FANOX

Safely protected

SIC-A

Redbox, Gateway & Redundant Protocols Gateway

USER'S MANUAL

1. RECEPTION, HANDLING, INSTALLATION

1.1. Unpacking

Communication devices must only be handled by qualified personnel and special care must be taken to protect all of their parts from any damage while they are being unpacked and installed. The use of good illumination is recommended to facilitate the equipment visual inspection. The facility must be clean and dry and relays should not be stored in places that are exposed to dust or humidity. Special care must be taken if construction work is taking place.

1.2. Reception of gateways

It is necessary to inspect the equipment at the time it is delivered to ensure that the device have not been damaged during transport.
If any defect is found, the transport company and FANOX should be informed immediately.
If the devices are not for immediate use, they should be returned to their original packaging.

1.3. Handling electronic equipment

Gateways contain an electronic component that is sensitive to electrostatic discharges.
Just by moving, a person can build up an electrostatic potential of several thousand volts. Discharging this energy into electronic components can cause serious damage to electronic circuits. It is possible that this damage may not be detected straight away, but the electronic circuit reliability and life will be reduced. This electronic component in the equipment is well protected by the metallic housing, which should not be removed as the equipment cannot be adjusted internally.

1.4. Installation, commissioning and service

The personnel in charge of installing, commissioning and maintaining this equipment must be qualified and must be aware of the procedures for handling it. The product documentation should be read before installing, commissioning or carrying out maintenance work on the equipment.
In order to guarantee the security, do not connect the gateway directly to the internet. Deploy the device only within a secure network perimeter.
Before supplying the equipment the value of the rated voltage and its polarity must be checked.
The equipment must be used within the stipulated electrical and environmental limits.

1.5. Transportation and Storage

SIC-A in the manufacturers package should be carefully stored in dry places with ambient temperature from -40 to +85 °C and relative air humidity not more than 80%. Air should not contain any chemically aggressive vapors.
When transporting customer should provide suitable packing that would protect the SIC-A from any mechanical damages, serious drops and vibrations that may affect the device integrity.

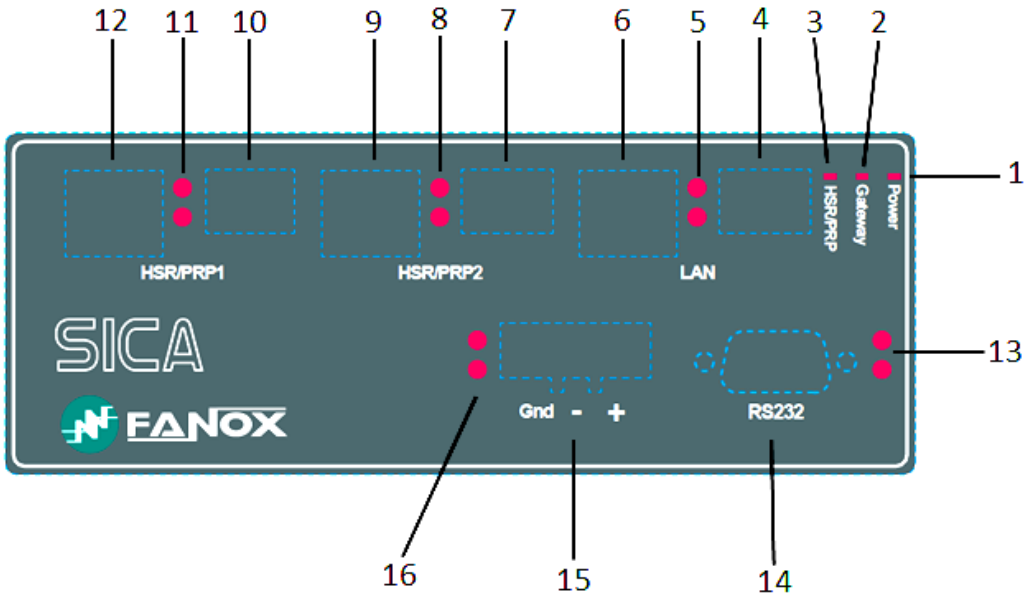
1.6. Recycling

All electrical power sources should be removed before performing this operation to avoid the risk of electrical discharge.
This product must be disposed of in a safe way. It should not be incinerated or brought into contact with water sources like rivers, lakes, etc…

2. DIMENSIONS AND CONNECTION DIAGRAMS

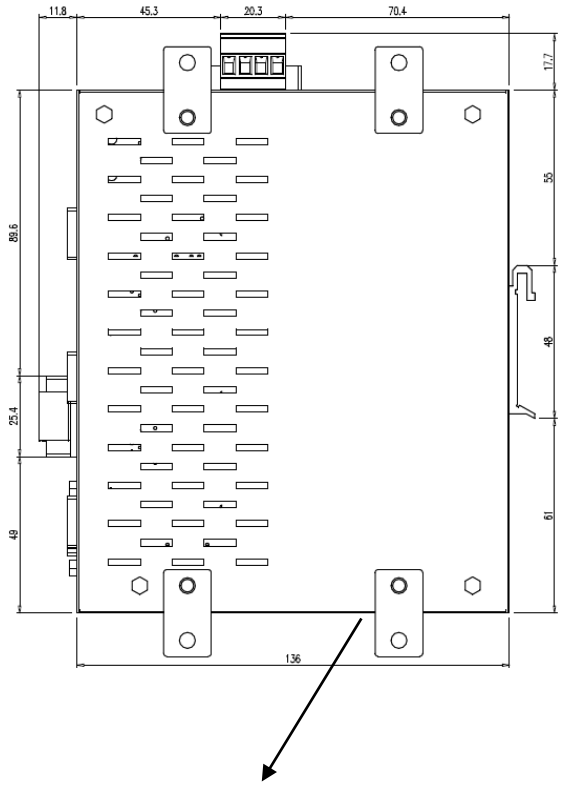
2.1. Dimensions and connection diagrams – Adaptation A

2.1.1. Equipment front view

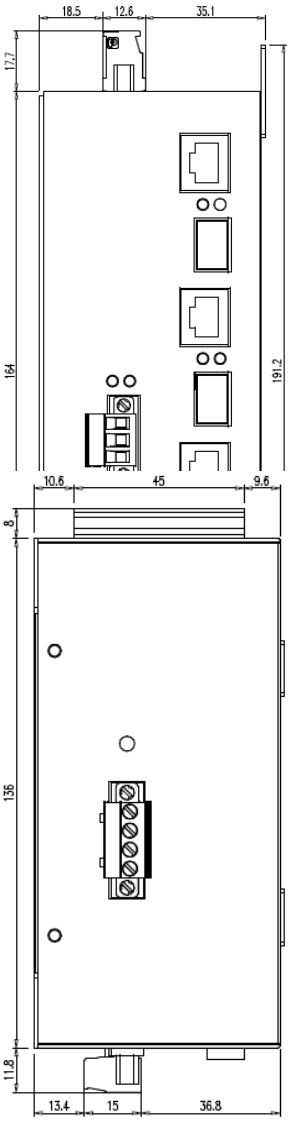


1. POWER – red LED, lit when the power supply is connected.
2. GATEWAY – green LED, lit when the device is working as a Gateway.
3. HSR/PRP– green LED, lit when the device is using PRP or HSR redundancy.
4. SFP LC LAN port – Fiber port to connect the device to a network without redundancy.
5. LINK and ACTIVITY LEDs of the LAN ports.
    - These are common LEDs for RJ45 LAN port and SFP LC LAN port.
    - Both ports do not work at the same time, if SFP is inserted, RJ45 port will be disabled
6. RJ45 LAN port – Electrical port to connect the device to a network without redundancy.
7. RJ45 port 2 for HSR/PRP redundancy – Electrical port to connect the device to an extreme of the redundant network.
8. LINK and ACTIVITY LEDs of the Redundant ports 2.
    - These are common LEDs for RJ45 HSR/PRP port 2 and SFP LC HSR/PRP port 2.
    - Both ports do not work at the same time, if SFP is inserted, RJ45 port will be disabled
9. SFP LC port 2 for HSR/PRP redundancy – Fiber port to connect the device to an extreme of the redundant network.
10. RJ45 port 1 for HSR/PRP redundancy – Electrical port to connect the device to an extreme of the redundant network.
11. LINK and ACTIVITY LEDs of the Redundant ports 1.
    - These are common LEDs for RJ45 HSR/PRP port 1 and SFP LC HSR/PRP port 1.
    - Both ports do not work at the same time, if SFP is inserted, RJ45 port will disabled
12. SFP LC port 1 for HSR/PRP redundancy – Fiber port to connect the device to an extreme of the redundant network.
13. Tx and Rx LEDs of the serial RS-232 port.
14. RS-232 port – Serial port to perform a protocol conversion from a local device.
15. RS-485 port – Serial port to perform a protocol conversion from a multidrop network.
16. Tx and Rx LEDs of the serial RS-485 port.

2.1.2. Equipment dimensions



Mount adapters Optional

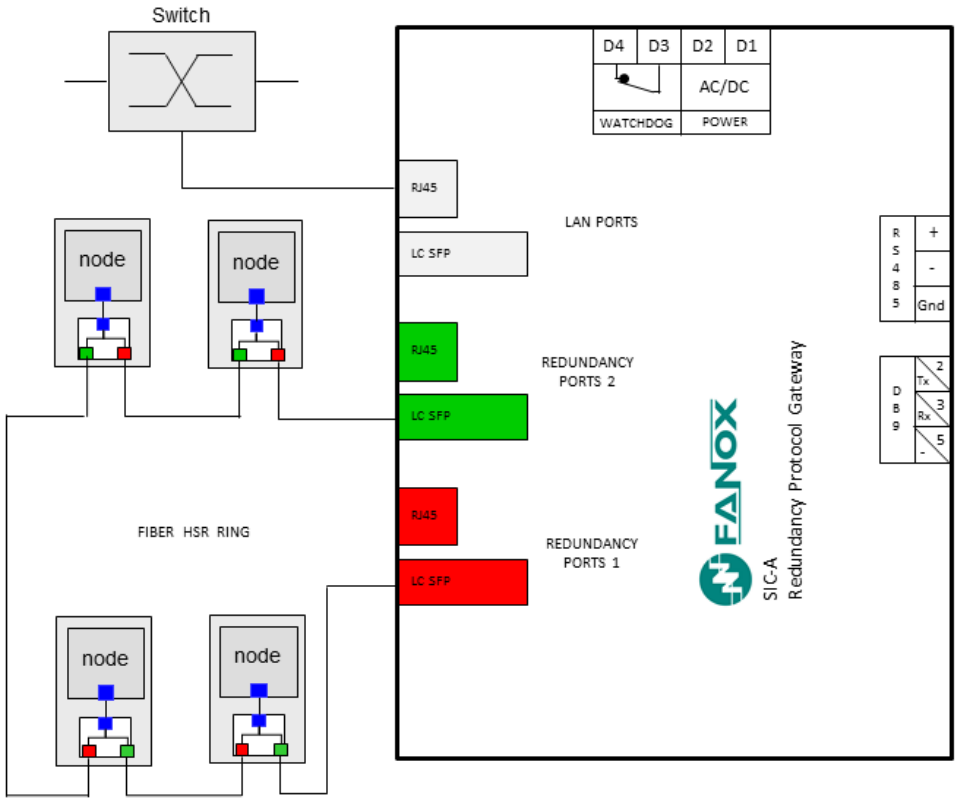


2.1.3. Connection diagrams

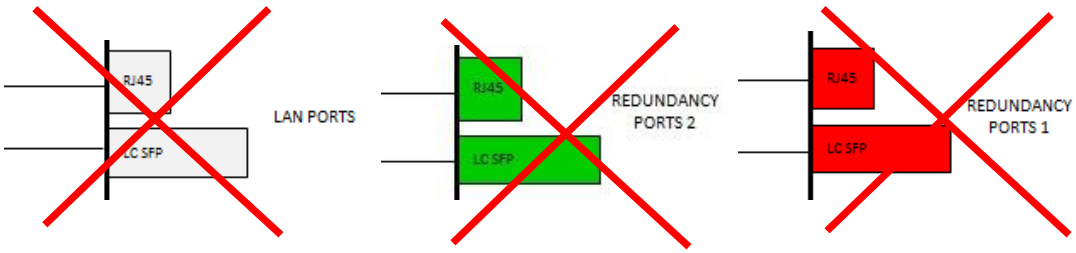
SIC-A communication device could perform different functions for different applications. The connection of the equipment would vary depending the application.

2.1.3.1 SIC-A working as a Redbox

Using SIC-A device as a Redbox, serial ports are disabled.



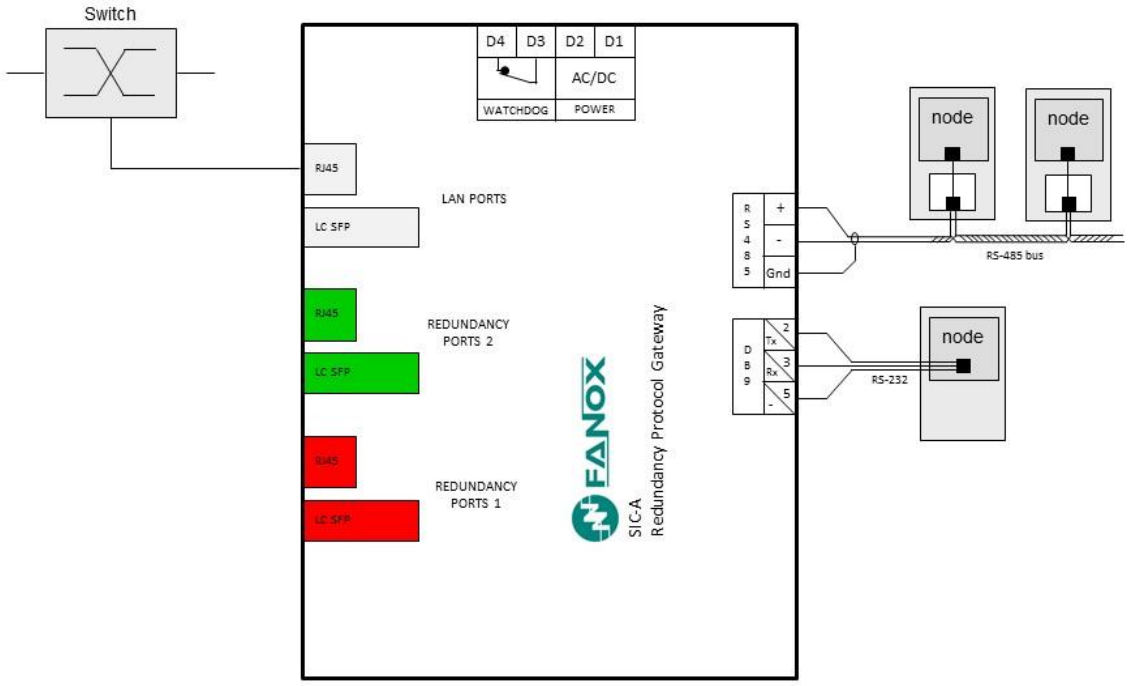
The connection to a port shall be to the SFP Fiber connector or to the RJ45 connector, never to both at the same time:



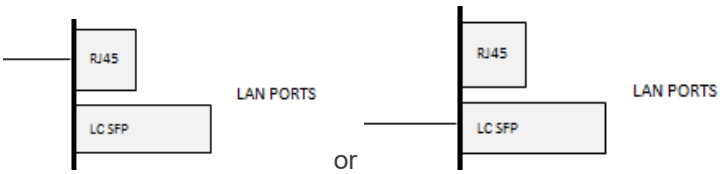
If a SFP transceiver is connected, the RJ45 connector disables.

2.1.3.2 SIC-A working as a Protocol Gateway

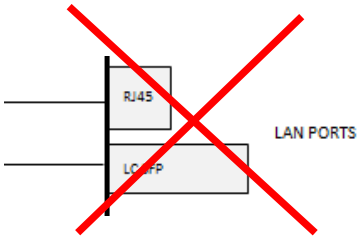
Using SIC-A device as a Protocol Gateway, Redundant ports are disabled.



The connection to the LAN port shall be to the SFP Fiber connector or to the RJ45 connector, never to both at the same time.



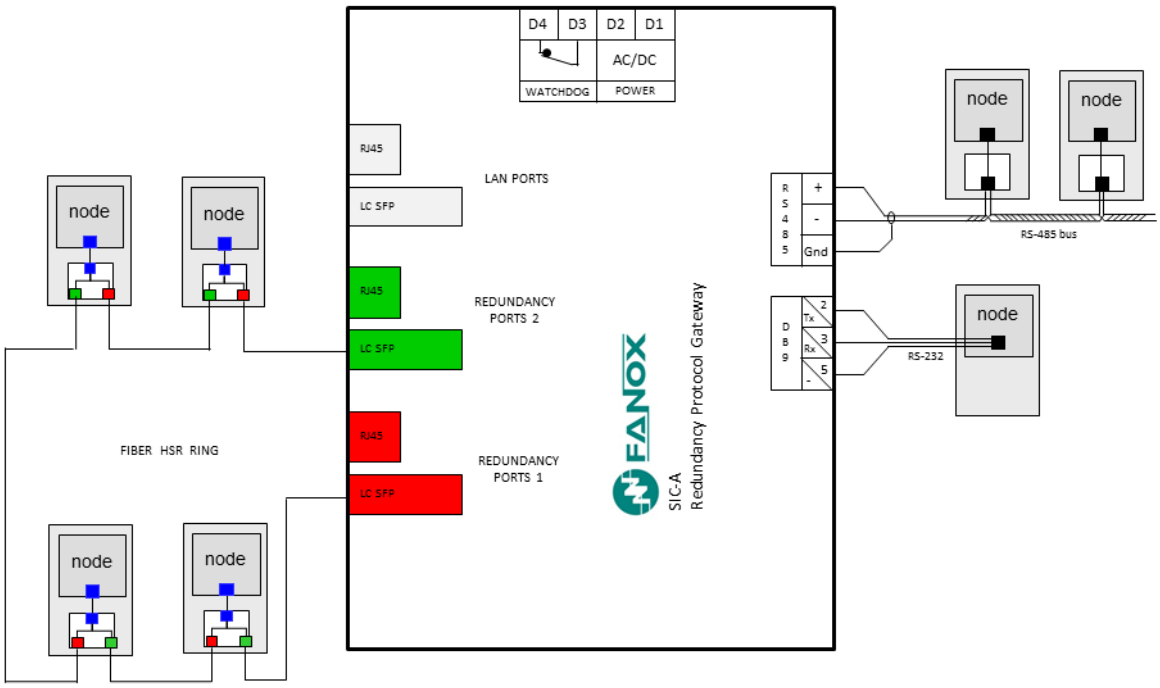
never



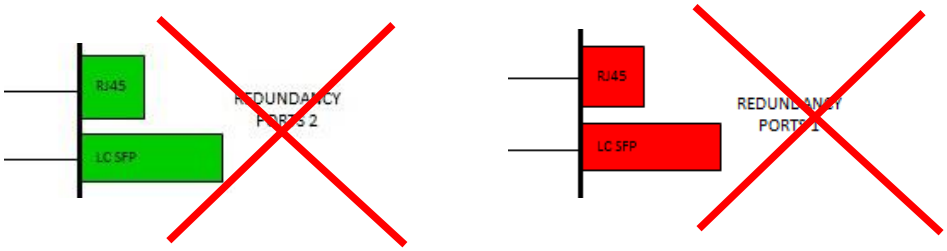
If a SFP transceiver is connected, the RJ45 connector disables.

2.1.3.3 SIC-A working as a Redundant Protocol Gateway

Using SIC-A device as a Redundant Protocol Gateway, LAN ports is disabled

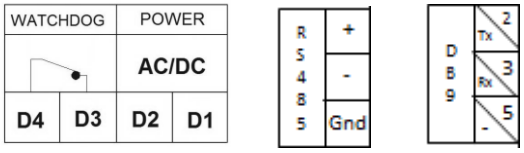


The connection to a port shall be to the SFP Fiber connector or to the RJ45 connector, never to both at the same time:



If a SFP transceiver is connected, the RJ45 connector disables.

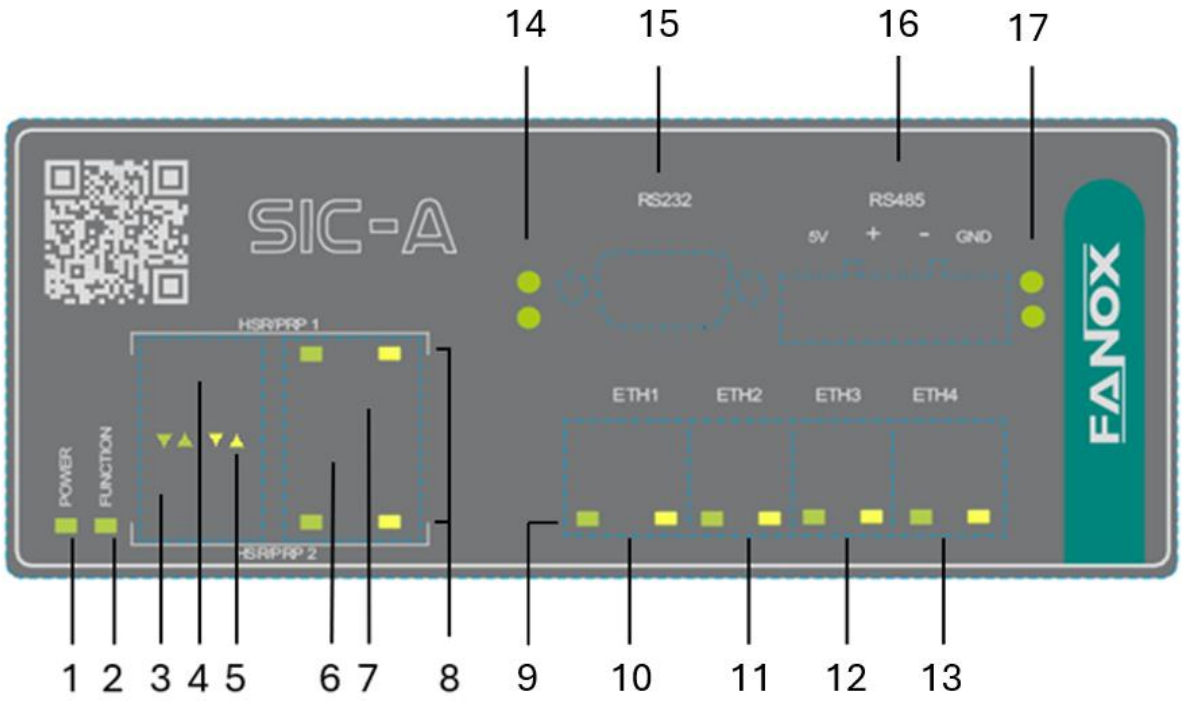
2.1.4. Terminals



D1-D2	Auxiliary Voltage
D3-D4	Watchdog output NC
+	RS-485 +
-	RS-485 -
Gnd	RS-485 Ground
⏚	Earthing screw

