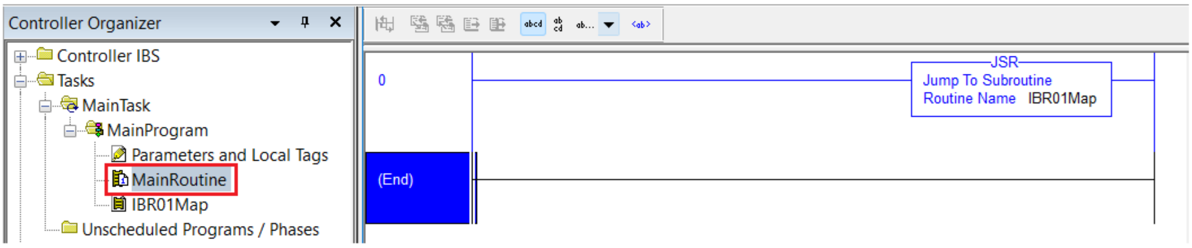


Figure 3.32 – Calling the mapping routine

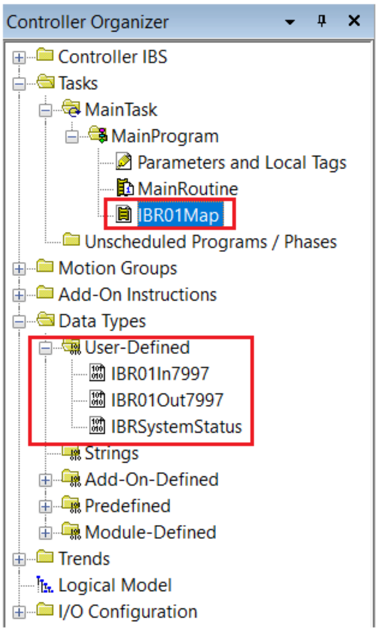


Figure 3.33 – Imported Logix Objects

There are two INTERBUS Router specific (UDT) tags created. One for the Input data ("…In") and one for the Output data ("…Out"). The structure of each tag's underlying UDT depends on the configured internal mapping.

If the ***System Status*** option was selected during the mapping, then the Module Status structure will be included in the Input tag.

The System tag displays the status and diagnostics information of the INTERBUS Router.

Name	Value	Style	Data Type	Description
IBR01In	{...}		IBR01In7997	
IBR01In.ModuleStatus	{...}		IBRSystemStatus	
IBR01In.ModuleStatus.ChcksmErrCount	0	Decimal	DINT	Checksum Error Count
IBR01In.ModuleStatus.ConfigValid	1	Decimal	BOOL	Configuration Valid
IBR01In.ModuleStatus.ControllerRun	1	Decimal	BOOL	Controller Mode: 0=Program, 1=Run
IBR01In.ModuleStatus.DataPcktCount	0	Decimal	DINT	Data Packet Count
IBR01In.ModuleStatus.EIPOriginatorCommsOk	0	Decimal	BOOL	EtherNet/IP Originator 0=Fail, 1=Ok
IBR01In.ModuleStatus.EIPOwned	1	Decimal	BOOL	EtherNet/IP Target 0=Not-Owned, 1=Owned
IBR01In.ModuleStatus.IdentPcktCount	0	Decimal	DINT	Ident Packet Count
IBR01In.ModuleStatus.IdleStateChgCount	0	Decimal	DINT	Idle State Change Count
IBR01In.ModuleStatus.IdleTimeoutCount	0	Decimal	DINT	Idle Timeout Count
IBR01In.ModuleStatus.INTERBUSActive	0	Decimal	BOOL	INTERBUS Active: 0=Off 1=Active
IBR01In.ModuleStatus.INTERBUSRun	0	Decimal	BOOL	INTERBUS Run: 0=Off 1=Run
IBR01In.ModuleStatus.ModbusOnline	0	Decimal	BOOL	0=Offline, 1=Online
IBR01In.ModuleStatus.NTPOk	0	Decimal	BOOL	NTP Status: 0=Fail, 1=Ok
IBR01In.ModuleStatus.RxPcktCount	0	Decimal	DINT	Rx Packet Count
IBR01In.ModuleStatus.TransactionRate	0	Decimal	DINT	Transaction Rate
IBR01In.ModuleStatus.TxPcktUpdateCount	0	Decimal	DINT	Tx Packet Update Count
IBR01In.ModuleStatus.UnknownCmdCount	0	Decimal	DINT	Unknown Command Count

Figure 3.34 – System Status tag

Each configured and mapped INTERBUS Slave data will be included in these tags.

Name	Value	Style	Data Type	Description
IBR01In	{...}		IBR01In7997	
IBR01In.ModuleStatus	{...}		IBRSystemStatus	
IBR01In.S03_ISL2028DI	{...}	Hex	SINT[4]	ISL 202 (8DI) Output Data
IBR01In.S03_ISL2028DI[0]	16#00	Hex	SINT	ISL 202 (8DI) Output Data
IBR01In.S03_ISL2028DI[1]	16#00	Hex	SINT	ISL 202 (8DI) Output Data
IBR01In.S03_ISL2028DI[2]	16#00	Hex	SINT	ISL 202 (8DI) Output Data
IBR01In.S03_ISL2028DI[3]	16#00	Hex	SINT	ISL 202 (8DI) Output Data
IBR01Out	{...}		IBR01Out7997	
IBR01Out.S01_ISL2018DO	{...}	Hex	SINT[4]	ISL 201 (8DO) Input Data
IBR01Out.S01_ISL2018DO[0]	16#00	Hex	SINT	ISL 201 (8DO) Input Data
IBR01Out.S01_ISL2018DO[1]	16#00	Hex	SINT	ISL 201 (8DO) Input Data
IBR01Out.S01_ISL2018DO[2]	16#00	Hex	SINT	ISL 201 (8DO) Input Data
IBR01Out.S01_ISL2018DO[3]	16#00	Hex	SINT	ISL 201 (8DO) Input Data
IBR01Out.S02_ISL2018DO	{...}	Hex	SINT[4]	ISL 201 (8DO) Input Data
IBR01Out.S02_ISL2018DO[0]	16#00	Hex	SINT	ISL 201 (8DO) Input Data
IBR01Out.S02_ISL2018DO[1]	16#00	Hex	SINT	ISL 201 (8DO) Input Data
IBR01Out.S02_ISL2018DO[2]	16#00	Hex	SINT	ISL 201 (8DO) Input Data
IBR01Out.S02_ISL2018DO[3]	16#00	Hex	SINT	ISL 201 (8DO) Input Data

Figure 3.35 – INTERBUS Device Data

3.6.1.2. 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 INTERBUS interface 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.

A. IDS COPY – ETHERNET/IP TARGET SOURCE

When copying data from a connection originator (e.g. the output assembly from the Logix Controller) to the INTERBUS interface, the source type needs to be EIP Target.

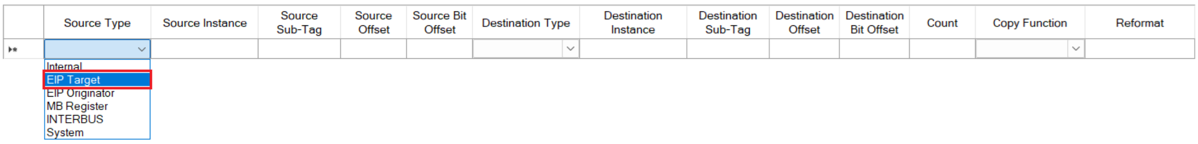


Figure 3.36 – IDS Copy – EtherNet/IP Target Source Type

The source instance will be the connection number, which can be connection 0 to 3, 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.

See the Internal Data Space Mapping section for more information regarding the operation.

B. IDS COPY – ETHERNET/IP TARGET DESTINATION

When copying data from the INTERBUS interface to the EtherNet/IP Target input assembly, the destination type needs to be EIP Target.

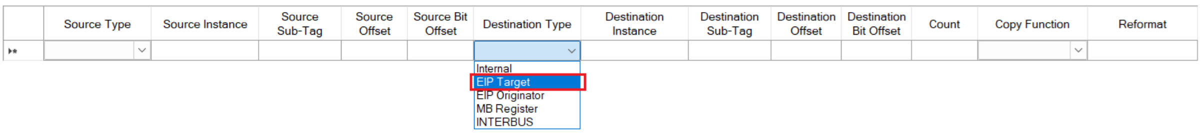


Figure 3.37 – IDS Copy – EtherNet/IP Target Destination Type

The destination instance will be the connection number, which can be connection 0 to 3, 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.

3.6.2. MODBUS (SERVER AND CLIENT)

The INTERBUS Router can operate as a Modbus Server or Modbus Client for Modbus TCP.

When configured as a Modbus Server, a remote Modbus Client can read and write to the Modbus Register range (0-4999) in the INTERBUS Router.

When configured as a Modbus Client, the user will need to configure 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 Parameters will need to be configured for either Modbus modes.

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.

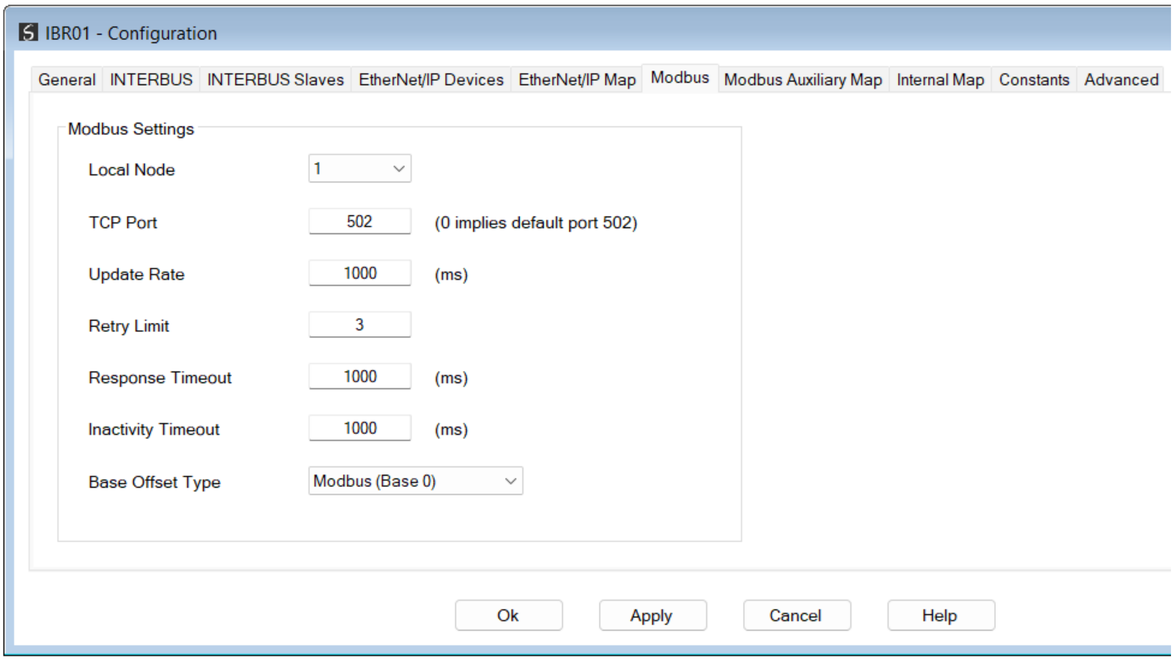


Figure 3.38 – Modbus Configuration

The Modbus Communication configuration consists of the following parameters:

Parameter	Description
Local Node	The Modbus Node address assigned to the INTERBUS Router. **(Modbus Client mode only)**
TCP Port	The TCP port to be used for the Modbus 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 INTERBUS Router 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.

Table 3.3 – Modbus parameters

3.6.2.1. INTERNAL DATA SPACE MAPPING

When the module is operating as a Modbus Server or Client, the internal Modbus Registers can be mapped to the INTERBUS data 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 INTERBUS status and data to recommended Modbus Registers.

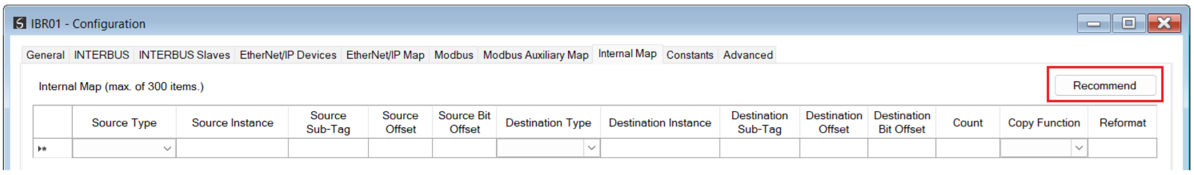


Figure 3.39 – Modbus – Internal Mapping Recommend

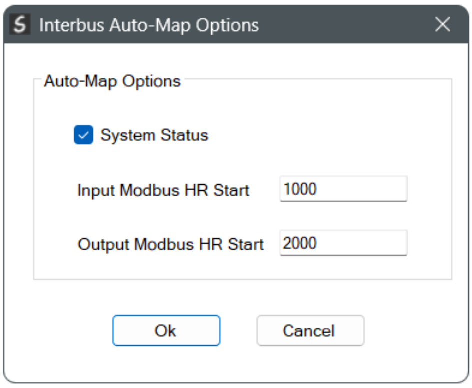


Figure 3.40 – Modbus – Auto-Map Options

	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count	Copy Function	Reformat
1	System		Status	0		MB Register	HR		1000		48	Byte to Byte	None
2	INTERBUS	01-ISL 201 (8DO)	Data	0		MB Register	HR		1024		2	Byte to Byte	None
3	INTERBUS	02-ISL 201 (8DO)	Data	0		MB Register	HR		1025		2	Byte to Byte	None
4	MB Register	HR		2000		INTERBUS	03-ISL 202 (8DI)	Data	0		2	Byte to Byte	None
*													

Figure 3.41 – Modbus Server – Internal Mapping Updated

A. IDS COPY – MODBUS SOURCE

When copying Modbus data to the INTERBUS interface, the source type needs to be MB Register.

	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count	Copy Function	Reformat
*													

Internal
EIP Target
EIP Originator
MB Register
INTERBUS
System

Figure 3.42 – IDS Copy - Modbus Source Type

The source instance will be the Modbus register type required.

	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count	Copy Function	Reformat
1	MB Register	CS		0					0		1	Byte to Byte	None
*													

CS
IS
IR
HR

Figure 3.43 – 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. See the Internal Data Space Mapping section for more information regarding the operation.

B. IDS COPY – MODBUS DESTINATION

When copying data from the INTERBUS interface to a Modbus Register, the destination type needs to be MB Register.

	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count	Copy Function	Reformat
1	INTERBUS	01-ISL 201 (8DO)	Data	0					0		1	Byte to Byte	None
*													

Internal
EIP Target
EIP Originator
MB Register
INTERBUS

Figure 3.44 – IDS Copy - Modbus Destination Type

The destination instance will be the Modbus register type required.

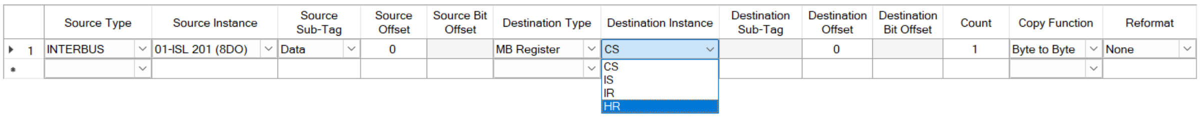


Figure 3.45 – IDS Copy - Modbus Destination Instance

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. See the Internal Data Space Mapping section for more information regarding the operation.

3.6.2.2. 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***.

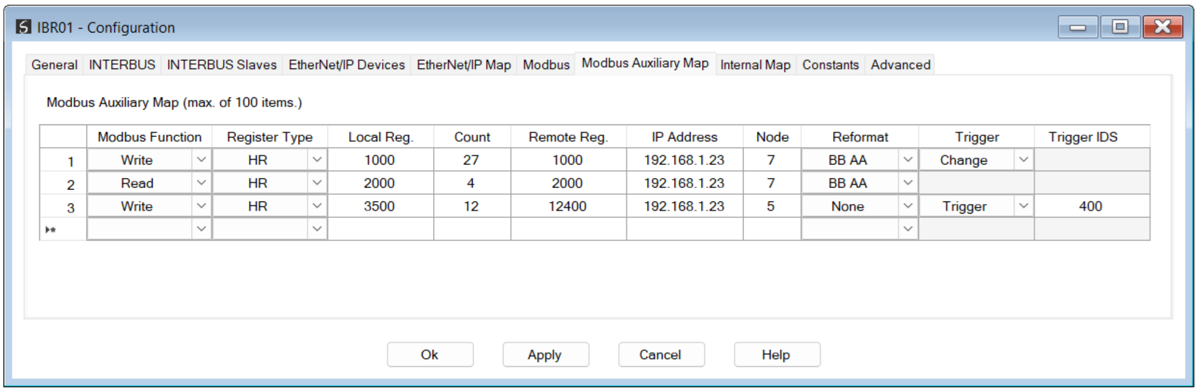


Figure 3.46 – Modbus Auxiliary Map Configuration

The Modbus Auxiliary Map configuration consists of the following parameters:

Parameter	Description
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) INTERBUS Router Modbus register address (0-4999).
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
Trigger	For Modbus **Write** Functions, the user can select one of three triggers for the write operation. **Cyclic** The specific mapped item will be executed at the update rate (similar to all the read functions). **Change** When any of the data has been changed in the Modbus register range used to write the mapping, then this mapped item will be executed. **Trigger** When Trigger is selected, then the user will need to provide an IDS register which is used to trigger the specific Modbus Auxiliary option. When the provided IDS register changes, then the mapped item transaction will execute.
Trigger IDS	The IDS Register Offset used to trigger the respective Mapped item.

Table 3.4 – Modbus Auxiliary Map parameters

3.6.3. EtherNet/IP Originator

The INTERBUS Router 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 Slate project tree.

3.6.3.1. ETHERNET/IP CLASS 1 DEVICE CONNECTIONS

The INTERBUS Router can establish up to 15 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

A. MANUAL CONFIGURATION

A class 1 connection can be added to the *EtherNet/IP Connections* tree by right-clicking on the tree in Slate and selecting ***Add EtherNet/IP Connection***.

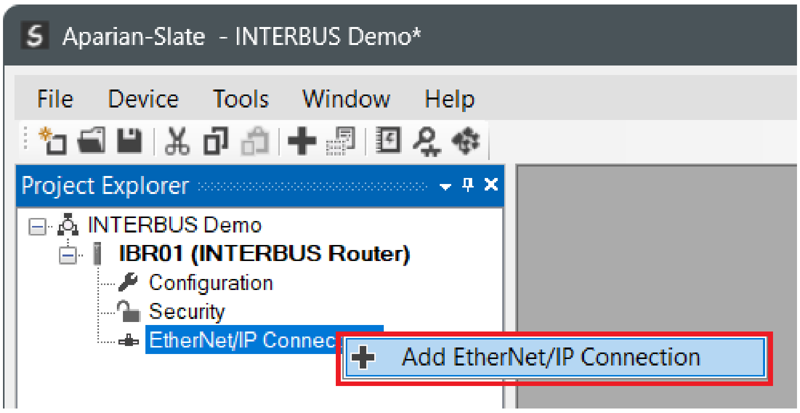


Figure 3.47 – Adding EtherNet/IP Class 1 Connection

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

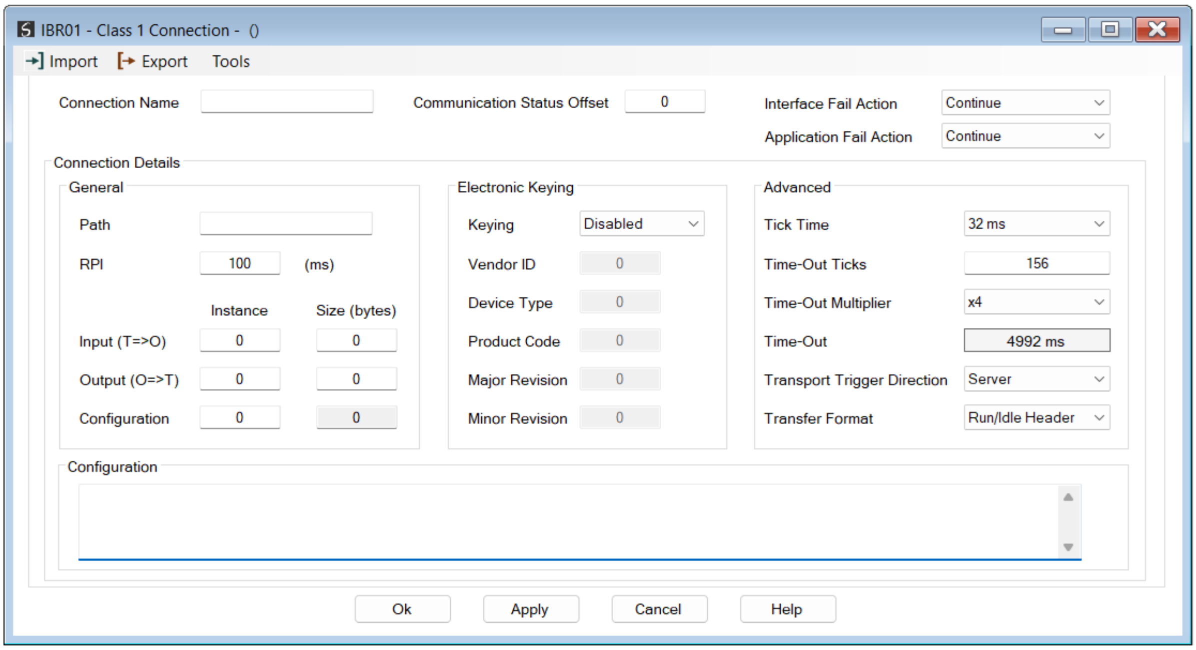


Figure 3.48 – EtherNet/IP Class 1 Connection Parameters

NOTE: 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 the INTERBUS communication has 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 INTERBUS communication fails.
Application Fail Action	This field determines the behavior of the INTERBUS communication when this EtherNet/IP communication fails. **Continue** INTERBUS communication continues using existing data. **Zero Data** INTERBUS communication continues, but the mapped data for this EtherNet/IP connection is set to zero. **Offline** The INTERBUS communication is stopped.
General	
Path	The path to the target device. If the device is an Ethernet device, then this will just be the IP address of the module.

	If the device is, for example, a module in a backplane or via an adapter, then the user will need to 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**.
Transfer Format	The Real Time Transfer Format for the O->T transfer. **Run/Idle Header** Includes a 16-bit sequence count, a 32-bit header with the Run/Idle notification, and the application data. **Modeless** Includes a 16-bit sequence count and the application data. **Heartbeat** Includes a 16-bit sequence count. **Zero-Length Idle** Includes a 16-bit sequence count and the application data only when not not in idle mode.
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 3.5 – EtherNet/IP Class 1 Connection Parameters

B. IMPORT FROM ONLINE CONTROLLER

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

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.

NOTE: When instantiating modules in Studio5000 do <u>not</u> make use of the "Rack Optimization" communication format.

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

NOTE: 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.

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.

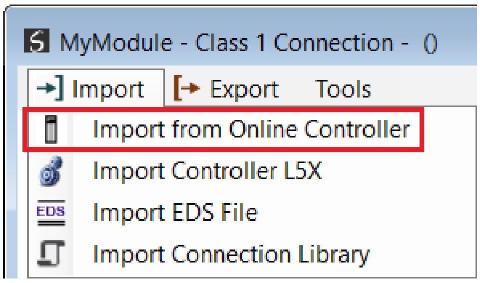


Figure 3.49 – Import from Online Controller

The Import Connection Parameters form will open.

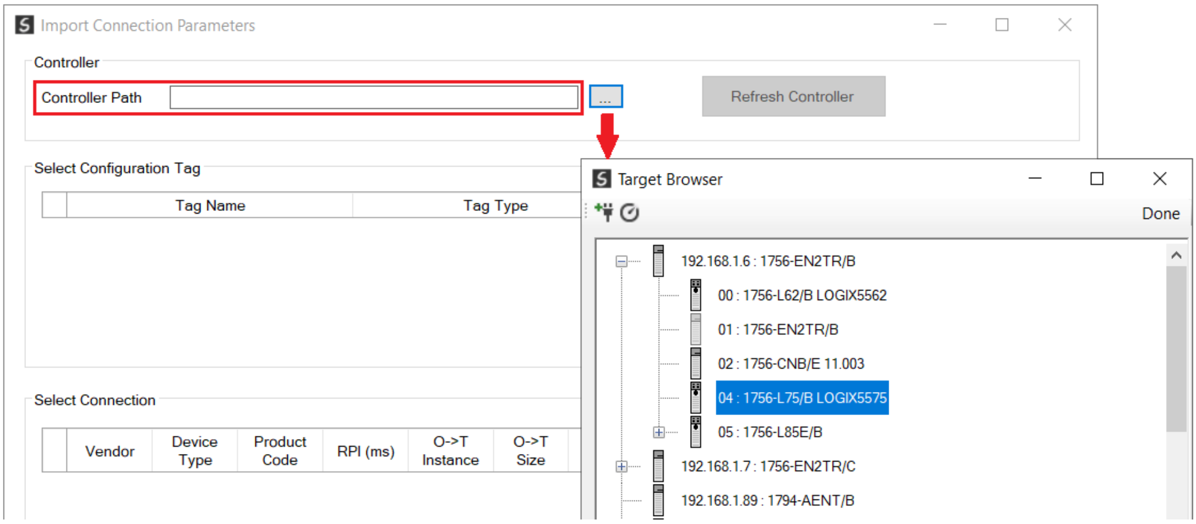


Figure 3.50 – Import Connection Parameters – Controller Path

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.

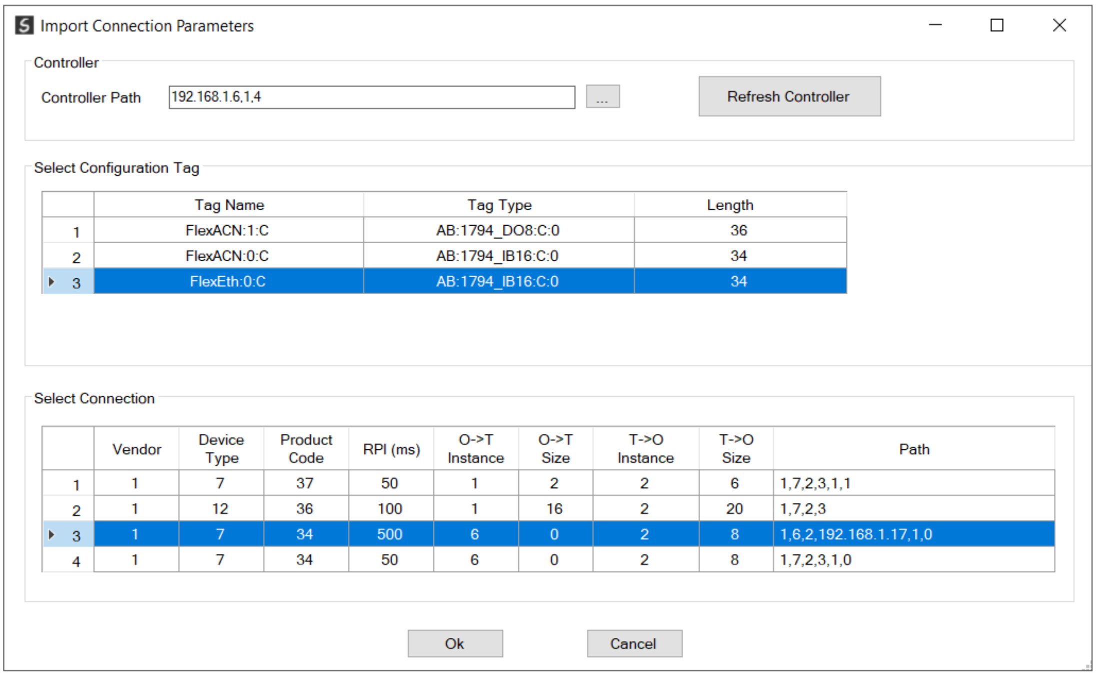


Figure 3.51 – Import Connection Parameters – Select Connection

In order 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.

C. IMPORT FROM CONTROLLER L5X FILE

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

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.

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

NOTE: 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.

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.

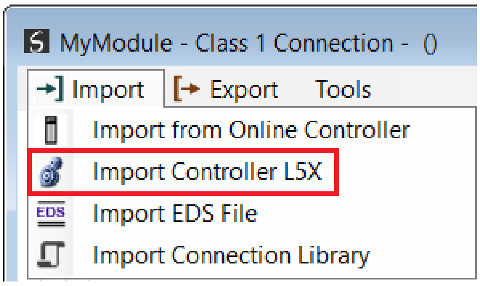


Figure 3.52 – Import from Controller L5X

The Import Connection Parameters form will open.

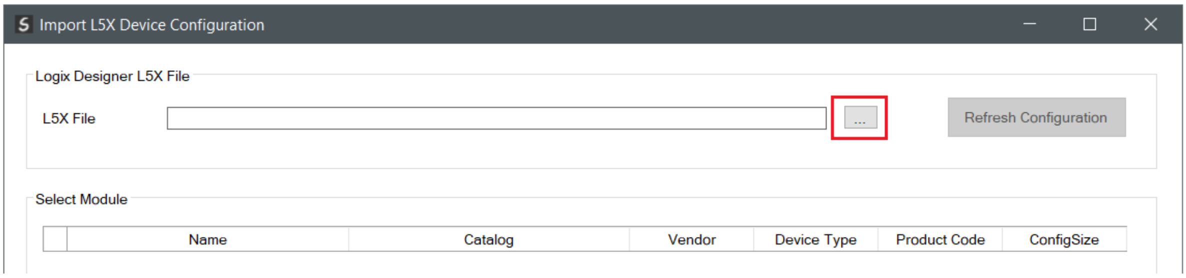


Figure 3.53 – Import L5X Device Configuration – Select L5X

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.