2.2. Dimensions and connection diagrams – Adaptation B

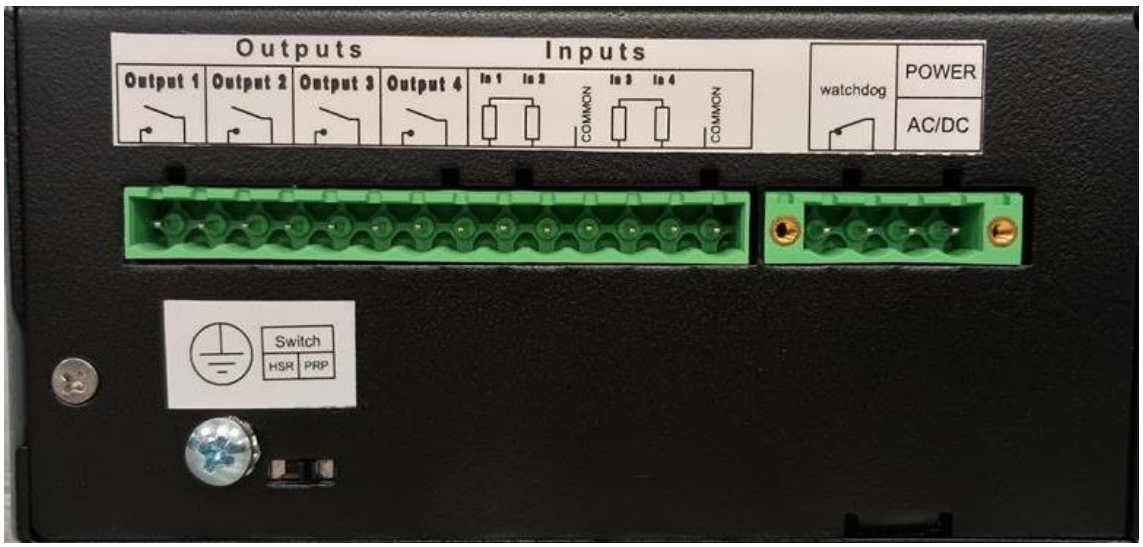
2.2.1. Equipment front view



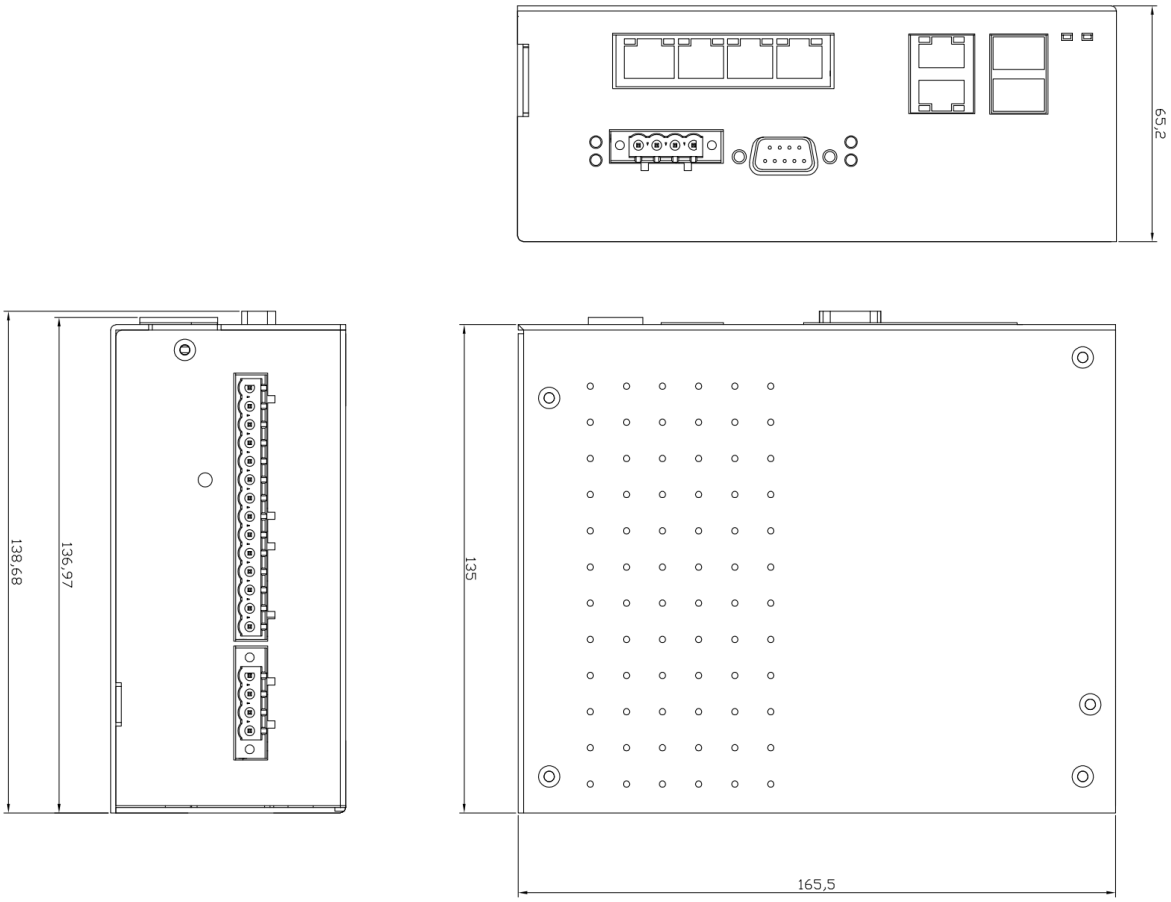
1. POWER – red LED, lit when the power supply is connected.
2. FUNCTION – green LED, lit when the device is working as a Gateway. Red LED, lit when the device is working as a Redbox. Orange LED, lit when the device is working as a Redundant Gateway.
3. SFP LC port 1 for HSR/PRP redundancy – Fiber port to connect the device to an extreme of the redundant network.
4. SFP LC port 2 for HSR/PRP redundancy – Fiber port to connect the device to an extreme of the redundant network
5. LINK and ACTIVITY LEDs of the SFP LC Redundant ports .
    - RJ45 HSR/PRP and SFP LC HSR/PRP ports do not work at the same time, if SFP is inserted, RJ45 port will be disabled.
6. RJ45 HSR/PRP port 1 – Electrical port to connect the device to an extreme of the redundant network.
7. RJ45 HSR/PRP port 2 – Electrical port to connect the device to an extreme of the redundant network.
8. LINK and ACTIVITY LEDs of the RJ45 HSR/PRP Redundant ports.
9. LINK and ACTIVITY LEDs of the RJ45 LAN ports
10. RJ45 LAN port 1 – Electrical port to connect the device to a network without redundancy.
11. RJ45 LAN port 2 – Electrical port to connect the device to a network without redundancy.
12. RJ45 LAN port 3 – Electrical port to connect the device to a network without redundancy.
13. RJ45 LAN port 4 – Electrical port to connect the device to a network without redundancy.

14. Tx and Rx LEDs of the serial RS-232 port.
15. RS-232 port – Serial port to perform a protocol conversion.
16. RS-485 port – Serial port to perform a protocol conversion from a multidrop network.
17. Tx and Rx LEDs of the serial RS-485 port.

2.2.2. Equipment side view



2.2.3. Equipment dimensions

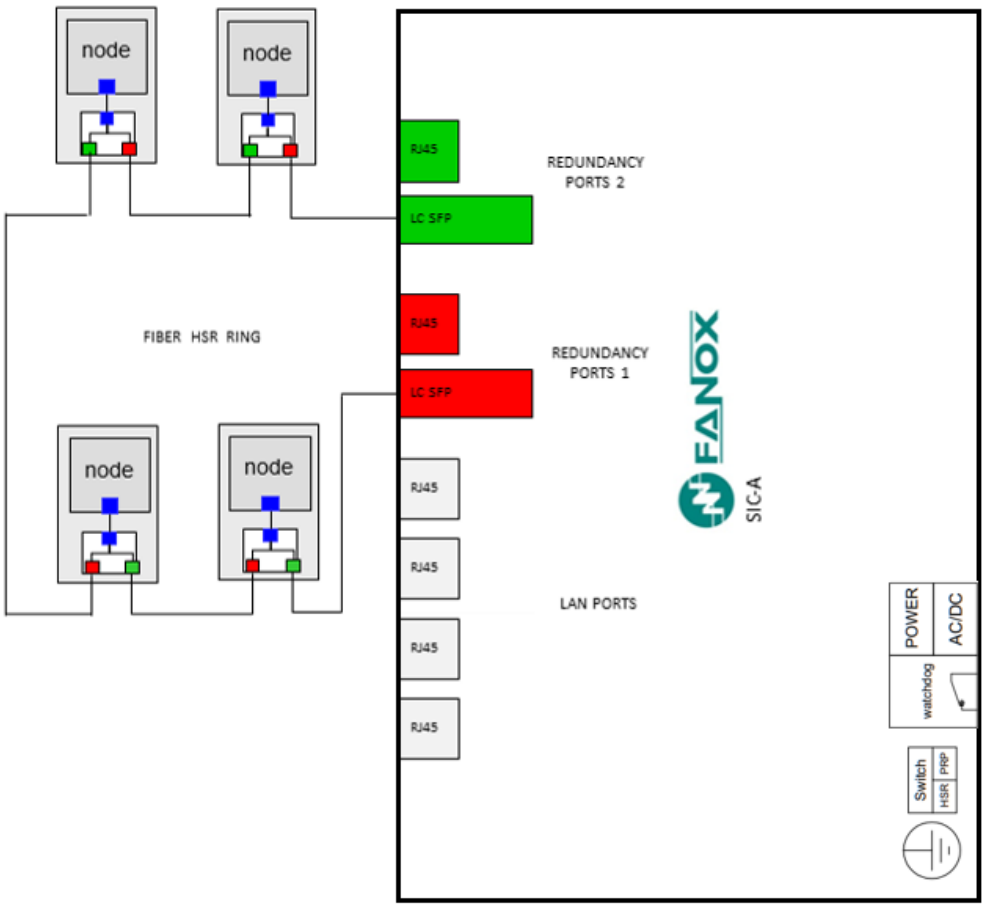


2.2.4. Connection diagrams

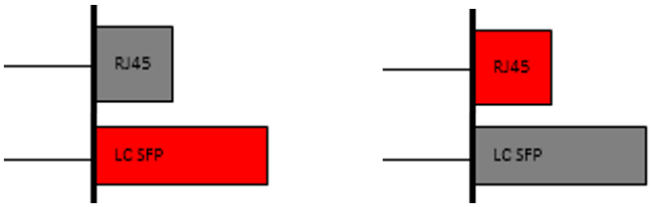
SIC-A communication device could perform different functions for different applications. The connection of the equipment would vary depending the application.

2.2.4.1. SIC-A working as a Redbox

Using SIC-A device as a Redbox, serial ports, inputs and outputs are disabled.



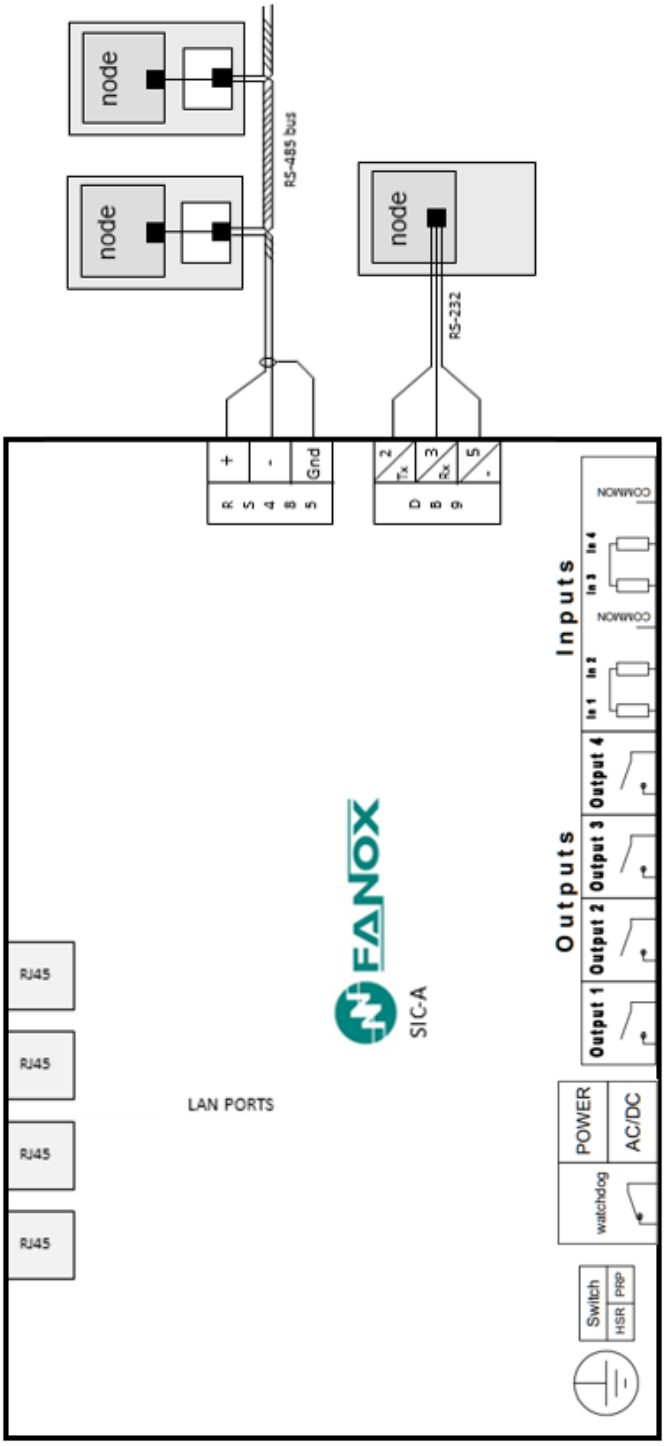
The connection to a port shall be to the SFP Fiber connector or to the RJ45 connector, never to both at the same time:



For each redundancy port, if a SFP transceiver is connected, the RJ45 connector disables.

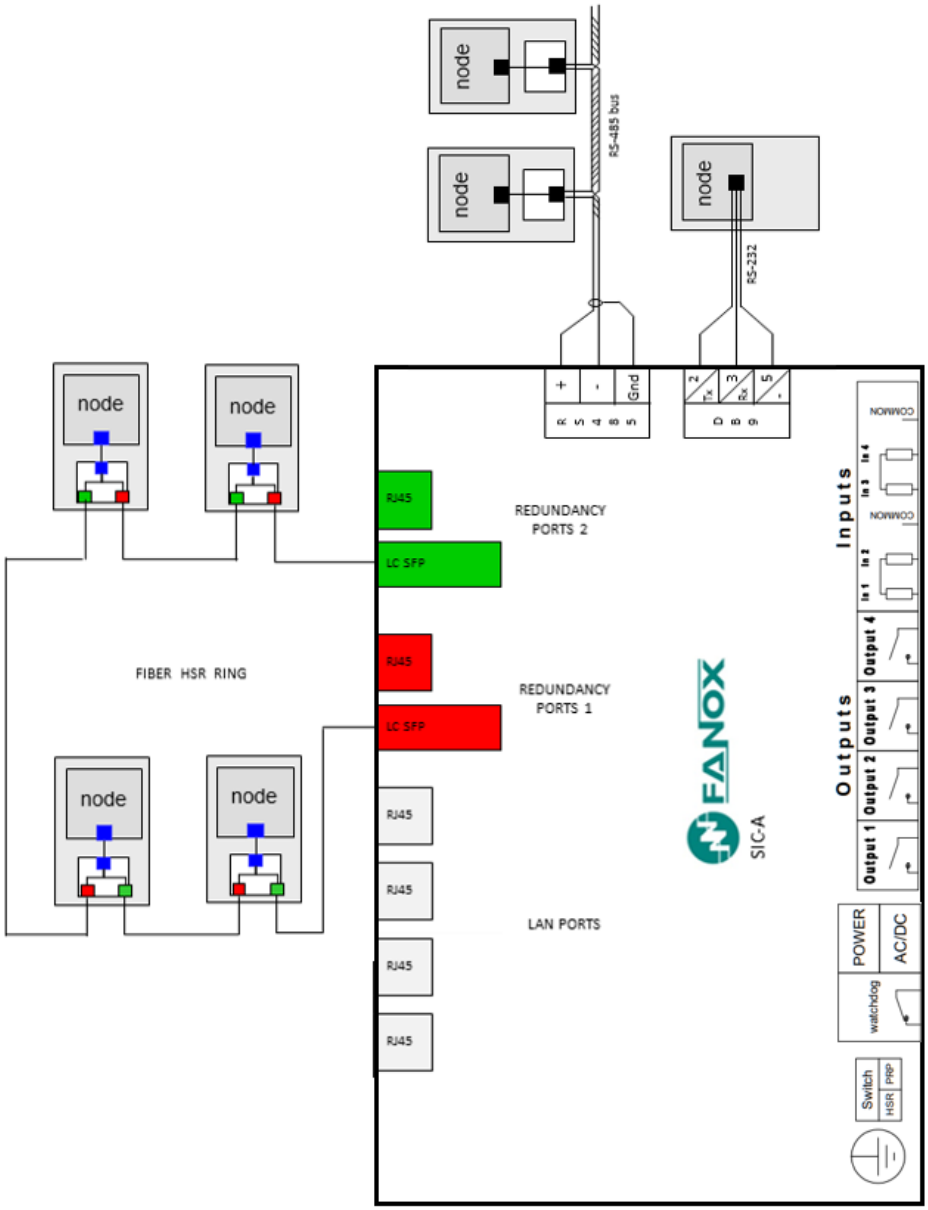
2.2.4.2. SIC-A working as a Protocol Gateway

Using SIC-A device as a Protocol Gateway, Redundant ports are disabled.

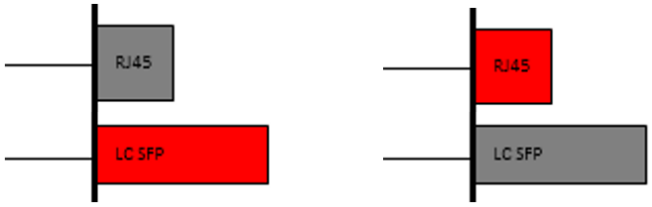


2.2.4.3. SIC-A working as a Redundant Protocol Gateway

Using SIC-A device as a Redundant Protocol Gateway, all ports are enabled

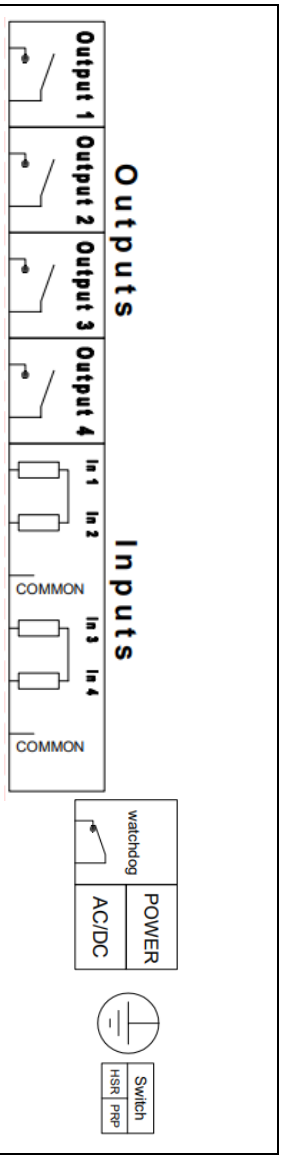


The connection to a port shall be to the SFP Fiber connector or to the RJ45 connector, never to both at the same time:



For each redundancy port, if a SFP transceiver is connected, the RJ45 connector disables.

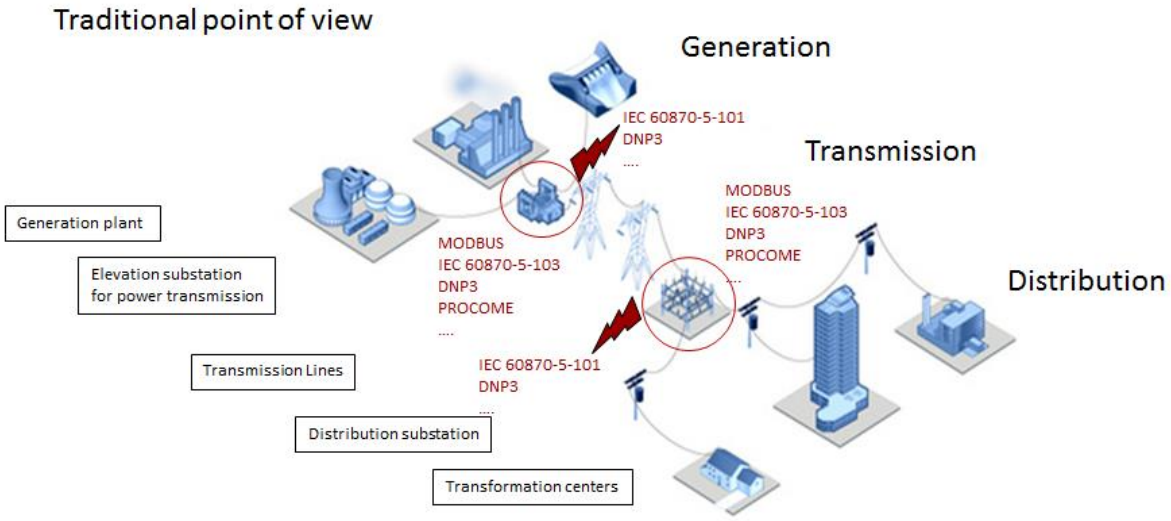
2.2.5. Terminals

Output 1 common	
Output 1 NO contact	
Output 2 common	
Output 2 NO contact	
Output 3 common	
Output 3 NO contact	
Output 4 common	
Output 4 NO contact	
Input 1	
Input 2	
Input 1 and input 2 common	
Input 3	
Input 4	
Input 3 and input 4 common	
Watchdog common	
Watchdog NC contact	
AC/DC Auxiliary Voltage	
AC/DC Auxiliary Voltage	
Ground connection screw	
Redundancy Mode Selector Switch Mode HSR	
Redundancy Mode Selector Switch Mode PRP	

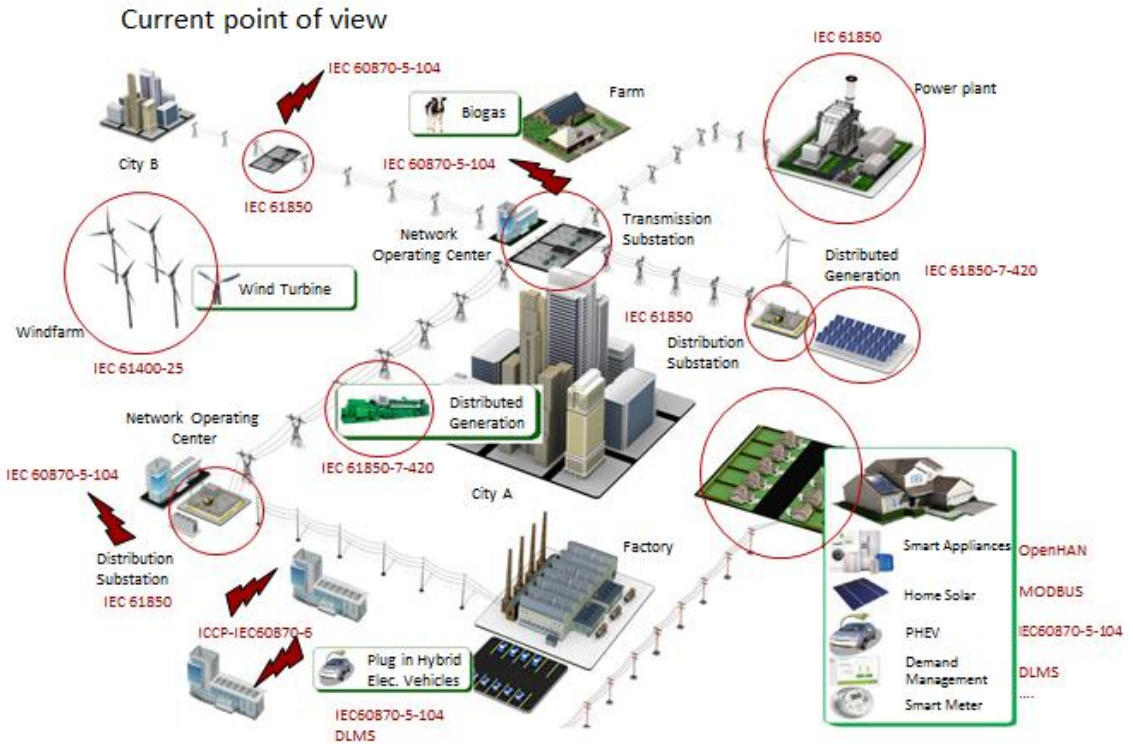
3. DESCRIPTION

3.1. Introduction

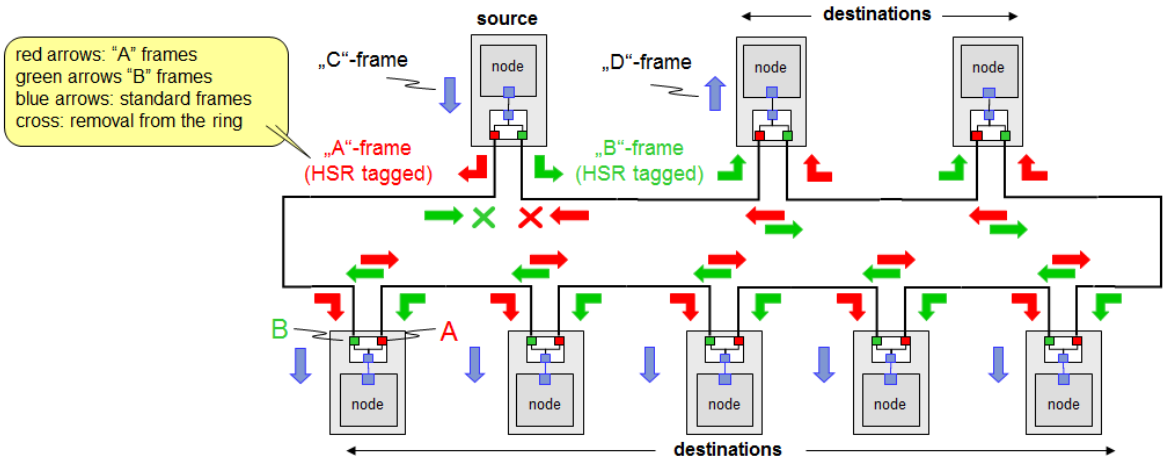
Industrial company management is gradually increasing its use of information technology and communication as the basis for predictive maintenance and monitoring of their facilities.
This ever increasing technology implies a technological leap for industries, as it requires the handling of a larger amount of data, and in many occasions in real time.
To implement these new technologies the industries require simple, flexible systems which adapt to the specific requirements of the same.
Protocol Gateways provide a simple way to adapt the existing equipment in an installation to the actual new technologies.
The traditional point of view of the Power sector was focused on a lineal generation, transmission and distribution of the energy, where the communications were limited to the substations. The equipment in substation shared their information on site and with a control center using serial protocols where the information was limited, unsecure and with long latency times.



With the evolution of the 'Smart Grid' concept, the generation of energy was not limited to punctual generation points. A vast radial infrastructure requires an advanced communication infrastructure with the last Ethernet protocols and in most cases redundant protocols.



The redundancy in communications is required when information lost is not acceptable. Redundancy methods have evolved from the basic method of equipment duplication to the most advanced redundancy protocol as HSR.
The HSR principle is as follows:



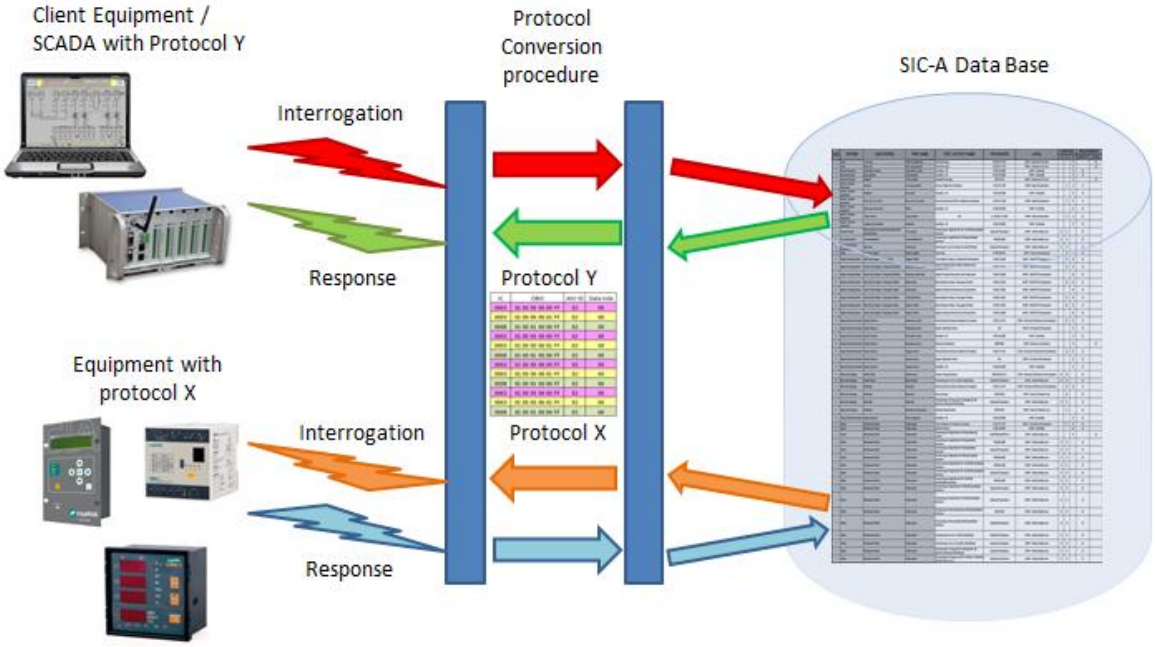
Nodes are arranged as a ring, each node has two identical interfaces, port A and port B.
For each frame to send ("C"-frame), the source node sends two copies over port A and B.
The source node removes the frames it injected into the ring.
Each node relays a frame it receives from port A to port B and vice-versa, except if already forwarded.
The destination nodes consumes the first frame of a pair ("D-frame") and discards the duplicate.
If the ring is broken, frames still arrive over the intact path, with no impact on the application.
Loss of a path is easily detected since duplicates cease to come.

3.2. Description

SIC is the denomination for the communication family products that complements the range of Fanox equipment for primary and secondary distribution.

SIC-A provide any-to-any protocol conversion that permit the integration of equipment with proprietary and legacy protocols in a modern infrastructure with the most recent protocols and redundant topologies.
SIC-A can work as a multi-protocol conversor, as an unmanaged Redbox or as a redundant protocol gateway.

The conversion 'concept' is based on a process that works as a Protocol X Master requesting data from devices with protocol X communications and stores this data to the SIC-A's data base. On the other side, there is another process that works as a Protocol Y Slave that responses the requests of a device with protocol Y, using the data that is in the data base of the gateway.



SIC-A can manage upto 3000 data points of the most common protocols (Modbus, IEC 60870, DLMS, DNP3,…) or upto 800 data points of advanced protocols as IEC 61850.
The number of equipment is not limited but it is recommended connecting no more than 10 devices to the serial RS-485.
For instance, if it is required converting data from 10 Modbus relays to IEC 61850, the calcs are as follows:
800/10= 80, Upto 80 Modbus data points per relay can be converted to IEC61850

For instance, if it is required converting data from 10 Modbus relays to DNP3, the calcs are as follows:
3000/10= 300, Upto 300 Modbus data per relay can be converted to DNP3

3.3. Selection & Ordering codes

SIC-A

Redundancy Protocols Gateway (PRP/HSR)

1 2 3									**FUNCTION** Redbox Gateway Redundant Protocol Gateway
	A B								**POWER SUPPLY** 24-48 Vdc 110-230 Vac/Vdc
		0							**ETHERNET PORT** 4xRJ45
			0 1						**REDUNDANT PORT** N/A (“For Gateway application”) RJ45 + SFP** Cage (“For Redbox and Redundant gateway application”)
				A B					**SERIAL PORTS** N/A (For Redbox application) RS232 (DB9) + RS485 (Terminal)
					0 1 2				**REDUNDANCY TYPE** N/A HSR PRP
						A B C D E F G H 2			**MASTER / CLIENT PROTOCOL** None Modbus IEC 60870-5-103 DNP3.0 IEC 60870-5-101 DLMS/COSEM IEC 61850 IEC 60870-5-104 Several Protocols
							A B C D E F G 2		**SLAVE / SERVER PROTOCOL** None IEC 61850 DNP3.0 IEC 60870-5-104 Modbus DLMS/COSEM IEC 60870-5-101 Several Protocols
								B	**ADAPTATION** -

Example of ordering code:

2	B	0	0	B	0	B	C	B	SIC A 2 B 0 0 B 0 B C B
SIC-A									

* SIC-A Gateway using FO will require a minimum voltage supply of 48 Vdc for its correct working

[1]The SFP for FO should be included by the user

4. FUNCTIONS AND FEATURES

4.1. List of Abbreviations

ARP – Address Resolution Protocol
CHAP – Challenge-Handshake Authentication Protocol
DCCP – Diagnostic and Converter Configuration Protocol
DPI – Dots Per Inch
EDGE – Enhanced Data rates for Global Evolution
GPC – Generic Protocol Conversion
GPRS – General Packet Radio Service
HSB Hot-Standby
HSR High-availability Seamless Redundancy
IP – Internet Protocol
LED – Light Emitting Diode
PAP – Password Authentication
PPP – Point to Point Protocol
PRP – Parallel Redundancy Protocol
RAM – Random Access Memory
SG – Shielded Ground
SNMP – Simple Network Management Protocol
UDP – User Datagram Protocol
VPN – Virtual Private Network
XML – Extensible Markup Language

4.2. General information

The equipment's general specifications are as follows:

Item	Unit	Value
Purpose of device	-	Protocol Gateway – Redbox – Protocol Redundant Gateway
Assembly (mounting) type	-	Mounted on standard 35 mm DIN bar and Wall mounting
Protection degree	-	IP20
Operating temperature range	°C	-40 to +85
Consumption	W	6 maximum
Auxiliary Power	Vdc/Vac	24*-110 / 48-230 ±20%
Weight	Kg	1
Diameter of adapters on terminals	mm^2	0.5-2.5

* SIC-A Gateway using optical fiber will require a minimum voltage supply of 48Vdc for its correct working

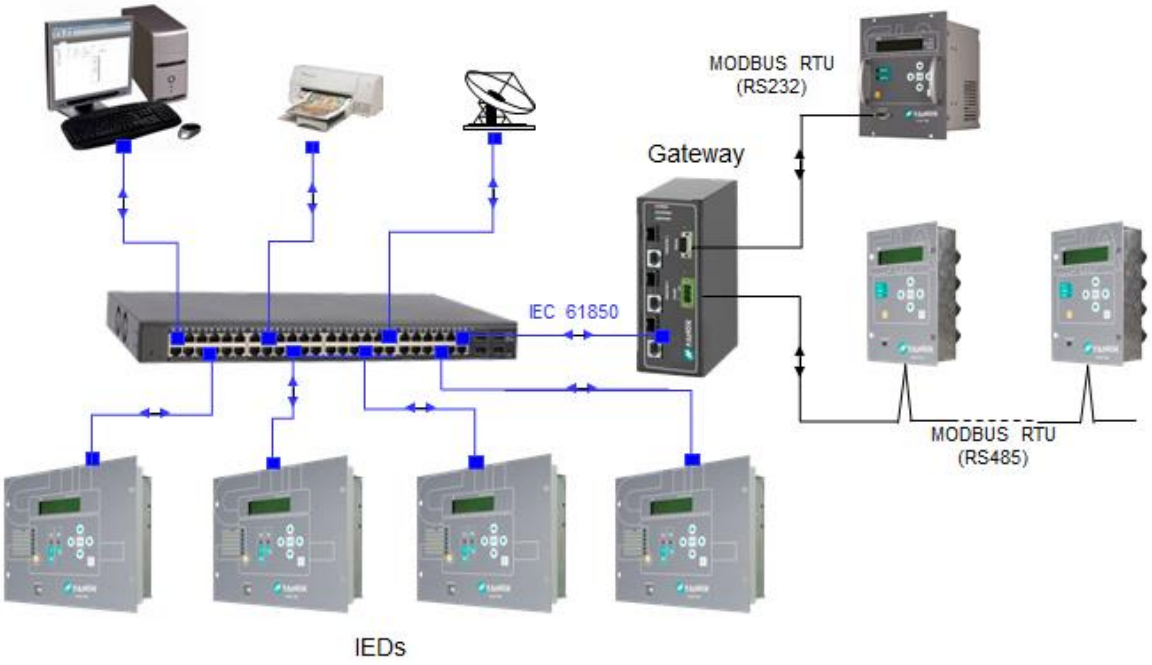
4.3. Main technical specifications

Main specifications	
Management	EasyConnect Configuration utility
System Protocols	TCP/IP, UDP/IP, SMTP, POP, HTTP, FTP, SNMP, ICMP, DHCP, BOOTP, Telnet, DNS, ARP, PPPoE, DDNS
Device Security	NERC/CIP Compliant, SSHv2
Communication Security	SSL based VPN tunnel using Blowfish/AES/3DES
Logic Programming	AND/OR/NOT/Bit SHIFT/Split/Index support for digital and analog data, Delay operations
Network Management	SNMP Agent
Protocol Support	IEC 60870-5-101/103/104, DNP3 serial/TCP, Modbus RTU/ASCII/TCP, IEC 62056-DLMS, IEC 61850, IEC 61400
Supported Data Point	IEC 61850: 800
	DNP3, IEC 60870, Modbus and other proprietary protocols: 3000
Devices Supported	20 (10 over serial RS-485 recommended)
Serial interfaces	1 or 2 RS-485 - Terminals and/or 1 or 2 RS-232- DB9 *
Ethernet interfaces	1 RJ45 or 1 LC SFP 100Base-FX 1300nm *
HSR/PRP interfaces**	2 RJ45 or 2 LC SFP 100Base-FX 1300nm *
Time Synchronization	NTC/SNTP/MEA, Protocol Specific (IEC 104,/DNP3, etc.) RTC on-board
Redundancy**	Unmanaged. Compliant implementation of both PRP (IEC 62439-3-4) and HSR (IEC 62439-3-5).

* Model dependent
** Redundant functionality and redundant ports will be disabled if SIC-A**2** model is selected

5. SIC-A WORKING AS A PROTOCOL GATEWAY

SIC-A device working as a protocol gateway, allows to integrate equipment with different protocols into a communication bus with another protocol.
Supports many to many protocol conversion that permits to achieve multiple configurations. Not only from serial protocols to Ethernet ones but between serial protocols.



SIC-A is based on the powerful of Kalkitech' s protocol gateways.
The complete configuration of SIC-A is done through a configuration utility software called EasyConnect, which includes defining protocol attributes, mapping data and achieving the functionalities like firmware updating, IP setting, diagnostics.

The associated SYNC model of **SIC-A** is **SYNC 241** under SYNC200 series: IED Upgrade card.
The whole configuration of SIC-A should be performed taking into account the **SYNC241** model.
EasyConnect generates a configuration file in Extensible Markup Language (XML) format as the output. User can download **the configuration file using the download function in EasyConnect for configuring the hardware** gateway.

5.1. Getting Started

This section familiarizes you with SIC-A and EasyConnect and gives step-by-step instructions to get started with SIC-A and EasyConnect. This section covers the following topics:

Installing EasyConnect
Removing EasyConnect
Starting EasyConnect
Exiting EasyConnect
Using the EasyConnect interface

5.1.1. Installing EasyConnect

To install EasyConnect perform the following steps:

1. Double-click the **EasyConnect** icon.
   The Welcome window appears.
2. Click **Next**.
   The Choose Destination Location **window appears.**
3. Click **Next**.
   The Setup Complete window appears.

5.1.2. Removing EasyConnect

You can remove all the installed contents of EasyConnect from your system.
To remove EasyConnect perform the following steps:

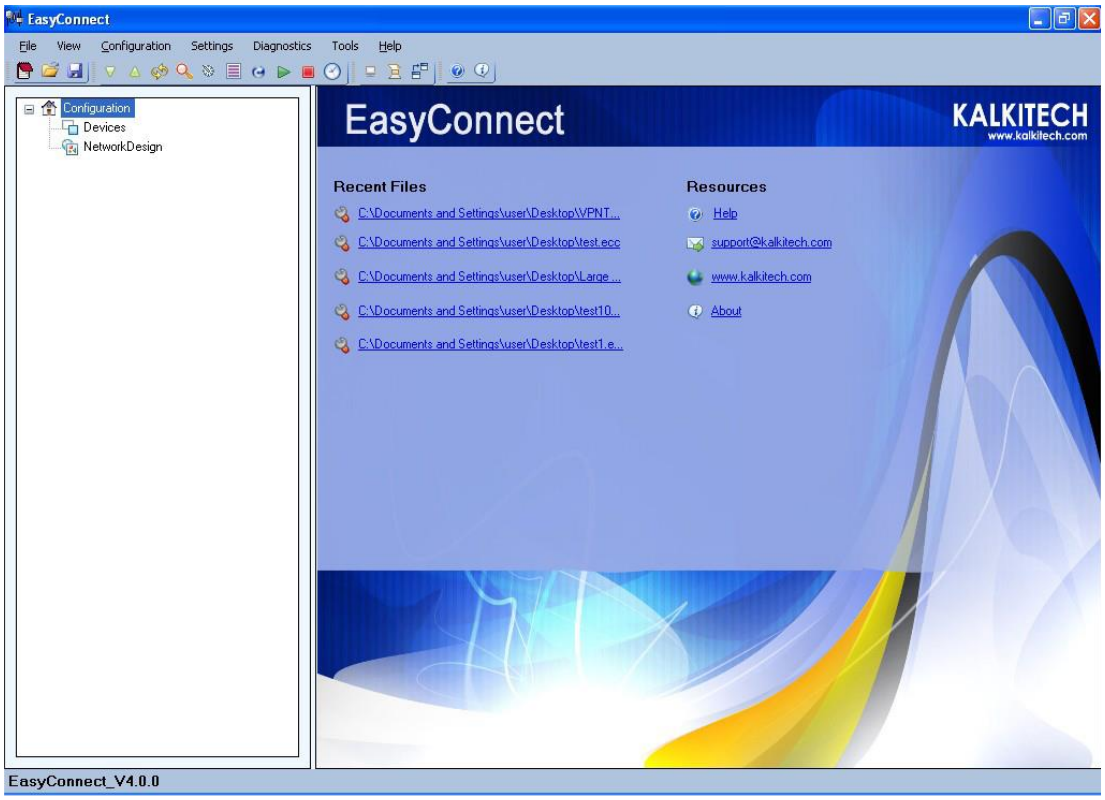
1. From **Start** menu, choose **Settings**, the corresponding window will get displayed. Choose
   Control Panel from the window, the **Control Panel** window get displayed. Select **Add** or **Remove** program.
2. From the program list in the Add or Remove Programs window, choose EasyConnect.
3. Click Change/Remove.
   The **Confirm File Deletion** window appears.
4. On the **Confirm File Deletion** window, click **Yes**.
   The uninstall shield wizard removes all components from your system.
5. On the uninstall shield wizard, Click **OK**.

5.1.3. Starting EasyConnect

EasyConnect helps you to configure files. You have to download the configured file to the SIC-A before running it. To access EasyConnect, as a first step, you have to start the EasyConnect..

From Start menu, choose Programs, the corresponding window will get displayed. Choose Kalkitech, the corresponding window will get displayed, Choose EasyConnect.

The EasyConnect user interface appears:



5.1.4. Exiting EasyConnect

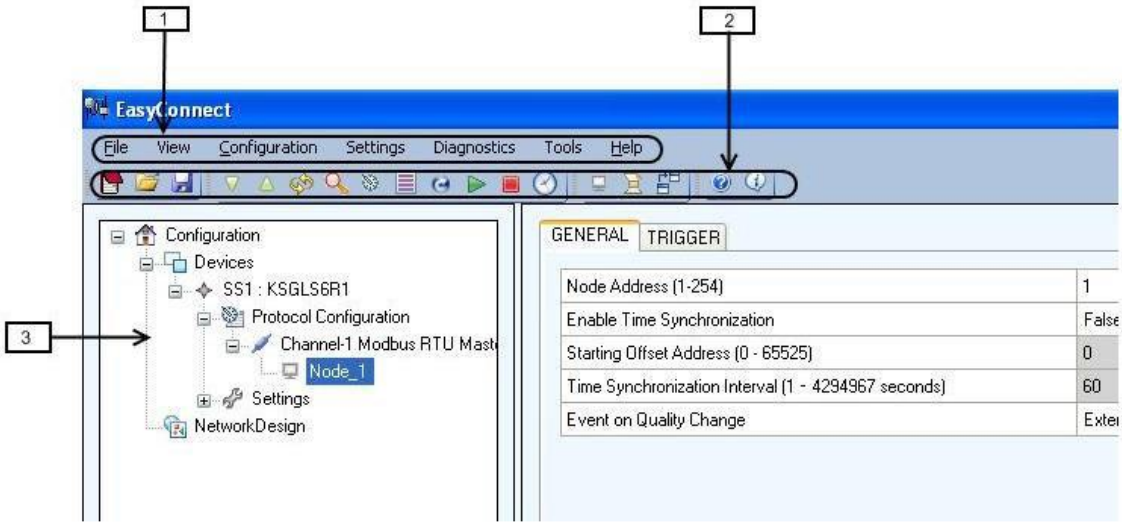
You can close EasyConnect at any point during the running of the application
To exit EasyConnect perform the following steps:

1. From File menu, choose Exit. If there is any open configuration, a warning window will appear to confirm whether the user would like to save the configuration before closing EasyConnect.

2. Click Yes, to save the configuration at desired location before exiting EasyConnect. Click No, not to save the configuration and to continue with exiting EasyConnect. Click Cancel to cancel exiting EasyConnect.

5.1.5. Using the Interface

This section gives you an overview of the elements and menus in the user interface using the graphical user interface diagram. The components in the user interface of EasyConnect are shown in Figure14 and each one is described in detail:



The Components are:

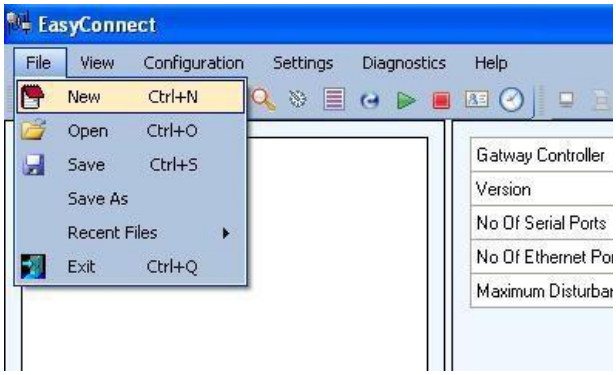
1. Menu
2. Toolbar
3. Workspace

5.1.5.1. Menu

The Menu contains options to execute all the actions that can be done using EasyConnect. The different Menus are:

1. File Menu

To Start a new configuration, opening a saved configuration file, saving the configuration are the options available in this menu. A few of these actions are also made available in the toolbar.



2. View Menu

The **View menu** contains the option to enable or disable the toolbar buttons.

3. Configuration Menu

The Configuration menu contains options corresponding to the node in the Tree-View that has been selected. Depending on the node selected, the options available in the Configuration menu

varies. These actions can also be availed by clicking the right mouse button on the node. This menu
is extensively used in configuring the SIC-A and is well explained in the respective sections.

4. Setting Menu

The Settings menu contains the generic actions which are listed below:

Download: Is used to download the configuration file to the device.
Upload: Used to upload the device configuration file from the device to the Easy Connect.
Restart: Used for restarting the device.
IP configuration: To configure the ip of the device.
Stop: Used to stop the firmware in the device.
Start: Used to start the firmware in the device.
Scan: Used to scan all the devices in the network. Scan will detect a device only if the device is connected in the network through its interface (LAN).
Version Information: To get the version and protocol details of the firmware in the device.
Time Settings: To get or set the time and timezone of the device.
Update: To update the firmware in the device

5. Diagnostics Menu

The **Diagnostic menu** contains action items for the diagnostic functionality. The options available in diagnostic menu are **Traffic Monitoring** , **PDC Diagnostics** and **Gateway Access** Log**.**

6. Tool Menu

Tools menu contains options to set the EasyConnect parameters like Timeout settings.