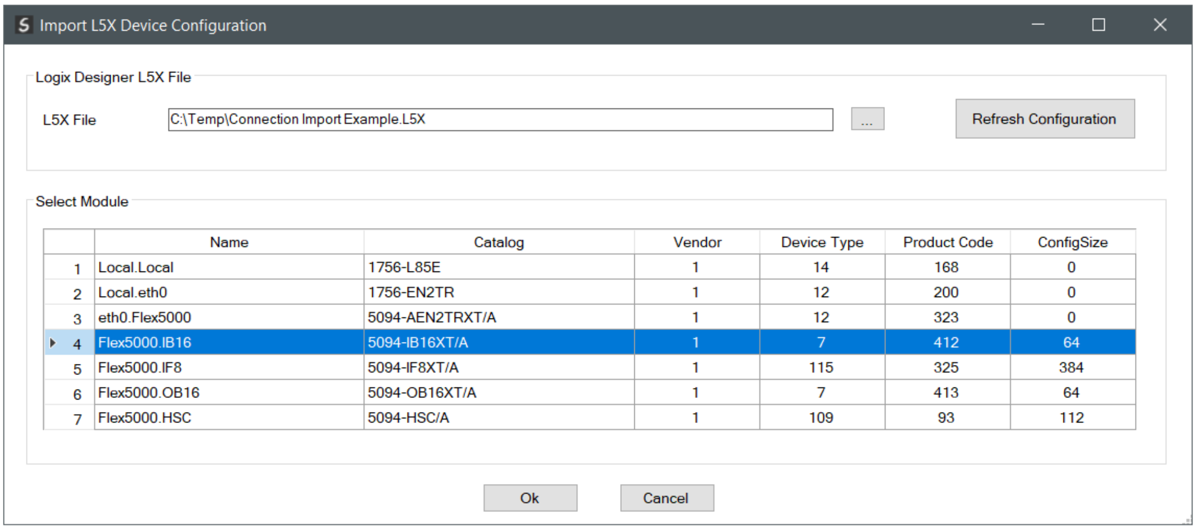


Figure 3.54 – Import L5X Device Configuration

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.

D. 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.

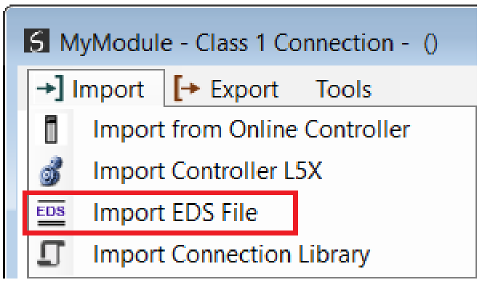


Figure 3.55 – Import EDS File

A File Open dialog will open allowing the user to select the EDS file.

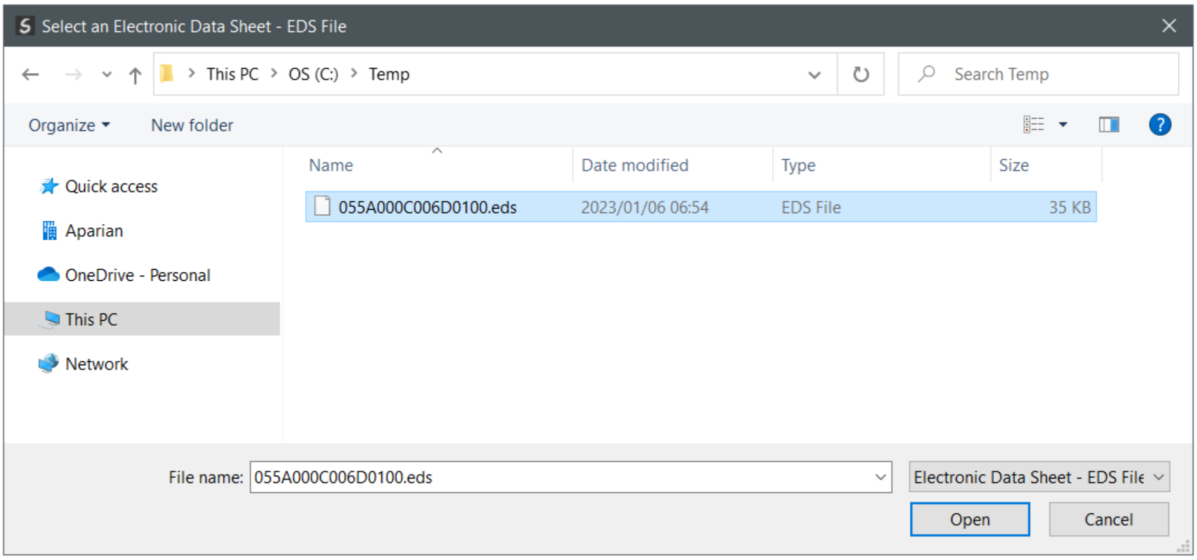


Figure 3.56 – Browse to EDS File

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.

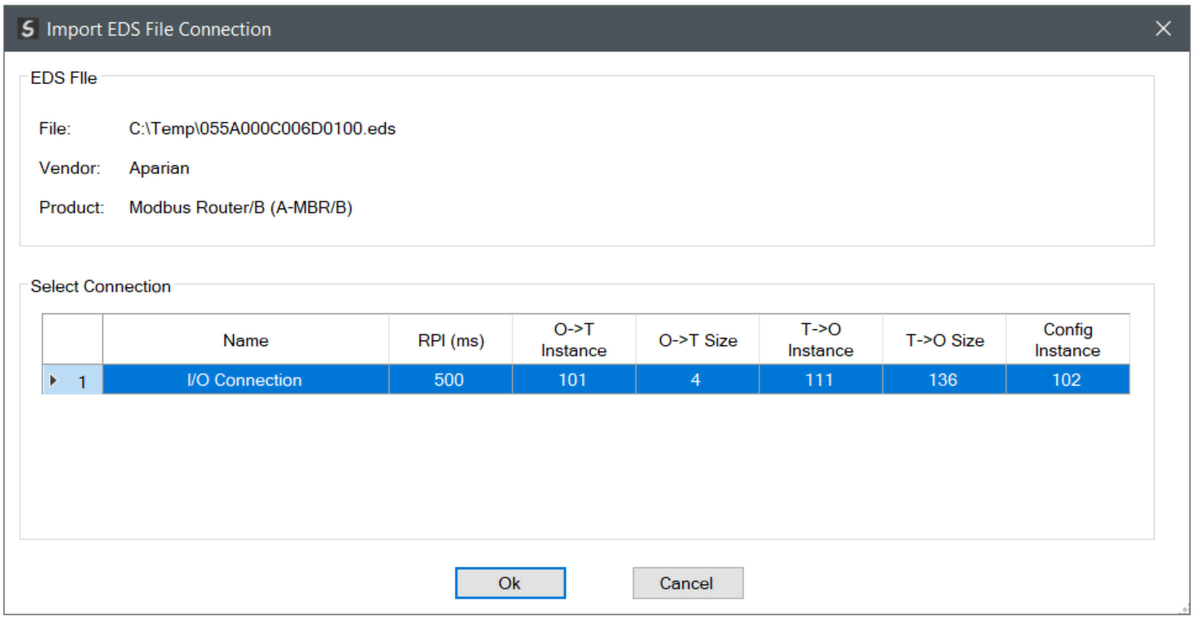


Figure 3.57 – Select Connection

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.

E. IMPORT CONNECTION LIBRARY

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

NOTE: Please contact support to receive a pack 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.

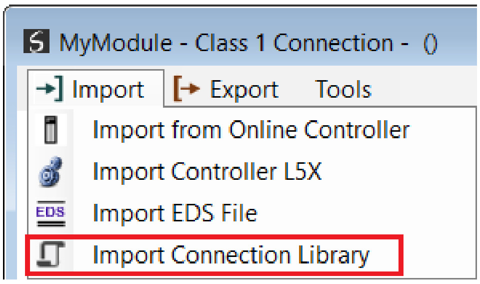


Figure 3.58 – Import Connection Library File

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.

EXPORT LIBRARY FILE

In order to create a Library file for future use, select the ***Export Connection Library*** option located under the ***Export*** menu.

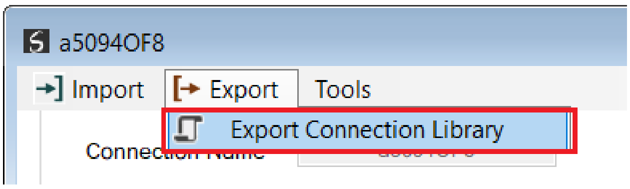


Figure 3.59 – Export Connection Library File

3.6.3.2. 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.

A. *ETHERNET/IP DEVICES*

This tab is enabled when the Primary Interface is set to *EtherNet/IP Originator*.

The EtherNet/IP Devices configuration is shown in the figure below. 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 5Kbytes. See the *Explicit EtherNet/IP Messaging* section for more details.

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

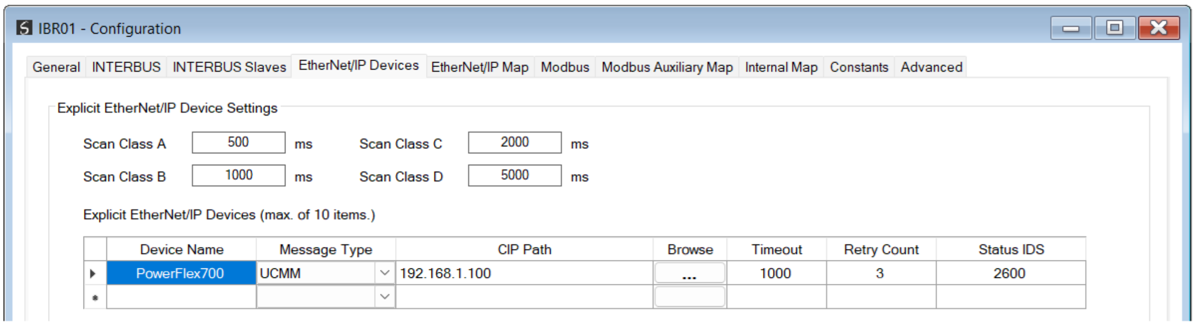


Figure 3.60 – EtherNet/IP Devices - Configuration

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

Parameter	Description
Scan Class A, B, C, D	The configurable update rates (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 to them by clicking the ***Browse*** button. The Target Browser will open and automatically scan for 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 amount of 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 3.6 – EtherNet/IP Devices configuration parameters

B. ETHERNET/IP MAP

This tab is enabled when the Primary Interface is set to *EtherNet/IP Originator*.

The EtherNet/IP Map configuration is shown in the figure below. 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 5Kbytes. See the *Explicit EtherNet/IP Messaging* section for more details.

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

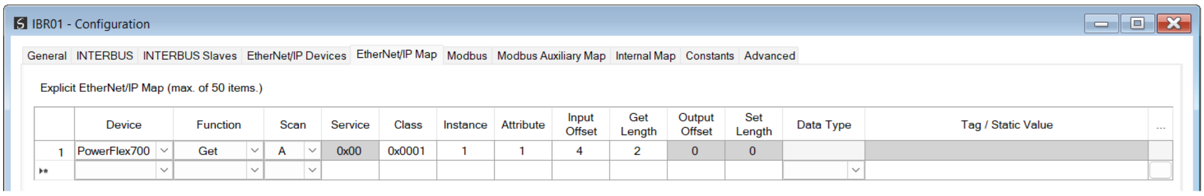


Figure 3.61 – EtherNet/IP Map configuration

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** Similar to 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 INTERBUS Router module can be setup 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 INTERBUS Router module 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 INTERBUS Router module 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 execute 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 <u>elements</u> 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 ***Set*** 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 3.7 – EtherNet/IP Map configuration parameters

3.6.3.3. INTERNAL DATA SPACE MAPPING

When the module is operating as an EtherNet/IP Originator, the data from the EtherNet/IP IO devices can be mapped to the INTERBUS interface 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.

A. IDS COPY – ETHERNET/IP ORIGINATOR SOURCE

When copying data from an EtherNet/IP IO to the INTERBUS interface, the source type needs to be EIP Originator.

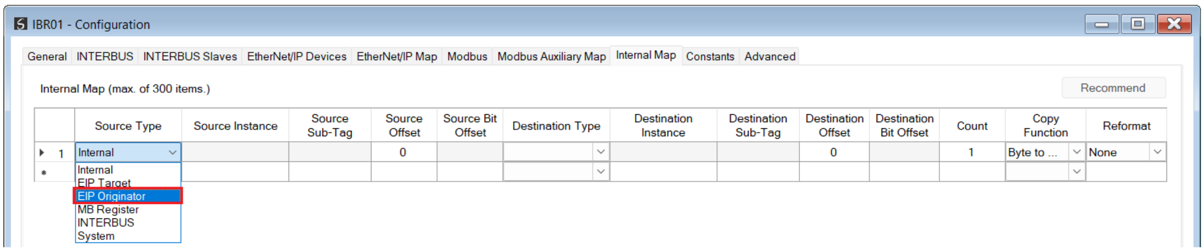


Figure 3.62 – IDS Copy – EtherNet/IP Originator Source Type

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

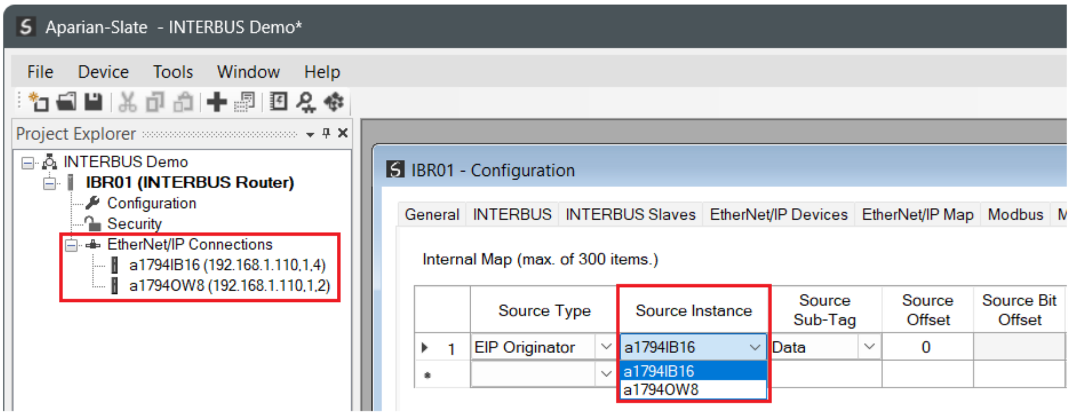


Figure 3.63 – IDS Copy – EtherNet/IP Originator Source Instance

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. See the Internal Data Space Mapping section for more information regarding the operation.

The user can select either the Data, or Status, to copy from the EtherNet/IP connection.

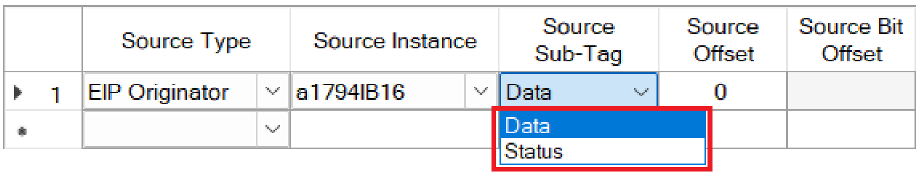


Figure 3.64 – IDS Copy – EtherNet/IP Originator Status

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 3.8 – EtherNet/IP Originator Connection Status

B. *IDS COPY – ETHERNET/IP TARGET DESTINATION*

When copying data from the INTERBUS interface to an EtherNet/IP IO device **Output** Assembly, the destination type needs to be EIP Originator.

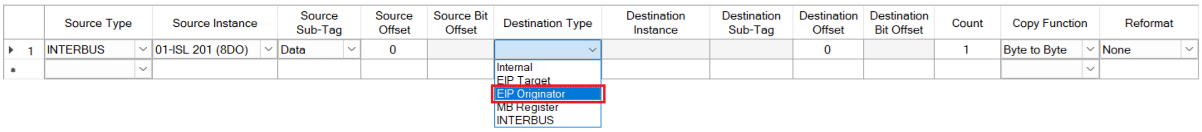


Figure 3.65 – IDS Copy – EtherNet/IP Originator Destination Type

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

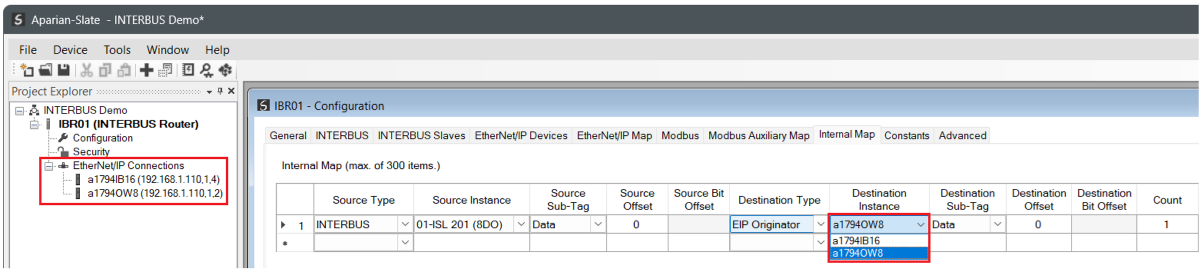


Figure 3.66 – IDS Copy – EtherNet/IP Originator Destination Instance

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 the Internal Data Space Mapping section for more information regarding the operation.

3.7. INTERNAL DATA SPACE MAP

The internal data map is used to exchange data from the Ethernet interface to the INTERBUS interface and vice versa. 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 incremented 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 incremented by one bit each time.

Table 3.9 – 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 3.10 – Internal Map Reformat Options

3.7.1. Copy From

One of six sources can be selected to copy from:
Internal, EIP Target, EIP Originator, MB Register, INTERBUS Device, and System.

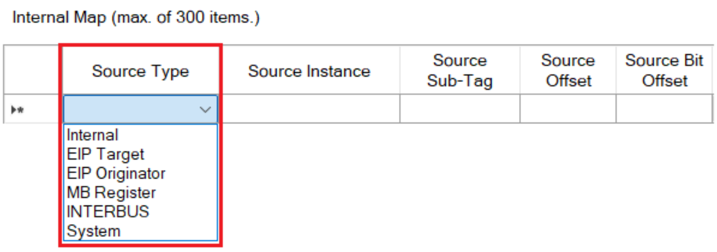


Figure 3.67 – Internal Map – Source Type

3.7.1.1. INTERNAL

When copying data from the internal data space (IDS), the source type needs to be Internal.

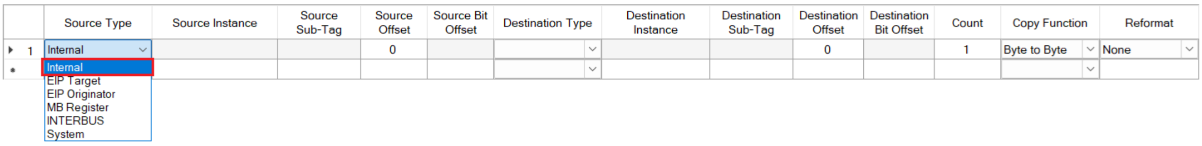


Figure 3.68 – IDS Copy – Internal Source Type

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 5,000 bytes. The Count is the number of **bytes** that will be copied.

3.7.1.2. EIP TARGET

When copying data from a connection originator (e.g. the output assembly from the Logix Controller) to the INTERBUS interface, the source type needs to be EIP Target.

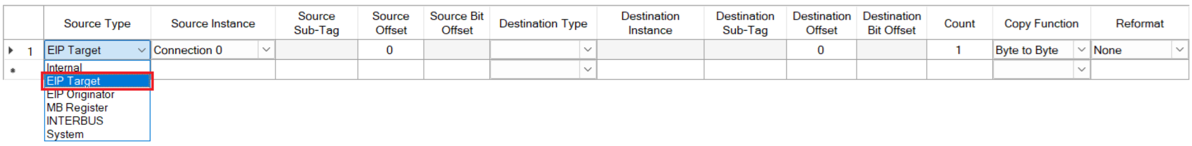


Figure 3.69 – IDS Copy – EtherNet/IP Target Source Type

The source instance will be the connection number, which can be connection 0 to 3, 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.

3.7.1.3. EIP ORIGINATOR

When copying data from an EtherNet/IP IO to the INTERBUS interface, the source type needs to be EIP Originator.

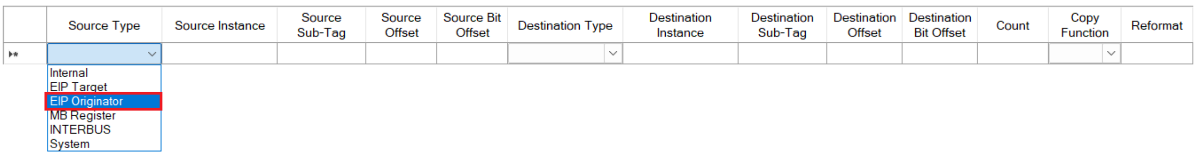


Figure 3.70 – IDS Copy – EtherNet/IP Originator Source Type

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

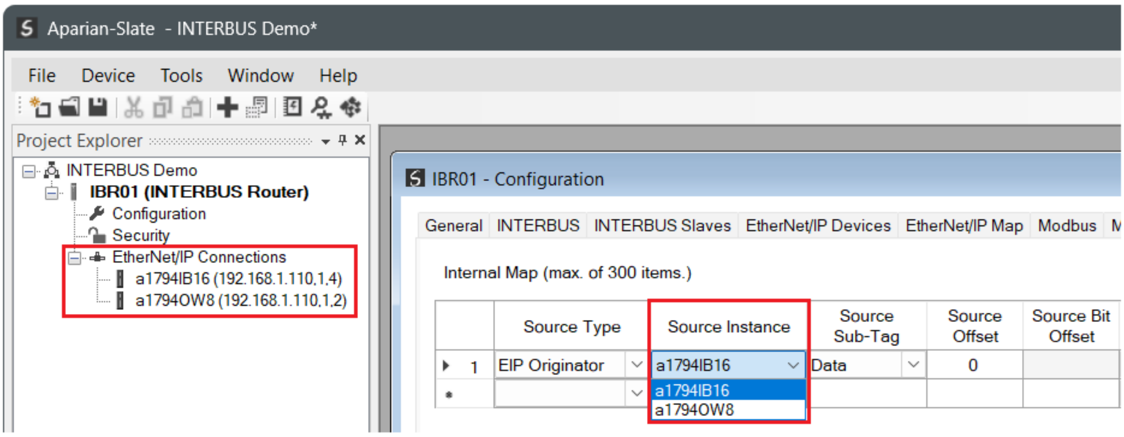


Figure 3.71 – IDS Copy – EtherNet/IP Originator Source Instance

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 the status.

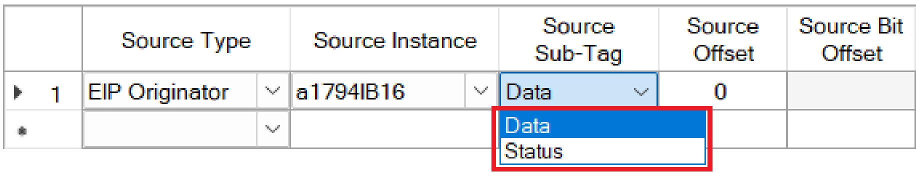


Figure 3.72 – IDS Copy – EtherNet/IP Originator Status

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 3.11 – EtherNet/IP Originator Connection Status

3.7.1.4. MODBUS REGISTER

When copying Modbus data to the INTERBUS interface, the source type needs to be MB Register.

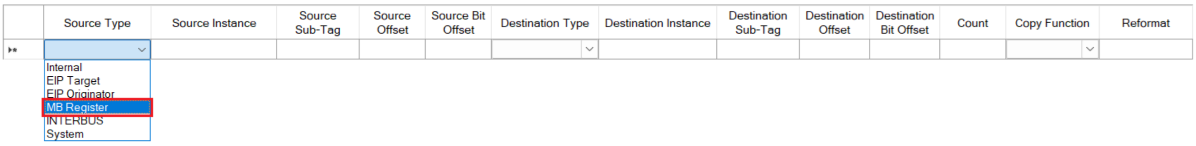


Figure 3.73 – IDS Copy - Modbus Source Type

The source instance will be the Modbus register type required.

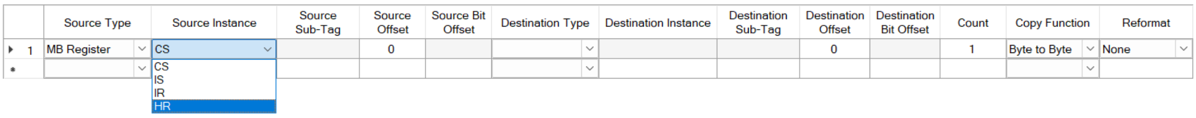


Figure 3.74 – IDS Copy - Modbus Source Instance

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.

3.7.1.5. INTERBUS

When copying data from an INTERBUS output, the source needs to be INTERBUS.

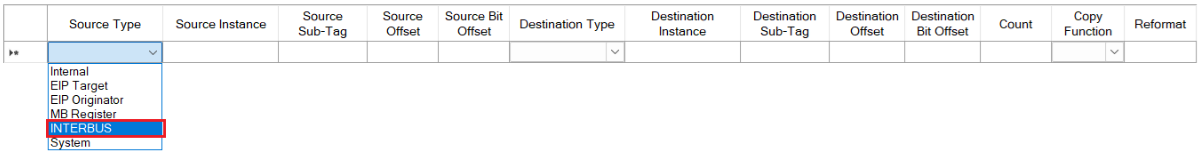


Figure 3.75 – IDS Copy – INTERBUS Source Type

The source instance will be the name of the configured INTERBUS slave. The Source Sub-Tag will be Data.

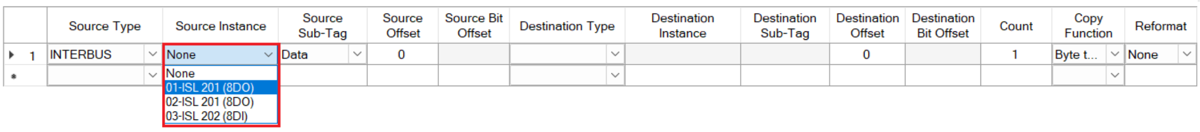


Figure 3.76 – IDS Copy – INTERBUS Source Instance

3.7.1.6. SYSTEM

When copying system information, the source type needs to be System.

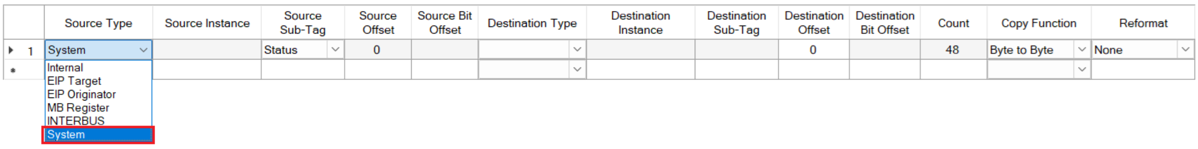


Figure 3.77 – IDS Copy – System Information

The module's System information has the following format.

Parameter	Data Type	Description
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 – Controller in Run Mode. Bit 5 – NTP Ok Bit 6 – INTERBUS Active Bit 7 – INTERBUS Running
INTERBUS Cycle Time	DINT	The INTERBUS Cycle Time in microseconds.
Frame Rx Count	DINT	The number of INTERBUS Frames received.
Frame Update Count	DINT	The number of Frame Updates (Input (Send) data changed)
Checksum Errors	DINT	The number of detected Frame Checksum errors.
Ident Frame Count	DINT	The number of INTERBUS Ident frames received.
Data Frame Count	DINT	The number of INTERBUS Data frames received.
Unknown Command Count	DINT	The number of unknown INTERBUS commands received.
Idle Timeout Count	DINT	The number of INTERBUS timeout occurrences.
Idle State Change Count	DINT	The number of INETRBUS Idle State changes.

Table 3.12 – System Information Format

3.7.2. Copy To

One of five destinations can be selected to copy to:
Internal, EIP Target, EIP Originator, MB Register, and INTERBUS Device.

3.7.2.1. INTERNAL

When copying data to the internal data space (IDS), the destination type needs to be Internal.

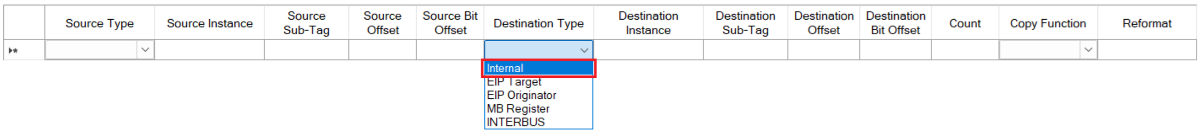


Figure 3.78 – IDS Copy – Internal Source Type

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 5,000 bytes. The Count is the number of **bytes** that will be copied.

3.7.2.2. EIP TARGET

When copying data from the INTERBUS interface to the EtherNet/IP Target input assembly, the destination type needs to be EIP Target.