7. Help Menu

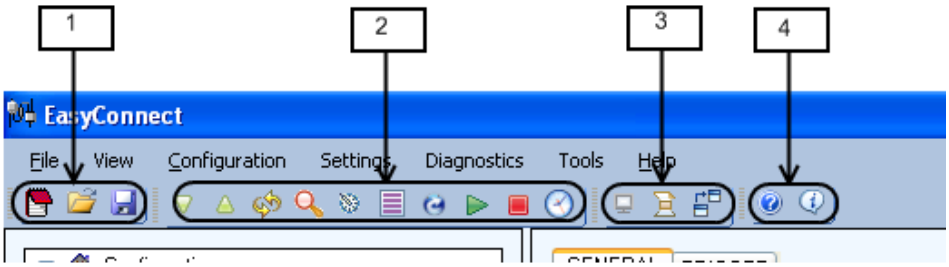
The **Help menu** contains the options to get EasyConnect Help documentation and Information about EasyConnect.

5.1.5.2. Toolbar

The toolbar provides easy access buttons to menu options and they are:

1. File
2. Settings
3. Diagnostics
4. Help

These are selected options from the respective menus. They can be enabled or disabled in the View Menu. Tool tips are available for each toolbar button, describing the functionality associated with each of them.



5.1.5.3. Workspace

The workspace section is the place where all the configurations regarding the different channels, stations etc are done. Depending on the node selected in the Tree-view, the options available in the Workspace may vary. These are described in the configuration of each item in detail.

5.2. Configuring the Gateway

You have to configure the SIC-A before it can be run. The configuration for any protocol conversion function can be divided into a few logical steps. Master protocol configuration will be divided into the following sections namely; Channel, Node, Profile and Row addition. For a slave, profile, Channel and Node are configured. A master and slave can be mapped by the Add Map option, The following steps explains how to configure protocol modules:

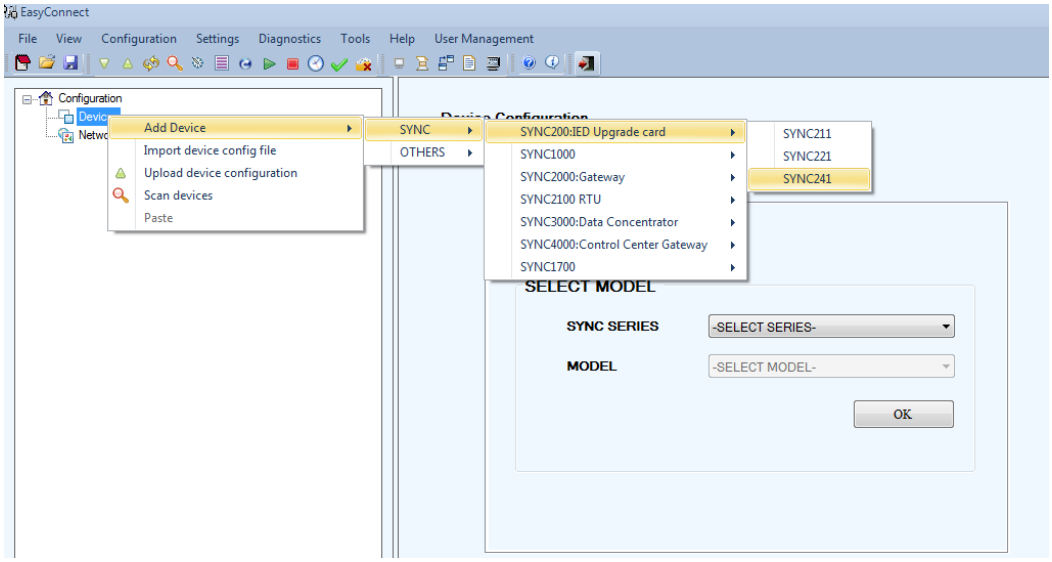
Steps to configure a gateway:

1. Add Master channels
2. Add Slave Channels
3. Add Master to Slave Map
4. Add Slave to Slave Map
5. Dialup/Modem Settings
6. VPN Settings
7. SNMP Support
8. Configuration Easiness
9. DCCP Packaging

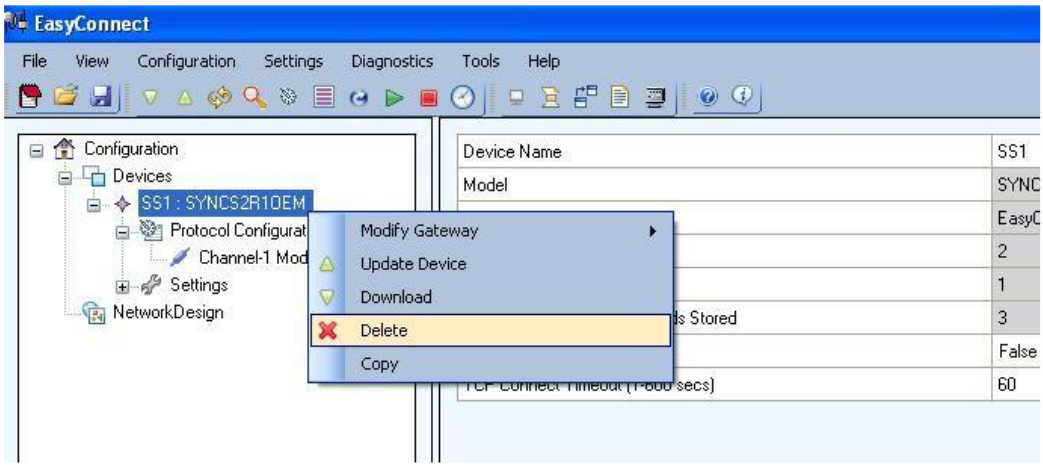
Step 1,2 and 3 deals with protocol conversion function of the gateway. Step 4 and 5 deals with additional/optional communication features of the gateway. For normal protocol conversion requirements users can stop at step 3. You may proceed to step 4 or step 5 when you use any of the described features.

5.2.1. Add Master Channel

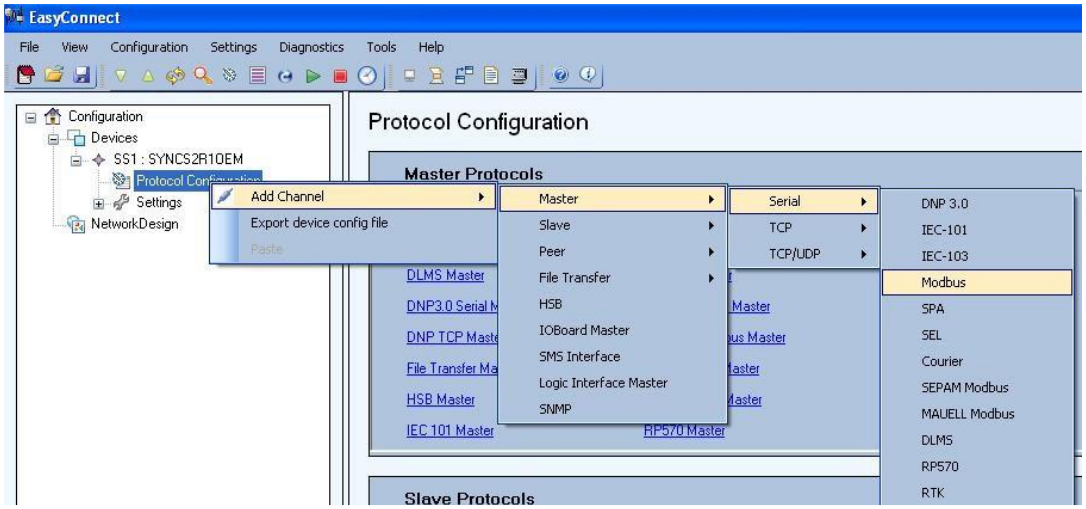
1. Add SYNC200:IED Upgrade card, **SYNC 241** by selecting the converter model from Device configuration section or right click on Devices in the left hand side pane, as shown in the figure below:



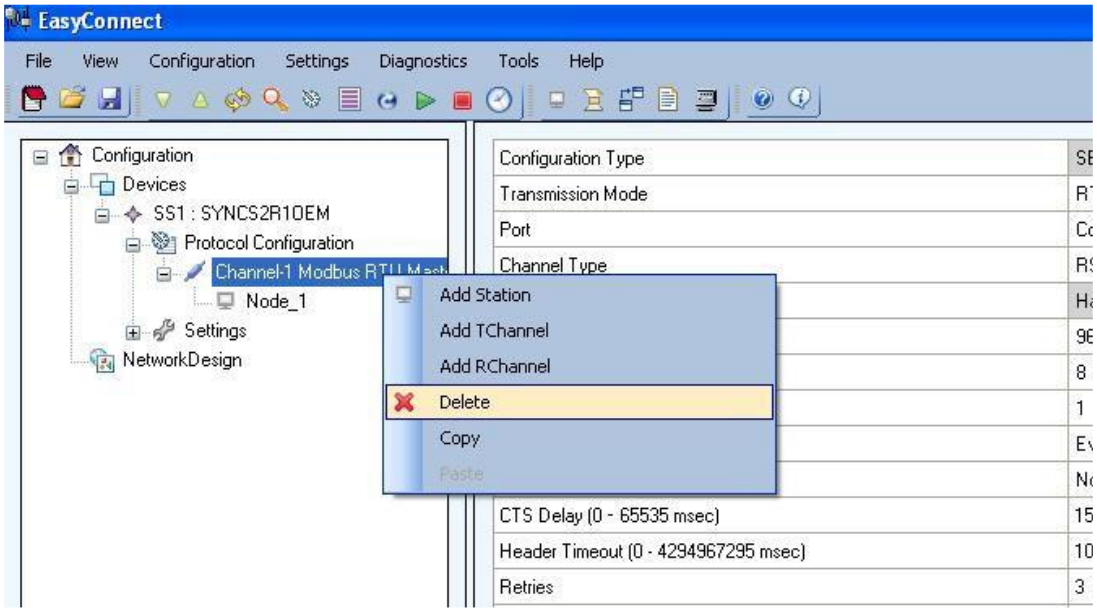
To delete the selected gateway, right click the selected gateway, and choose **Delete** as shown in the figure below:



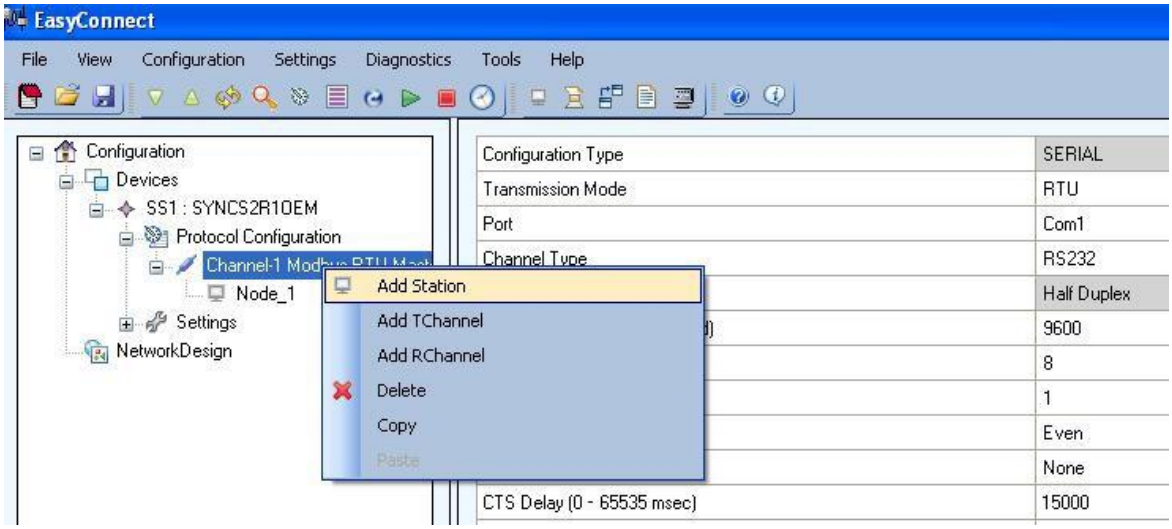
2. Add **Master channels** to the converter model as shown in the figure below:



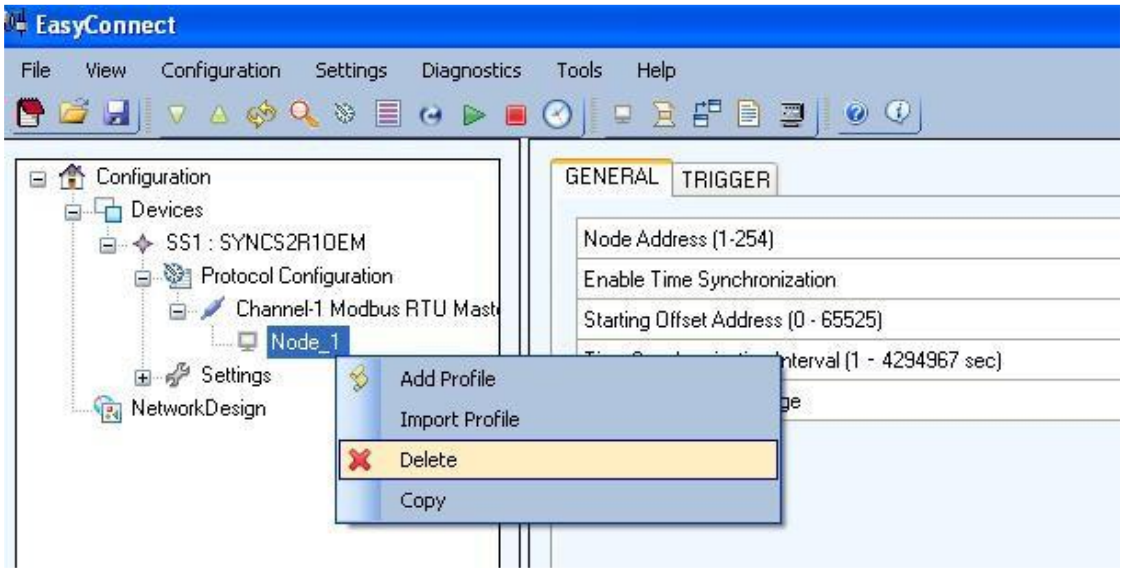
User can delete a protocol specific communication channel by selecting Delete option from menu on right clicking on the selected channel as shown below:



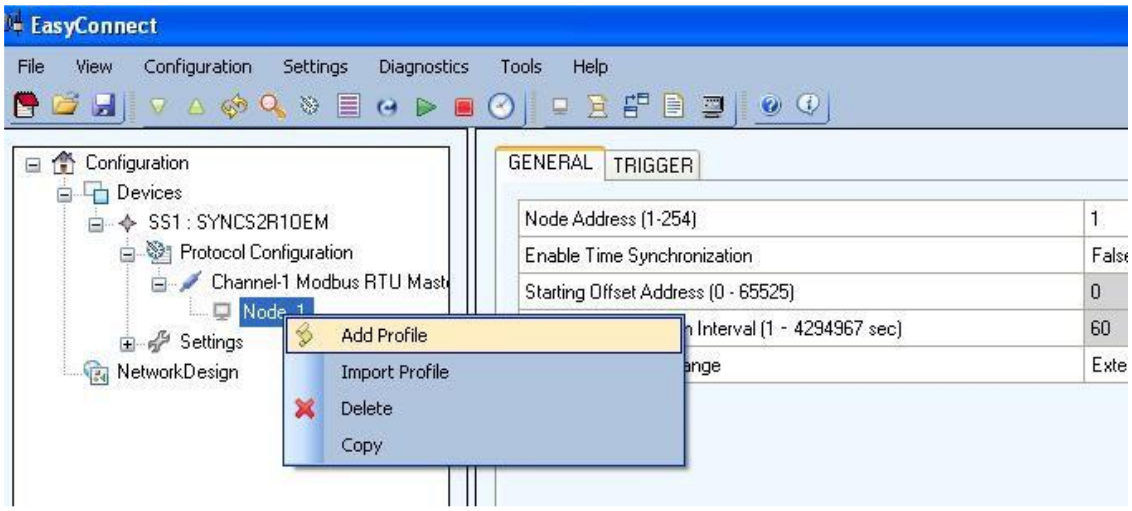
3. Add **Node** or **Station** as shown in the figure below:

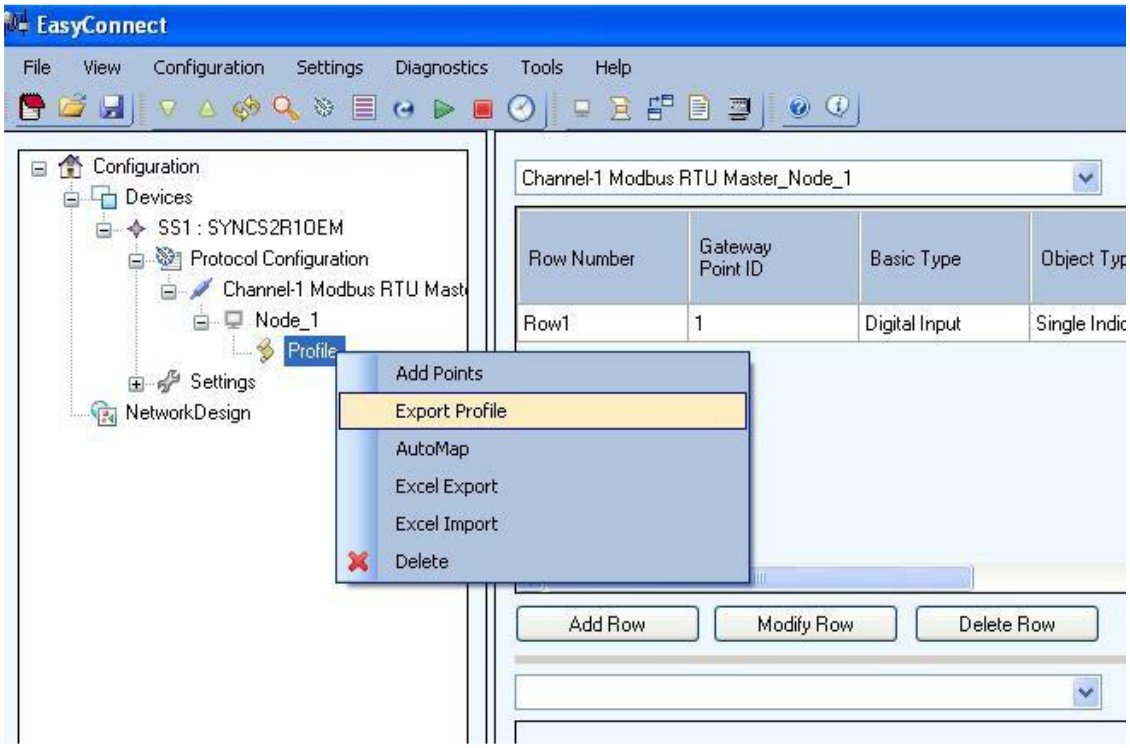


4. Delete a station by selecting **Delete** from menu displayed on right click of selected station:



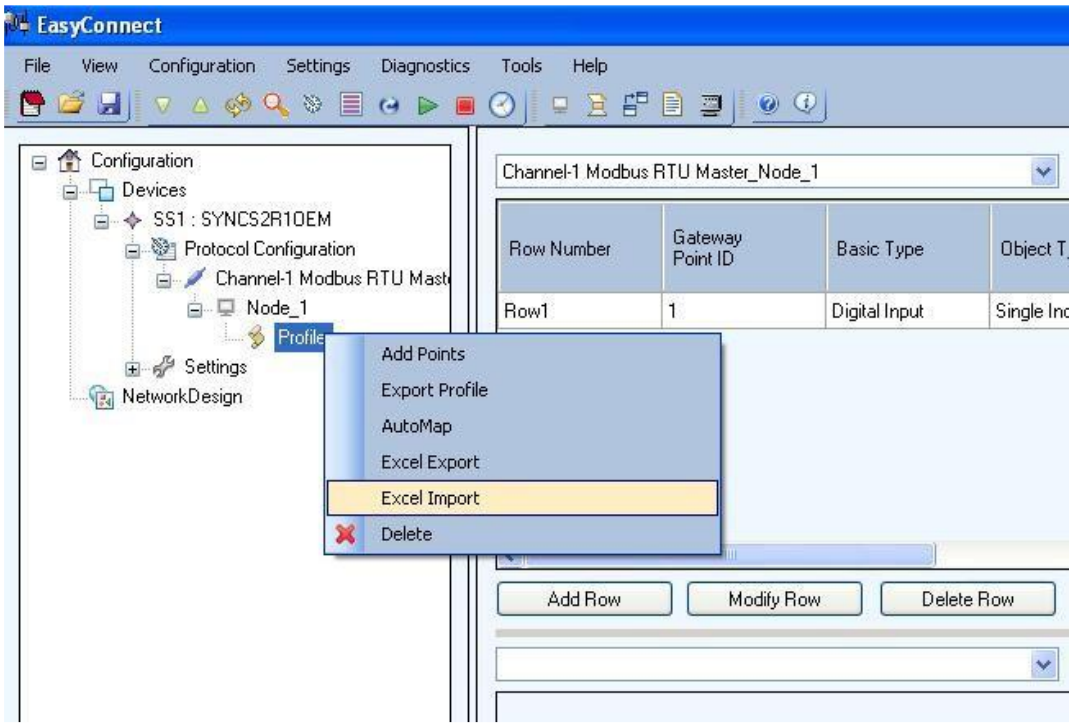
5. To add **Master Profile** right click on **Node** and select **Add Profile**.



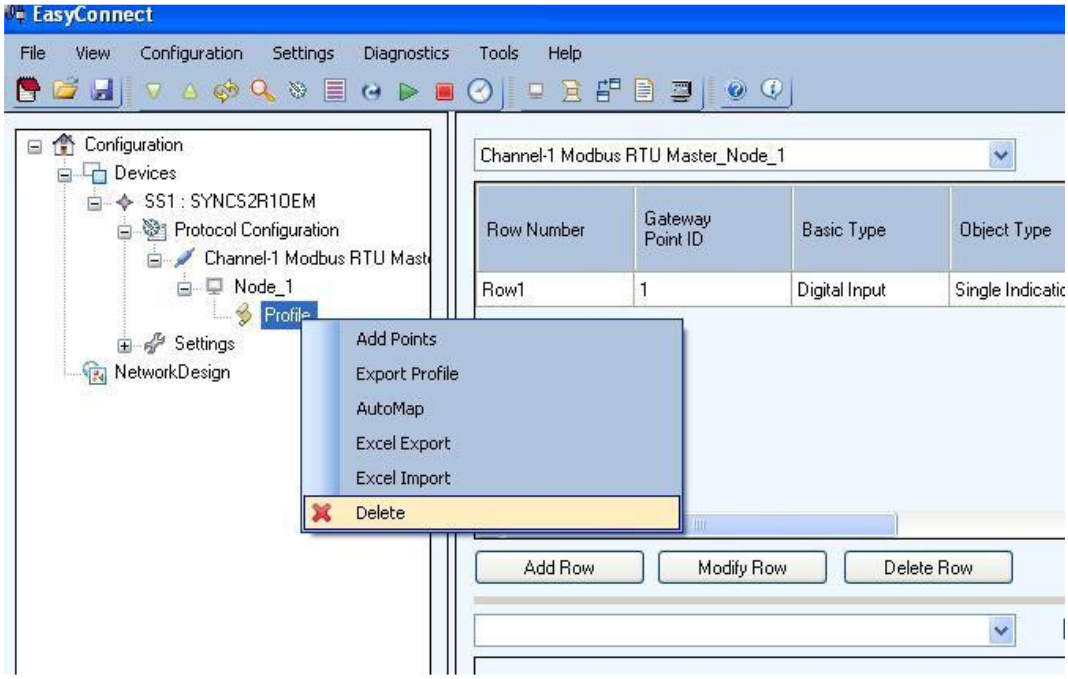


Profiles can be saved for reusing the same address configuration for different masters. Right click a Profile tree node and select Export Profile, a Save File window will pop up. Save the profile in desired name in the desired location.

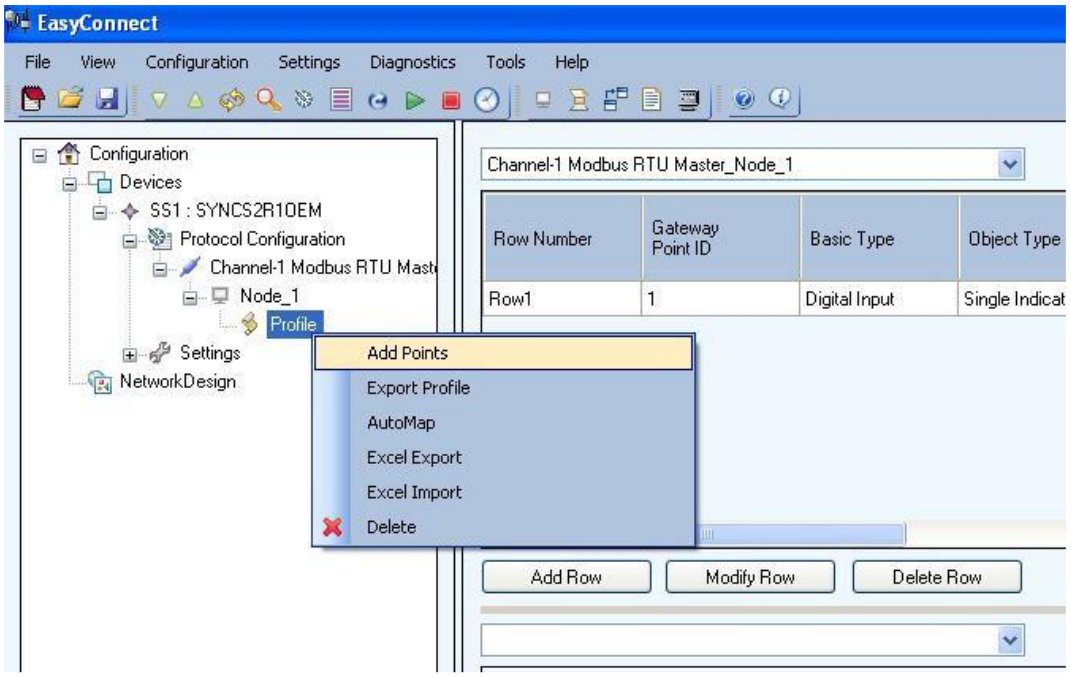
Instead of adding a new profile user can also import previously saved profile data. Right click on a master station and select Import Profile option, an Open File window will pop up. Open a saved profile file. Refer the figure given below:



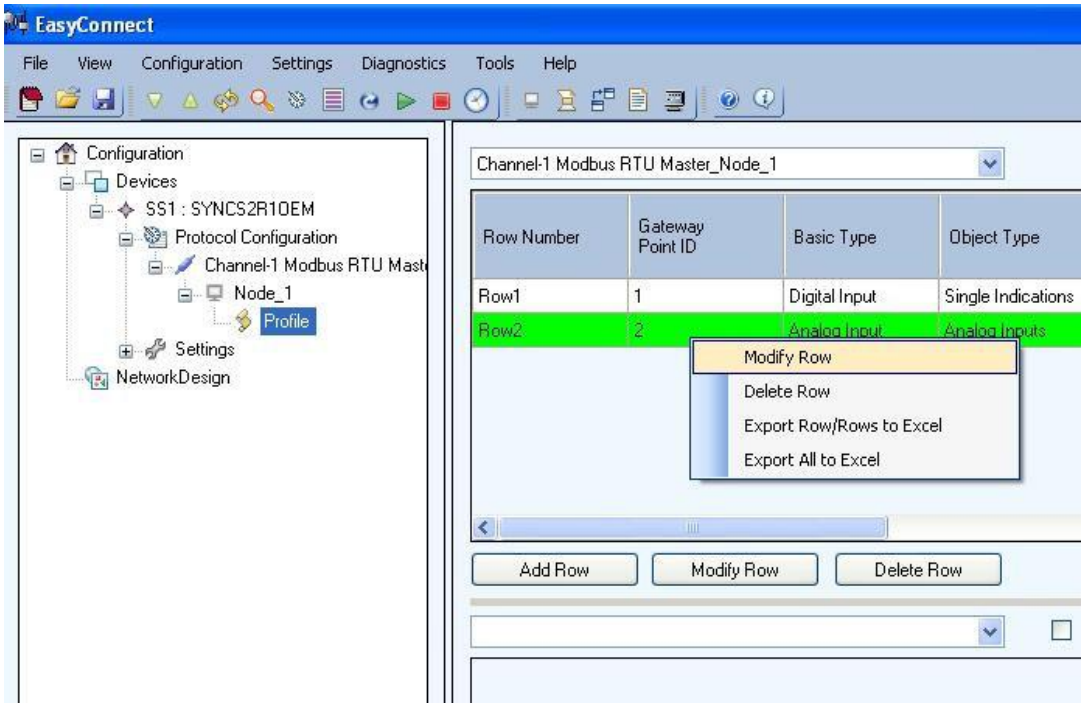
To delete a Profile, right click on added **Profile** and select **Delete**



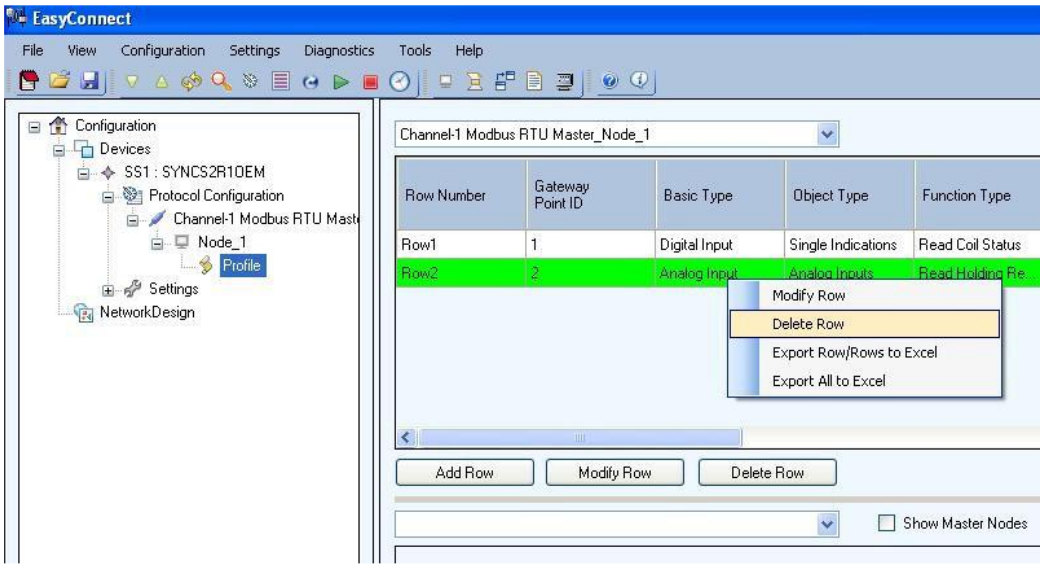
6. To add Master Row right click on **Profile** and select **Add Points** as shown in the figure below:



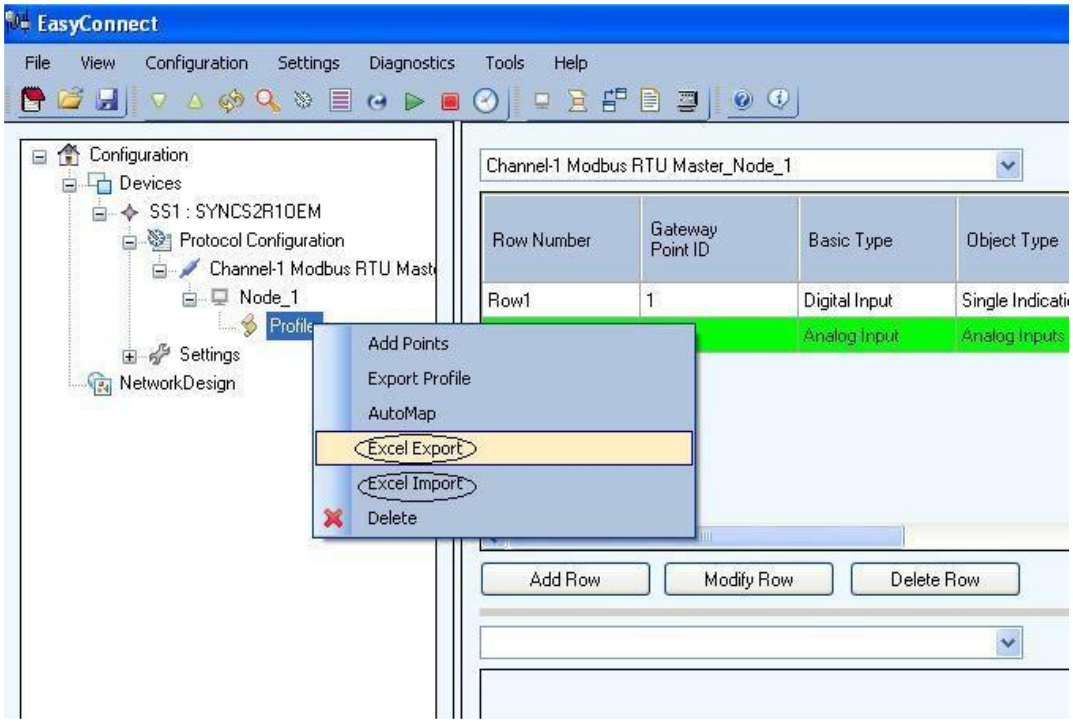
Select a row from the profile grid. Click on Modify Row button. A new window will pop up with values of selected row.



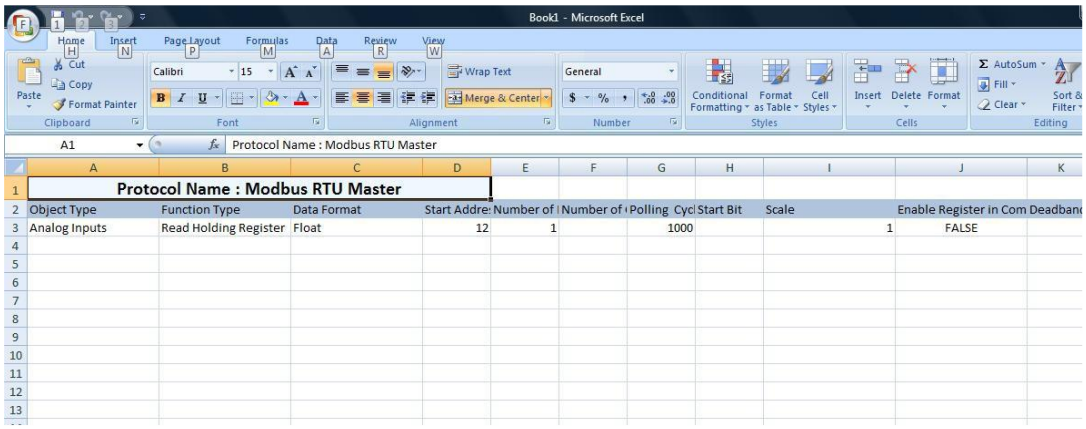
For deleting added rows, select rows from profile grid and click **Delete Row** on the right panel.



Adding large number of points in a profile using Easy Connect Add Row button can be time consuming.
Easy Connect Configuration Utility provides facility to export profile rows to an excel worksheet and import the points form an excel worksheet to the profile rows. User can configure the required points in an excel worksheet and it can be imported to the required profile.
After adding required rows in the profile, select Excel Export from the context menu as shown in the figure below:



Exported excel worksheet format is shown in the figure below. The worksheet will contain the protocol
Name. All the configurable parameters in the Profile Row window of the specified protocol form individual columns. All the available options for a parameter will be available in the combo box independent of the type of point selected.
Note: Communication diagnostic point will not be imported to the excel worksheet.



Excel Import:

Select Excel Import from the context menu of profile and choose the excel worksheet prepared to import. Refer above given figure. Certain conditions are applicable for the Excel Import functionality.

• Only worksheets previously exported from EasyConnect can be imported. User should add at least one point (other than communication diagnostic point) in the profile and use Excel Export to generate an excel worksheet template. Configure required points in this file and save. Note that EasyConnect expects a specific format for the worksheet. So the user should refrain from modifying the format of the sheet in any manner. Only the contents may be changed.

• The protocol name in the Excel worksheet should match with the protocol of the profile to which it is
imported. For example, an excel worksheet exported from IEC104 Master can only be imported to a profile under an IEC104 Master Channel.

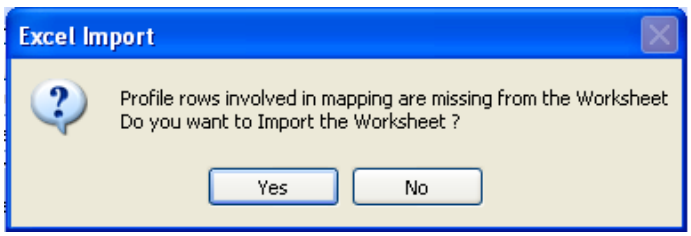
• EasyConnect validates all the parameters configured in the excel worksheet before importing and will push an error message if the validation fails. All the available options for a parameter will be available in the worksheet cells independent of the type of point selected. For example, in Modbus Master, Function Type 'Read Coil status' is not applicable for object type 'Analog Input'. But this option will be available in the excel worksheet cell. User should select the valid options while editing the worksheet. Any failure in validation will terminate excel import.

• After validation, all the existing profile rows will be replaced by the points configured in the worksheet.

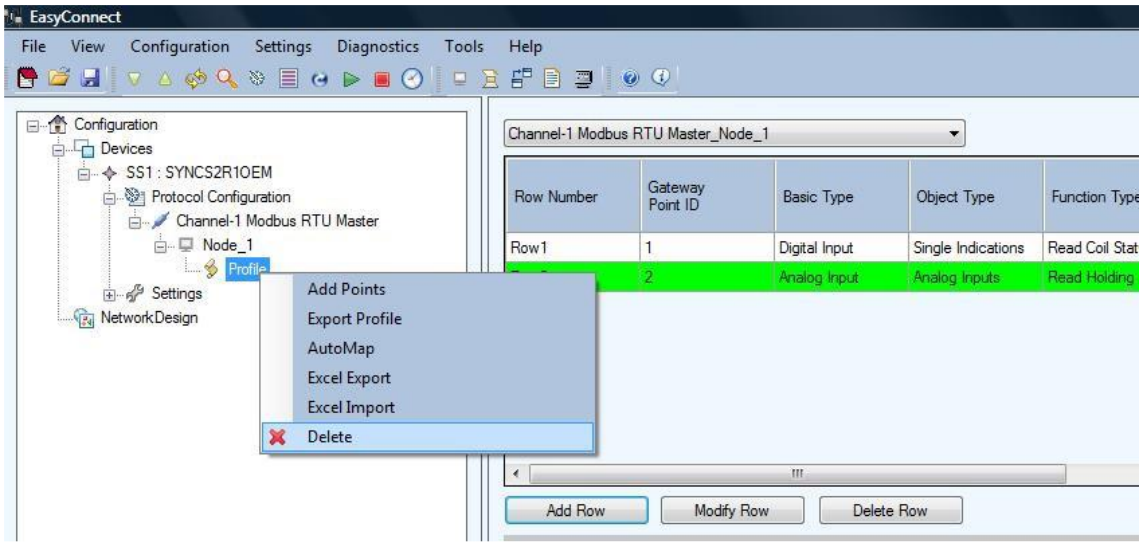
• For points that are already mapped to a destination protocol.

• For all the rows where the address parameters are not modified, the other parameter values are read in from the worksheet.

• If the address parameters are changed in the worksheet, Easy connect will pop up a message as shown in the figure below. On selecting Yes, the mapping will be deleted and the points in worksheet will be imported. On selecting No, the excel worksheet will not be imported.



To delete a Profile, right click on added **profile** and select **Delete**.

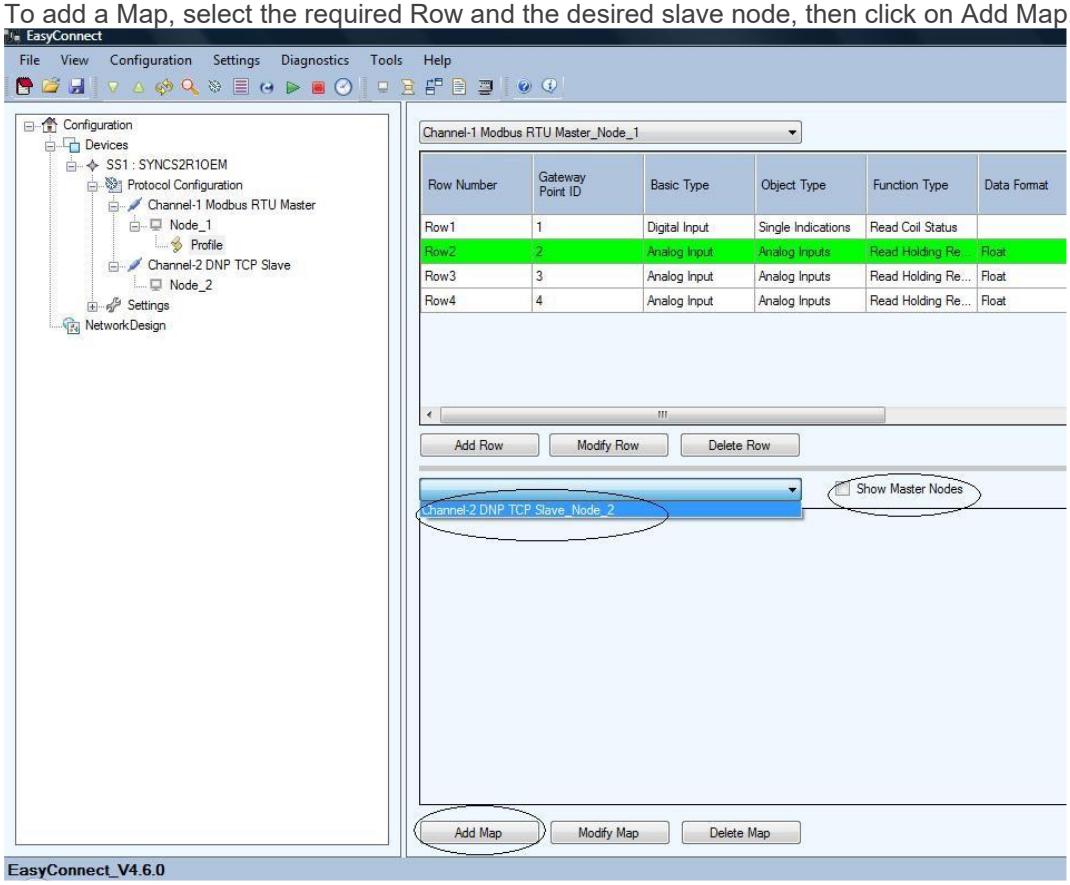

EasyConnect
File
View
Configuration
Settings
Diagnostics
Tools
Help
Configuration
Devices
SS1 : SYNCS2R1OEM
Protocol Configuration
Channel-1 Modbus RTU Master
Node_1
Profile
Settings
NetworkDesign
Add Points
Export Profile
AutoMap
Excel Export
Excel Import
Delete
Channel-1 Modbus RTU Master_Node_1
Row Number
Gateway Point ID
Basic Type
Object Type
Function Type
Row1
1
Digital Input
Single Indications
Read Coil Stat
2
Analog Input
Analog Inputs
Read Holding
Add Row
Modify Row
Delete Row

5.2.2. Add Slave Channel

To add a slave channel and node follow the procedures mentioned above.

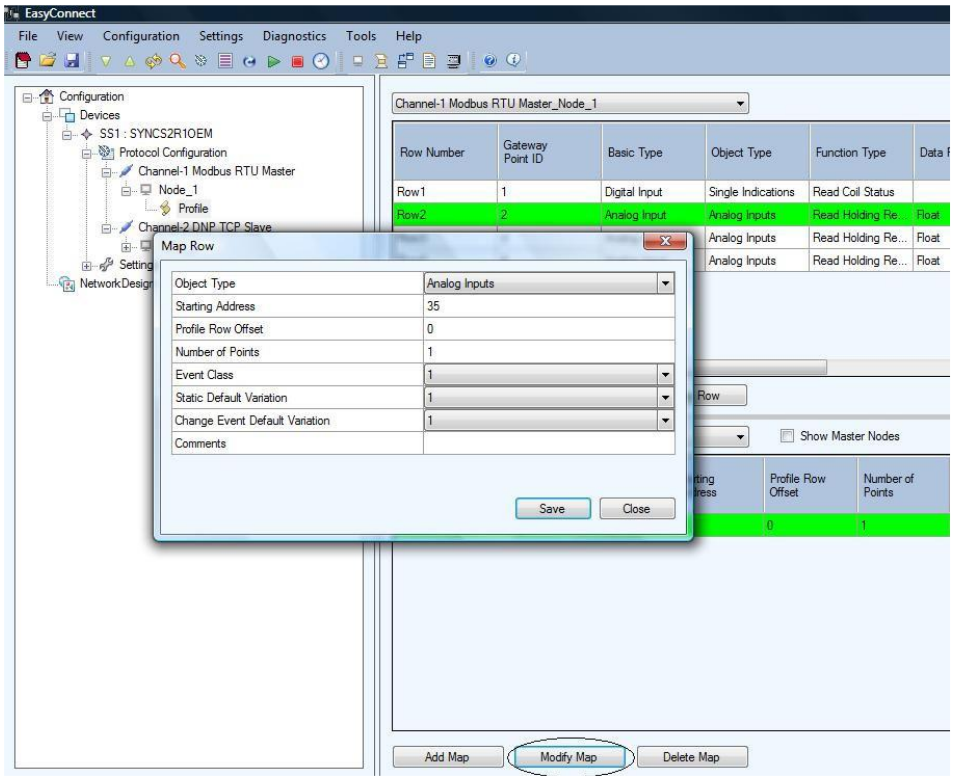
5.2.3. Add Master to Slave Map

To add a Map, select the required Row and the desired slave node, then click on Add Map.

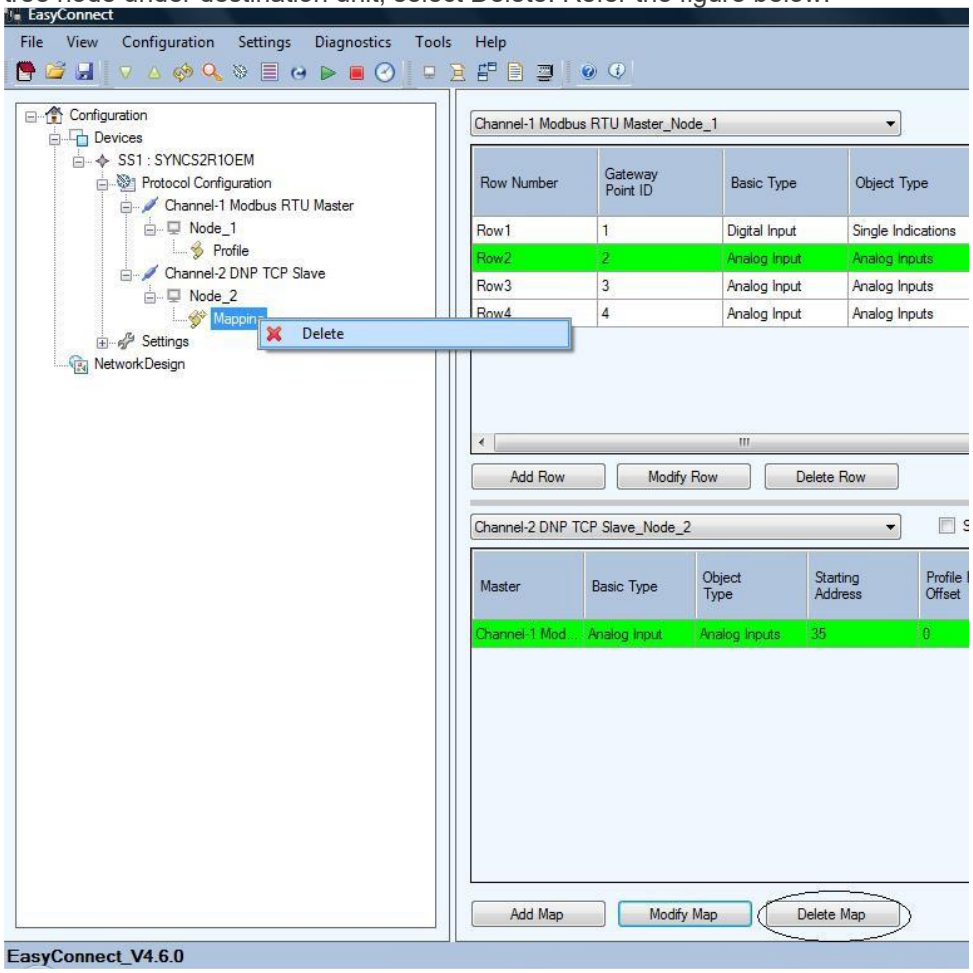


Note: To Enable Master to Master mapping, select **Show Master Nodes**.(Master to Master mapping is used when input data from an external device is translated to a command/ output and sent to an external device.)