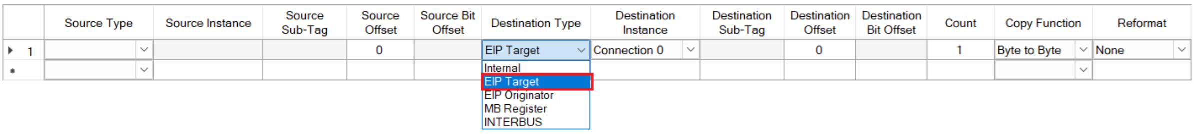


Figure 3.79 – IDS Copy – EtherNet/IP Target Destination Type

The destination instance will be the connection number, which can be connection 0 to 3, 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.

3.7.2.3. EIP ORIGINATOR

When copying data from the INTERBUS interface to an EtherNet/IP IO device **Output** Assembly, the destination type needs to be EIP Originator.

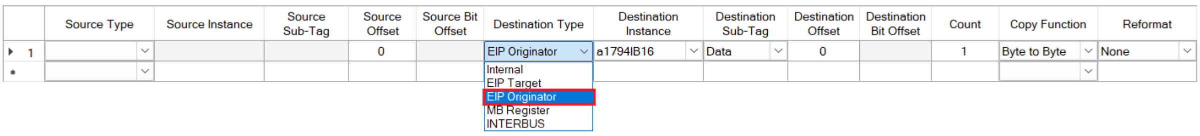


Figure 3.80 – IDS Copy – EtherNet/IP Originator Destination Type

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

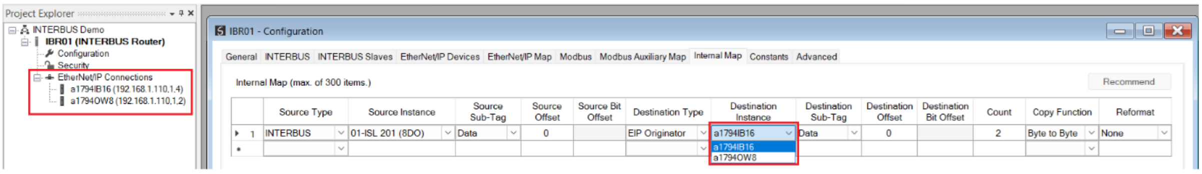


Figure 3.81 – IDS Copy – EtherNet/IP Originator Destination Instance

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.

3.7.2.4. MODBUS REGISTER

When copying data from the INTERBUS interface to a Modbus Register, the destination type needs to be MB Register.

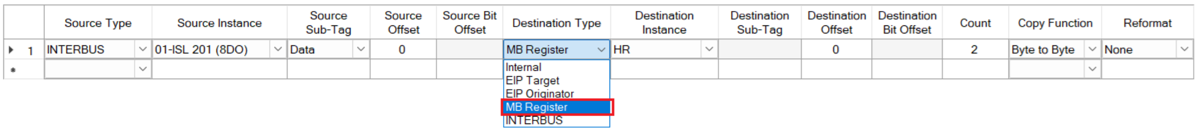


Figure 3.82 – IDS Copy - Modbus Destination Type

The destination instance will be the Modbus register type required.

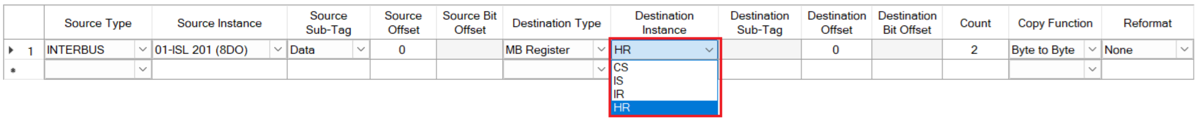


Figure 3.83 – IDS Copy - Modbus Destination Instance

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.

3.7.2.5. INTERBUS

When copying data to a virtual INTERBUS slave, the destination type needs to be INTERBUS.

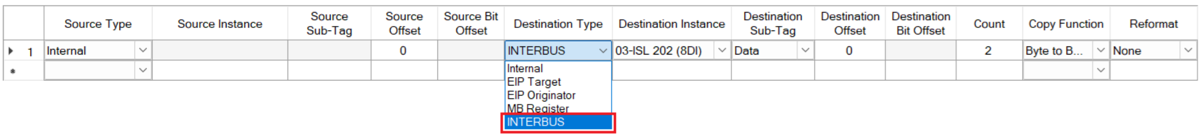


Figure 3.84 – IDS Copy – INTERBUS Destination Type

The destination instance will be the configured name of the INTERBUS virtual slave. The Destination Offset is the offset in the INTERBUS data to where the data must be copied. The Count is the number of **bytes** that will be copied.

NOTE: For more information regarding the specific Internal Map operation for specific interfaces, see the setup and configuration sections for the various INTERBUS and Primary Interfaces.

3.8. 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 INTERBUS slaves, as well as Modbus and EtherNet/IP devices.

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

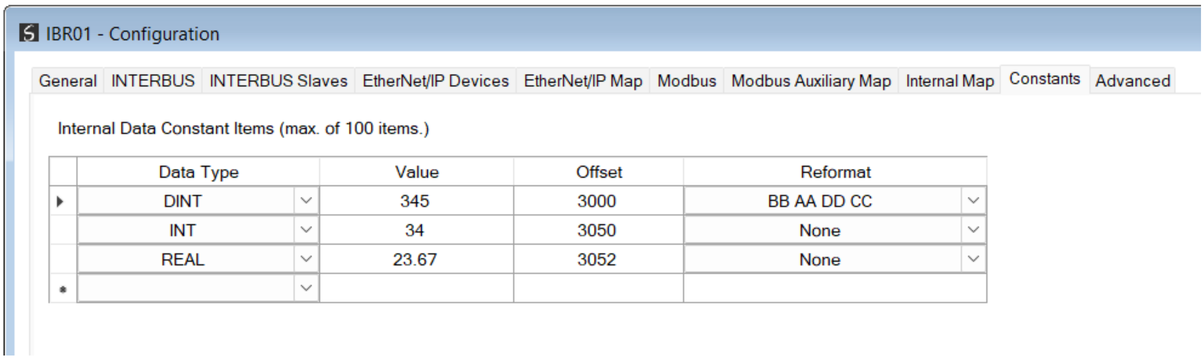


Figure 3.85 – Constants configuration

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 3.13 – Constants configuration parameters

3.9. ADVANCED

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

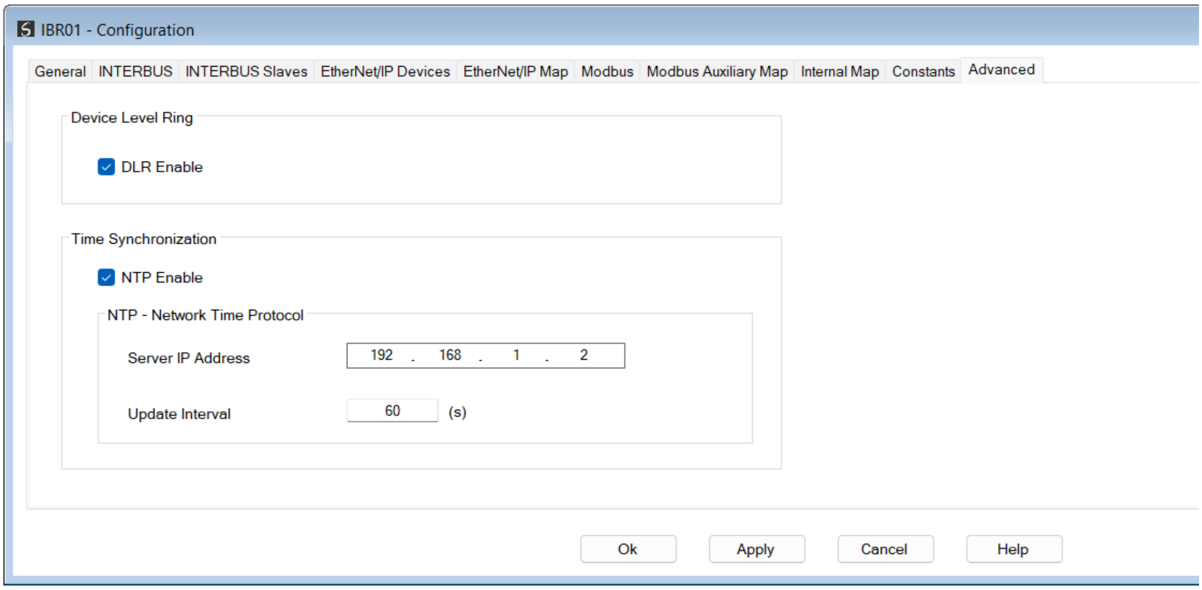


Figure 3.86 – Advanced configuration

The Advanced configuration consists of the following parameters:

Parameter	Description
DLR Enable	Enable the Ethernet Device Level Ring functionality.
NTP Enable	The INTERBUS Router can synchronize its onboard clock to an NTP Server by enabling NTP.

NTP – Server IP Address	This setting is the IP address of the NTP Server which will be used as a time source.
NTP – Update Interval	This setting is the updated interval (in seconds) that the INTERBUS Router will request time from the NTP Server.

Table 3.14 – Advanced configuration parameters

3.10. MODULE DOWNLOAD

Once the INTERBUS Router configuration has been completed, 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 however be modified, if the INTERBUS Router is not on a local network.

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

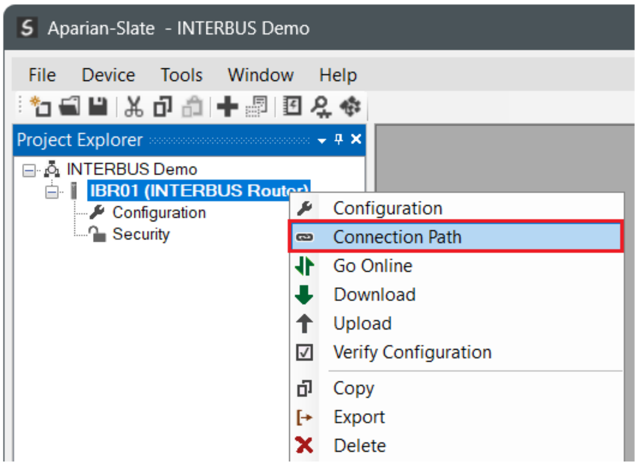


Figure 3.87 - Selecting Connection Path

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

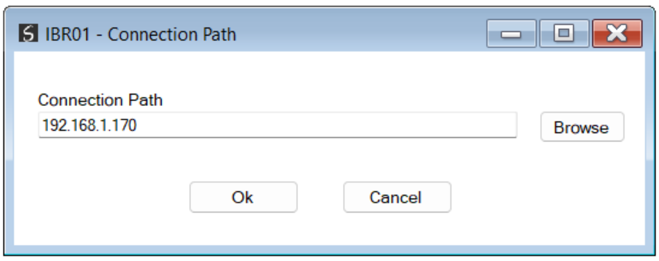


Figure 3.88 - Connection Path

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

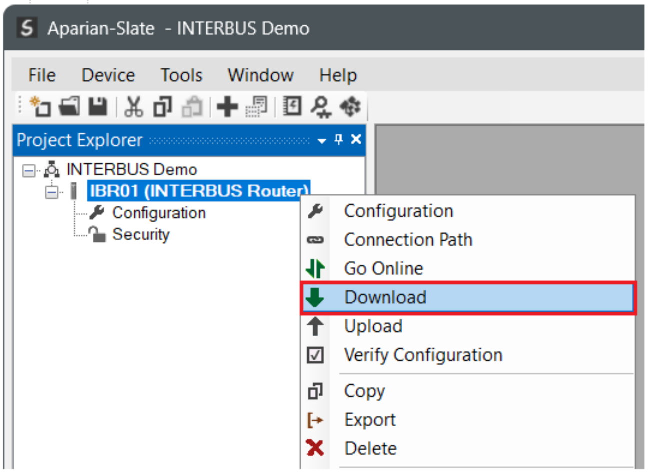


Figure 3.89 - Selecting Download

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

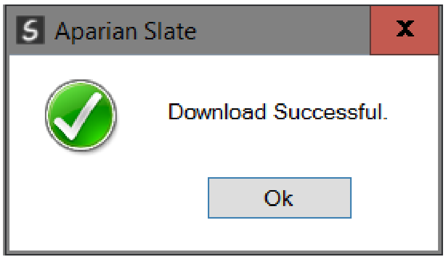


Figure 3.90 - Successful download

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

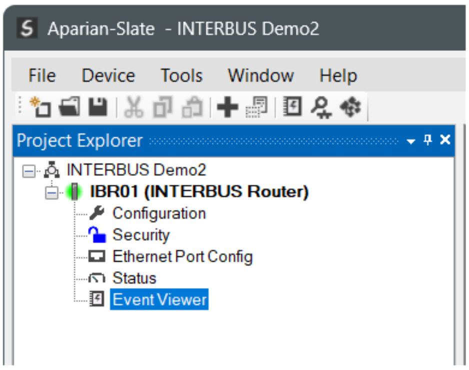


Figure 3.91 - Module online

4. SD CARD

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

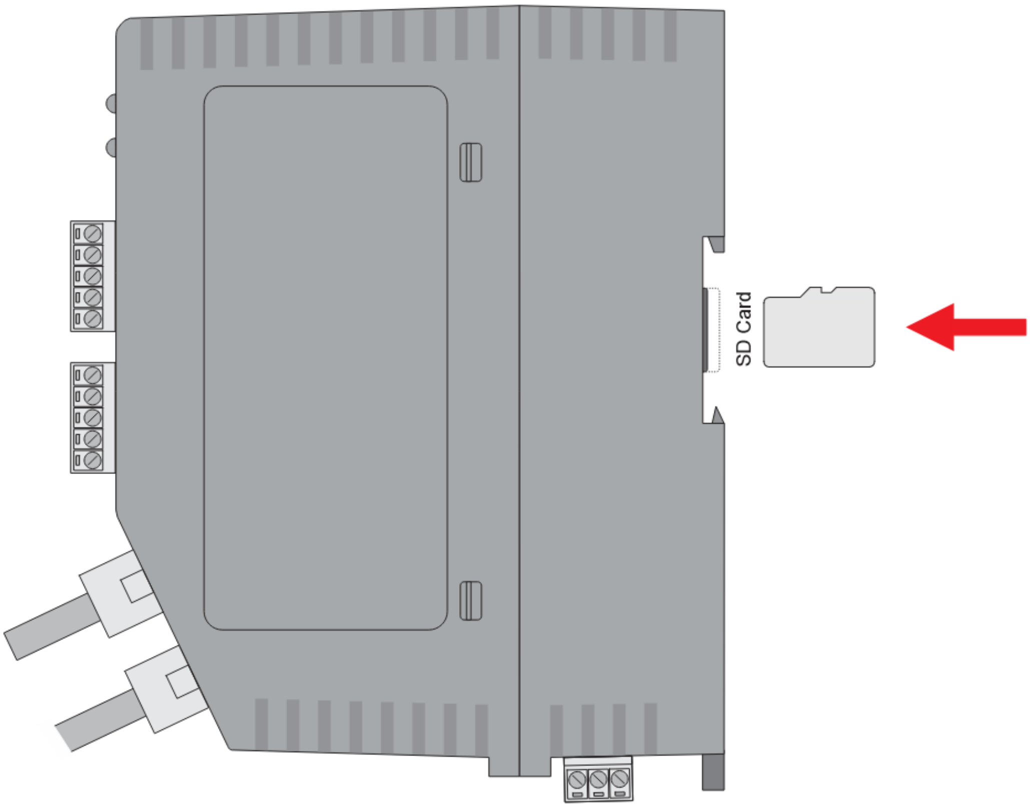


Figure 4.1 – Module Side View – SD Card Slot

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

NOTE: All needed files must be copied into the root directory of the SD Card. The module will not use files which are located in folders.

4.1. FIRMWARE

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

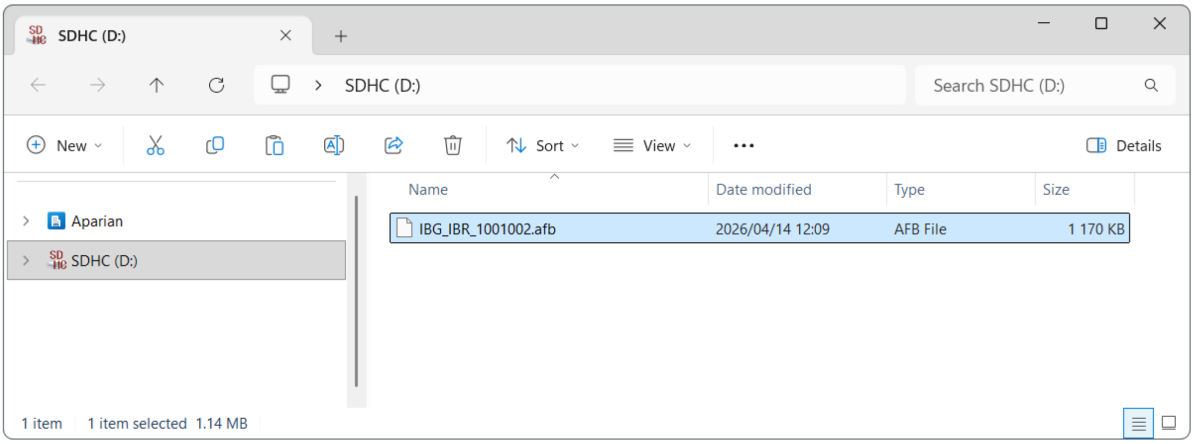


Figure 4.2 – SD Card – Firmware file

NOTE: The filename of the firmware file must not be changed. The specific module will use only the firmware that is valid (e.g. the INTERBUS Router will only use the "IBG_IBR_xxxxxxx.afb" firmware file).

NOTE: 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 with the firmware file on 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 yes, the firmware will either be upgraded or downgraded to the firmware revision on the SD Card.

4.2. NETWORK PARAMETERS

When the SD Card has been inserted into the module and the user is online with the module in Slate, then the user has the option to directly upload the network parameters (e.g., IP Address, Subnet Mask, etc.) on to the SD Card using the *Save Network Parameters to SD Card* option. This will copy the module's current network parameters to the SD Card.

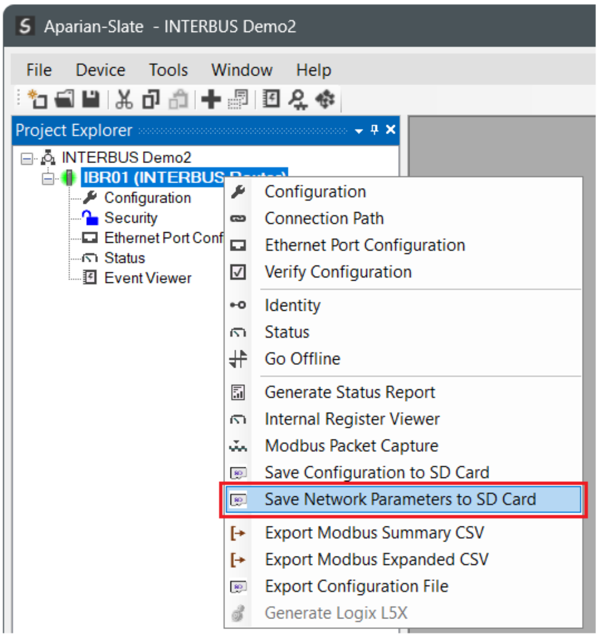


Figure 4.3 – SD Card – Network Parameters

When the module powers up with an SD Card inserted and there exist network parameters saved onto the SD Card, it will update the existing network parameters if they are different.

4.3. CONFIGURATION

If a module needs to be replaced, the user can insert the SD Card (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 user can add the Slate configuration file to the SD Card root directory in one of two ways.

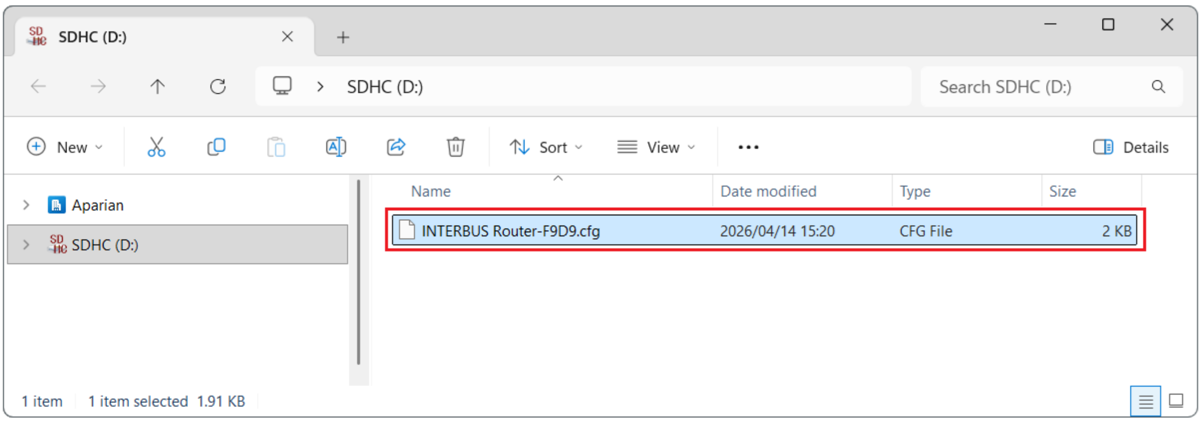


Figure 4.4 – SD Card – Configuration file

4.3.1. Manual Copy

Once the user has created the application configuration in the Slate, 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.

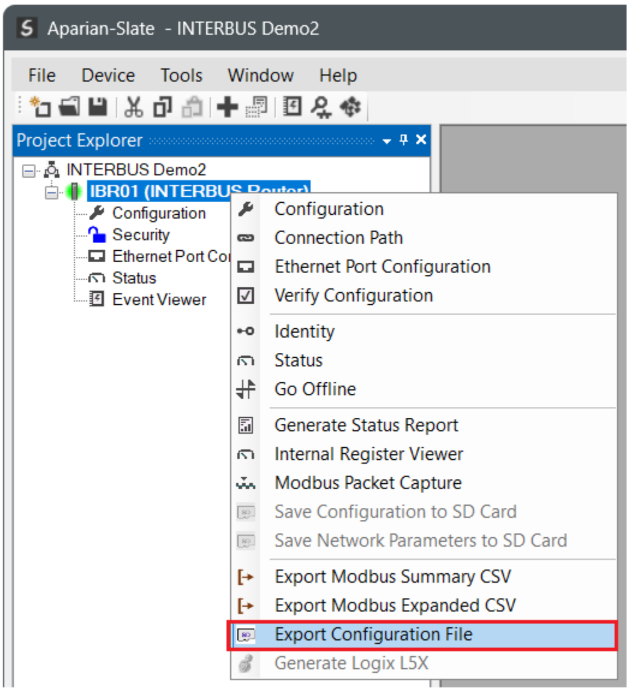


Figure 4.5 – Configuration Export for SD Card

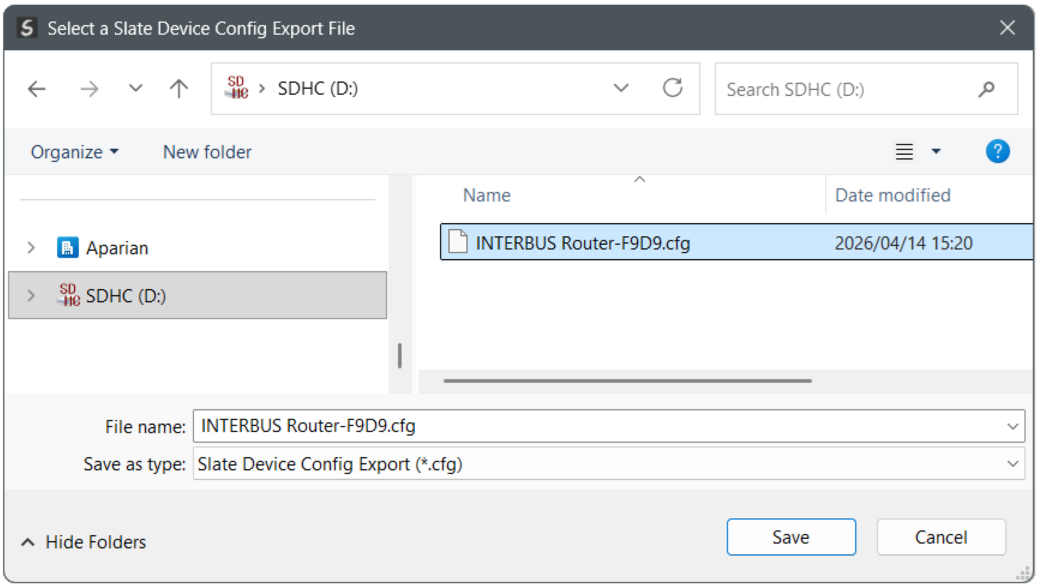


Figure 4.6 – Configuration Export for SD Card

NOTE: The filename of the configuration file must **not** be changed. The specific module will use only the configuration that is valid (e.g. the INTERBUS Router will only use the INTERBUS configuration file).

NOTE: 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.

4.3.2. Slate Triggered Upload

When the SD Card has been inserted into the module and the user is online with the module in Slate, 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.

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

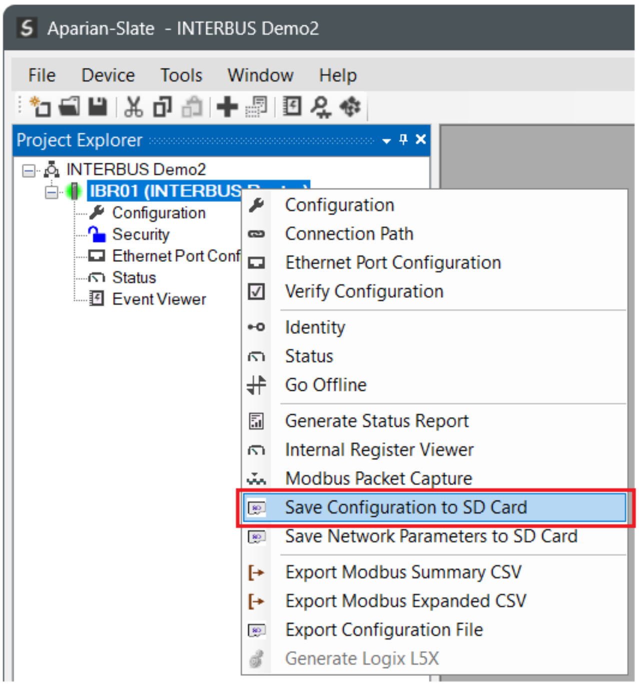


Figure 4.7 – Save Configuration to SD Card

5. DEVICE FIRMWARE UPDATE

The INTERBUS Router module supports in-field firmware upgrading. The latest firmware for the module can be downloaded from the Aparian website ***www.aparian.com***. The firmware is digitally signed, so only the correct firmware can be used.

To firmware upgrade the module, follow the steps below:

- From the ***Tools*** menu in Slate, select the ***DeviceFlash*** utility.

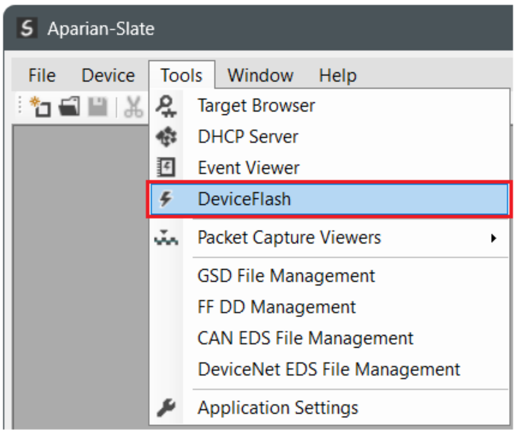


Figure 5.1 – Select DeviceFlash utility from Slate

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

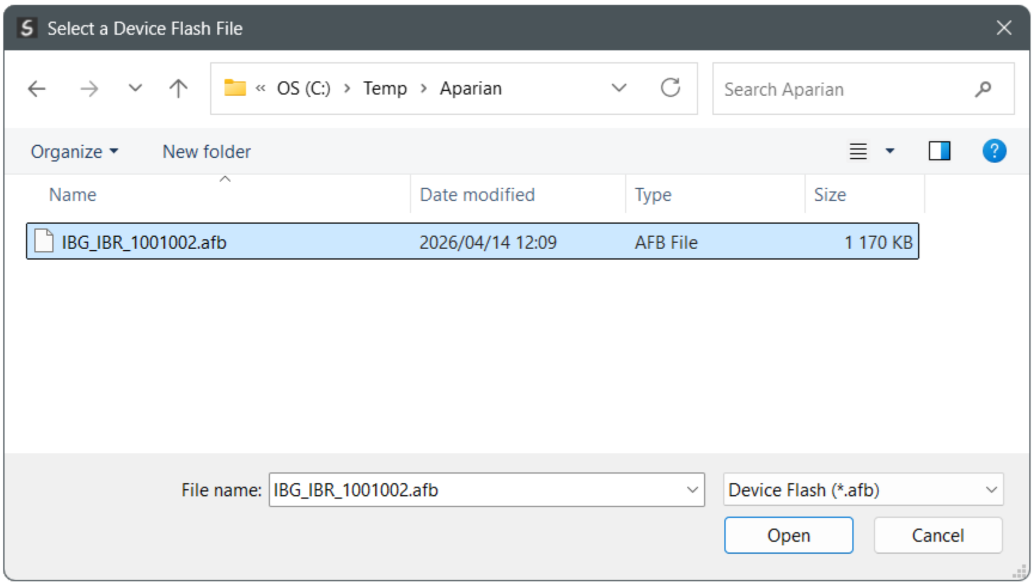


Figure 5.2 – Select the binary file

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

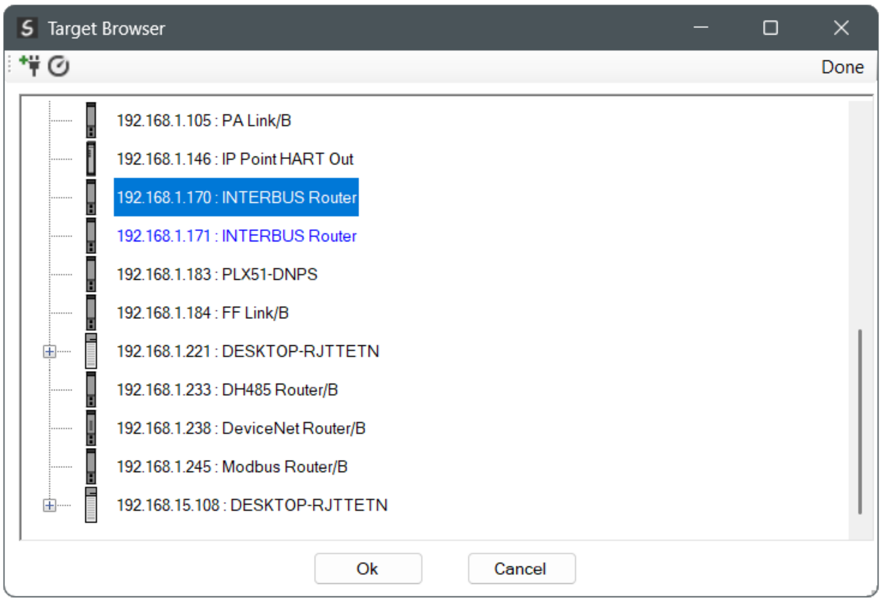


Figure 5.3 – Select the device to be updated

- After the device selection, the user will be prompted to start the device flash process. The firmware update will take less than 2 minutes to complete.