To modify a mapped row, select a row from the destination unit and click on **Modify Map** button. A new window will open with added mapped values. Edit the parameter values. Click on **Save** to update the modified mapped point. Refer the figure below:



To delete a mapped row or group of rows from the conversion, select mapped row from the destination unit and click Delete Map. To delete destination unit profile, right click on Mapping tree node under destination unit, select Delete. Refer the figure below:

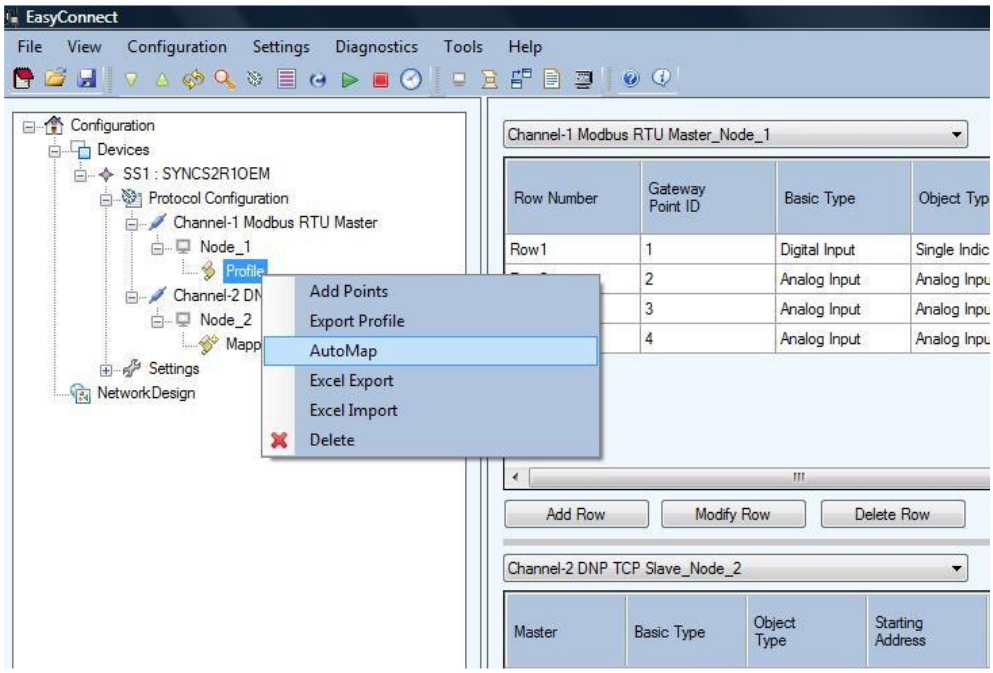


5.2.3.1. Auto Mapping – Master to Slave

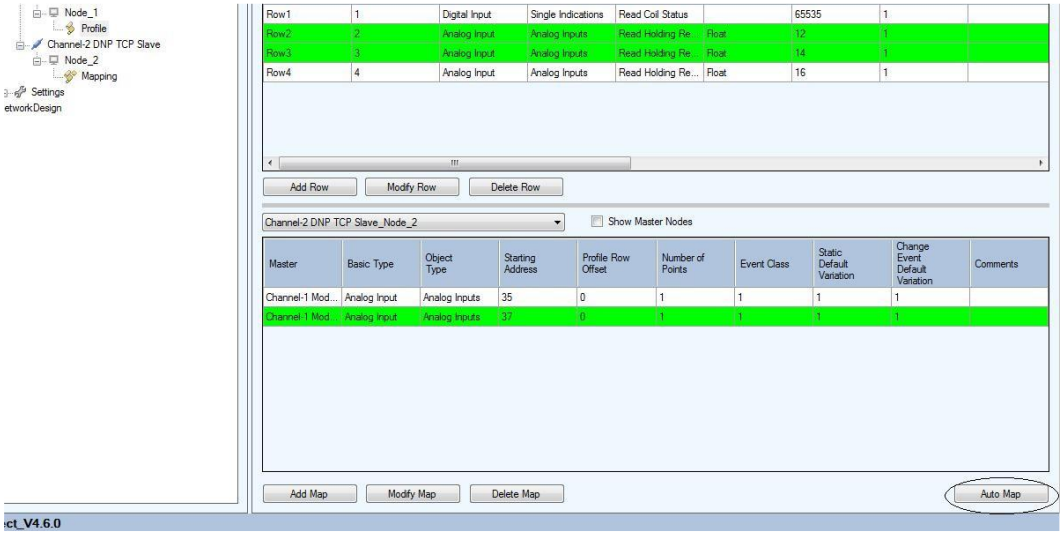
EasyConnect provides options for mapping the master points automatically to a selected slave node. User can either auto map the entire row configured in the master profile or some selected rows. The steps for automatic mapping are given below:

1. Select the slave protocol to which the points are to be mapped.

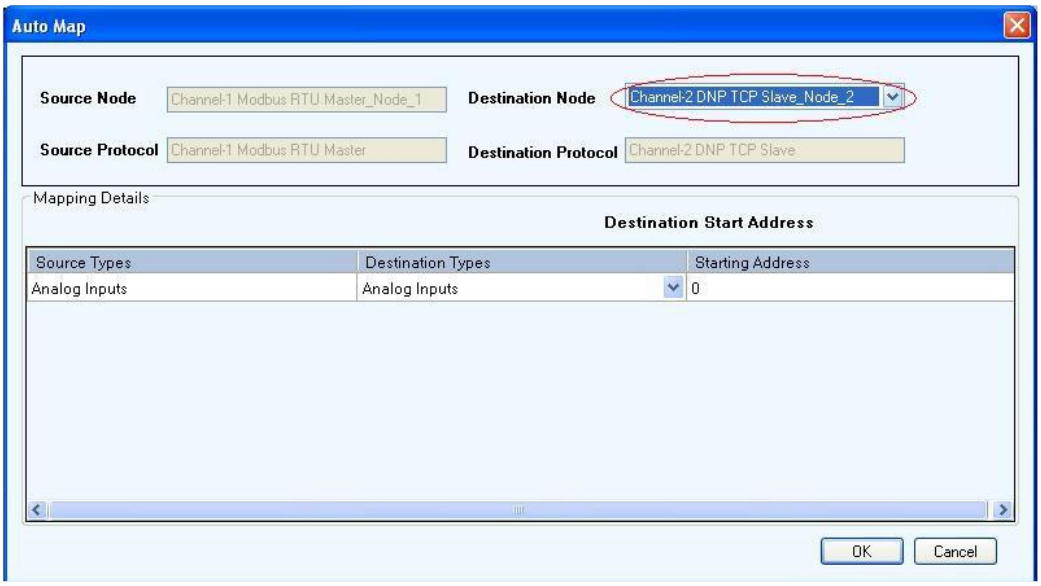
2. For mapping the entire rows in a profile, Right click on the corresponding profile and click the
option Auto Map as shown in figure below:



1. For mapping the selected rows in a profile, select the needed rows in the profile for which the automatic mapping needs to be done. Click on **Auto Map** (slave/destination mapping part) as shown in the figure below:



2. Step 2 or 3 will pop up the **Auto Map** window as shown in the figure below. User can configure the details in the Auto Map window and generate auto mapping.



5.2.3.2. Auto Map Window

Auto Map window shows the master (source) types that are considered for automatic mapping corresponding slave types automatically considered as mapping type (user can change using combo options) and corresponding start address in the slave. The parameter details of Auto Map window are given in the table.

SL. No	Parameter	Details
1	Source Node	Indicates the node number whose profile needs to be mapped. This parameter is not editable
2	Destination Node	Indicates the node to which the mapping needs to be done. The default will be the node selected in the mapping window. User will be able to change the same to any other nodes which is available in the configuration system
3	Source Protocol	Protocol of the source node. This parameter is not editable.
4	Destination Protocol	Protocol of the destination node. This parameter is not editable.
5	Source Types	Indicates source data types from which mapping is carried out.
6	Destination Types	Indicates suggested destination data type for the specific source type to which mapping is carried out. This indicates default suggestion and user can even change the same from the allowed types available in combo box.
7	Destination Start Address	This indicates the destination start address for the specific destination type. This is generated after evaluating all the existing address and last address + 1 of the already existing address is considered as default. User can change the start address but it will again undergo evaluation. There will be multiple address parameters based on the protocol used. For eg: if it is IEC101/104, the same will have IOA but if it is IEC 103, it will have ftype and inumber as address parameters.

The following points will be applicable to the Auto Mapping Window:

1. Only data types which has at least a point available for mapping to the current slave shall be displayed in the auto-mapping window
2. Similar source types will be grouped and displayed as a single row in the Auto Map window. In each protocol the grouping of source types differ.
3. All the types coming under the Basic type of the source type will be available in the combo box options of Destination Types.

4. In case, where destination address range is not sufficient to map all the points, an error message would be displayed in the validation stage after clicking the **'OK'** button.
5. Points will not be split and mapped for numerical address based protocols. A continuous address space large enough to hold the points in a single row (source) is found and the points are mapped to that range.
6. Auto-map shall be provided for all Master protocols except 'HSB Master' and 'Logic Master'.
7. On pressing **OK** from Auto-map window, points that can be successfully mapped are processed and for those which could not be mapped, an error message is displayed.

Note: All the other profile parameters will be default when auto mapped. User can modify the row if required.

5.2.4. Slave to Slave Mapping Feature

Introduction

The Slave to Slave mapping provides the facility to transfer some critical information between two
master stations.

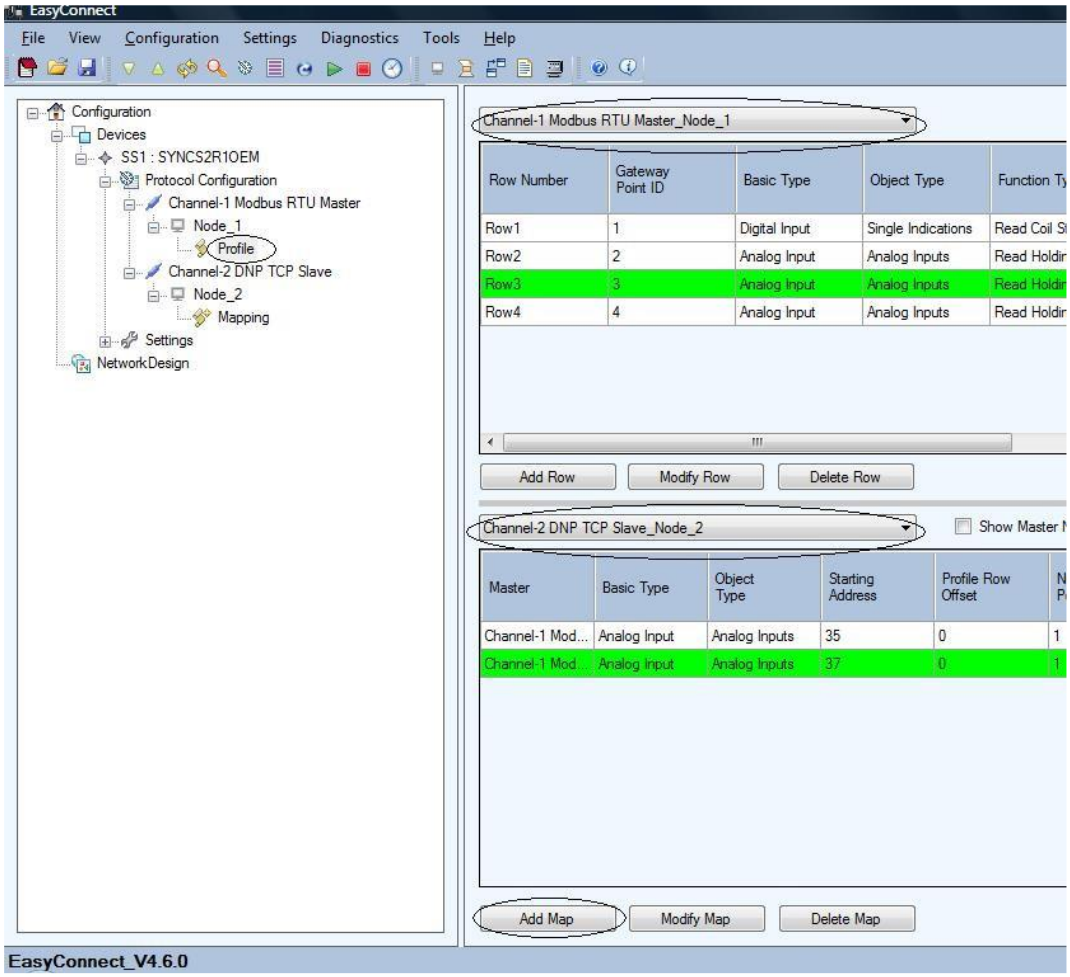
For provisioning communication between masters, the corresponding source slave should be mapped to the destination slave. The source slave is the 'slave which transacts with the master from which data has to be transferred and the destination slave is the slave which transacts with the master to which the data has to be transferred. User can add profile and configure command points under the source slave nodes. These command points can be mapped to input points. A command received on the source slave will be sent as an event to the mapped destination slave.

Depending on the command type and protocol, a positive acknowledgment will be sent back to the source slave after sending the event notification. If the command point is not mapped, a negative acknowledgment will be sent back. For the protocols and particular data types which do not support event intimations, the data can be retrieved by polling.

Note: Slave to Slave Mapping does not allow multiple mapping. Also, a single row can only be mapped to a single node. For example consider a row with three points. Each of these three points should be mapped to a single node. Splitting and mapping to different nodes is not permissible. Also, the quality of the points configured will always be good. And the time stamp of the event will be the time taken from the converter when the command is processed.

Configuration Details

1. Add slave channels and nodes (source and destination).
2. Add Profile under source Slave and configure Points as shown in the figure below:



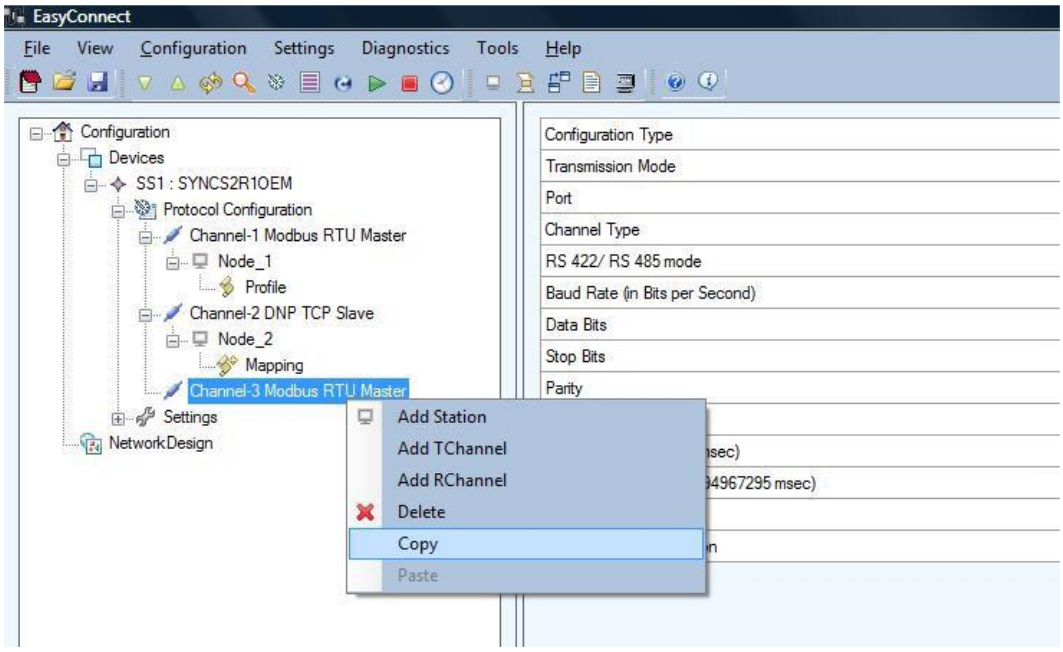
Select destination Slave and click on **Add Map** to add the mapping as shown in the figure above. **Modify Map** and Delete Map functions identically to the master to slave mapping counterparts

5.2.5. Configuration Easiness

5.2.5.1. Copy/Paste

EasyConnect allows the user to copy and paste a device, a channel or a node. Depending on the
protocol, the no.of channels/nodes up to which it can be copied varies.

The **Copy** option is made available on right clicking on a device, channel or a node. Consider the
case, a node is copied, in-order to paste multiple copies of the nodes under a channel, the user must right click on the channel and click **Paste**. Refer the figure given below:



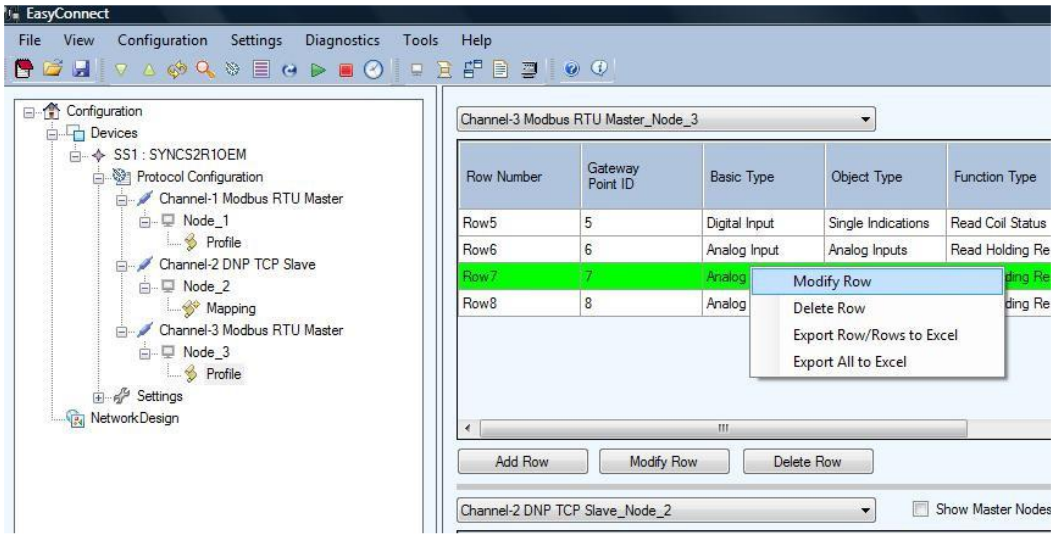
While clicking on paste option in the right click of device, channel or node, a form pops up, which gives
the user, an option to enter the no of copies required, as shown in the figure below:

Copying a device copies all information under that device including mapping and Serial port settings.
The settings like Dial up Settings, LAN Settings and SNMP Settings will not be copied along with the device.

5.2.5.2. Profile Row Options
This is another feature of configuration easiness, where EasyConnect allows the user to modify, delete a particular row by selecting the corresponding option available on right clicking on that selected row.

User can modify only a single row at a time. The Delete row option is available for multiple selected rows. The user can also export a single or multiple rows to Excel. It can be done by selecting single or multiple rows and right clicking Export Row/ Rows to Excel option.

Export All to Excel option is also made available on right clicking, if user wants to export all the rows in the profile. Refer the figure given below:



5.2.6. SNMP Support

Simple Network Management Protocol (SNMP) is a UDP based network protocol. It helps to manage network-attached devices and make sure they are not only up and running but also performing optimally. SNMP exposes management data in the form of variables on the managed systems, which describes the system configuration. These variables can then be queried or set by managing applications.
SIC-A specific objects managed by SNMP are Model Name, Hardware Information such as Ethernet
Interfaces Details, Serial Port Details, Memory Usage and Software Information such as GPC health,
DCCP health. Additionally, it is possible to monitor the gateway database points by mapping those
points to an SNMP Slave channel.

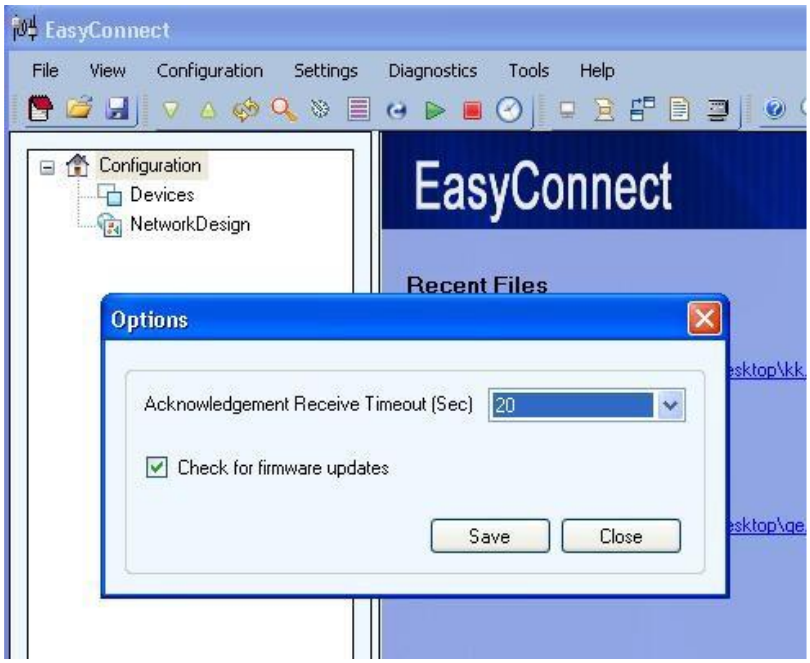
5.2.7. DCCP Packaging

DCCP Packaging allows the user to update the DCCP firmware in the gateway with the latest EasyConnect compatible DCCP firmware.

From the EasyConnect version 4.6.0 onwards, the latest version of DCCP firmwares are provided in the EasyConnect application folder. If the gateway is having an older DCCP version, EasyConnect provides a provision for automatic up-gradation of the DCCP firmware.

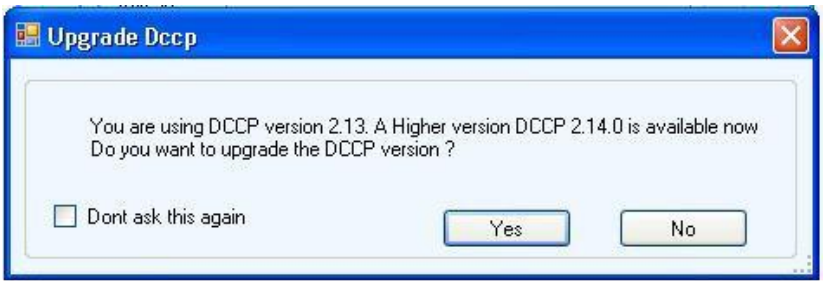
During various operations such as 'Download', 'Upload', 'Stop firmware' and 'Start firmware' , EasyConnect will check the DCCP firmware version in the device and prompt the user to download the latest version if the DCCP version in the gateway is lower.

For enabling the DCCP version check user must check the Check for firmware updates box in the
Option window found in Tools and click **Save**. Refer the figure as given below.



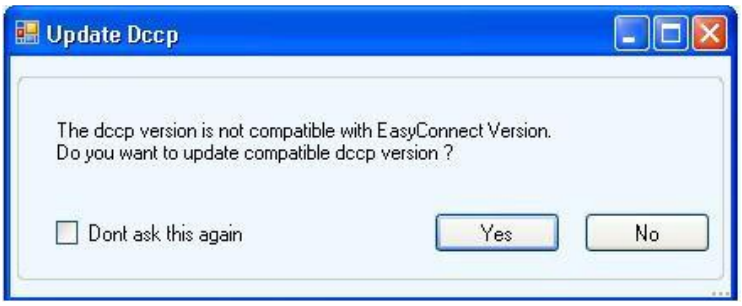
In order to disable the version check, uncheck the **Check for firmware updates** box and click **Save**.

If the gateway is having a lower DCCP version, EasyConnect prompts the user for up gradation of the
DCCP firmware. On clicking **Yes**, the gateway gets upgraded with the latest version of DCCP. Refer Figure.

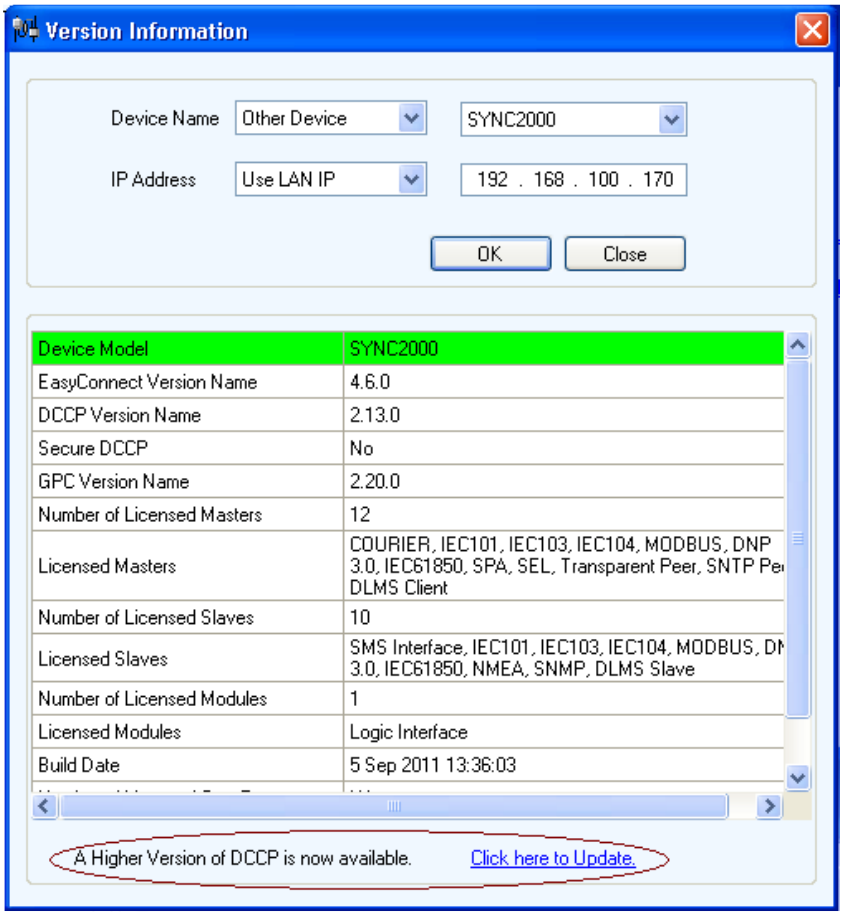


Note: On checking the Don't ask this again box, the version check will be disabled for that EasyConnect instance irrespective of checking the Check for firmware updates box from the Option
window in Tools.

For DCCP versions older than 2.9, EasyConnect asks the user to upgrade to a compatible version of
DCCP, as shown in the figure and on clicking Yes, it will prompt the user to browse the model name from the combo box, as shown in the figure and when clicked OK, it will update the DCCP firmware after automatically getting the corresponding DCCP firmware.

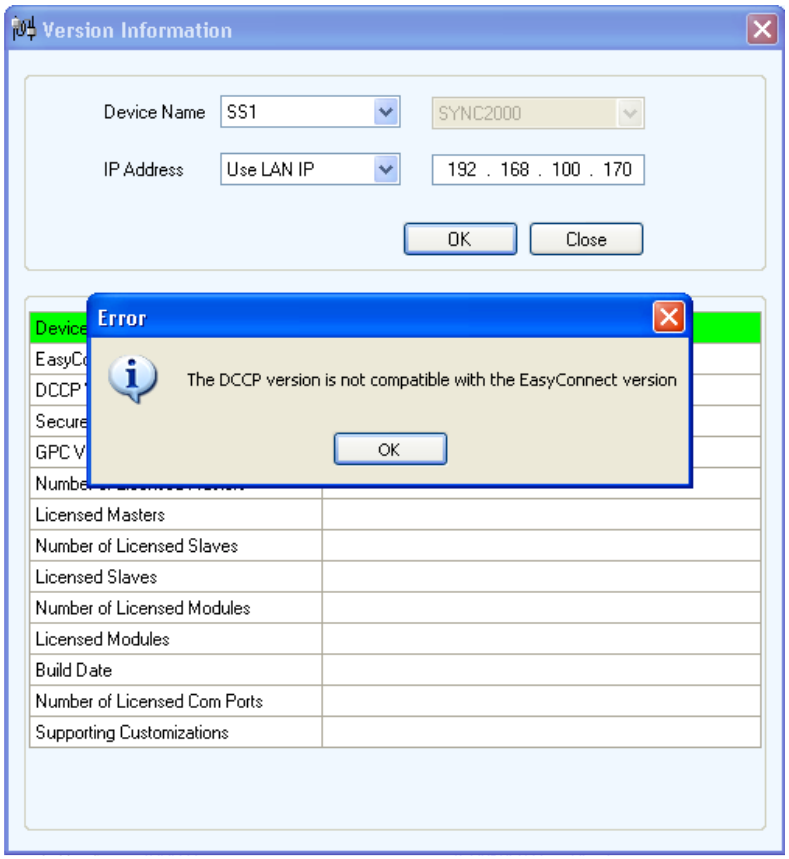


In the Version Information window, an option Click here to update is provided to update the DCCP
version if the gateway uses an older DCCP version. This feature is shown only for the DCCP Packaging supported devices. Refer the below figure.



Note: This option is not available if the **Check for firmware updates** box in the Option window found in Tools is unchecked .

In case of older DCCP version having no version information (DCCP version less than v2.9.0) , the
following message will be displayed on checking the version information.



5.3. Download/ Save Configuration File

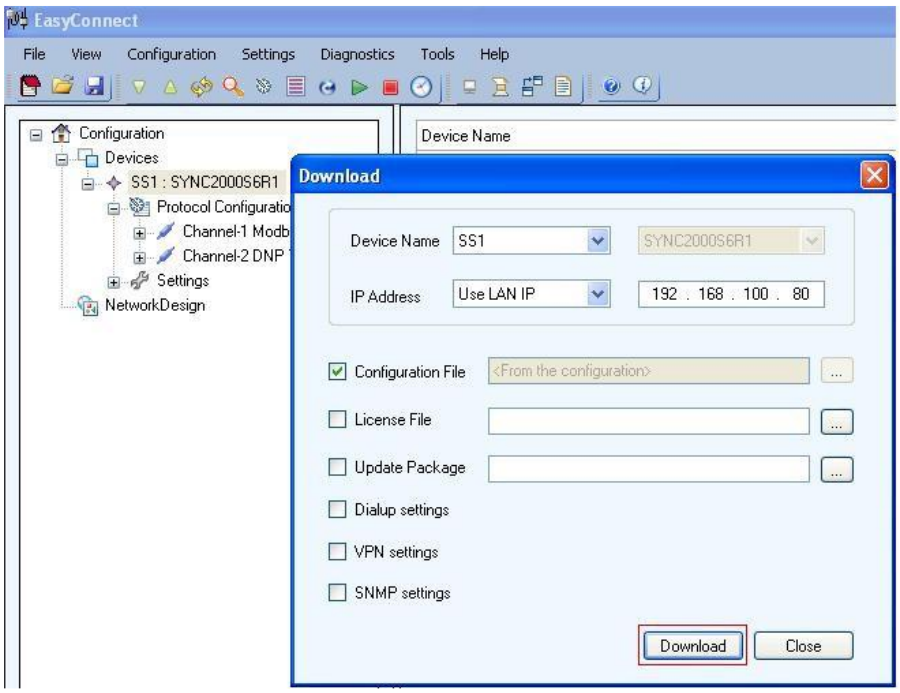
5.3.1. Downloading

User have to download the configuration file to SIC-A after creating or editing. In case of editing user have to stop and start the firmware for the changes to take effect.

To download the configured and mapped file perform the following steps:

1. On the user interface, click **Download**
   The **EasyConnect-Download** window appears.

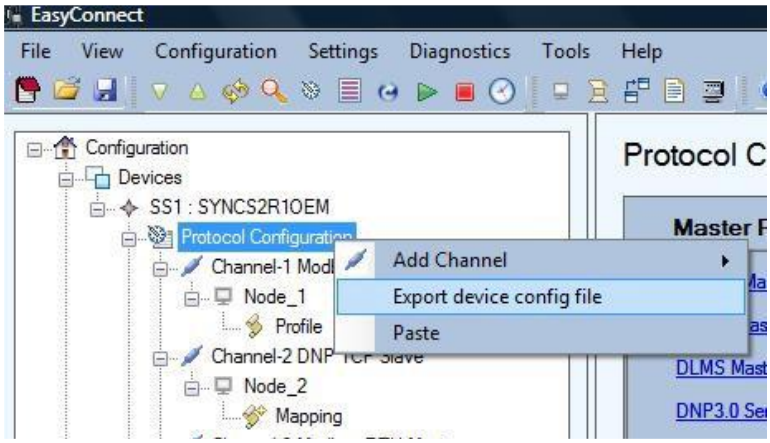
2. Click **Download**. The file is downloaded to the SIC-A and a corresponding success message is
   displayed.



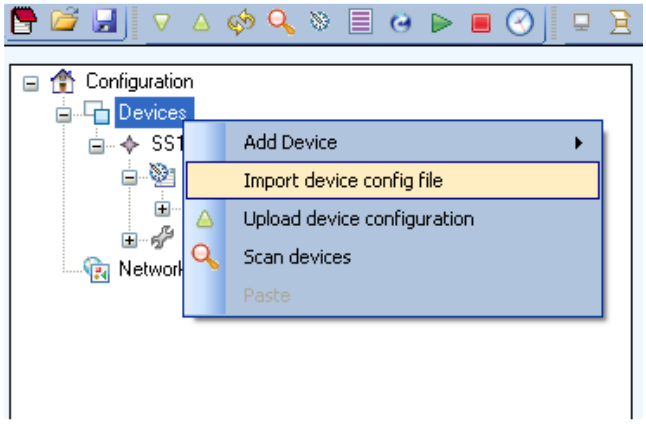
5.3.2. Save Configuration File

Cilck on the save button or **File** → **Save** to save the configured file. The saved file will be in .ecc format.

Also user can export the XML format of the configuration. Right click on Protocol configuration in the
work space and select Export device config file to export the file as shown in the figure. Save or export option can be used for keeping the file for future use.



The ecc format file can be opened directly while using the EasyConnect application. But the xml file has to be imported to the EasyConnect while using it again. Right click on **Devices** in the work space and select **Import device config file** to import the file as shown in the figure below:



5.4. File Transfer Support

SIC-A protocol gateways have support for uploading and downloading all kinds of files through the File Transfer channel, if they are supported in the firmware. File transfer is done by configuring a File Transfer Master/Slave channel through EasyConnect.

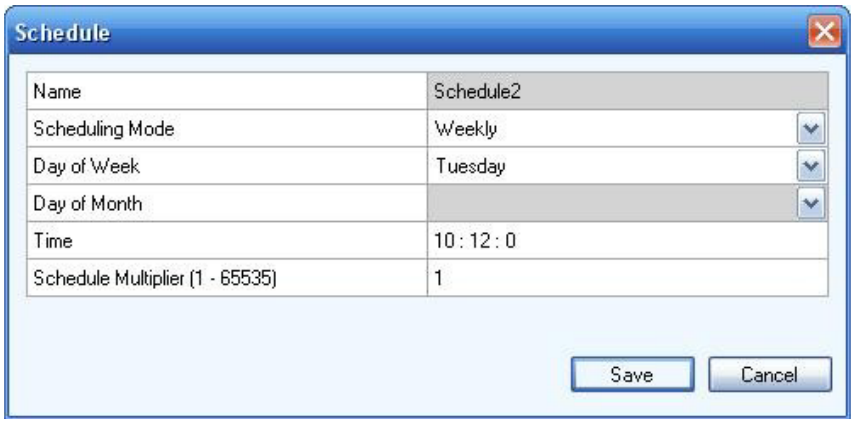
File transfer master channel is able to connect with FTP/SFTP server programs running on a given remote system and upload/download files and folders. File transfer master configuration includes a schedule and file/folder details. File transfer slave will setup FTP/SFTP sever inside the gateway to which FTP/SFTP clients can connect. There is a folder size limiting functionality implemented for these protocols, which helps in keeping the given folders within a maximum size.

Following is a brief description of the steps involved in configuring a File Transfer master/slave channel in EasyConnect.

5.4.1. Configuring File Transfer Master Channel

The steps for configuring File Transfer Master channel are as follows:

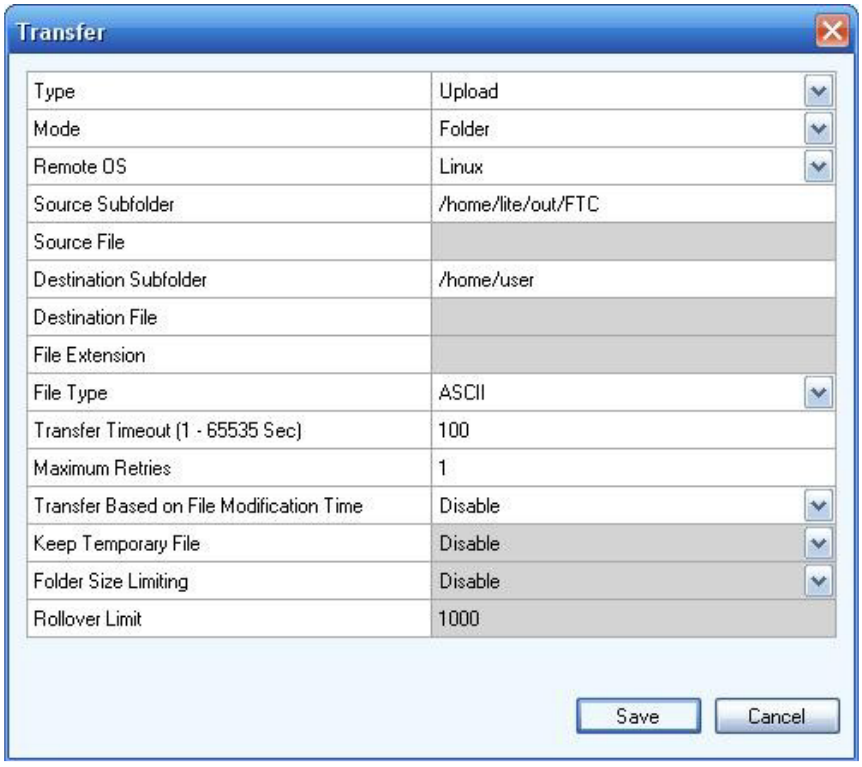
1) Choose File Transfer Master from Add Channel menu in Protocol Configuration
2) Type **Remote IP Address** in which FTP/SFTP server is running
3) Select **Protocol Supported** and type **Port No** in the corresponding fields.
4) Now right click on the **File Transfer Master** channel and choose the option **Add Station**.
5) In the **General** tab of node parameters, select **Authentication Scheme**, type **user name**, **password** and type the **Connection Timeout**.
6) In **Scheduled Transfer** tab, add a schedule by specifying the time period for the scheduled transfer to run. User can add as many schedules as required.



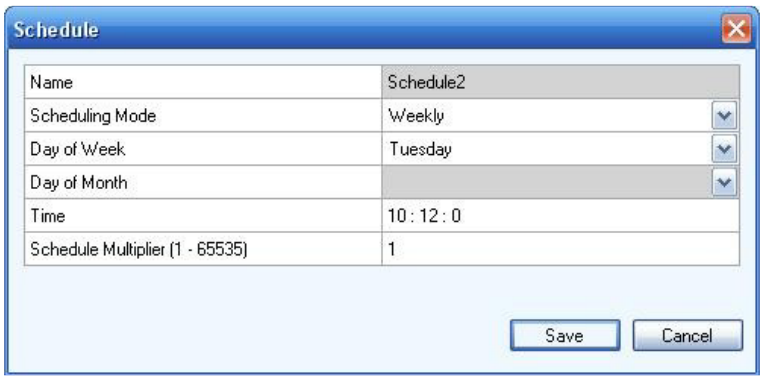
7) Now click on the schedule under which user want to add a transfer task. Add a new transfer by
specifying the transfer details.

5.4.2. Configuring File Transfer Slave Channel

Steps for configuring file transfer slave are as follows:
1) Choose File Transfer Slave from Add Channel menu in Protocol Configuration
2) Select Protocol Supported, type **Listen Port** and **Inactivity Time Period** in the corresponding fields.
3) Now right click on the **File Transfer Slave** channel and choose the option **Add Station**.
4) In the General tab of node parameters select **Authentication Scheme**.
5) In the **Users List** tab, add users by specifying **User name** and **Password**. The remote clients can use them for password authentication.



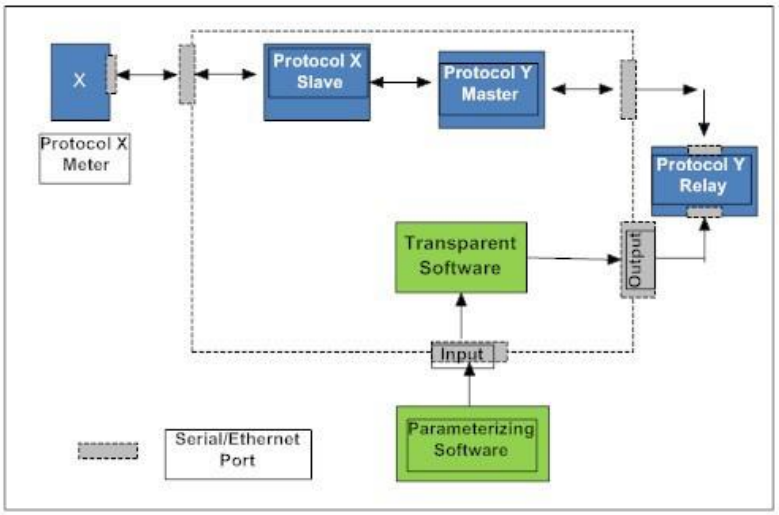
6) In **Size Limit** tab add a schedule for running size limiter by specifying the time period. User can add
many schedules as required. Now click on the schedule and add folder by specifying the **Folder Name** and **Rollover Limit**. The size of the specified folder will be checked and limited to the rollover limit in the scheduled interval.




Folder
Folder Name
/home/lite/out/
Rollover Limit
1024
Save
Cancel

5.5. Parametrization Through Pass-Through (Transparent) Channel

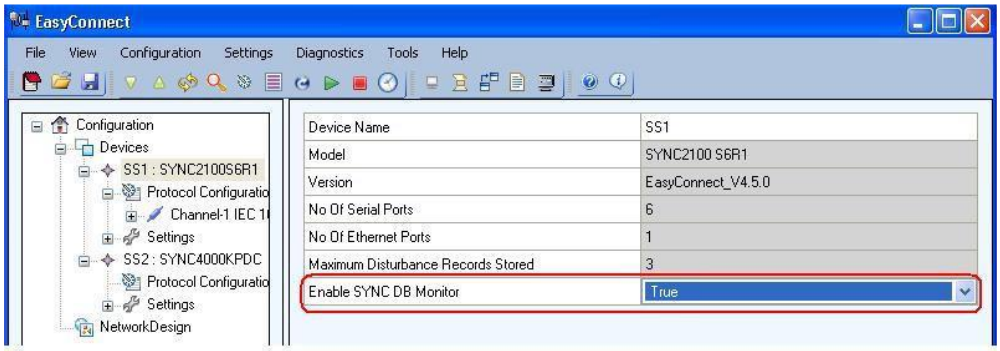
This module in the SIC-A protocol converter enables to parametrize the relays or IEDs with the particular configuration software for the relay/IED. The transparent channel (pass-through) routes the frames directly from the input (server) port to the output (client) port and in the reverse direction. The Transparent Peer protocol can be associated to either any of the serial communication port of the SIC-A or a TCP/IP client port. SIC-A must be loaded with the license and firmware supporting Transparent Peer interface module and the configuration file containing all the specific information for the communication.
The detailed block diagram is shown in the figure below:



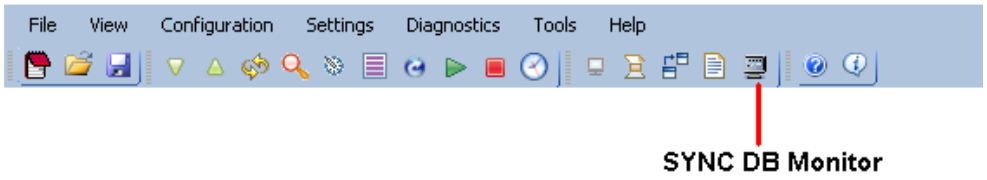
5.6. SYNC DB Monitor

SYNC DB Monitor provides an option to view the internal database of the gateways. It provides an online Gateway Database monitoring facility within the EasyConnect. It displays the data along with their value, quality and time stamp.

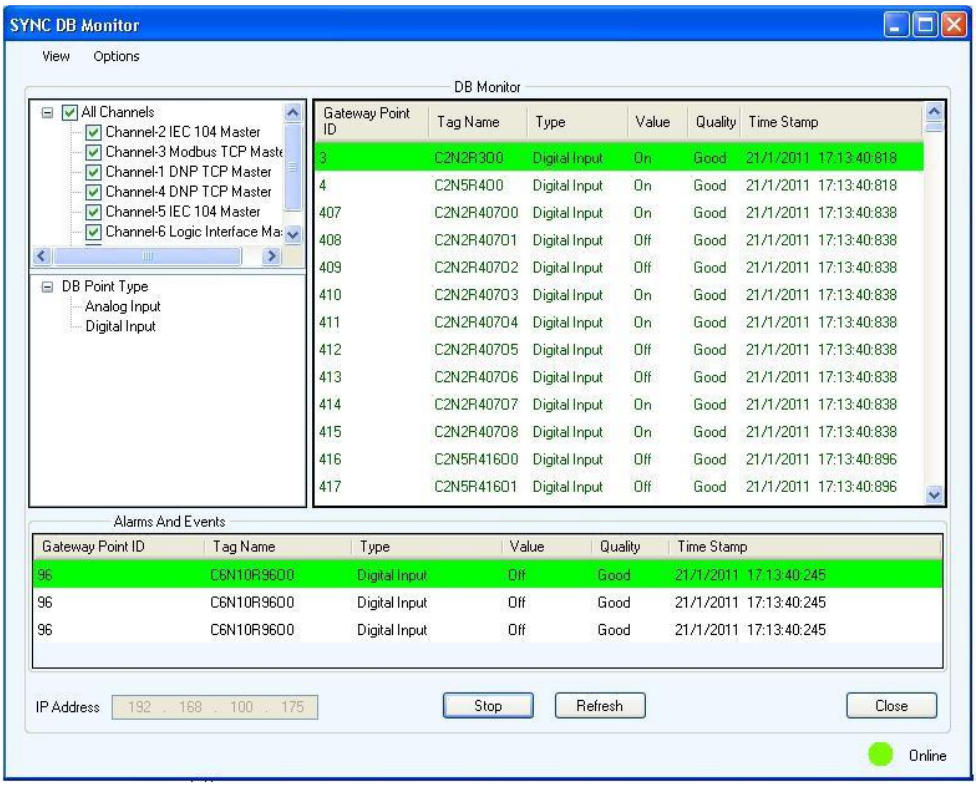
Note: The TCP port number 64727 is used for the SYNC DB communication.
The firmware recommended for SYNC DB is GPC (2.19.0 or above) and DCCP (2.13.0 or above).
For enabling SYNC DB Monitor, user must select **True** for **Enable SYNC DB Monitor** option in device
configuration and download the configuration. Refer the figure given below:



The user must select a device and launch the SYNC DB Monitor by clicking the **SYNC DB Monitor** button provided on the toolbar as shown in the below figure:



Now the **SYNC DB Monitor** window will appear on the screen as shown in the following figure. This window displays the details of Gateway Point IDs configured for the internal master channels.