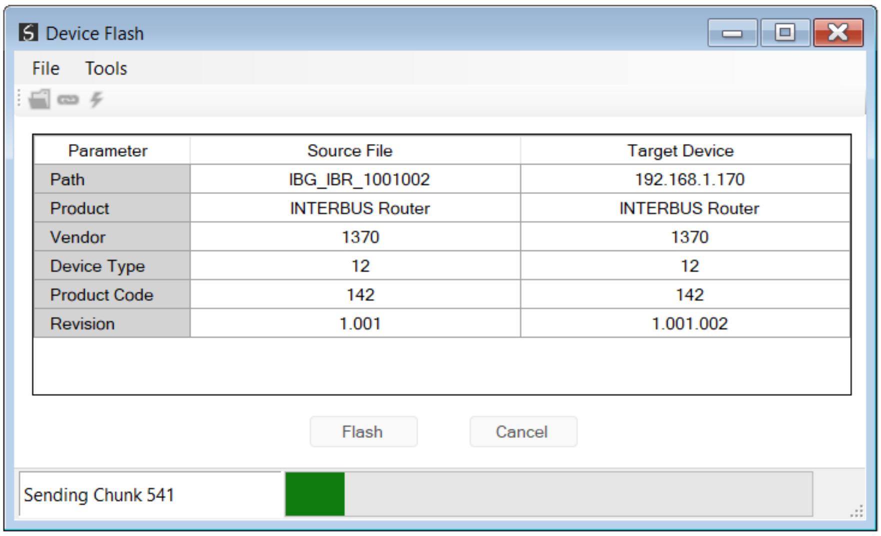


Figure 5.4 – Firmware update busy

- Once the firmware update has successfully completed, the Target Device textboxes will display green.

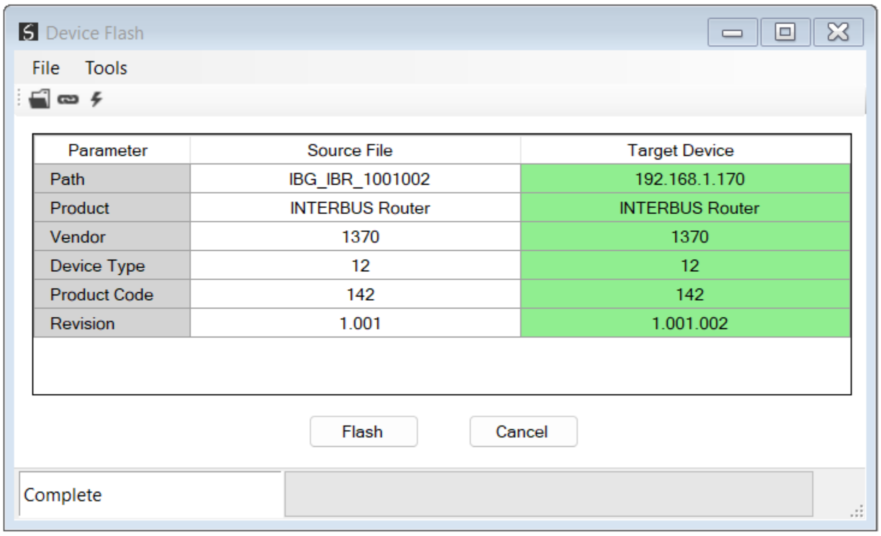


Figure 5.5 – Firmware update successfully completed

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

6. SECURITY

The INTERBUS ROUTER supports security services allowing the user to configure various levels of module security.

When security is enabled all EtherNet/IP communication between Slate 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 aforementioned fixed roles.

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

Associated privileges for each user role, is tabulated below:

Privileges / Roles	**Administrator**	**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:

- Setup 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.

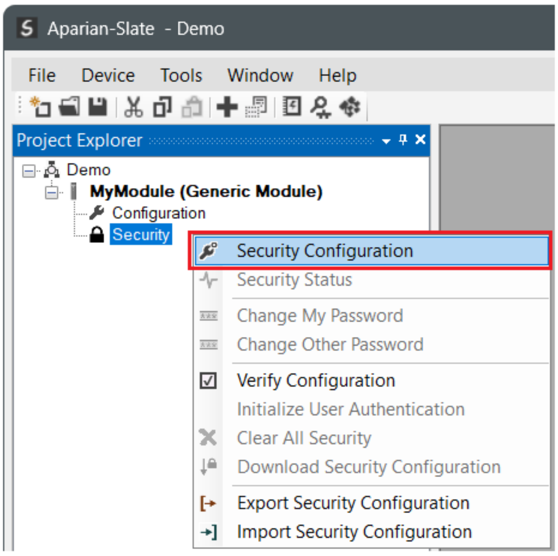


Figure 6.1 – Selecting Security Configuration

The configuration form will open and display multiple configuration tabs.

6.1.1.1. GENERAL CONFIGURATION

The ***General*** configuration tab is shown below.

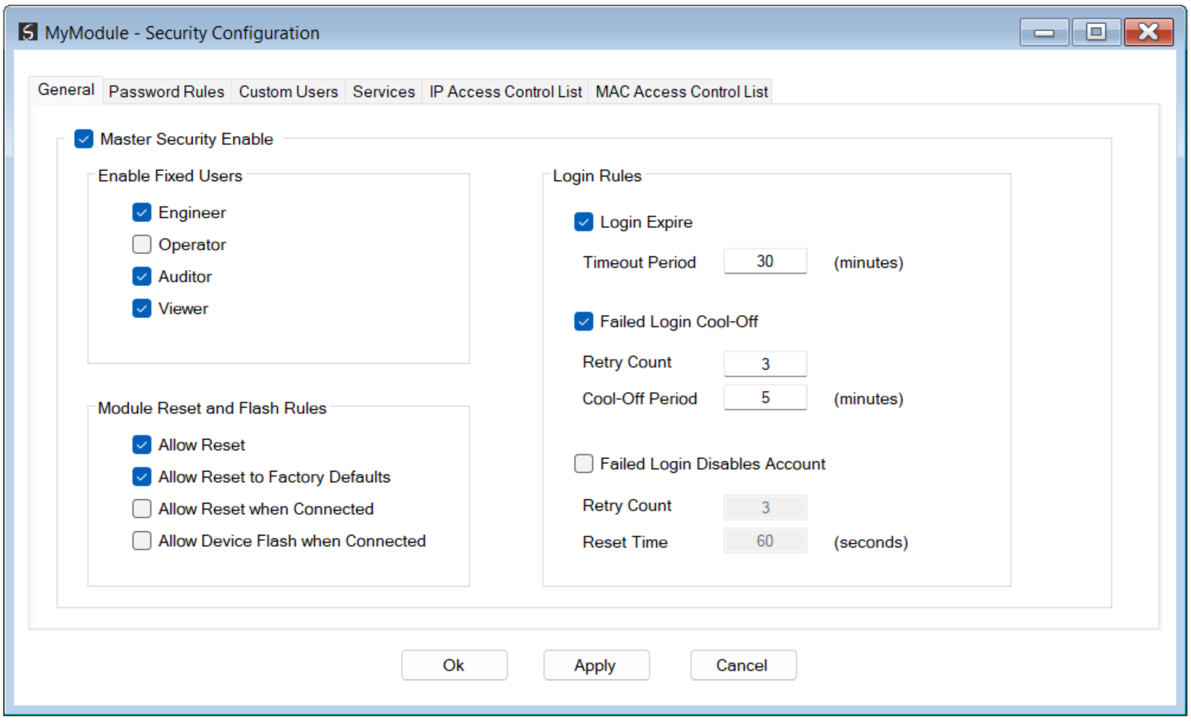


Figure 6.2 – Security Configuration – General

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 the Retry Count 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 Retry Count	The number of retries before the Login Cool-Off period is applied.
Failed Login Cool-Off Period	The Cool-Off duration, in minutes. Once a user has entered an incorrect password the Retry Count times in succession, they would need to wait 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 the Retry Count times in succession before the Reset Time has expired. **NOTE**: Once the user's account has been disabled, an Administrator would need to reset their password. **NOTE**: This option will not be applicable for the Administrator user account.
Failed Login Disables Account Retry Count	The number of retries while the Reset Time is active before the user's account is disabled.
Failed Login Disables Account Reset Time	The Reset Time duration, in seconds. Once a user has entered an incorrect password, the Disable Account Reset Time will be applied and starts counting down to zero. If the user enters the incorrect Password the Retry Count times before the Reset Time has expired, the user's account will be disabled. Once the Reset Time has expired (gone back to zero), then the login process can be restarted. Min: 1 second. Max: 65000 seconds (18 hours)

Table 6.2 – Security Configuration – General

6.1.1.2. PASSWORD RULE CONFIGURATION

The ***Password Rules*** tab is shown below.

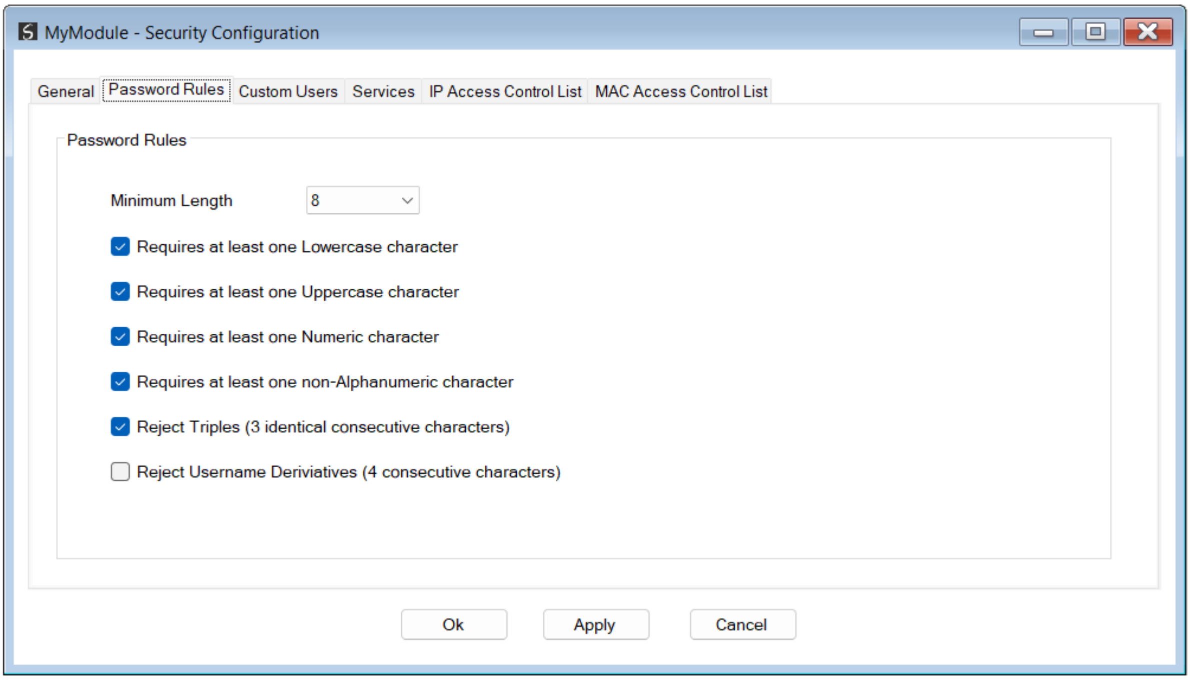


Figure 6.3 – Security Configuration – Password Rules

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.

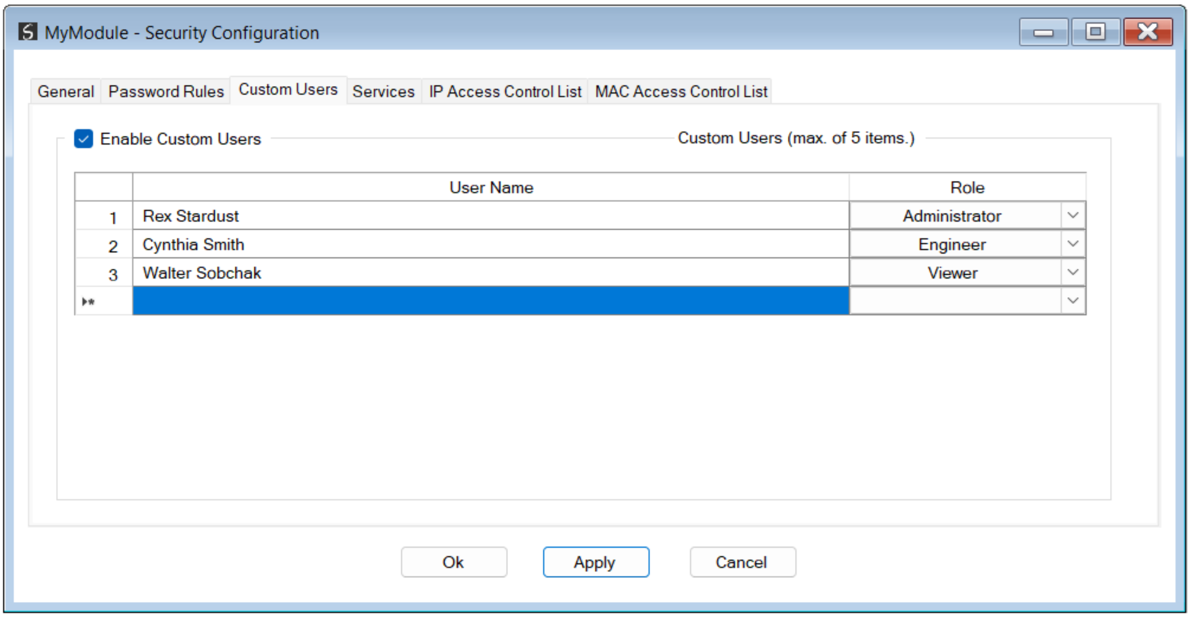


Figure 6.4 – Security Configuration – Custom Users

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.

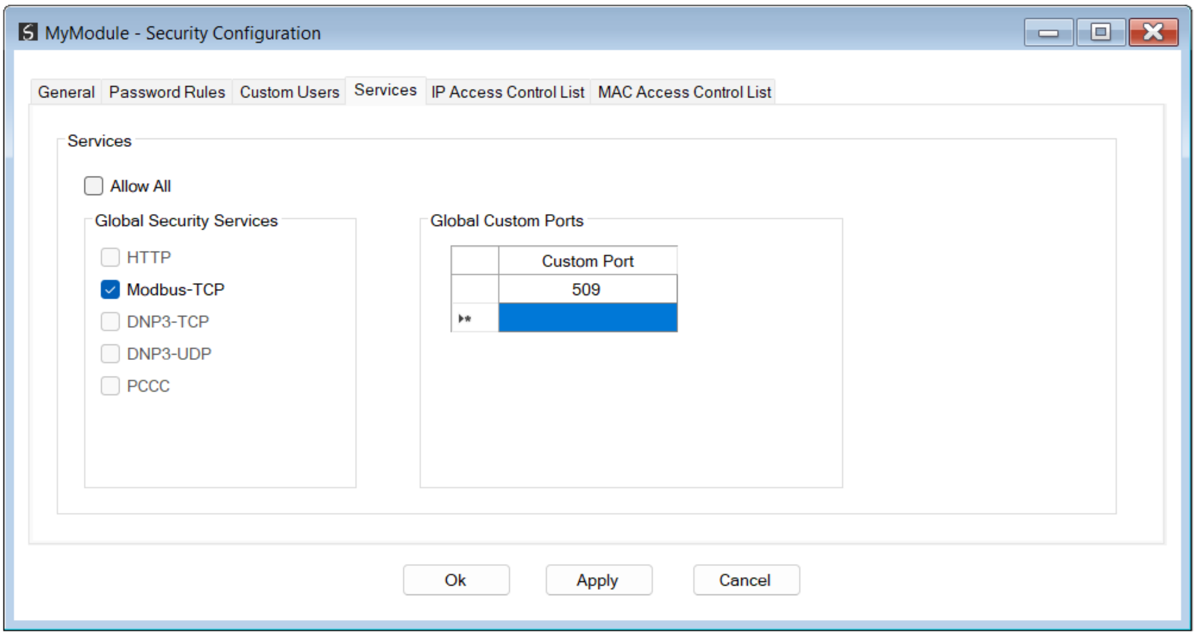


Figure 6.5 – Security Configuration – Services

The ***Services*** configuration tab comprises the following parameters:

Parameter	Description
Allow All	When selected all services are allowed by default.
HTTP	Allow HTTP web server connections to be accepted.
Modbus-TCP	Allow Modbus-TCP connections to be accepted.
DNP3-TCP	Allow DNP3 TCP connections to be accepted.
DNP3-UDP	Allow DNP3 UDP connections to be accepted.
PCCC	Allow PCCC 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. Modus-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.

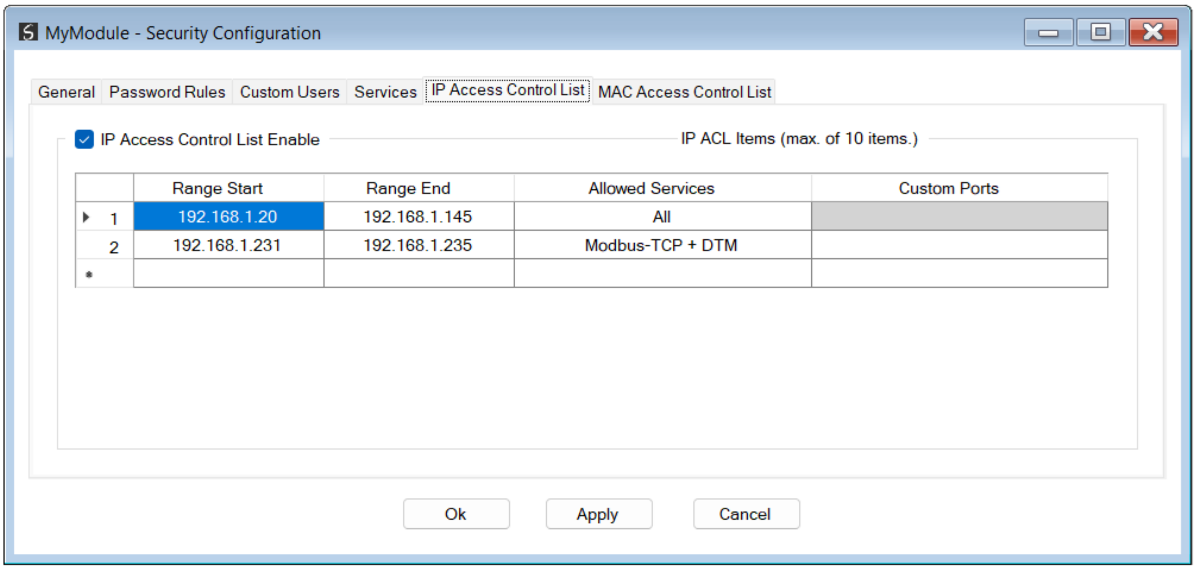


Figure 6.6 – Security Configuration – IP Access Control List

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.

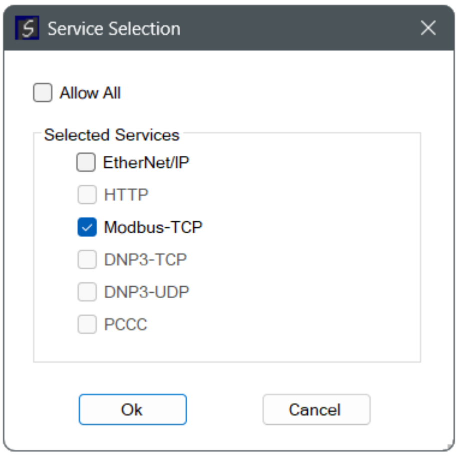


Figure 6.7 – Security Configuration – Service Selection

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.

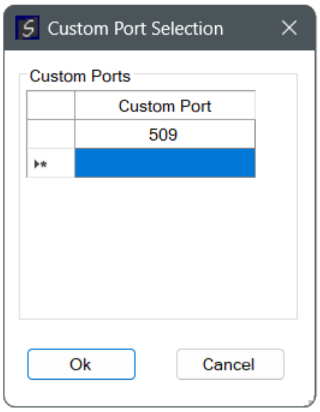


Figure 6.8 – Security Configuration – Custom Ports

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

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

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

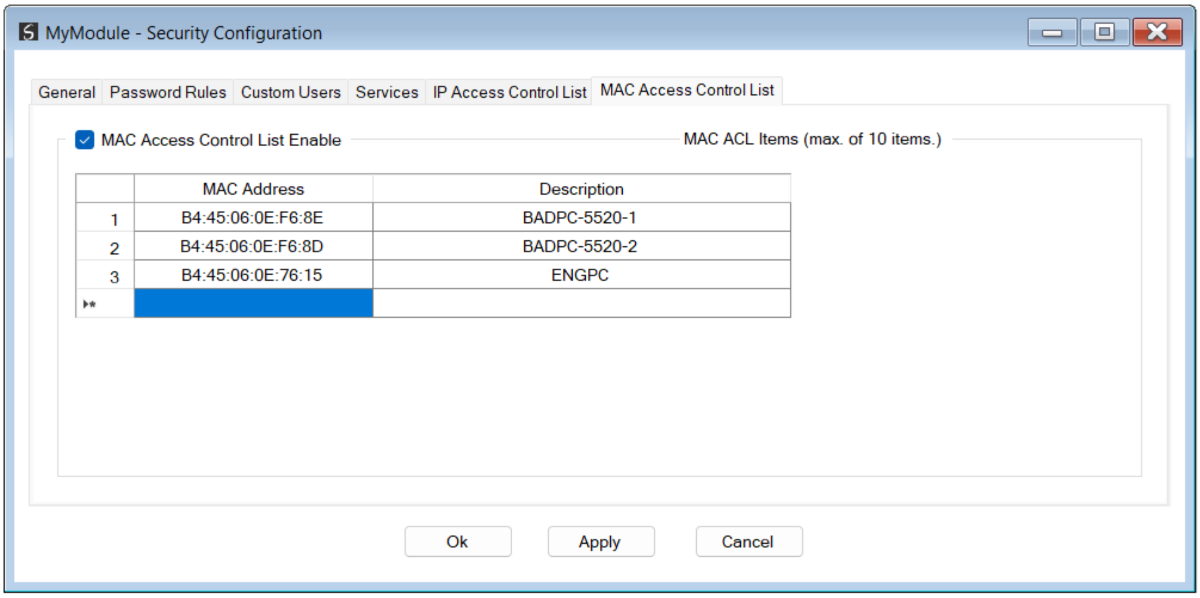


Figure 6.9 – Security Configuration – MAC Access Control List

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.

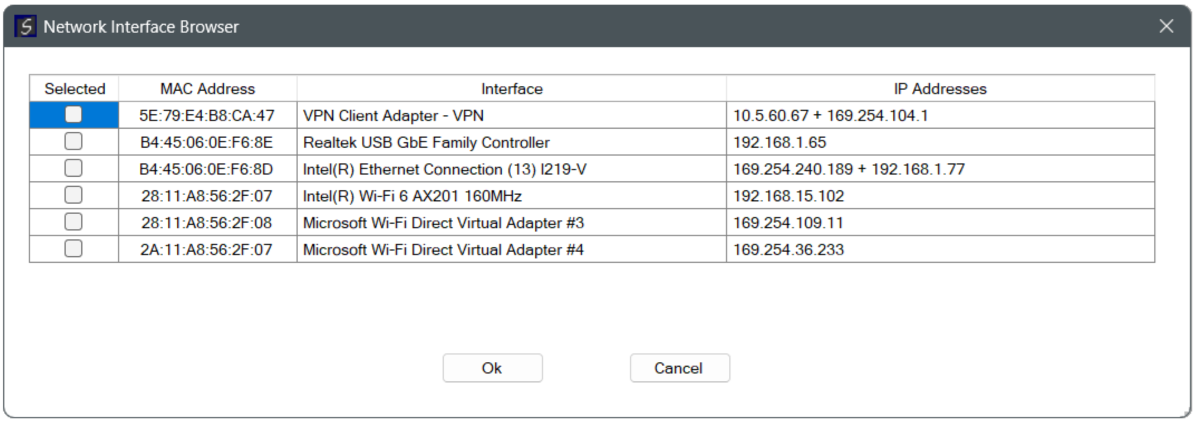


Figure 6.10 – Security Configuration – Network Interface Browser

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.

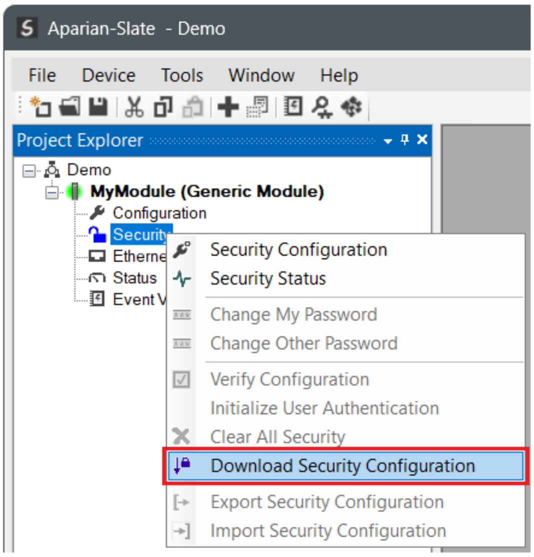


Figure 6.11 – Download Security Configuration

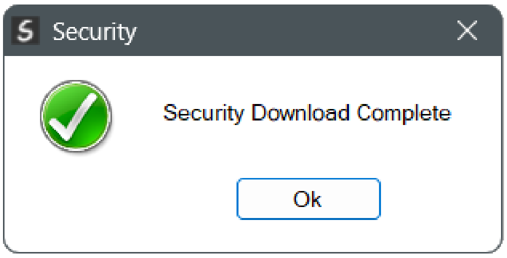


Figure 6.12 – Download Security Configuration Complete

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.

To commence with this step, right-click on the Security node in the project tree and select the ***Initialize User Authentication*** option.

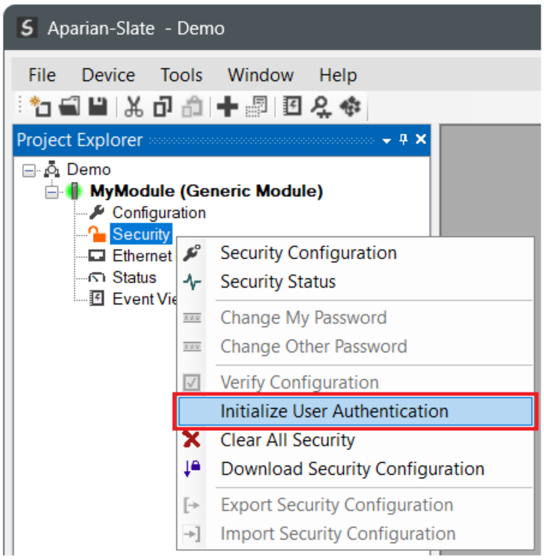


Figure 6.13 – Initialize User Authentication

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

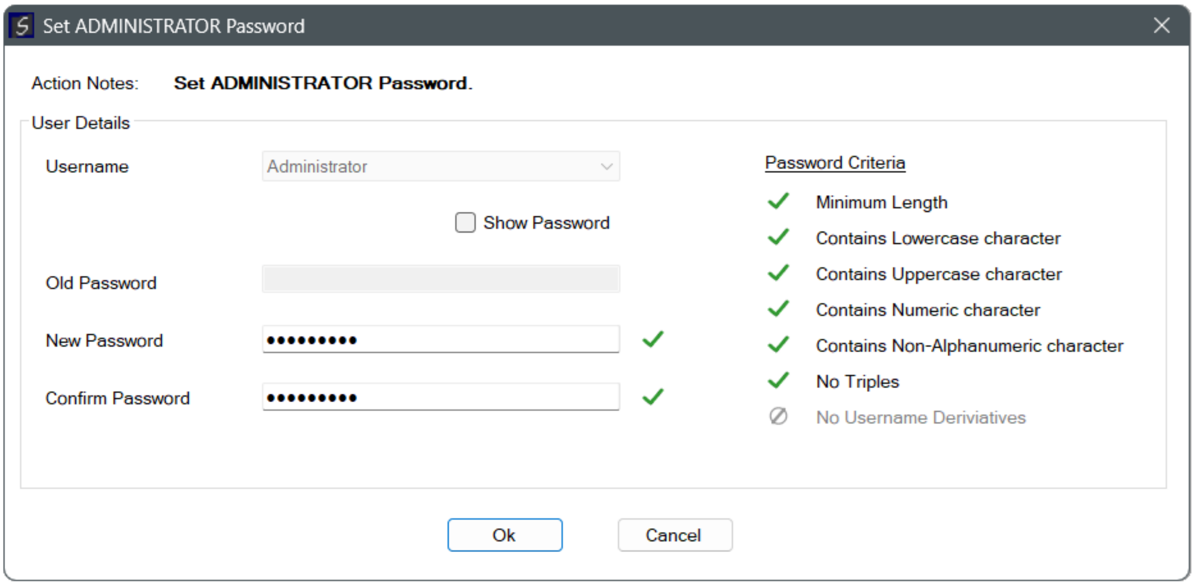


Figure 6.14 – Set Administrator Password.

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.

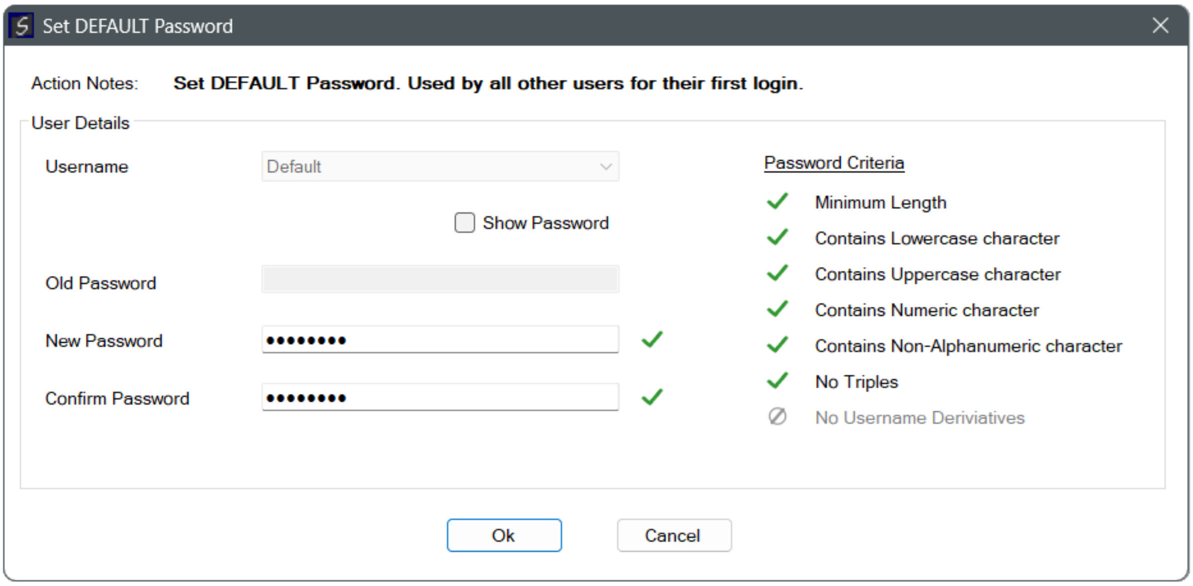


Figure 6.15 – Set Default Password.

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.

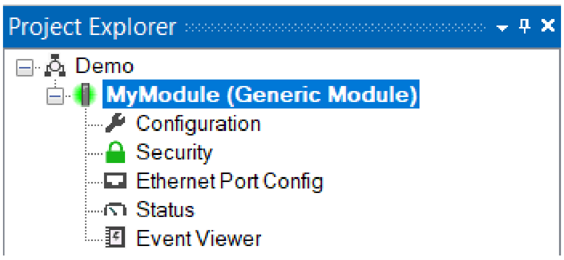


Figure 6.16 – Secured Module

6.2. OPERATION

To interact with a secured, and user initialized module, each user will need to first login.

6.2.1. Initial User Login

Similar, to an unsecured module, a user would open the existing Slate project, right-click on the module, and select ***Go Online***.

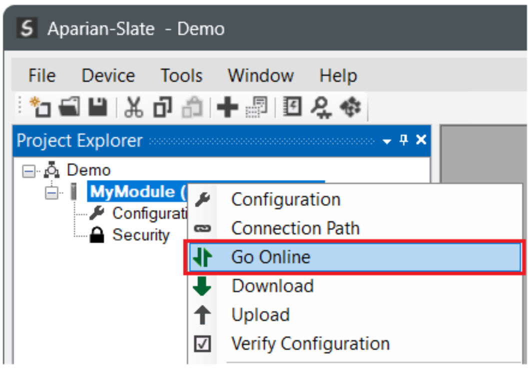


Figure 6.17 – Go Online

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

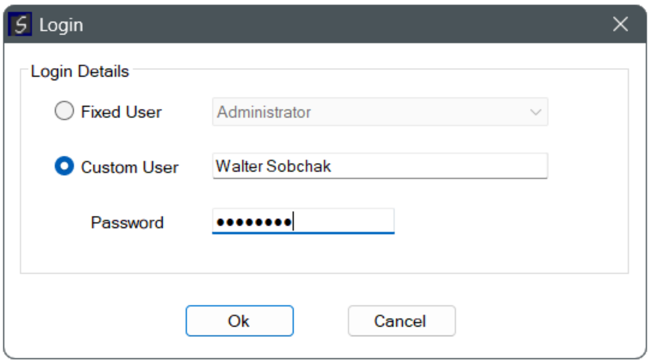


Figure 6.18 – Custom User Login

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.

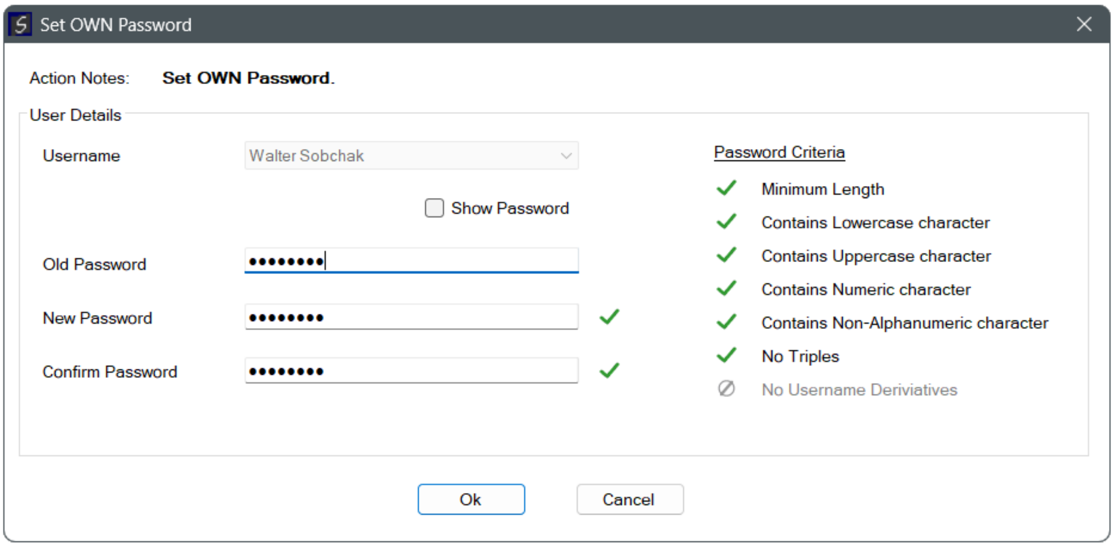


Figure 6.19 – Change Own Password

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.

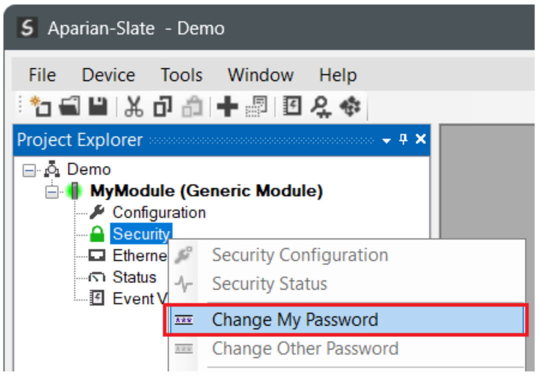


Figure 6.20 – Select Change My Password

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.

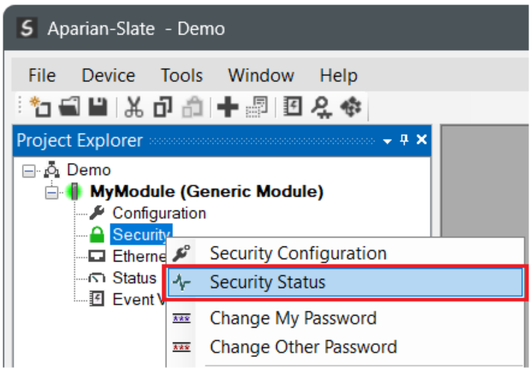


Figure 6.21 – Select Security Status

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

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

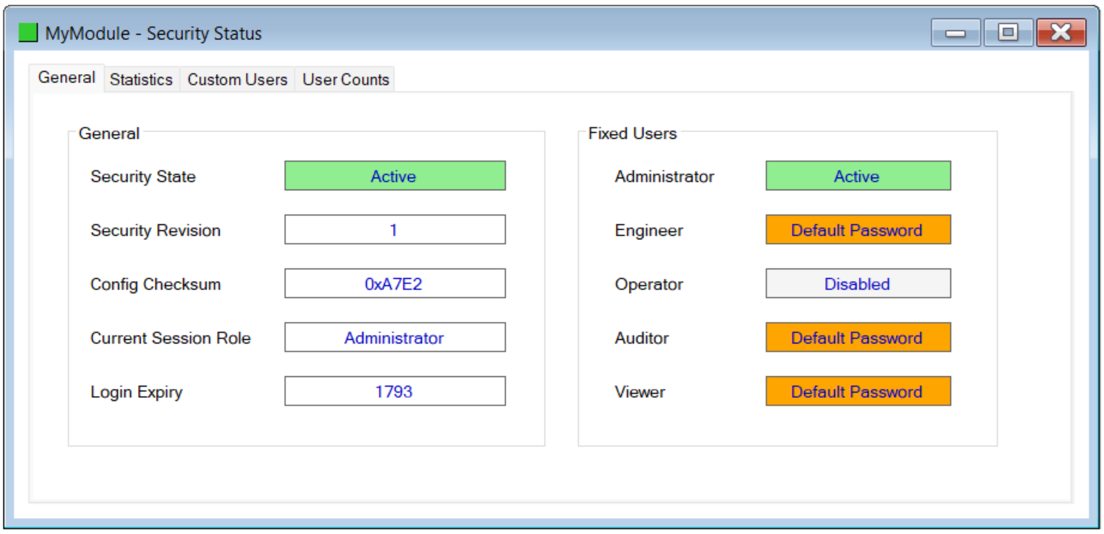


Figure 6.22 – Security Status – General

The General status tab displays the following:

Parameter	**Description**
General	
Security State	The current 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 a number of security service statistics.

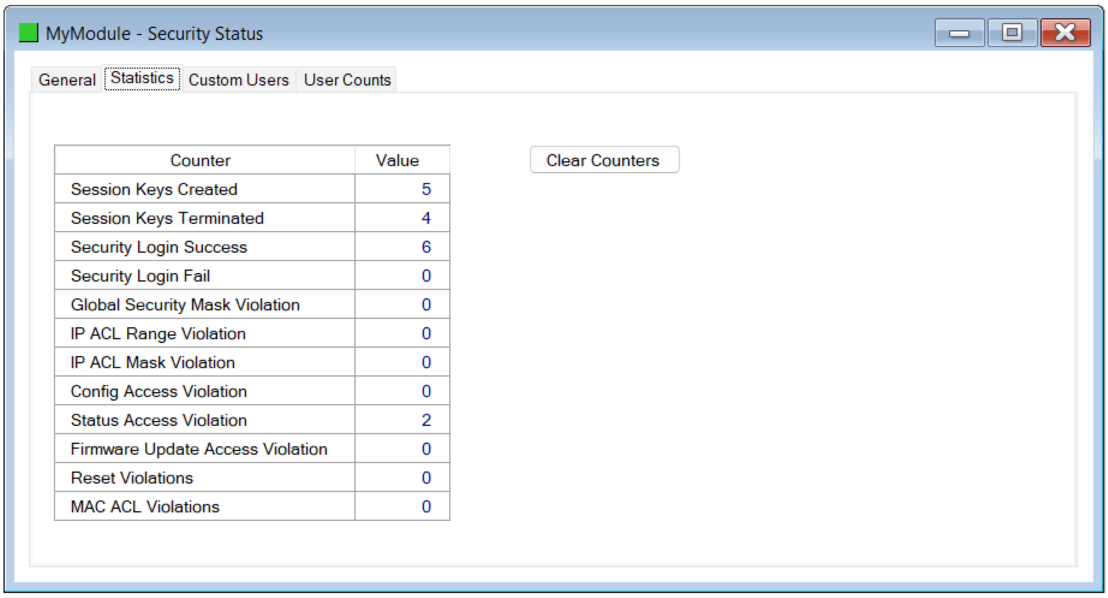


Figure 6.23 – Security Status – Statistics

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) was made.
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) was made.
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:

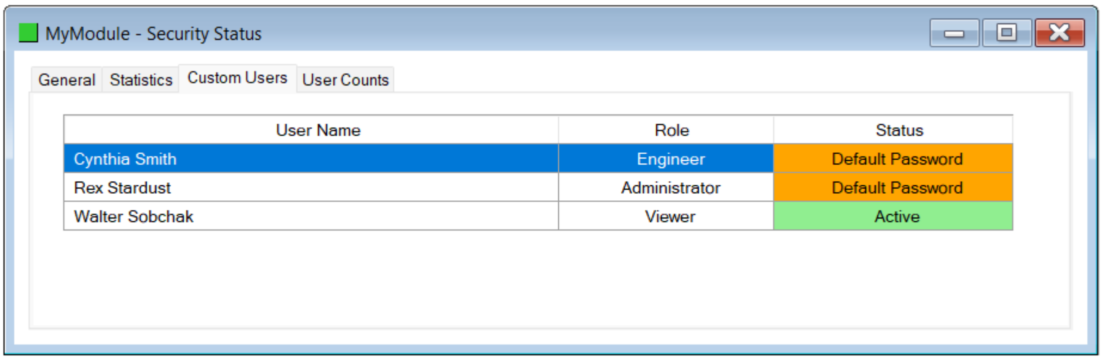
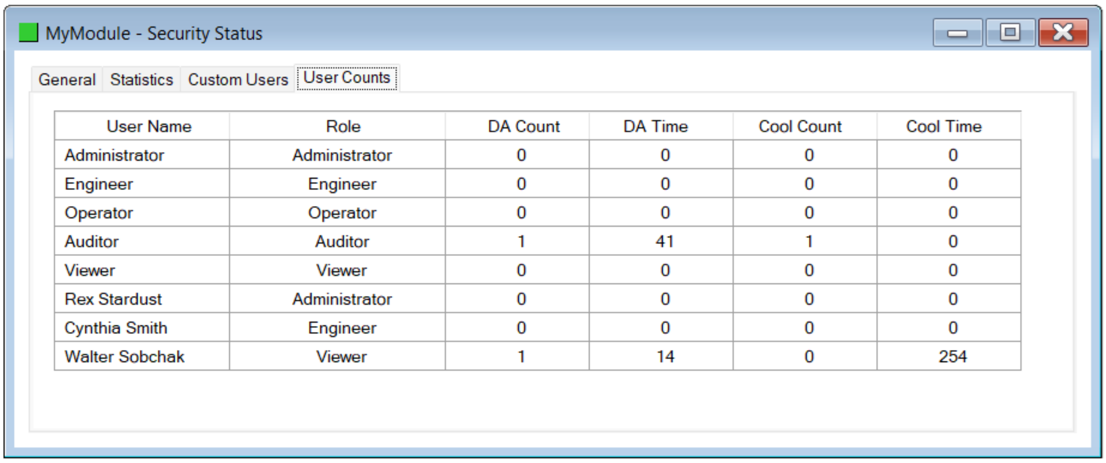


Figure 6.24 – Security Status – Custom Users

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 – Custom Users

The User Counts status tab displays the following:



User Name	Role	DA Count	DA Time	Cool Count	Cool Time
Administrator	Administrator	0	0	0	0
Engineer	Engineer	0	0	0	0
Operator	Operator	0	0	0	0
Auditor	Auditor	1	41	1	0
Viewer	Viewer	0	0	0	0
Rex Stardust	Administrator	0	0	0	0
Cynthia Smith	Engineer	0	0	0	0
Walter Sobchak	Viewer	1	14	0	254

Figure 6.25 – Security Status – User Counts

The following statistics are displayed for each user:

Parameter	Description
User Name	The configured user name.
Role	The configured role for this specific user.
DA Count	The number of failed login occurrences with respect to Disabling the account.

DA Time	The time (seconds) since the last failed login occurrence with respect to Disabling the account.
Cool Count	The number of failed login occurrences with respect to account Cool Down period.
Cool Time	The time (seconds) remaining for the account cool down period.

Table 6.13 – Security Status – User Count

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.

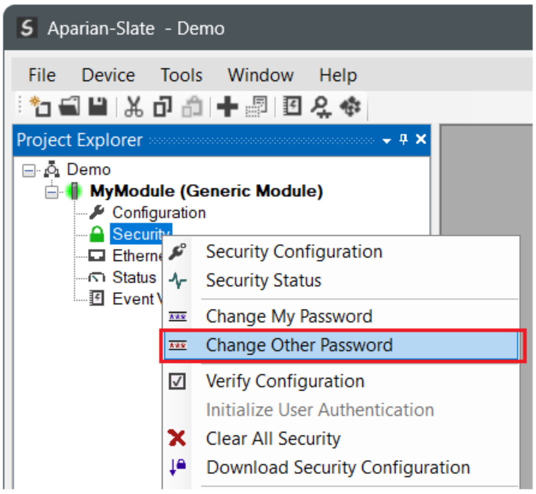


Figure 6.26 – Select Change Other Password.

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 forces that user to change the password the next time they login.

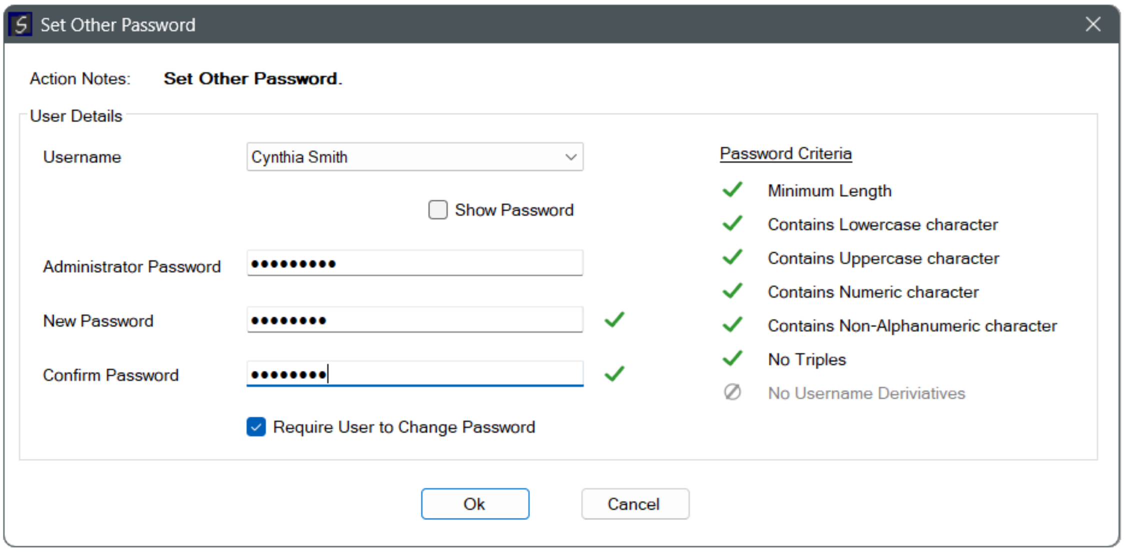


Figure 6.27 – Set Other Password

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.

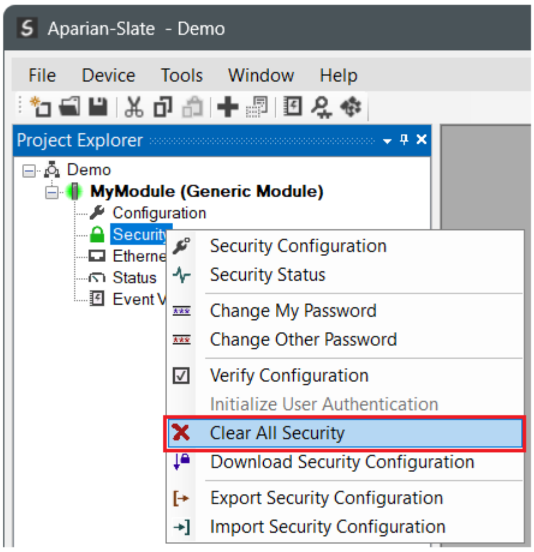


Figure 6.28 – Select Clear All Security.

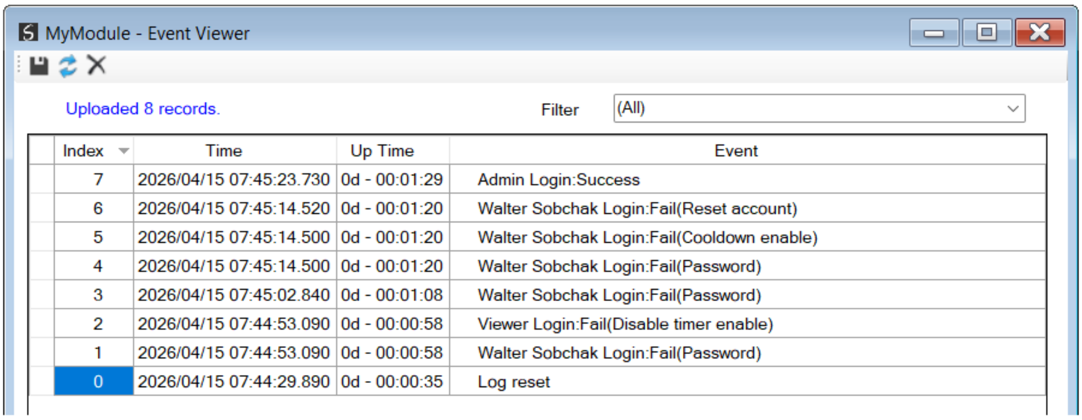
This action will require the Administrator to enter their password. The security configuration and all passwords will be removed with this action.

NOTE: 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.



Index	Time	Up Time	Event
7	2026/04/15 07:45:23.730	0d - 00:01:29	Admin Login:Success
6	2026/04/15 07:45:14.520	0d - 00:01:20	Walter Sobchak Login:Fail(Reset account)
5	2026/04/15 07:45:14.500	0d - 00:01:20	Walter Sobchak Login:Fail(Cooldown enable)
4	2026/04/15 07:45:14.500	0d - 00:01:20	Walter Sobchak Login:Fail(Password)
3	2026/04/15 07:45:02.840	0d - 00:01:08	Walter Sobchak Login:Fail(Password)
2	2026/04/15 07:44:53.090	0d - 00:00:58	Viewer Login:Fail(Disable timer enable)
1	2026/04/15 07:44:53.090	0d - 00:00:58	Walter Sobchak Login:Fail(Password)
0	2026/04/15 07:44:29.890	0d - 00:00:35	Log reset

Figure 6.29 – Event Log

6.4. RESET SECURITY CONFIGURATION

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

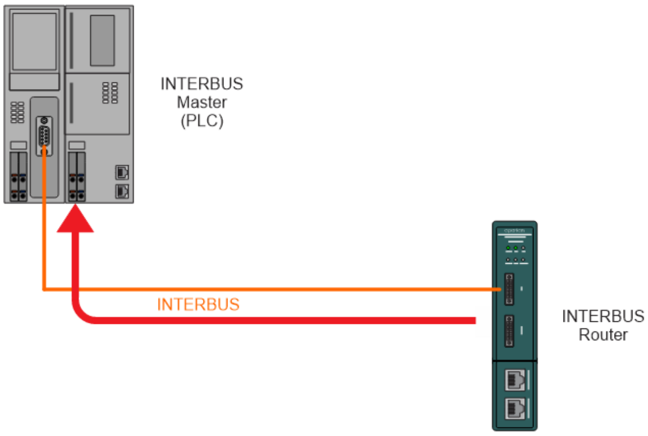
NOTE: This process will remove all module application configuration and security configuration including all passwords.

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. OPERATION

7.1. INTERBUS

The INTERBUS Router operates as multiple (1..15) virtual INTERBUS slaves. These slaves can be input, output or input and output devices. When a virtual INTERBUS slave is configured as an Input device, it will be Sending data on the INTERBUS network.

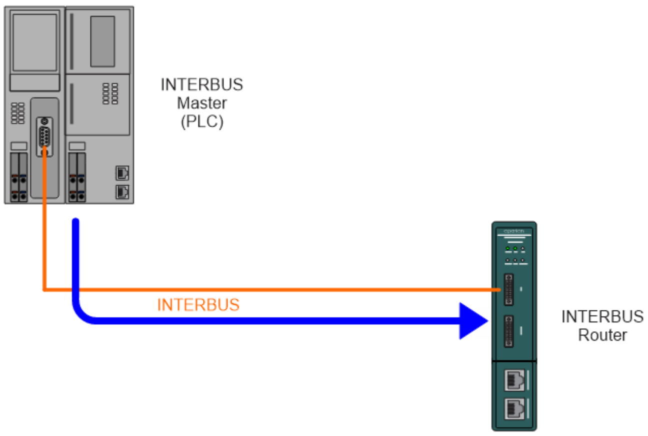


INTERBUS Devices (max. of 15 items.)

	Description	Device Class	Device Type	Data Direction	Data Width	Device Code
1	ISL 202 (8DI)	0 - Digital Remote Bus Device	2	Input	2 bytes	0x010A

Figure 7.1 – INTERBUS Input – Send Data

When a virtual INTERBUS slave is configured as an Output device, it will be Receiving data on the INTERBUS network.



INTERBUS Devices (max. of 15 items.)

	Description	Device Class	Device Type	Data Direction	Data Width	Device Code
1	ISL 202 (8DI)	0 - Digital Remote Bus Device	2	Input	2 bytes	0x010A
2	ISL 201 (8DO)	0 - Digital Remote Bus Device	2	Output	2 bytes	0x0109

Figure 7.2 – INTERBUS Output – Receive Data

7.2. ETHERNET/IP TARGET

A controller (e.g. Logix controller) can own the INTERBUS Router over EtherNet/IP using up to 4 Class 1 EtherNet/IP connections when the INTERBUS Router is operating as an EtherNet/IP target. This will allow the INTERBUS Router to exchange data with the controller using the input and output assembly of the Class 1 EtherNet/IP connection.

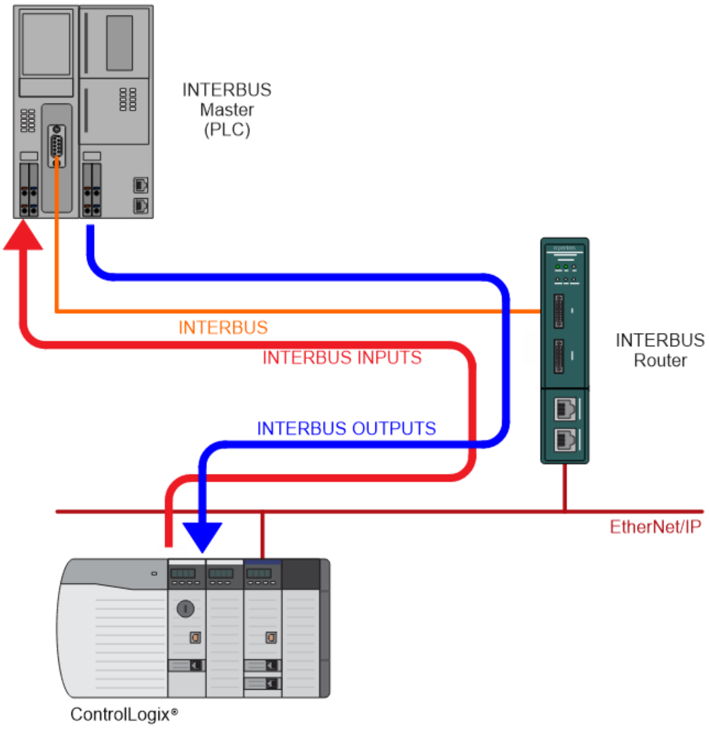


Figure 7.3 – INTERBUS – EtherNet/IP Target

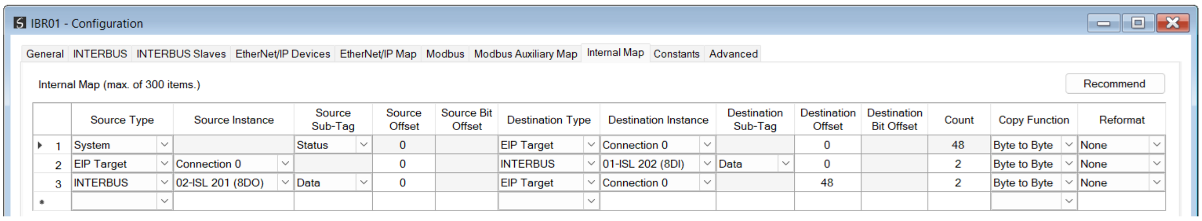
NOTE: When using EtherNet/IP Target, it is recommended to use the ***Recommend*** button in the Internal Map configuration. This will automatically map and reformat all the required data in the Internal Map.

7.2.1. Class 1 Assembly Mapping

When the module operates in a Logix "owned" mode the Logix controller will establish a class 1 cyclic communication connection to the INTERBUS Router. Up to four input and output assemblies are exchanged at a fixed 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 Slate) will copy this data to the input and output assemblies.

Once the generate 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 INTERBUS Router.



	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count	Copy Function	Reformat
1	System		Status	0		EIP Target	Connection 0		0		48	Byte to Byte	None
2	EIP Target	Connection 0		0		INTERBUS	01-ISL 202 (8DI)	Data	0		2	Byte to Byte	None
3	INTERBUS	02-ISL 201 (8DO)	Data	0		EIP Target	Connection 0		48		2	Byte to Byte	None
*													

Figure 7.4 – Internal Map – EtherNet/IP Target

The Output tag (example “IBR01Out”) will typically include all the virtual Input INTERBUS slaves’ data.

Name	Value	Style	Data Type	Description
IBR01Out	{...}		IBR01Out17E4	
IBR01Out.S01_ISL2028DI	{...}	Hex	SINT[2]	ISL 202 (8DI) Input Data
IBR01Out.S01_ISL2028DI[0]	16#00	Hex	SINT	ISL 202 (8DI) Input Data
IBR01Out.S01_ISL2028DI[1]	16#00	Hex	SINT	ISL 202 (8DI) Input Data

Figure 7.5 – Logix – INTERBUS “Out” Tag

The Input tag (example “IBR01In”) will typically include the Module (System) Status, and all the virtual Output INTERBUS slaves’ data.

Name	Value	Style	Data Type	Description
IBR01In	{...}		IBR01In17E4	
IBR01In.ModuleStatus	{...}		IBRSystemStatus	
IBR01In.ModuleStatus.ChcksmErrCount	0	Decimal	DINT	Checksum Error Count
IBR01In.ModuleStatus.ConfigValid	1	Decimal	BOOL	Configuration Valid
IBR01In.ModuleStatus.ControllerRun	1	Decimal	BOOL	Controller Mode: 0=Program, 1=Run
IBR01In.ModuleStatus.DataPcktCount	23459	Decimal	DINT	Data Packet Count
IBR01In.ModuleStatus.EIPOriginatorCommsOk	0	Decimal	BOOL	EtherNet/IP Originator 0=Fail, 1=Ok
IBR01In.ModuleStatus.EIPOwned	1	Decimal	BOOL	EtherNet/IP Target 0=Not-Owned, 1=Owned
IBR01In.ModuleStatus.IdentPcktCount	4560	Decimal	DINT	Ident Packet Count
IBR01In.ModuleStatus.IdleStateChgCount	1	Decimal	DINT	Idle State Change Count
IBR01In.ModuleStatus.IdleTimeoutCount	0	Decimal	DINT	Idle Timeout Count
IBR01In.ModuleStatus.INTERBUSActive	1	Decimal	BOOL	INTERBUS Active: 0=Off 1=Active
IBR01In.ModuleStatus.INTERBUSCycle	1194	Decimal	DINT	INTERBUS Cycle Time (us)
IBR01In.ModuleStatus.INTERBUSRun	1	Decimal	BOOL	INTERBUS Run: 0=Off 1=Run
IBR01In.ModuleStatus.ModbusOnline	0	Decimal	BOOL	0=Offline, 1=Online
IBR01In.ModuleStatus.NTPOk	0	Decimal	BOOL	NTP Status: 0=Fail, 1=Ok
IBR01In.ModuleStatus.RxPcktCount	19443	Decimal	DINT	Rx Packet Count
IBR01In.ModuleStatus.TxPcktUpdateCount	6218	Decimal	DINT	Tx Packet Update Count
IBR01In.ModuleStatus.UnknownCmdCount	0	Decimal	DINT	Unknown Command Count
IBR01In.S02_ISL2018DO	{...}	Hex	SINT[2]	ISL 201 (8DO) Output Data
IBR01In.S02_ISL2018DO[0]	16#00	Hex	SINT	ISL 201 (8DO) Output Data
IBR01In.S02_ISL2018DO[1]	16#00	Hex	SINT	ISL 201 (8DO) Output Data

Figure 7.6 – Logix – INTERBUS "In" Tag

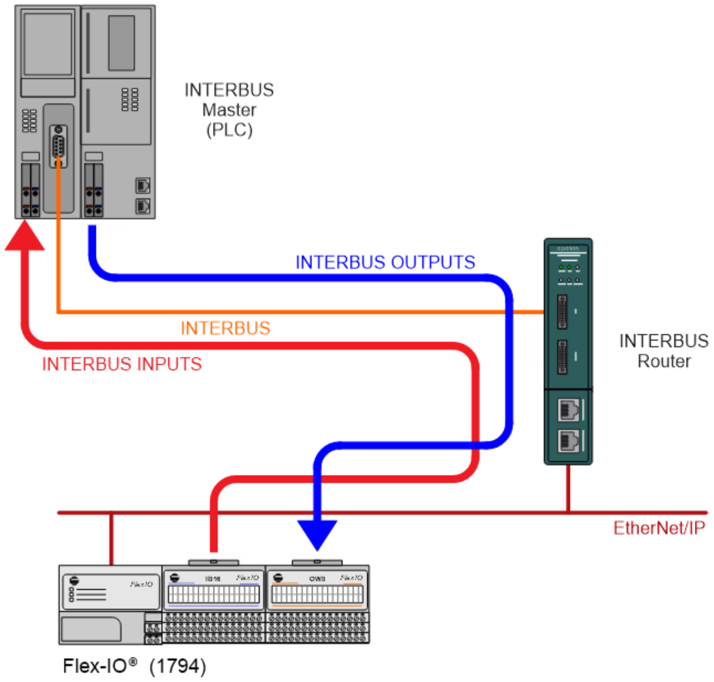
7.3. ETHERNET/IP ORIGINATOR

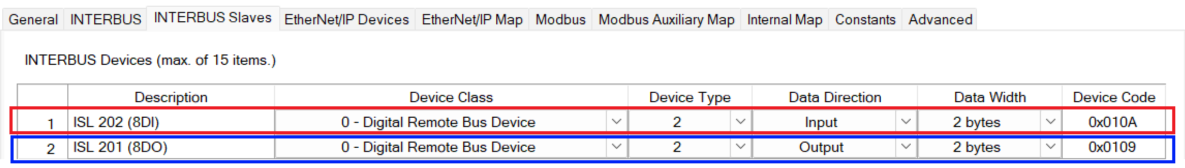
The INTERBUS Router module can operate as an EtherNet/IP originator. In this mode the module can exchange data from the INTERBUS network with EtherNet/IP devices using either the input and output assemblies of the Class 1 EtherNet/IP connection to the device or using explicit (Class 3 or UCMM) EtherNet/IP messages.

7.3.1. EtherNet/IP Class 1 Connections

In the example below, the INTERBUS Router is exchanging INTERBUS slave data with owned EtherNet/IP I/O devices.

Once the EtherNet/IP Class 1 connections are configured and established, then any Internal Map copying to an EtherNet/IP device will be written to the output assembly of the selected EtherNet/IP device (Originator to Target). In the Internal Map the user will specify which device instance is the target and at what offset the data must be written in the output assembly.

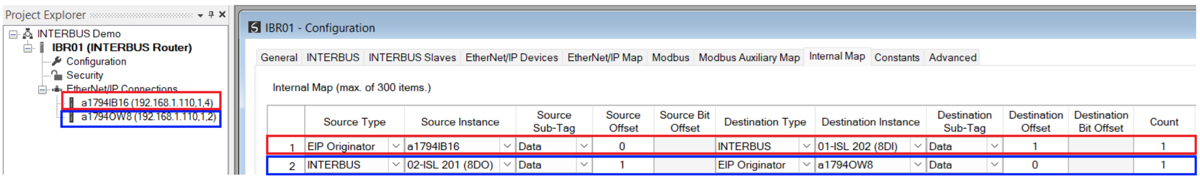




General | INTERBUS | INTERBUS Slaves | EtherNet/IP Devices | EtherNet/IP Map | Modbus | Modbus Auxiliary Map | Internal Map | Constants | Advanced

INTERBUS Devices (max. of 15 items.)

	Description	Device Class	Device Type	Data Direction	Data Width	Device Code
1	ISL 202 (8DI)	0 - Digital Remote Bus Device	2	Input	2 bytes	0x010A
2	ISL 201 (8DO)	0 - Digital Remote Bus Device	2	Output	2 bytes	0x0109



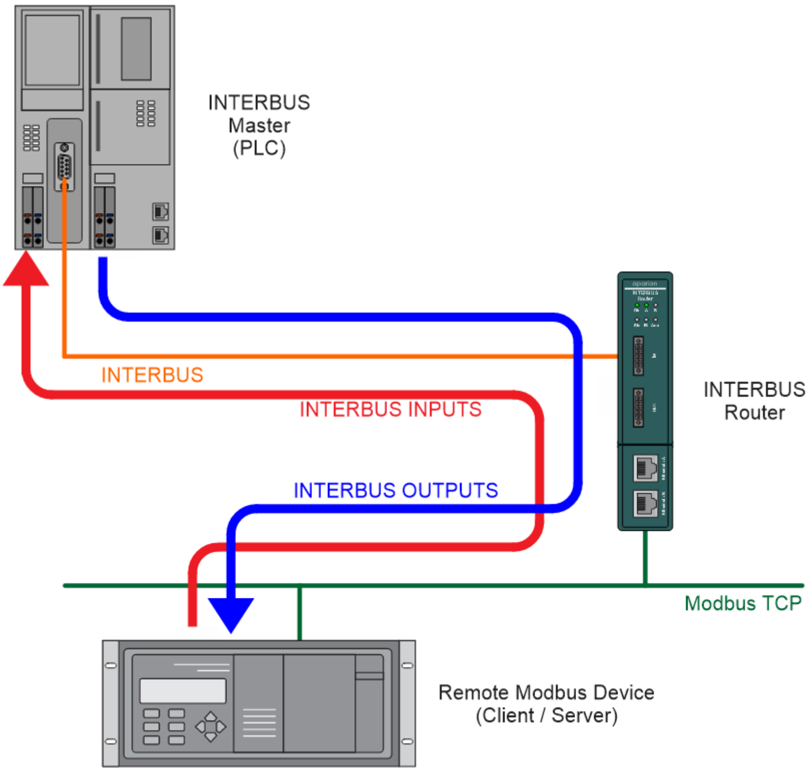
Internal Map (max. of 300 items.)

	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count
1	EIP Originator	a1794IB16	Data	0		INTERBUS	01-ISL 202 (8DI)	Data	1		1
2	INTERBUS	02-ISL 201 (8DO)	Data	1		EIP Originator	a1794OW8	Data	0		1

Figure 7.7 – Internal Mapping - EtherNet/IP Originator

7.4. MODBUS

When the INTERBUS Router has the Primary Interface set to either Modbus Client or Modbus Server, then the INTERBUS slave data can be mapped to and from configurable internal Modbus Registers using the Internal Map.



General | INTERBUS | INTERBUS Slaves | EtherNet/IP Devices | EtherNet/IP Map | Modbus | Modbus Auxiliary Map | Internal Map | Constants | Advanced

INTERBUS Devices (max. of 15 items.)

	Description	Device Class	Device Type	Data Direction	Data Width	Device Code
1	ISL 202 (8DI)	0 - Digital Remote Bus Device	2	Input	2 bytes	0x010A
2	ISL 201 (8DO)	0 - Digital Remote Bus Device	2	Output	2 bytes	0x0109

General | INTERBUS | INTERBUS Slaves | EtherNet/IP Devices | EtherNet/IP Map | Modbus | Modbus Auxiliary Map | Internal Map | Constants | Advanced

Internal Map (max. of 300 items.) Recommend

	Source Type	Source Instance	Source Sub-Tag	Source Offset	Source Bit Offset	Destination Type	Destination Instance	Destination Sub-Tag	Destination Offset	Destination Bit Offset	Count	Copy Function	Reformat
1	System		Status	0		MB Register	HR		1000		48	Byte to Byte	None
2	MB Register	HR		2000		INTERBUS	01-ISL 202 (8DI)	Data	0		2	Byte to Byte	None
3	INTERBUS	02-ISL 201 (8DO)	Data	0		MB Register	HR		1024		2	Byte to Byte	None

Figure 7.8 – Modbus Client / Server

In the case of a Modbus Client, the Modbus Auxiliary map will also need to be configured to exchange this data with a remote Modbus Server.

IBR01 - Configuration

General | INTERBUS | INTERBUS Slaves | EtherNet/IP Devices | EtherNet/IP Map | Modbus | Modbus Auxiliary Map | Internal Map | Constants | Advanced

Modbus Auxiliary Map (max. of 100 items.)

	Modbus Function	Register Type	Local Reg.	Count	Remote Reg.	IP Address	Node	Reformat
1	Write	HR	1000	26	1000	192.168.1.23	7	None
2	Read	HR	2000	4	2000	192.168.1.23	7	None

Figure 7.9 – Modbus Auxiliary Map

7.5. INTERNAL MAP DATA FORMATS

The following tables describe the raw format of the data structures that can be mapped in the Internal Map table configuration.

NOTE: When using EtherNet/IP Target, Modbus Server, or Modbus Client, it is recommended to use the Recommended Mapping feature in the internal mapping. This will automatically map all the required data in the Internal Map.

7.5.1. SYSTEM STATUS

When copying system information, the source type needs to be System.

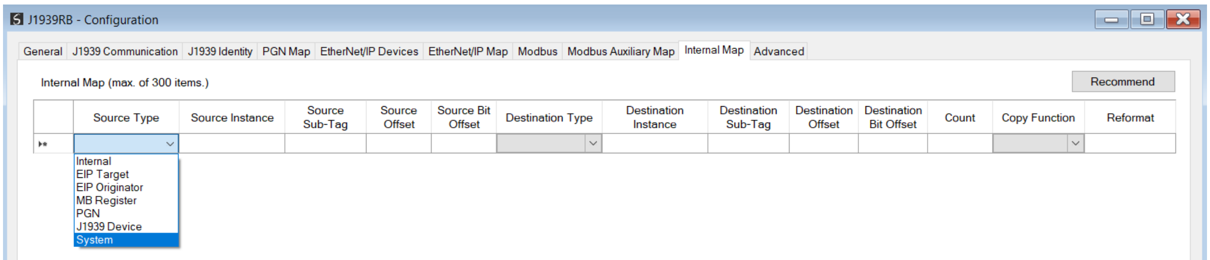


Figure 7.10 – IDS Copy – System Information

The module's system information has the following format.

Parameter	Data Type	Description
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 – Controller in Run Mode. Bit 5 – NTP Ok Bit 6 – INTERBUS Active Bit 7 – INTERBUS Running
INTERBUS Cycle Time	DINT	The INTERBUS Cycle Time in microseconds.
Frame Rx Count	DINT	The number of INTERBUS Frames received.
Frame Update Count	DINT	The number of Frame Updates (Input (Send) data changed)
Checksum Errors	DINT	The number of detected Frame Checksum errors.
Ident Frame Count	DINT	The number of INTERBUS Ident frames received.

Data Frame Count	DINT	The number of INTERBUS Data frames received.
Unknown Command Count	DINT	The number of unknown INTERBUS commands received.
Idle Timeout Count	DINT	The number of INTERBUS timeout occurrences.
Idle State Change Count	DINT	The number of INETRBUS Idle State changes.

Table 7.1 – System Information Format

8. DIAGNOSTICS

8.1. LEDS

The module provides six LEDs for diagnostics purposes as shown in the front view figure below. A description of each LED is provided in the table below.

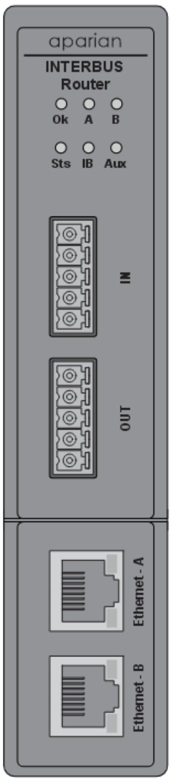


Figure 8.1 – INTERBUS Router front view

LED	Description
Ok	The module LED will provide information regarding the system-level operation of the module. If the LED is **red**, then 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. If the LED is briefly **flashing red**, and then returning to either flashing green or solid green, then there is a duplicate IP address on the Ethernet network similar to that of the local module. If the LED is **green (flashing)**, then the module has booted and is running correctly **without** any application configuration loaded.

	If the LED is **green (solid)**, then the module has booted and is running correctly **with** application configuration loaded.
A / B	The Ethernet LED will light up when an Ethernet link has been detected (by plugging in a connected Ethernet cable). The LED will flash every time traffic is detected. This module has two Ethernet ports A and B. Each LEDs represents each specific port.
Sts	The Status LED indicates if the module is currently in an active state where the primary interface is operational and the INTERBUS communication is active. <u>Solid Green</u> – Both the INTERBUS communication and the Primary Interface communication is active and running. <u>Flashing Green</u> – Either the INTERBUS communication or the Primary Interface communication is active and running (not both). <u>Off</u> - Both the INTERBUS communication and the Primary Interface communication is **not** running.
IB	The INTERBUS LED indicates the activity on the INTERBUS network. <u>Flashing Red</u> – A corrupted or incorrect INTERBUS packet was received. <u>Flashing Green</u> – A valid INTERBUS packet was received. <u>Off</u> – No INTERBUS packets are being received or sent.
Aux	The Aux LED will flash each time there is activity on any of the primary interfaces. <u>Flashing Red</u> – A corrupted or incorrect packet was received on one of the Primary Interfaces (EtherNet/IP, Modbus TCP). <u>Flashing Green</u> – A valid packet was received on one of the Primary Interfaces (EtherNet/IP, Modbus TCP). <u>Off</u> – No activity.

Table 8.1 - Module LED operation

8.2. MODULE STATUS MONITORING IN SLATE

The INTERBUS Router provides various statistics which can assist with module operation, maintenance, and fault finding. The statistics can be accessed in full by Slate or using the web server in the module.

To view the module's status in the Aparian-Slate 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.

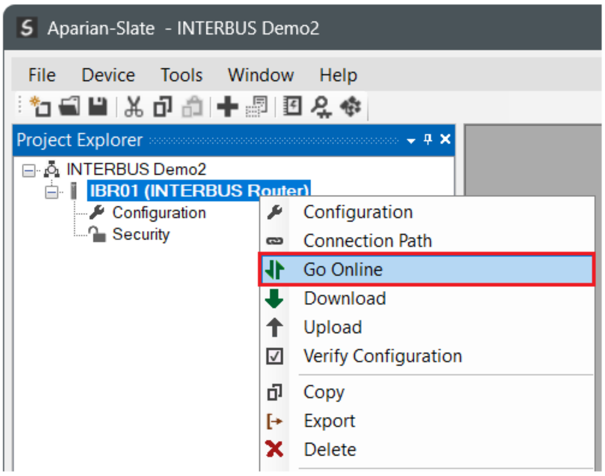


Figure 8.2 - Selecting to Go Online

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

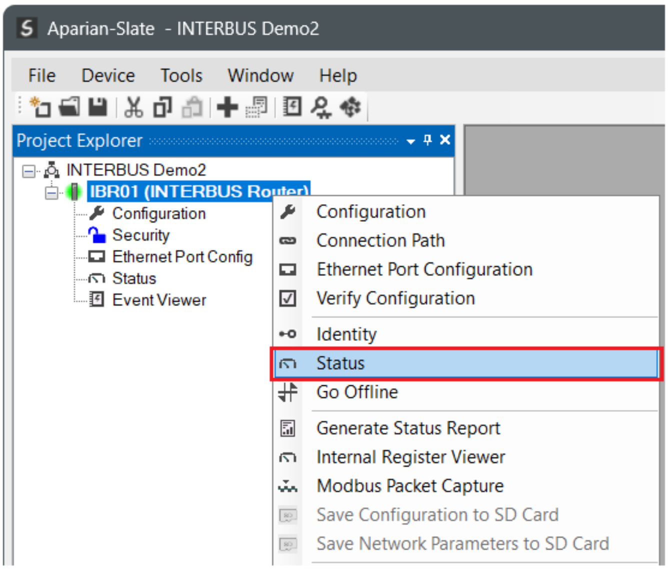


Figure 8.3 - Selecting online Status

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 current status of the module.

8.2.1. GENERAL

The General tab displays the general status for the local INTERBUS Router module.

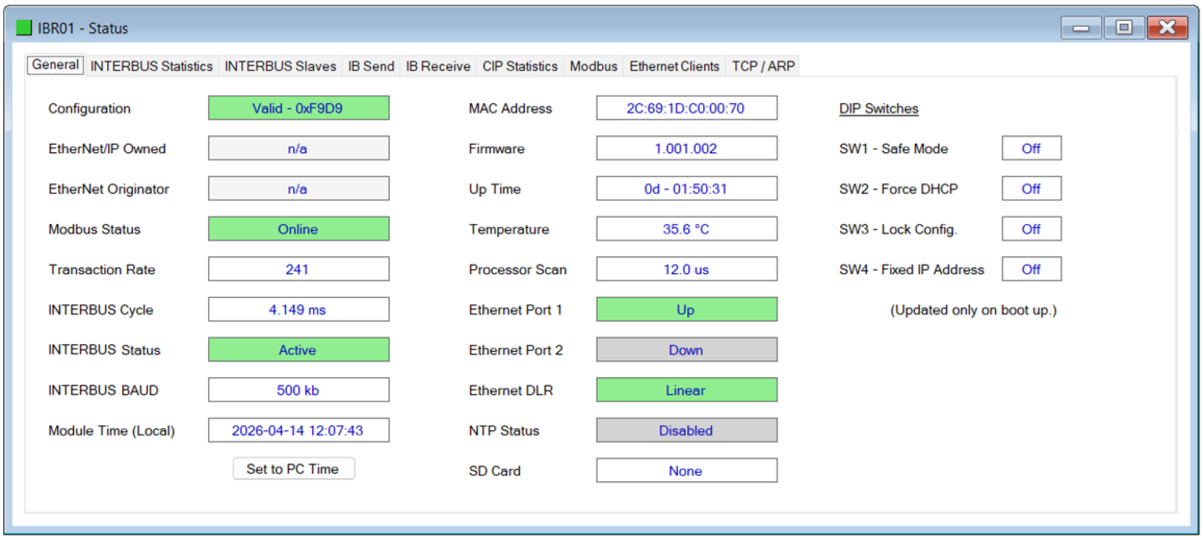


Figure 8.4 - Status monitoring – General

The General tab displays the following general parameters:

Parameter	Description
Configuration	Indicates whether the current configuration is valid or not, as well as the configuration 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 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.
Transaction Rate	Number of INTERBUS transactions executed per second.
INTERBUS Cycle	The current INTERBUS Cycle period, in milliseconds.
INTERBUS Status	The status of the INTERBUS communication.
INTERBUS BAUD	The BAUD rate of the configured INTERBUS communication, either 500 kb or 2Mb.
Module Time	The current module time.
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's CPU.
Processor Scan	The amount of time (microseconds) taken by the module's processor in the last scan.
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.
SD Card	Indicates if a SD Card is present or not.

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 8.2 - Parameters displayed in the Status Monitoring – General Tab

8.2.2. INTERBUS Statistics

The INTERBUS Statistics tab displays the statistics associated with the INTERBUS communication network.

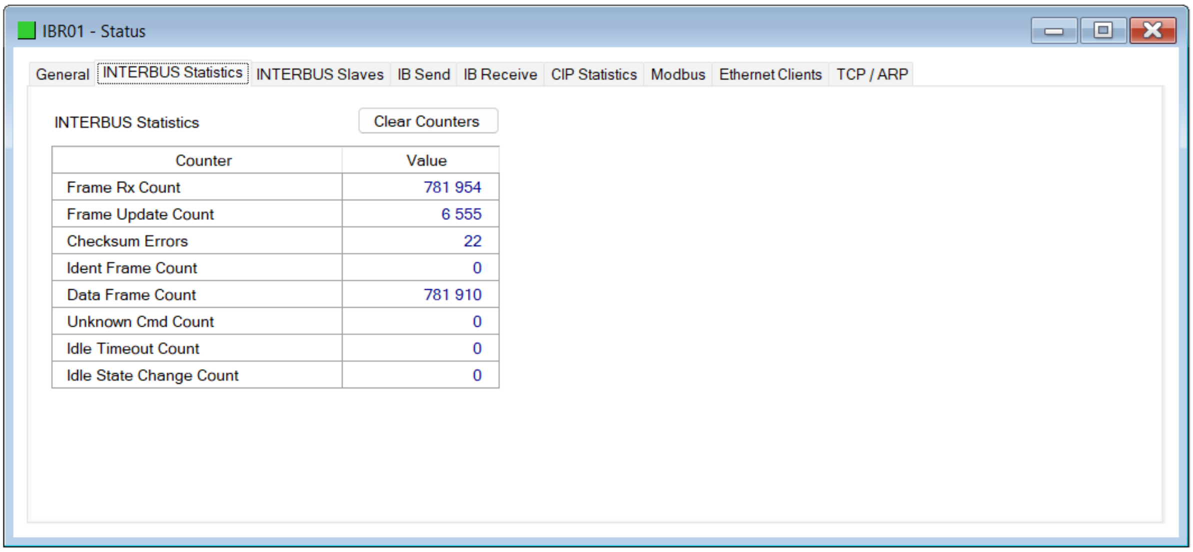


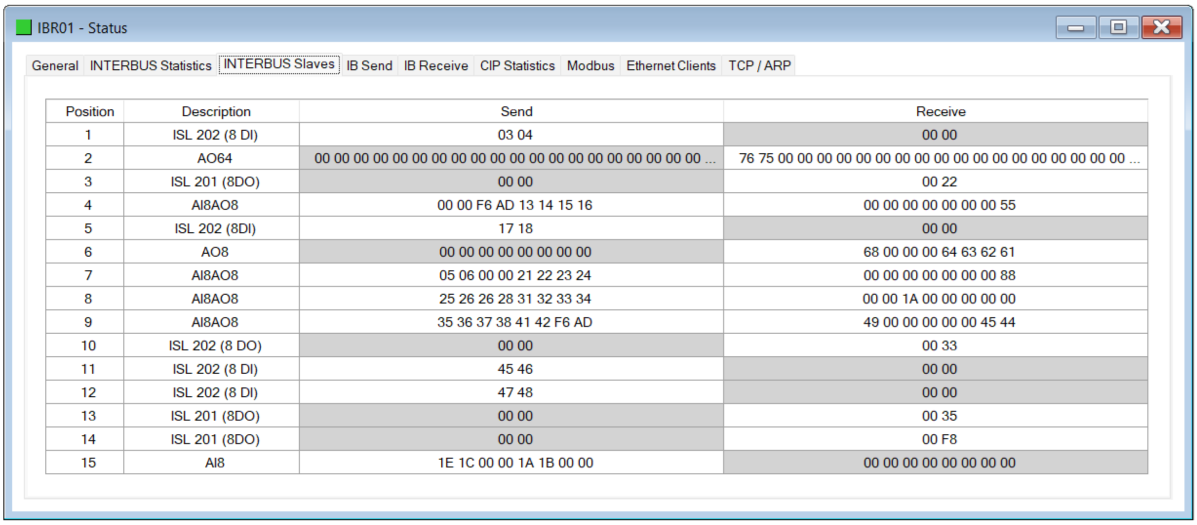
Figure 8.5 - Status monitoring – INTERBUS Statistics

Statistic	**Description**
Frame Rx Count	The number of INTERBUS Frames received.
Frame Update Count	The number of Frame Updates (Input (Send) data changed)
Checksum Errors	The number of detected Frame Checksum errors.
Ident Frame Count	The number of INTERBUS Ident frames received.
Data Frame Count	The number of INTERBUS Data frames received.
Unknown Cmd Count	The number of unknown INTERBUS commands received.
Idle Timeout Count	The number of INTERBUS timeout occurrences.
Idle State Change Count	The number of INTERBUS Idle State changes.

Table 8.3 – INTERBUS statistics

8.2.3. INTERBUS SLAVE

The INTERBUS Slaves tab displays the configured slaves and their current Send and Receive data.



Position	Description	Send	Receive
1	ISL 202 (8 DI)	03 04	00 00
2	AO64	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...	76 75 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
3	ISL 201 (8DO)	00 00	00 22
4	AI8AO8	00 00 F6 AD 13 14 15 16	00 00 00 00 00 00 00 55
5	ISL 202 (8DI)	17 18	00 00
6	AO8	00 00 00 00 00 00 00 00	68 00 00 00 64 63 62 61
7	AI8AO8	05 06 00 00 21 22 23 24	00 00 00 00 00 00 00 88
8	AI8AO8	25 26 26 28 31 32 33 34	00 00 1A 00 00 00 00 00
9	AI8AO8	35 36 37 38 41 42 F6 AD	49 00 00 00 00 00 45 44
10	ISL 202 (8 DO)	00 00	00 33
11	ISL 202 (8 DI)	45 46	00 00
12	ISL 202 (8 DI)	47 48	00 00
13	ISL 201 (8DO)	00 00	00 35
14	ISL 201 (8DO)	00 00	00 F8
15	AI8	1E 1C 00 00 1A 1B 00 00	00 00 00 00 00 00 00 00

Figure 8.6 - Status monitoring – INTERBUS Slaves

Parameter	Description
Position	The slave position (starting at 1) within the INTERBUS Router.
Description	The configured description of the virtual slave.
Send	The Send data (inputs) associated with the virtual slave, displayed in Hex format. Note: A gray background indicates that the data is not relevant.
Receive	The Receive data (outputs) associated with the virtual slave, displayed in Hex format. Note: A gray background indicates that the data is not relevant.

Table 8.4 – INTERBUS Slaves

8.2.4. INTERBUS SEND DATA

The IB Send Data tab displays all the data the INTERBUS Router will send in the INTERBUS summation frame.

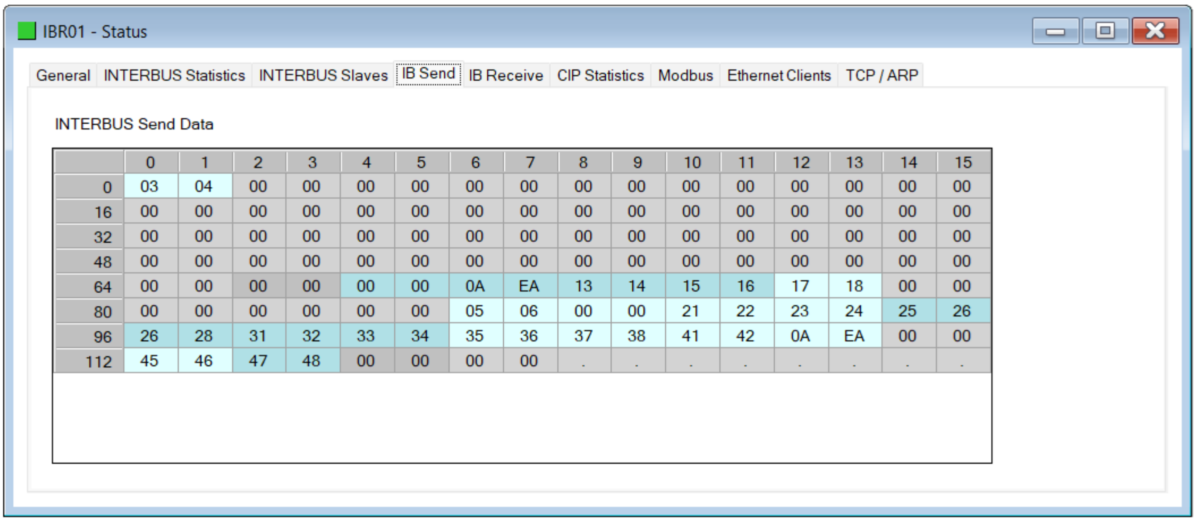


Figure 8.7 - Status monitoring – INTERBUS Send Data

The data is displayed in Hex format, and a gray background indicates that the data is not relevant to any specific virtual slave.
The background color alternates between shades of blue for each configured virtual slave.

8.2.1. INTERBUS Receive Data

The IB Receive Data tab displays all the data received by the INTERBUS Router from the INTERBUS summation frame.

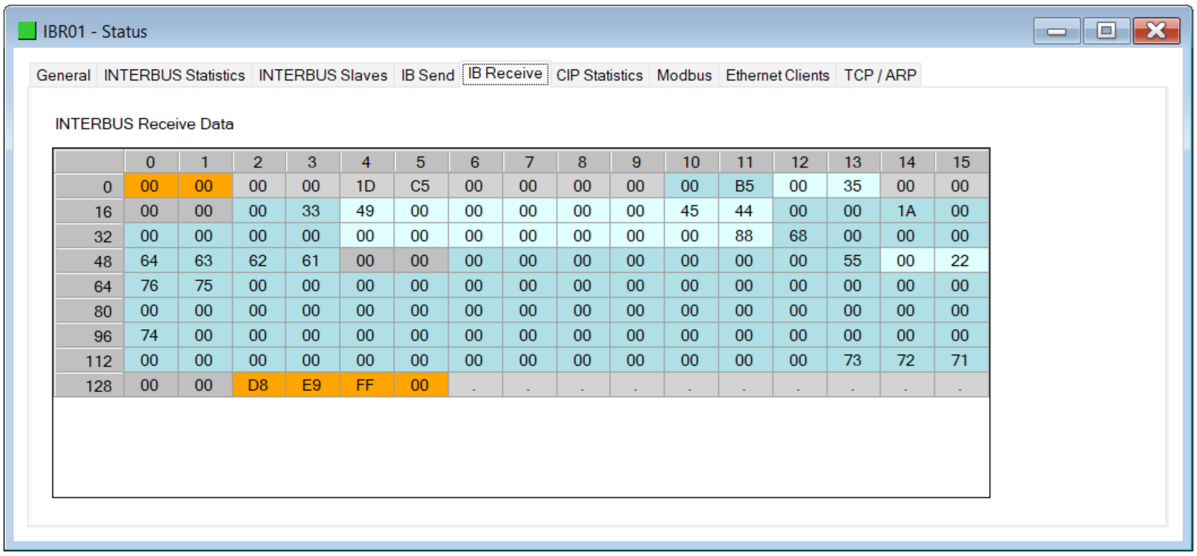


Figure 8.8 - Status monitoring – INTERBUS Receive Data

The data is displayed in Hex format, and a gray background indicates that the data is not relevant to any specific virtual slave. An orange background indicates summation frame control data.

The background color alternates between shades of blue for each configured virtual slave.

8.2.2. 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.

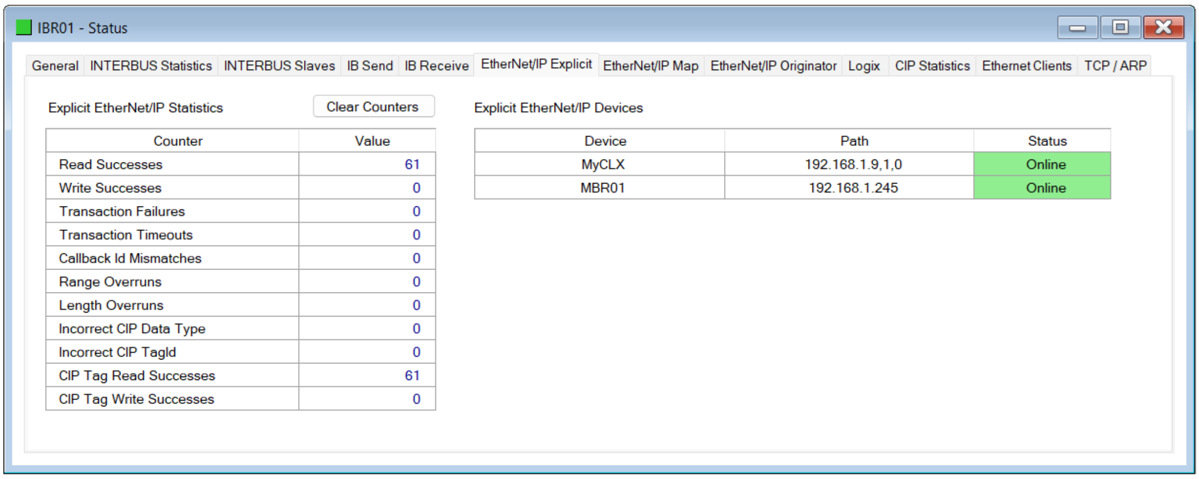


Figure 8.9 - Status monitoring – EtherNet/IP Explicit

Statistic	Description
Read Successes	The number of successful reads from the target EtherNet/IP device.
Write Successes	The number of successful write 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 8.5 – EtherNet/IP Explicit Statistics

8.2.3. 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.

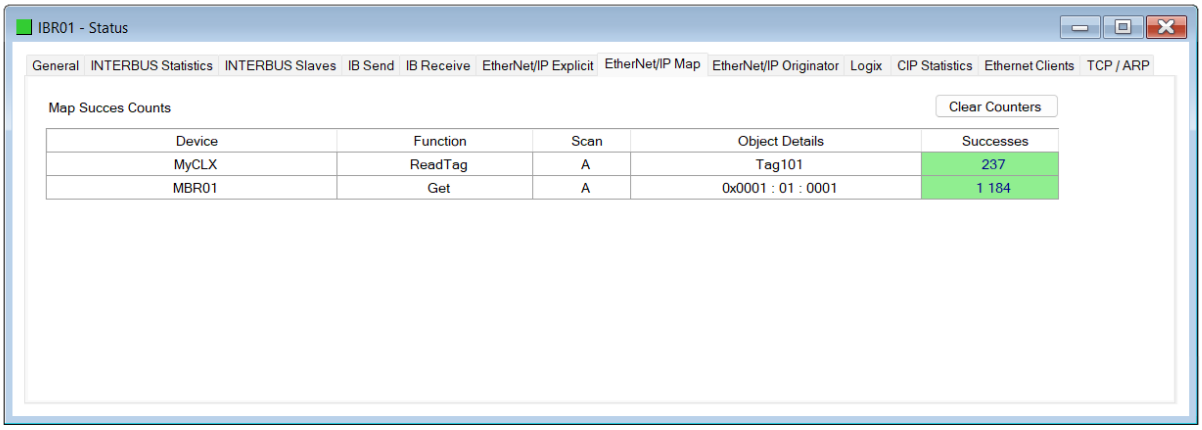


Figure 8.10 - Status monitoring – EtherNet/IP Map

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.

8.2.4. 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.

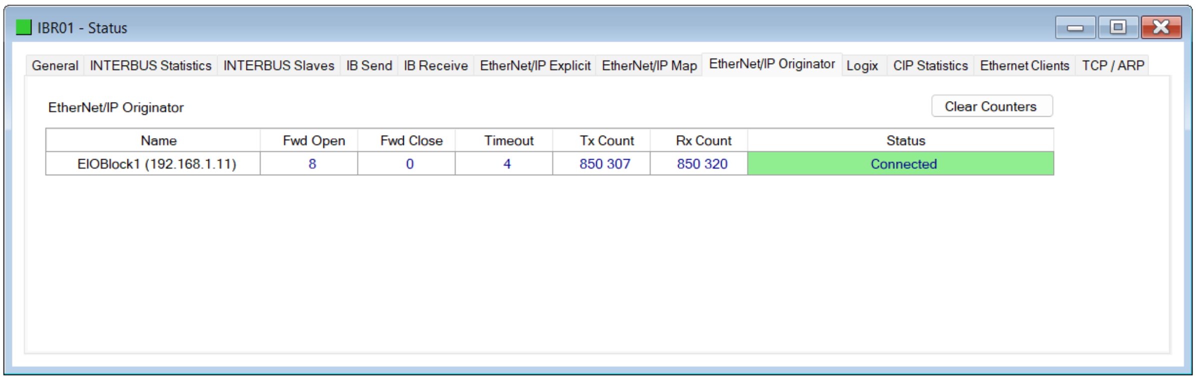


Figure 8.11 - Status monitoring – EtherNet/IP Originator

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 rejection, 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 8.6 – EtherNet/IP Class 1 status and statistics

8.2.5. 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.

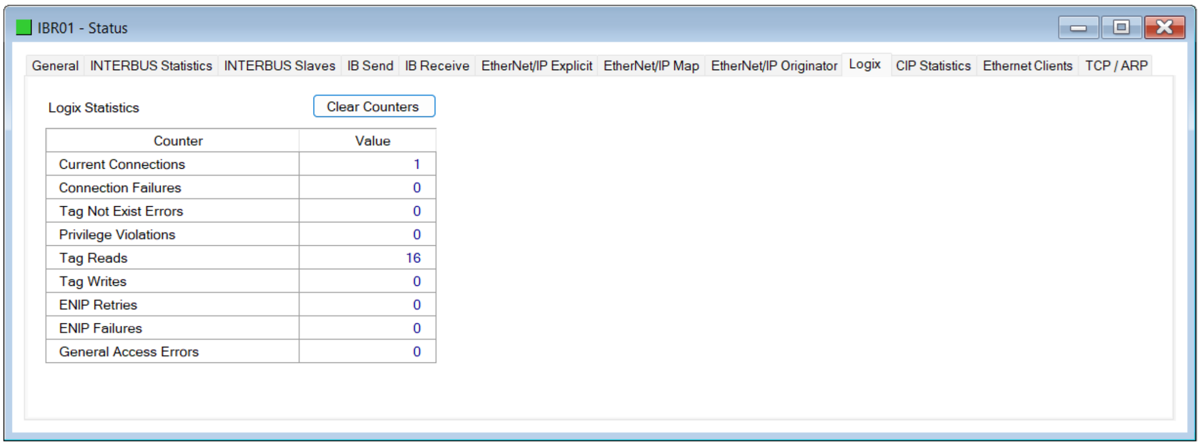


Figure 8.12 - Status monitoring – Logix Statistics

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 INTERBUS Router module.
Tag Writes	The number of tag write transactions executed by the INTERBUS Router module.
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 8.7 – Logix Statistics Tab

8.2.6. Modbus

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

NOTE: The Modbus statistics tab is only displayed if the module has the primary interface set to Modbus TCP Client or Modbus TCP Server.

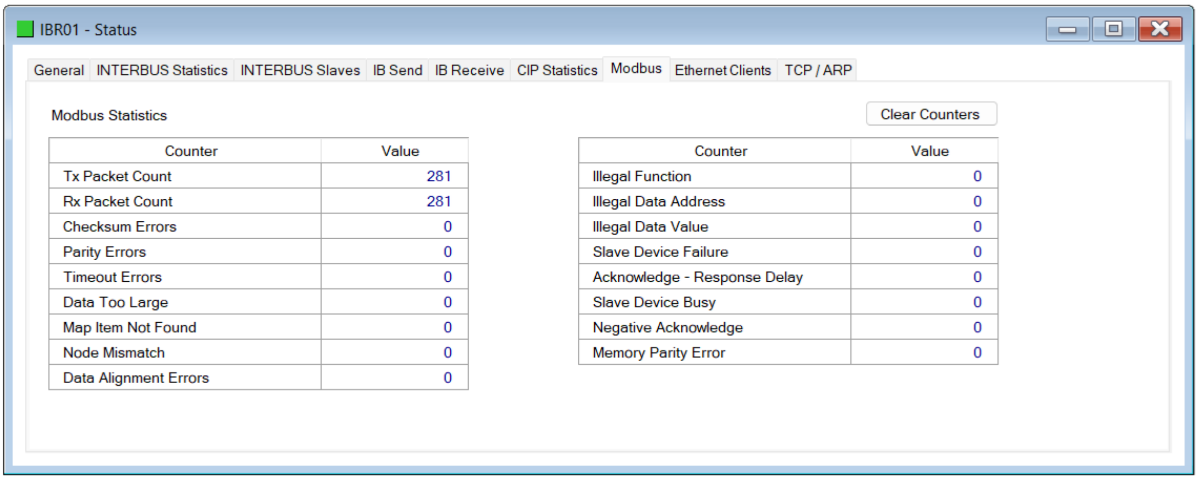


Figure 8.13. - Status monitoring – Modbus Statistics

The Modbus tab displays the following parameters:

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 8.8 - Modbus Statistics Tab

8.2.7. CIP Statistics

The CIP tab displays the Ethernet CIP statistics.

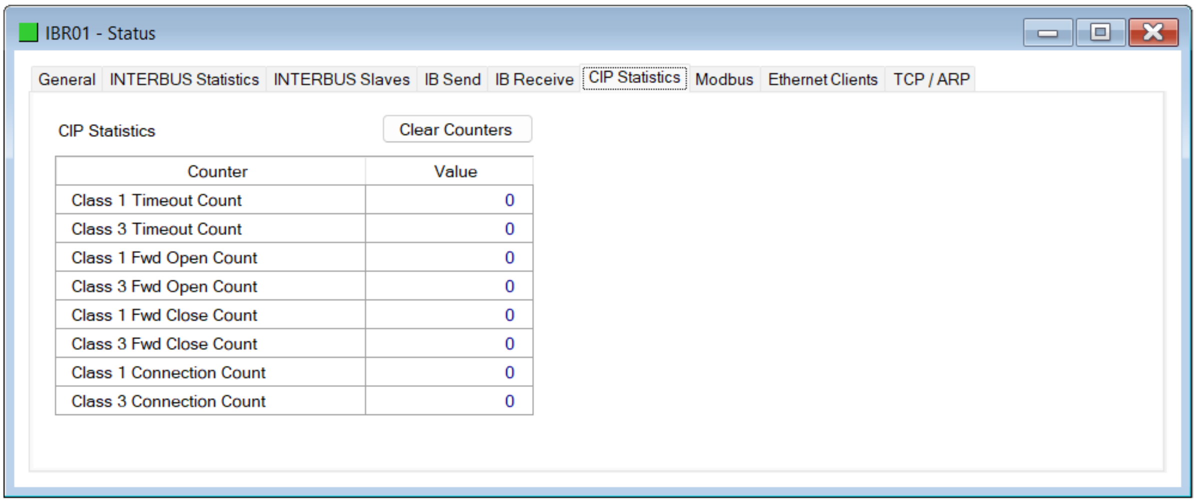


Figure 8.14 - Status monitoring – CIP Statistics

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 8.9 – Mapped Item statistics

8.2.8. Ethernet Clients

The Ethernet Clients tab displays details of the Ethernet and EtherNet/IP clients connected to the INTERBUS Router.

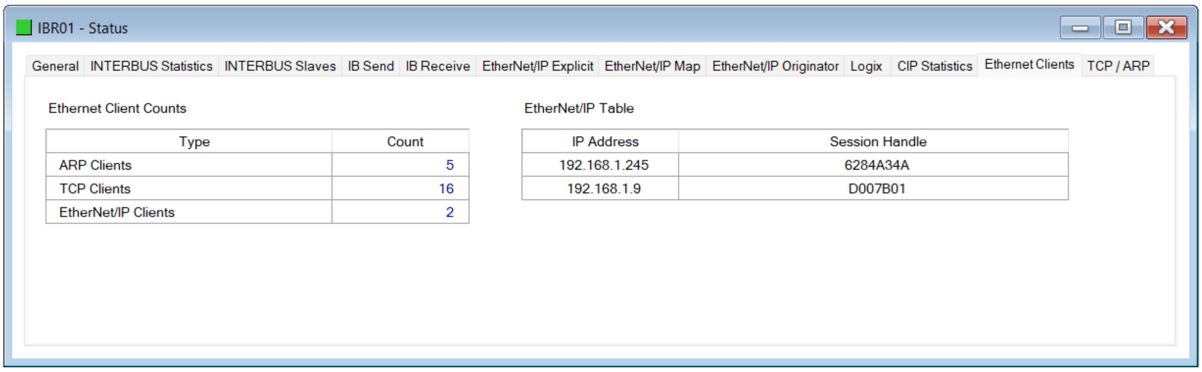


Figure 8.15 –Status monitoring – Ethernet Client Statistics

8.2.9. TCP/ARP

The TCP/ARP tab displays details of the internal Ethernet ARP and TCP lists of the INTERBUS Router.

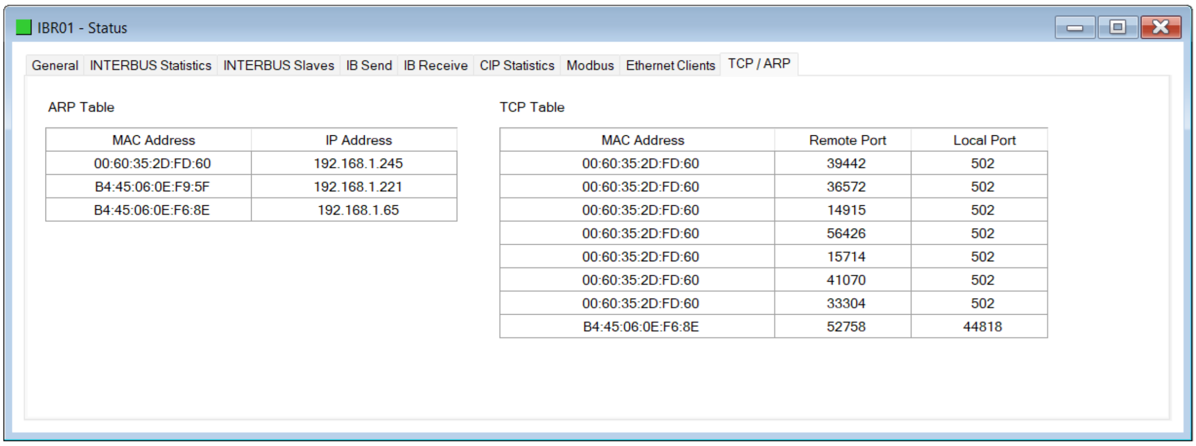


Figure 8.16 – Status monitoring – Ethernet TCP / ARP Statistics

8.3. TARGET DEVICE STATUS MONITORING IN SLATE

The INTERBUS Router can also provide individual statistics and status for each for each of the EtherNet/IP Class 1 or INTERBUS Cyclic IO devices when the Primary Interface is *EtherNet/IP Originator.*

8.3.1. ETHERNET/IP

When online with the module in Slate, right-click on the desired EtherNet/IP device under the *EtherNet/IP Connections* tree in Slate and select *Status*.

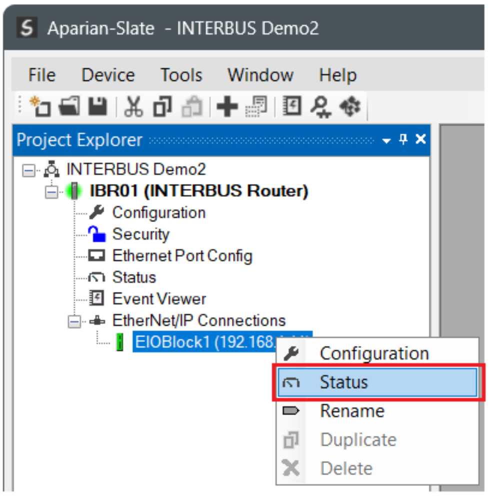


Figure 8.17 – EtherNet/IP Device Status – Status selection

8.3.1.1. GENERAL

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

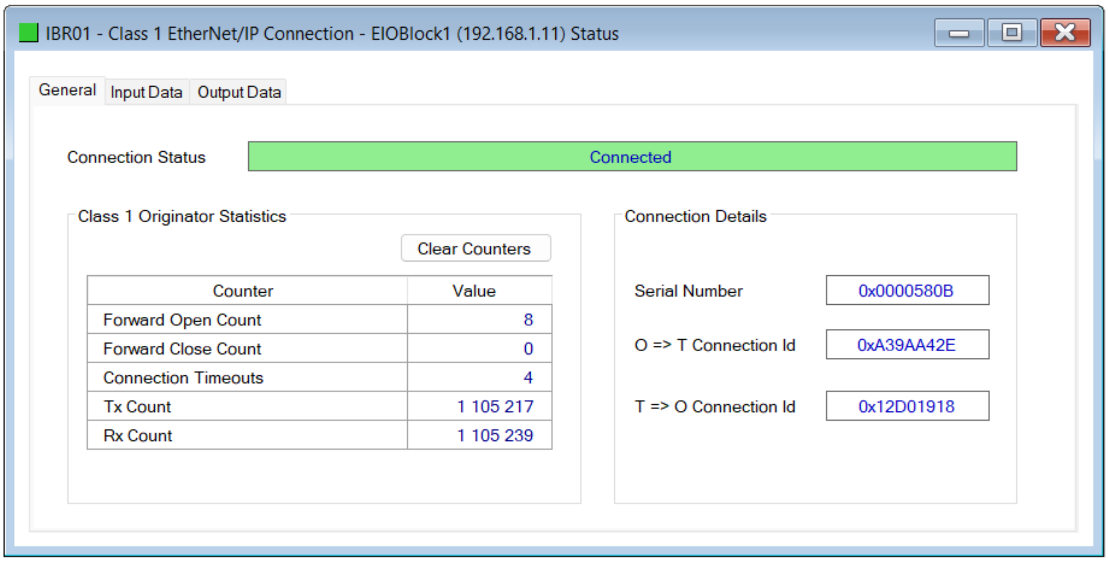


Figure 8.18 – EtherNet/IP Device Status – General Status

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, then generally the target device will reply with the specific reason for the connection rejection, for example: 
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 8.10 – EtherNet/IP Class 1 Device status and statistics

8.3.1.2. INPUT DATA

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

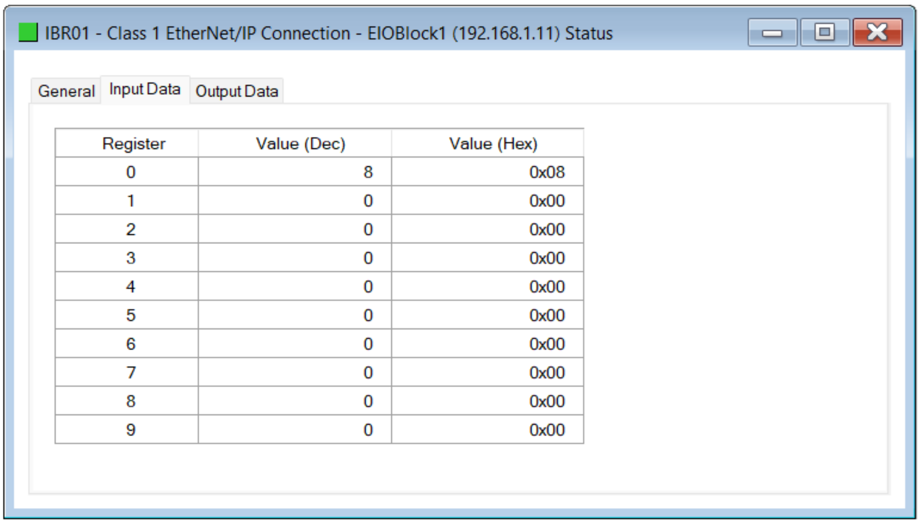
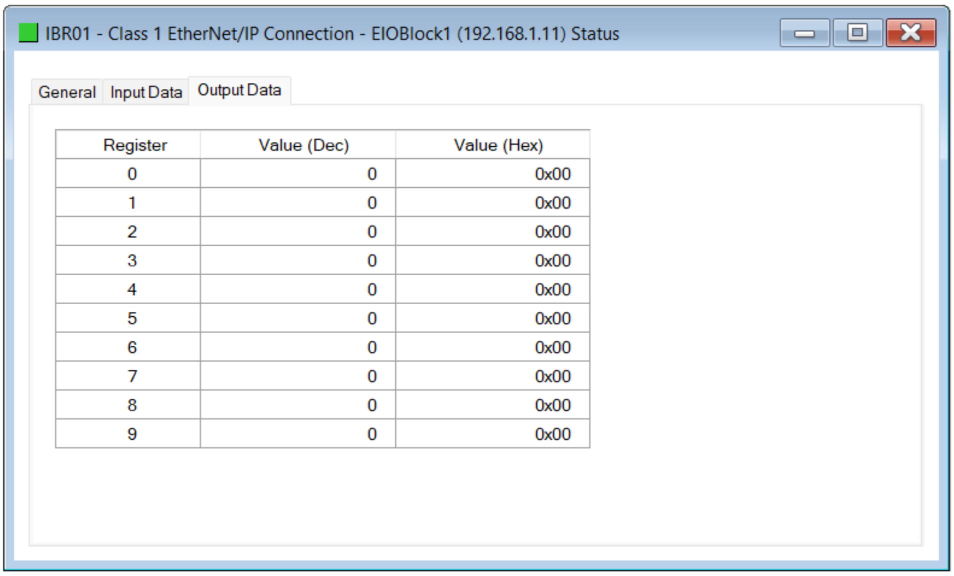


Figure 8.19 – EtherNet/IP Device Status – Input Data

8.3.1.3. OUTPUT DATA

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



Register	Value (Dec)	Value (Hex)
0	0	0x00
1	0	0x00
2	0	0x00
3	0	0x00
4	0	0x00
5	0	0x00
6	0	0x00
7	0	0x00
8	0	0x00
9	0	0x00

Figure 8.20 – EtherNet/IP Device Status – Output Data

8.4. MODULE EVENT LOG

The INTERBUS Router module logs various diagnostic records to an internal event log. These logs are stored in non-volatile memory and can be displayed using Slate or via the web interface. To view them in Slate, select the ***Event Viewer*** option in the Project Explorer tree.

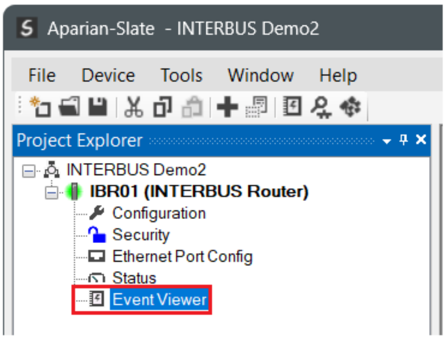


Figure 8.21 - Selecting the module Event Log

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

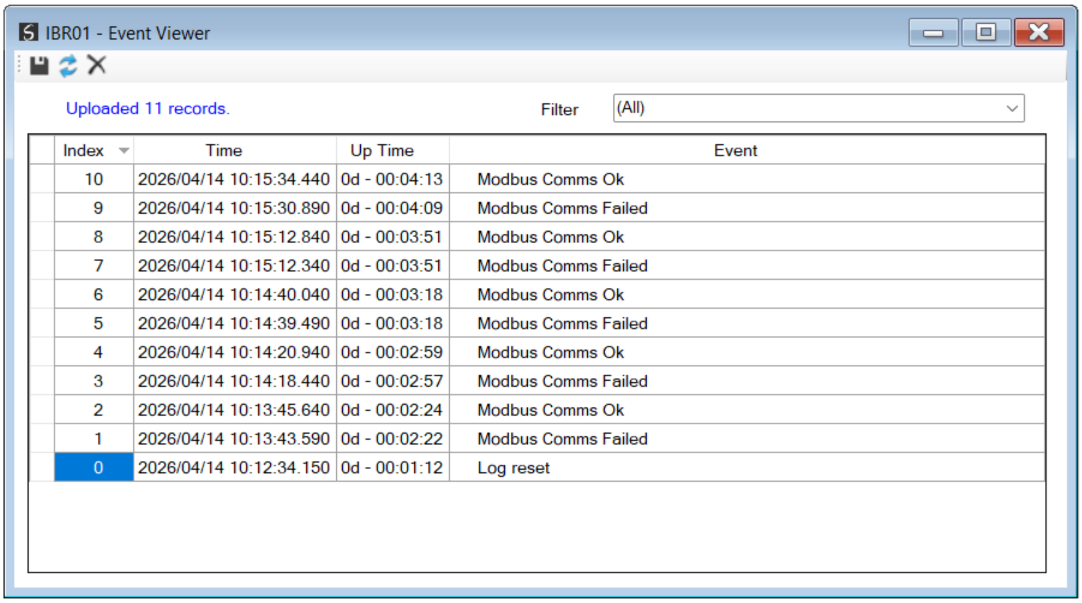


Figure 8.22 - Module Event Log

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.

8.5. 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.

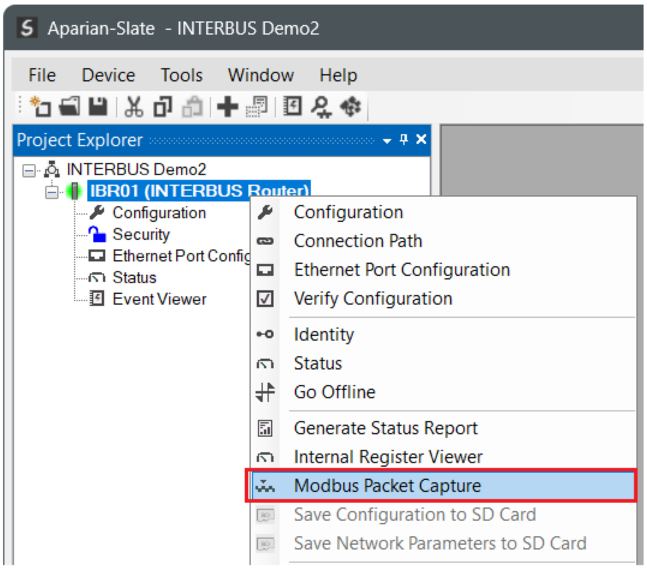


Figure 8.23 - Selecting Modbus Packet Capture

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

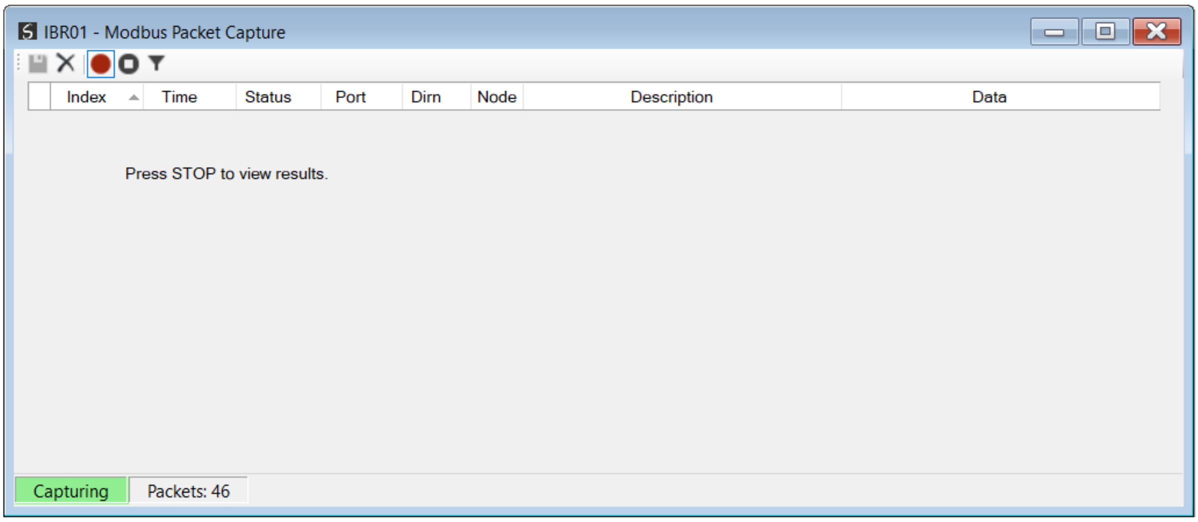


Figure 8.24 – Modbus packet capture

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

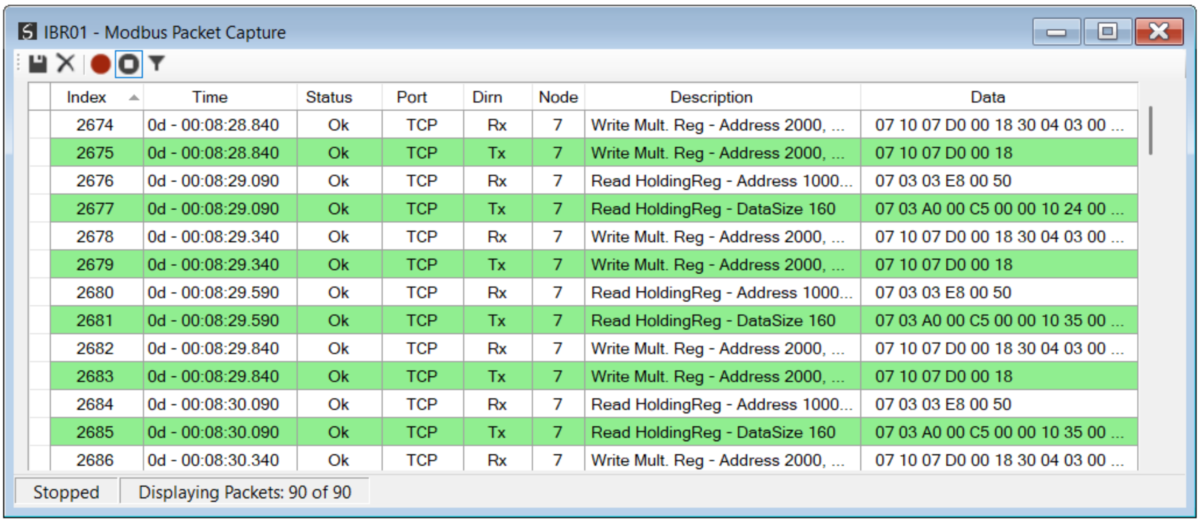


Figure 8.25 – Modbus Packet Capture complete

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)
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 8.11 – 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.

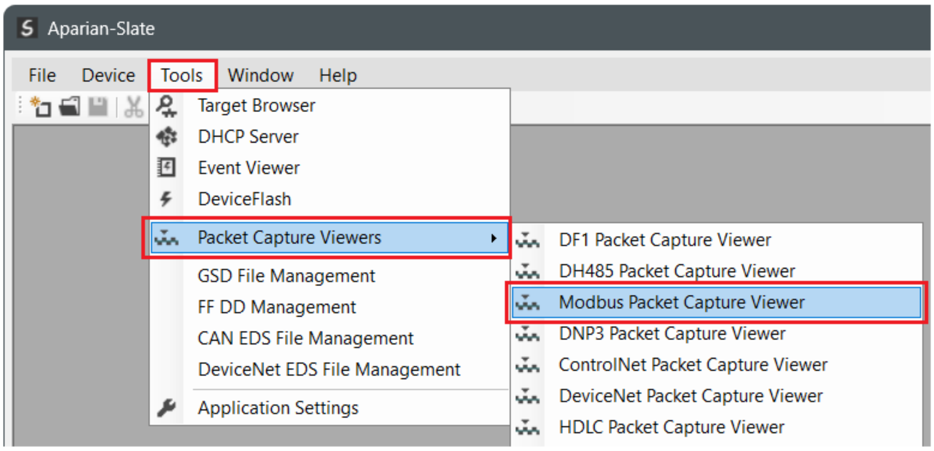


Figure 8.26 - Selecting the Modbus Packet Capture Viewer

8.6. MODULE STATUS REPORT

For assisting with support Slate can generate a status report for the module 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 Slate) and select *Generate Status Report*.

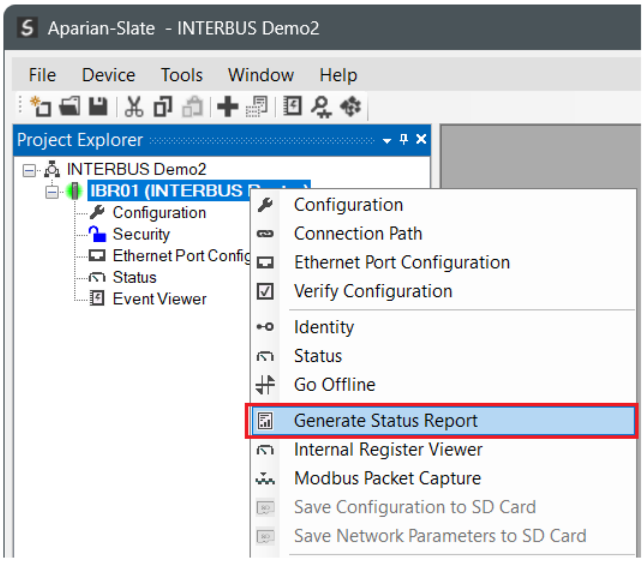


Figure 8.27 – Module Status Report

8.7. MODBUS SUMMARY CSV

Slate 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 INTERBUS Router module configuration). To generate the Modbus Summary CSV, right-click on the module (when online in Slate), and select *Export Modbus Summary CSV*.

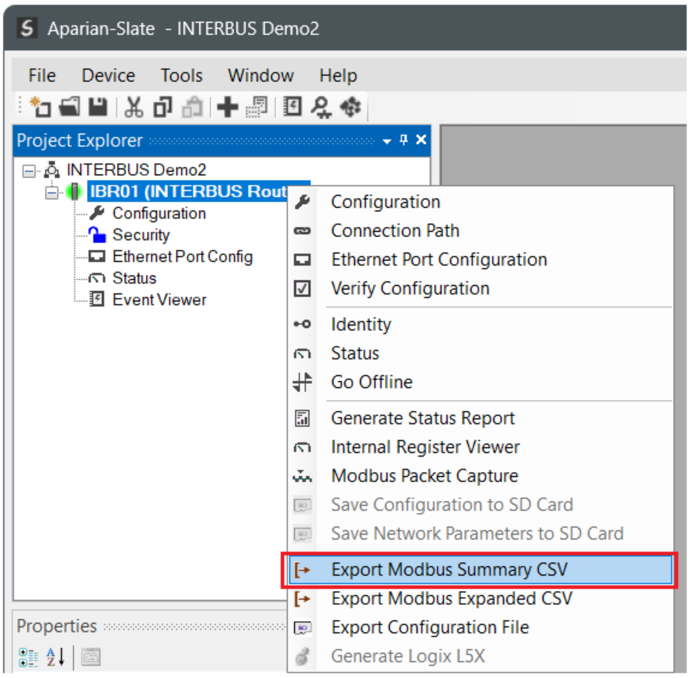


Figure 8.28 – Modbus Summary Report Generation

	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	1055	32	INTERBUS.S02_AO64.Data
4	HR	Read	1056	1056	1	INTERBUS.S03_ISL2018DO.Data
5	HR	Read	1057	1060	4	INTERBUS.S04_AI8AO8.Data
6	HR	Read	1061	1064	4	INTERBUS.S06_AO8.Data
7	HR	Read	1065	1068	4	INTERBUS.S07_AI8AO8.Data
8	HR	Read	1069	1072	4	INTERBUS.S08_AI8AO8.Data
9	HR	Read	1073	1076	4	INTERBUS.S09_AI8AO8.Data
10	HR	Read	1077	1077	1	INTERBUS.S10_ISL2028DO.Data
11	HR	Read	1078	1078	1	INTERBUS.S13_ISL2018DO.Data
12	HR	Read	1079	1079	1	INTERBUS.S14_ISL2018DO.Data
13	HR	Write	2000	2000	1	INTERBUS.S01_ISL2028DI.Data
14	HR	Write	2001	2004	4	INTERBUS.S04_AI8AO8.Data
15	HR	Write	2005	2005	1	INTERBUS.S05_ISL2028DI.Data
16	HR	Write	2006	2009	4	INTERBUS.S07_AI8AO8.Data
17	HR	Write	2010	2013	4	INTERBUS.S08_AI8AO8.Data
18	HR	Write	2014	2017	4	INTERBUS.S09_AI8AO8.Data
19	HR	Write	2018	2018	1	INTERBUS.S11_ISL2028DI.Data
20	HR	Write	2019	2019	1	INTERBUS.S12_ISL2028DI.Data
21	(End)					

Figure 8.29 – Modbus Summary CSV

8.8. MODBUS EXPANDED CSV

Slate 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 INTERBUS Router module configuration). To generate the Modbus Expanded CSV, right-click on the module (when online in Slate), and select *Export Modbus Expanded CSV*.

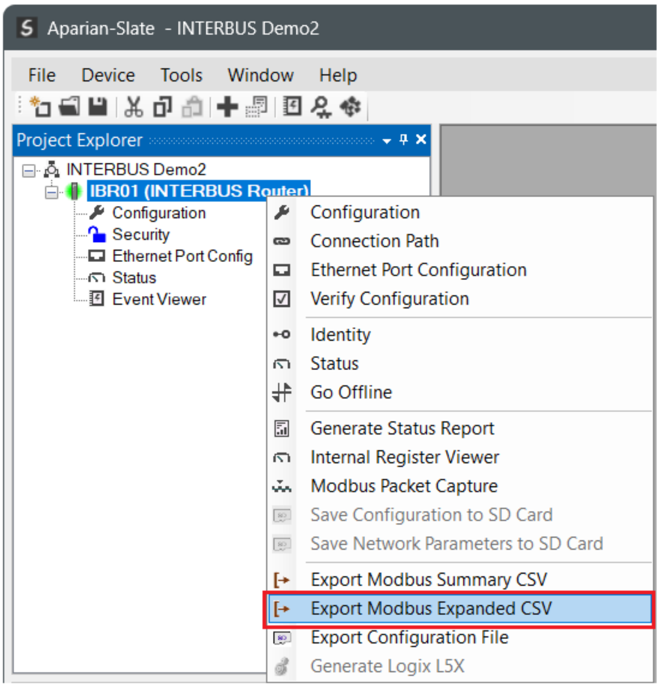


Figure 8.30 – Modbus Expanded Report Generation

	A	B	C	D	E	F
1	Reg Type	Modbus Function	Start Address	End Address	Element Count	Description
2	HR	Read	1000	1001	2	ModuleStatus.GeneralStatus
3	HR	Read	1002	1003	2	ModuleStatus.InterbusCycleTime
4	HR	Read	1004	1005	2	ModuleStatus.RxPcktCount
5	HR	Read	1006	1007	2	ModuleStatus.TxPcktUpdateCount
6	HR	Read	1008	1009	2	ModuleStatus.ChcksmErrCount
7	HR	Read	1010	1011	2	ModuleStatus.IdentPcktCount
8	HR	Read	1012	1013	2	ModuleStatus.DataPcktCount
9	HR	Read	1014	1015	2	ModuleStatus.UnknownCmdCount
10	HR	Read	1016	1017	2	ModuleStatus.IdleTimeoutCount
11	HR	Read	1018	1019	2	ModuleStatus.IdleStateChgCount
12	HR	Read	1024	1055	32	INTERBUS.S02_AO64.Data
13	HR	Read	1056	1056	1	INTERBUS.S03_ISL2018DO.Data
14	HR	Read	1057	1060	4	INTERBUS.S04_AI8AO8.Data
15	HR	Read	1061	1064	4	INTERBUS.S06_AO8.Data
16	HR	Read	1065	1068	4	INTERBUS.S07_AI8AO8.Data
17	HR	Read	1069	1072	4	INTERBUS.S08_AI8AO8.Data
18	HR	Read	1073	1076	4	INTERBUS.S09_AI8AO8.Data
19	HR	Read	1077	1077	1	INTERBUS.S10_ISL2028DO.Data
20	HR	Read	1078	1078	1	INTERBUS.S13_ISL2028DO.Data
21	HR	Read	1079	1079	1	INTERBUS.S14_ISL2018DO.Data
22	HR	Write	2000	2000	1	INTERBUS.S01_ISL2028DI.Data
23	HR	Write	2001	2004	4	INTERBUS.S04_AI8AO8.Data
24	HR	Write	2005	2005	1	INTERBUS.S05_ISL2028DI.Data
25	HR	Write	2006	2009	4	INTERBUS.S07_AI8AO8.Data

Figure 8.31 – Modbus Expanded CSV

8.9. INTERNAL REGISTER VIEWER

The module provides an Internal Register Viewer that allows the user to view the data registers in the Internal Data Space (IDS) and Modbus Registers.

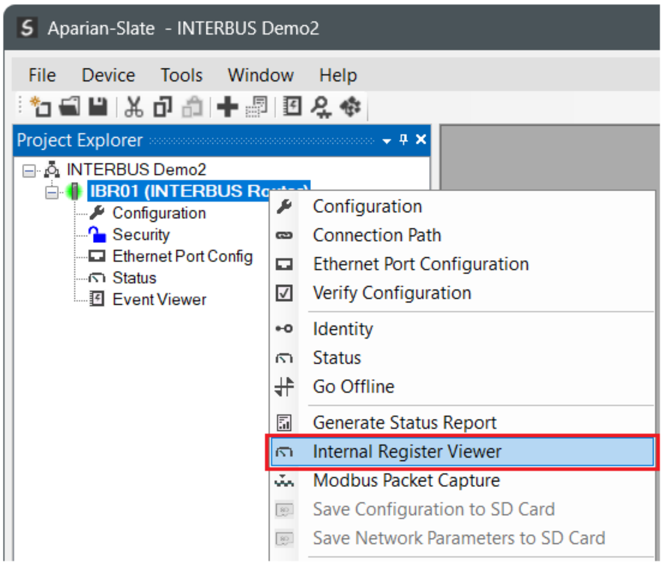


Figure 8.32 – Internal Register Viewer - Select

Once opened, the register type can be selected. Note that the Modbus Registers will only be available if the Primary Interface configured is for Modbus Server or Modbus Client.

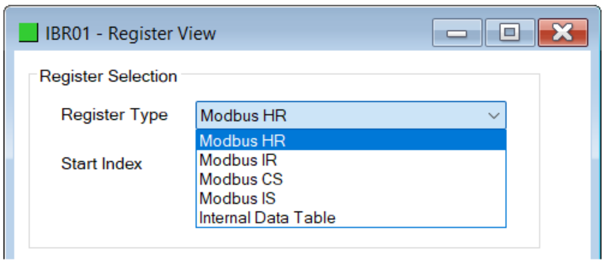


Figure 8.33 – Internal Register Viewer – Register Type

The Start and Stop Index can then be selected to determine how much data to display and refresh.

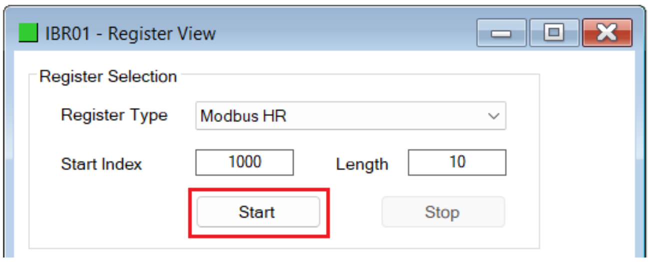
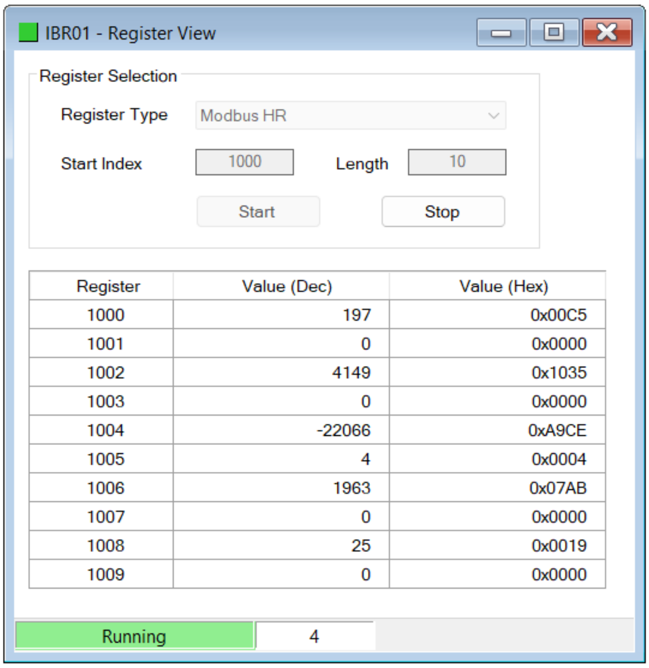


Figure 8.34 – Internal Register Viewer – Indexes

The data will appear and start refreshing by pressing the *Start* button.



Register	Value (Dec)	Value (Hex)
1000	197	0x00C5
1001	0	0x0000
1002	4149	0x1035
1003	0	0x0000
1004	-22066	0xA9CE
1005	4	0x0004
1006	1963	0x07AB
1007	0	0x0000
1008	25	0x0019
1009	0	0x0000

Figure 8.35 – Internal Register Viewer – Running

9. TECHNICAL SPECIFICATIONS

9.1. DIMENSIONS

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

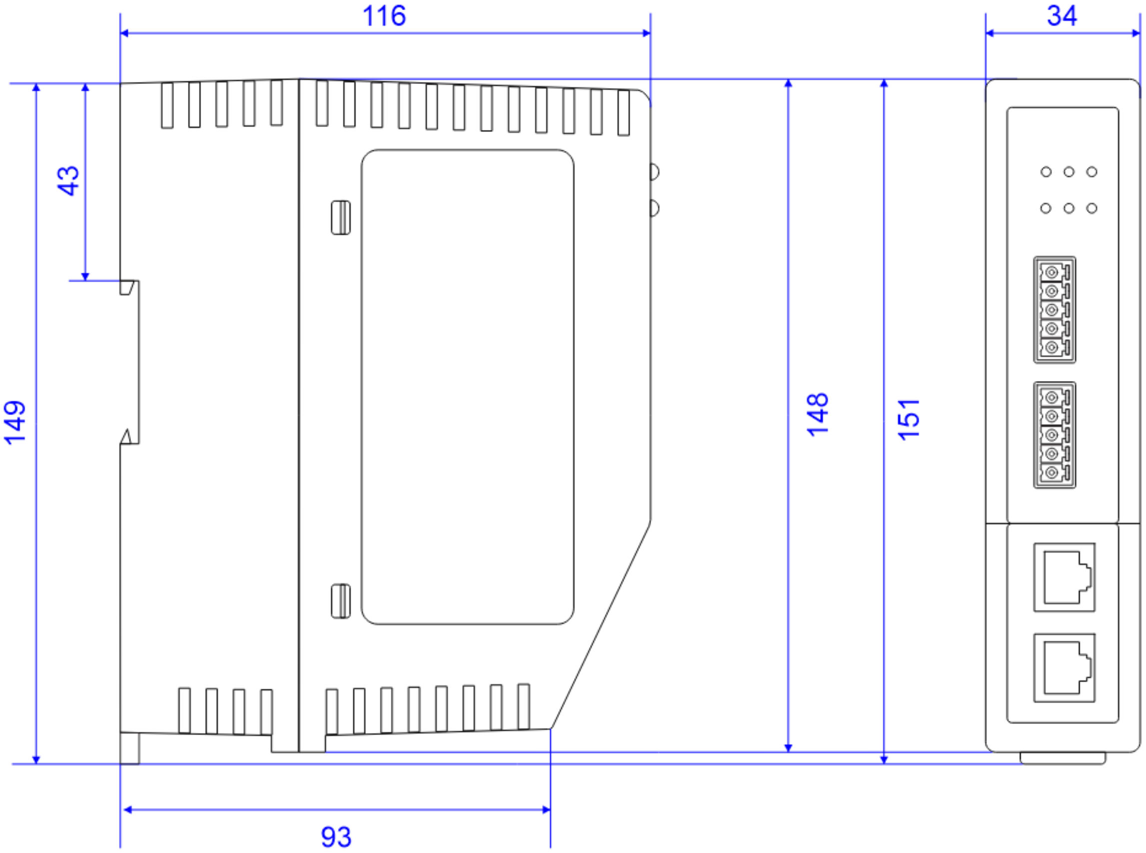


Figure 9.1 – INTERBUS Router enclosure dimensions

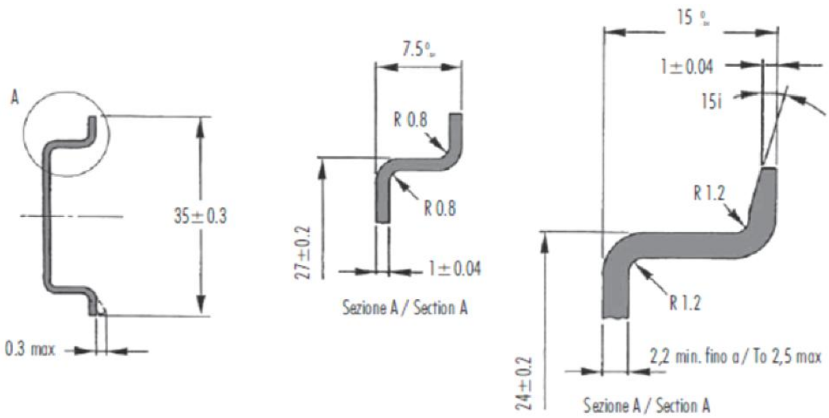


Figure 9.2 - Required DIN dimensions

9.2. ELECTRICAL

Specification	Rating
Power requirements	Input: 10 – 32 VDC (Class 2)
Power consumption	3.0 W (Max.) Current: 260 mA @ 10 V Current: 120 mA @ 24 V
Connector	3-way terminal
Conductors	24 – 18 AWG
Enclosure rating	IP20, NEMA/UL Open Type
Temperature	-20 – 70 °C
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 9.1 - Electrical specification

9.3. ETHERNET

Specification	Rating
Connector	RJ45
Conductors	CAT5 STP/UTP
ARP connections	Max 20
TCP connections	Max 20
CIP connections	Max 15
Communication rate	10/100Mbps
Duplex mode	Full/Half
Auto-MDIX support	Yes

Embedded switch	Yes, 2 x Ethernet ports
Device Level Ring (DLR)	Supported
Network Time Protocol (NTP)	Supported

Table 9.2 - Ethernet specification

9.4. INTERBUS PORTS

Specification	Rating
Connector	5-way terminal
Conductor	24 – 18 AWG
Electrical Isolation	1000 Vrms for 1 minute.

Table 9.3 – INTERBUS Port specification

9.5. INTERBUS

Specification	Rating
Type	Slave
Max. Device Count	15
Max. Total INTERBUS Data	128 bytes
Max. Summation Frame	128 bytes
Parameter Channel (PCP)	Not Supported
Supported BAUD Rates	500kbps, 2Mpbs

Table 9.4 – INTERBUS specification

9.6. ETHERNET/IP TARGET

Specification	Rating
Class 1 Cyclic connection count	4
Logix Direct-to-Tag Supported	Yes

Table 9.5 – EtherNet/IP Target specification

9.7. ETHERNET/IP ORIGINATOR

Specification	Rating
Class 1 Cyclic Connections Supported	Yes
Class 3 / UCMM Connections Supported	Yes
Class 1 Connection Count	15
Class 3 / UCMM Target Device Count	10
Class 3 / UCMM Mapping Count	50

Table 9.6 – EtherNet/IP Originator specification

9.8. MODBUS CLIENT

Specification	Rating
Modes Supported	Modbus TCP
Max. Modbus Server Devices	20
Max. Modbus Mapping	100
Mapping Ranges	Holding Register 0 – 4999 Input Register 0 – 4999 Input Status 0 – 4999 Coil Status 0 – 4999
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 9.7 – Modbus Client specification

9.9. MODBUS SERVER

Specification	Rating
Modes Supported	Modbus TCP

Mapping Ranges	Holding Register 0 – 4999 Input Register 0 – 4999 Input Status 0 – 4999 Coil Status 0 – 4999
Base Offset	Modbus (Base 0) PLC (Base 1)
Configurable Modbus TCP Port	Yes

Table 9.8 – Modbus Server specification

9.10. CERTIFICATIONS

Certification	Mark
CE Mark	
RoHS2 Compliant	
UL Mark File: E494895	CLASS 1, DIV 2, GROUPS A, B, C, D T4A
UKCA	
ATEX	II 3 G Ex ec IIC T4A -20°C ≤ Ta ≤ 70 °C **PENDING**
ODVA Conformance	**PENDING**

Table 9.9 – Certifications

10.INDEX