Each configured point in the profile has a unique row number and the Gateway Point ID is same as the unique row number. The starting Gateway Point ID of each row will be displayed in the profile view itself as shown below. User can monitor the status of each point by using its Gateway Point ID.

Row Number	Gateway Point ID	Basic Type	Object Type	Starting Point Index	Number Of Points
Row1	1	Digital Input	Binary Inputs	65535	1
Row2	2	Digital Input	Binary Inputs	1	10
Row12	12	Analog Input	Analog Inputs	1	10
Row22	22	Analog Input	Analog Inputs	11	10
Row32	32	Digital Input	Binary Output Sta...	1	10
Row42	42	Analog Input	Analog Output St...	1	10
Row52	52	Digital Output	Binary Output Co...	1	2

5.6.1. SYNC DB Monitor – Menu Items

The SYNC DB Monitor contains menu items like view and option that allows the user to add or remove various options and values in the DB window as required

5.6.1.1. View

The view item in the menu bar enables user to include the type and tag name in the DB monitor window.

It can be done by selecting or deselecting type and tag name from the view item.

5.6.1.2. Option

The Option in the menu bar facilitates the user to add or remove Alarm window from the DB Monitor

Window. It can be done by selecting and deselecting Alarm window from Option menu.

5.6.2. Function Keys

The following buttons are used in the SYNC DB Monitor to start, stop and refresh the Monitoring window:

5.6.2.1. Start
User can start DB Monitor after entering IP of the configured Gateway in the space provided for IP
address. It shows error if:

1.The firmware is not running
2.IP address is not valid or empty
3.Current configuration is not matching with gateway configuration
4.Unable to start communication.

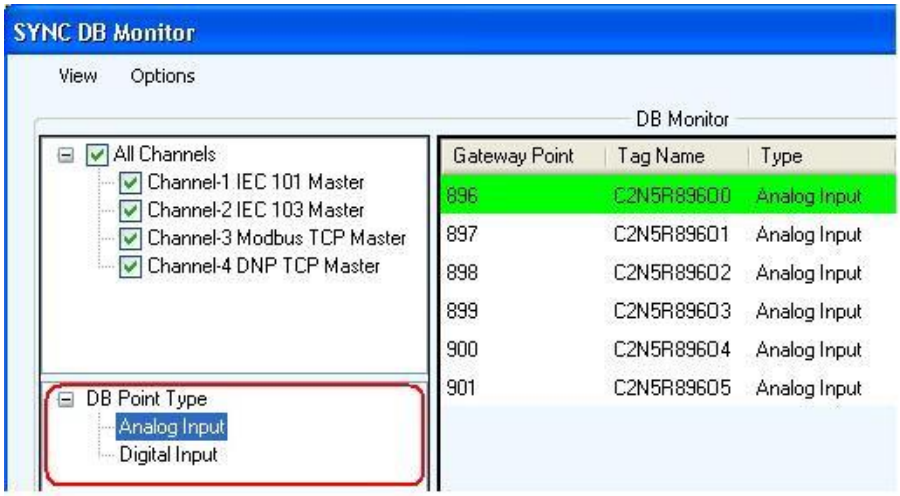
5.6.2.2. Stop
User can stop DB monitor at anytime in between the communication by clicking the stop button. It shows error if it is unable to stop communication.

5.6.2.3. Refresh
The DB monitor is automatically updated in every 5 minutes. A refresh button is provided on the window which enables the user to manually refresh the data populated on the DB window. It will display new values of all database points.

5.6.3. Support Features
The SYNC DB Monitor provides various features to the user like Channel Filtering, Data Type Filtering, Status Monitor, Alarm Window and Watch Window.

5.6.3.1. Channel Filtering
Channel filtering option in DB monitor allows the user to monitor the Gateway Point IDs of the specified channels. This can be done by selecting or deselecting the required channels. Only the data points of selected channels will be displayed on the right hand side of DB Monitor. This filtering can be done even in between communication.

5.6.3.2. Data Type Filtering
This enables the user to filter the Analog and Digital points separately so that the points of selected type will only be displayed on the form. User must select the required type in the tree view as shown below:

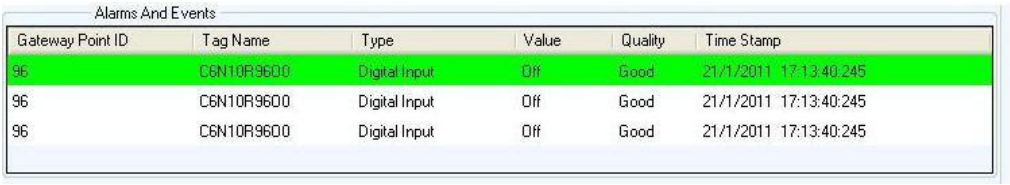


5.6.3.3. Status Monitor
The SYNC DB Monitor notifies the user whenever a communication breakage occurs. An indication is
provided on the bottom right of the DB Window. It shows a green color with the status as Online when

communication session is online. It shows a red color with the status as Offline when communication
failure occurs. This helps the user to easily monitor the communication status in SYNC DB Monitor.

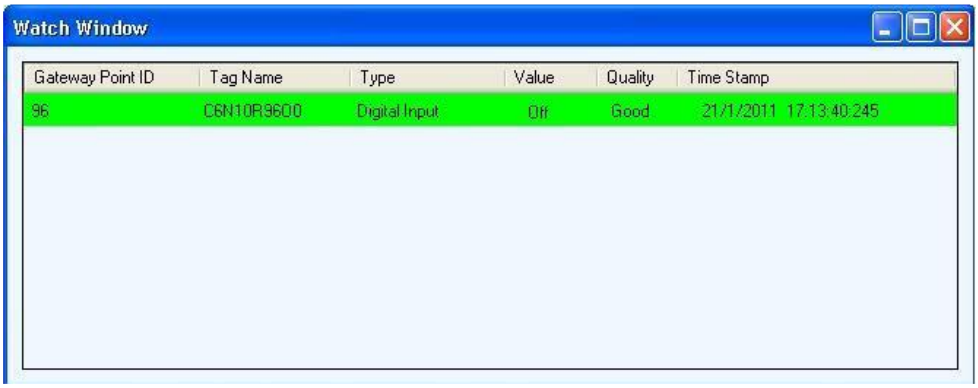
5.6.3.4. Alarm Window

Within the SYNC DB monitor, an alarm window is provided which displays the events occurring in the
digital input points. It facilitates the user to check the changes occurring in the data points very easily
along with its time stamp. The user can also remove the events from alarm window whenever required
by right click on the mouse button from the alarm window.

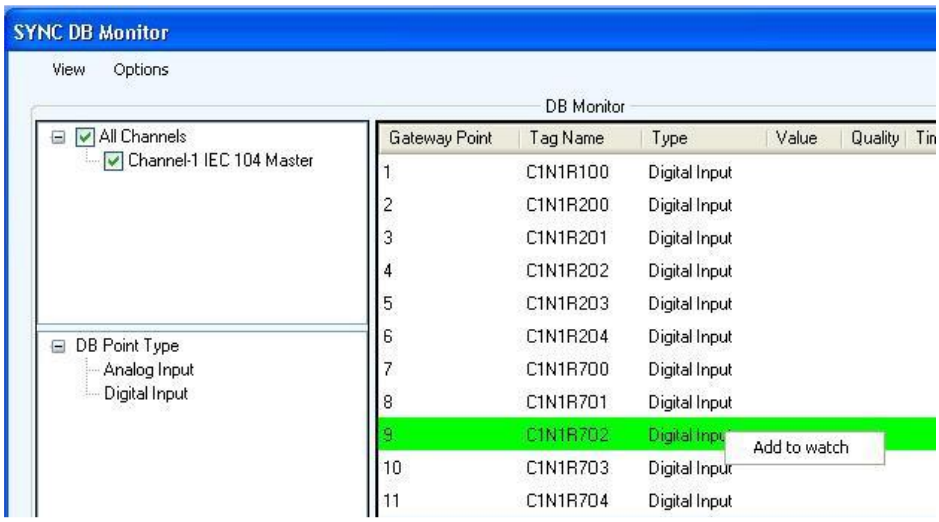


5.6.3.5. Watch Window

This is an important feature available in SYNC DB monitor. User can add critical/important points to the watch window and can easily monitor points from the window. There is also an option to remove the points from the watch window by right click on the mouse button within the watch window.

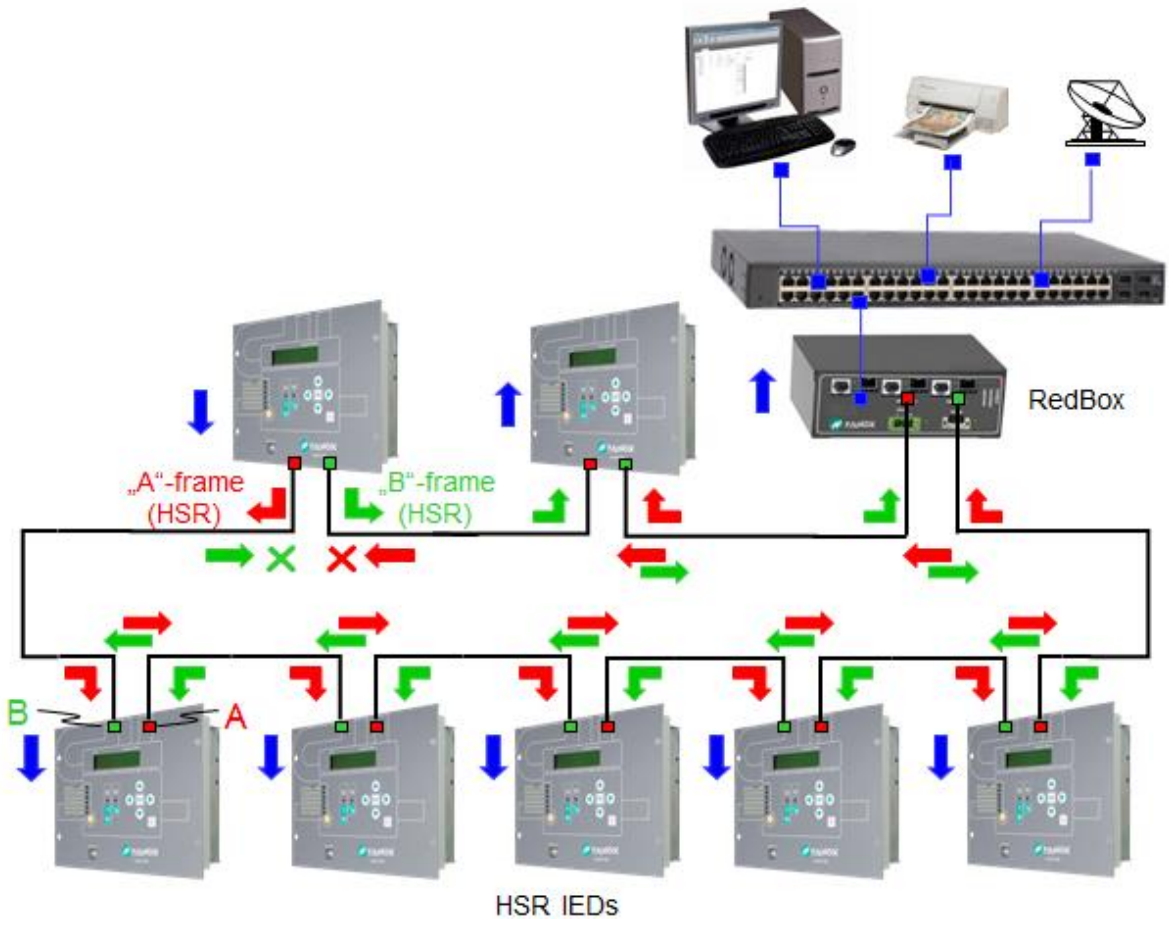


User can right click on the mouse button to add points to the watch window. It is also possible to select multiple points and can add it in the watch window.

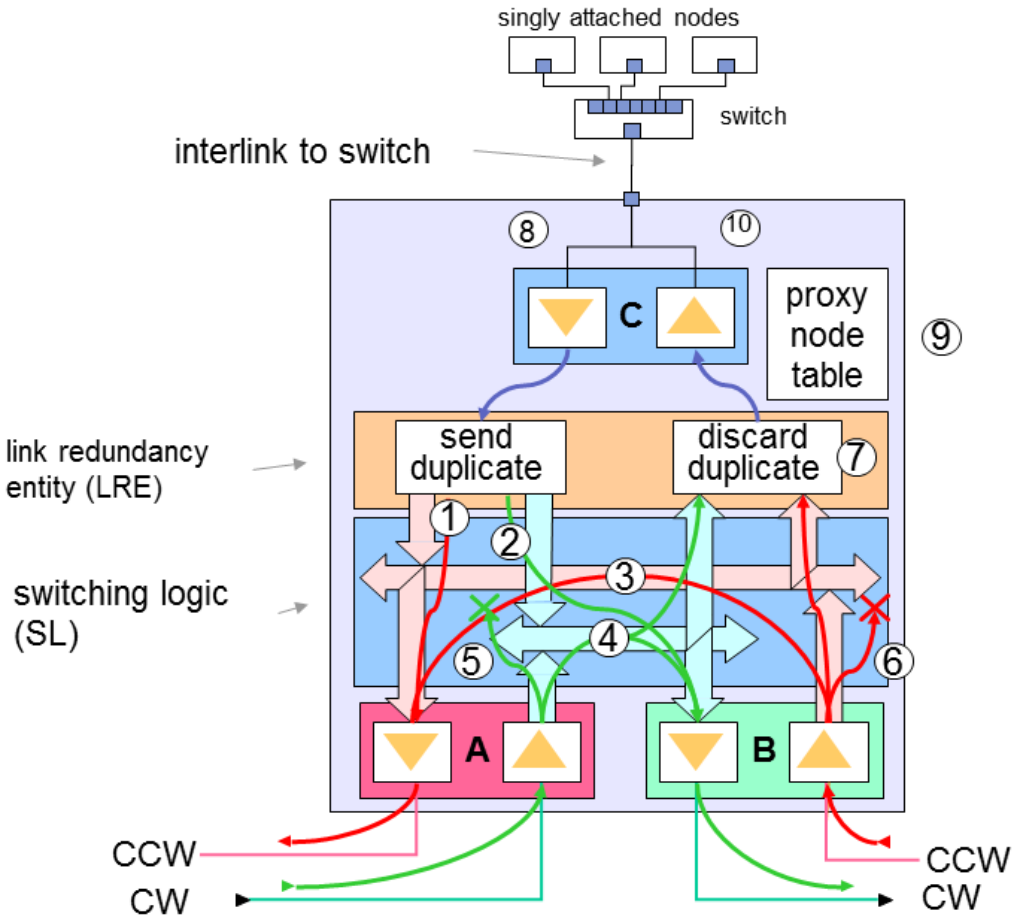

SYNC DB Monitor
View
Options
DB Monitor
All Channels
Channel-1 IEC 104 Master
DB Point Type
Analog Input
Digital Input
Gateway Point
Tag Name
Type
Value
Quality
1 C1N1R100 Digital Input
2 C1N1R200 Digital Input
3 C1N1R201 Digital Input
4 C1N1R202 Digital Input
5 C1N1R203 Digital Input
6 C1N1R204 Digital Input
7 C1N1R700 Digital Input
8 C1N1R701 Digital Input
9 C1N1R702 Digital Input
10 C1N1R703 Digital Input
11 C1N1R704 Digital Input
Add to watch

6. SIC-A WORKING AS A REDBOX

SIC-A device working as a RedBox, allows to join HSR rings to the conventional Ethernet.
Legacy nodes such as laptops or printers do not recognize the HSR tag and must be attached through a RedBox (Redundancy Box) which acts as their proxy.
The RedBox generates the same management frames as if its represented nodes would be inserted directly in the ring, and removes the frames it injected into the ring when they come back.



The RedBox operates as a proxy for a number of singly attached nodes.
To remove the frames it send from the ring, the RedBox keeps a table of nodes for which it is the proxy, e.g. by listening to the received frames (8).
It can ping the SANs to clean up the list of removed or inoperative nodes, or remove the entries after a time-out (e.g. 1 minute).
The RedBox behaves as a bridge for non-HSR traffic.



6.1. Using the RedBox

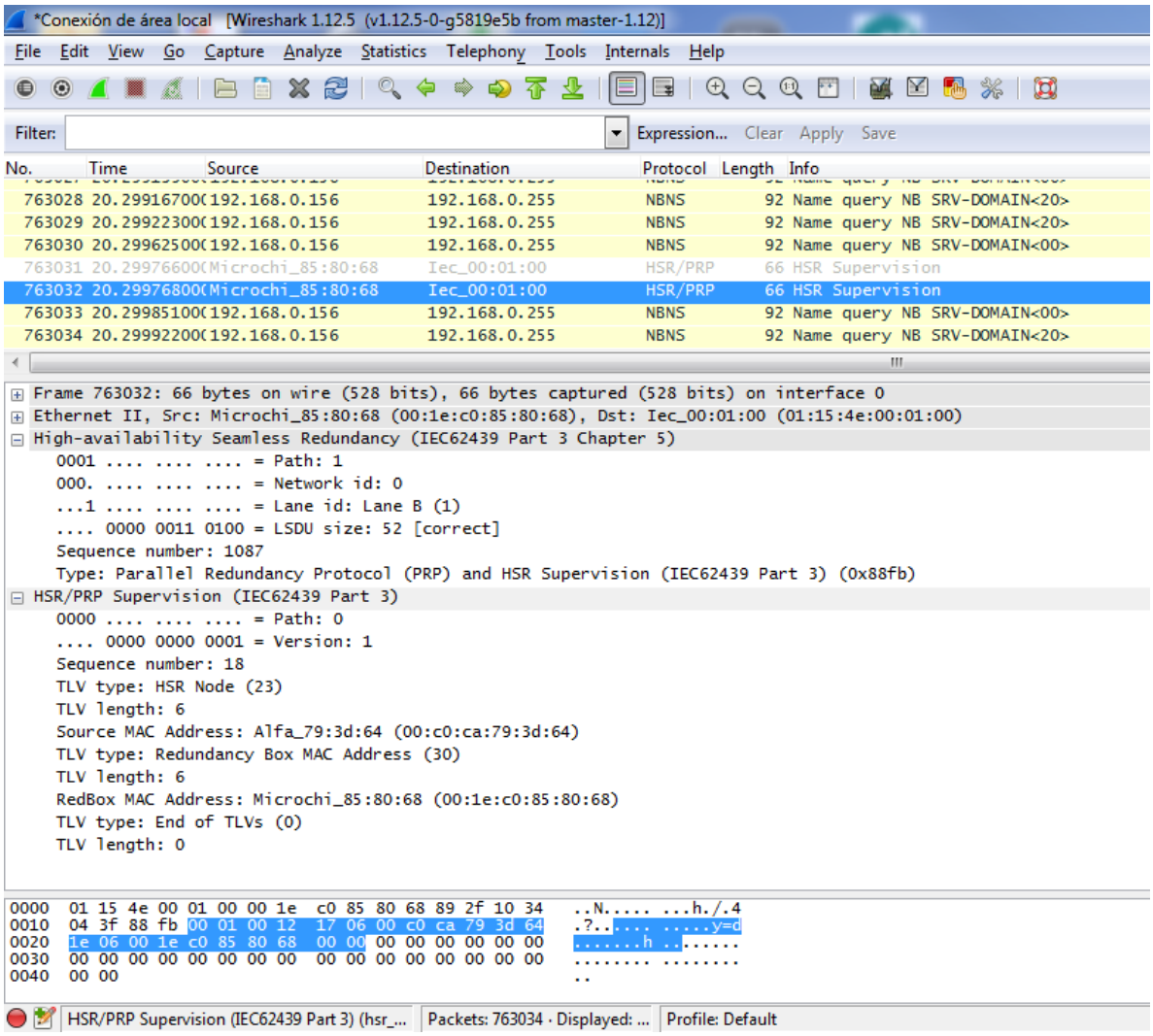
SIC-A device working as a RedBox, is an unmanaged device, this mean that it is not necessary to configure it.
It is only necessary to distinguish the redundant ports HSR1 and HSR2 from the conventional port LAN and connect the cables in the correct connector.

If the connection is not correct, the communication won't work. The redundant ports should not be connected to conventional Ethernet ports and SIC-A's Ethernet port should not be connected to a HSR ring.

The RedBox sends HSR/PRP supervision frames to the conventional port in order to inform the existing devices in each part of the net.
It is necessary to take this into account not to produce a malfunction of the network.

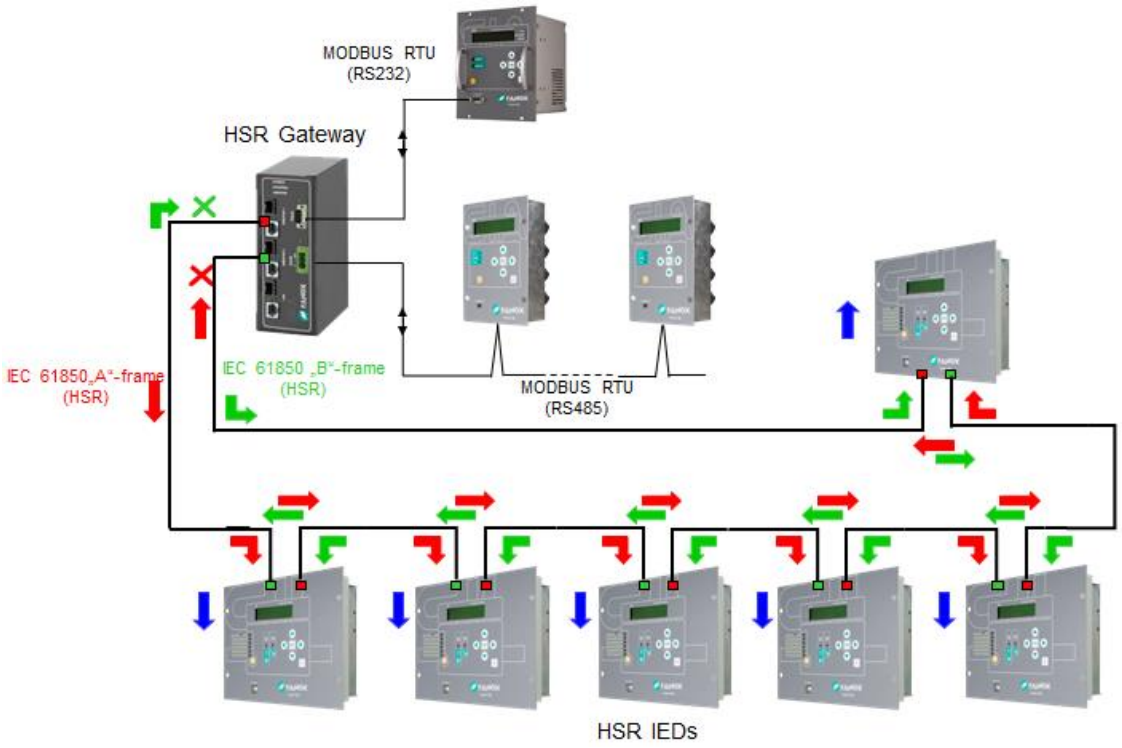
NOTE: It is recommendable to independent the communication of the equipment of a substation from the conventional network.

HSR/PRP Supervision frames:

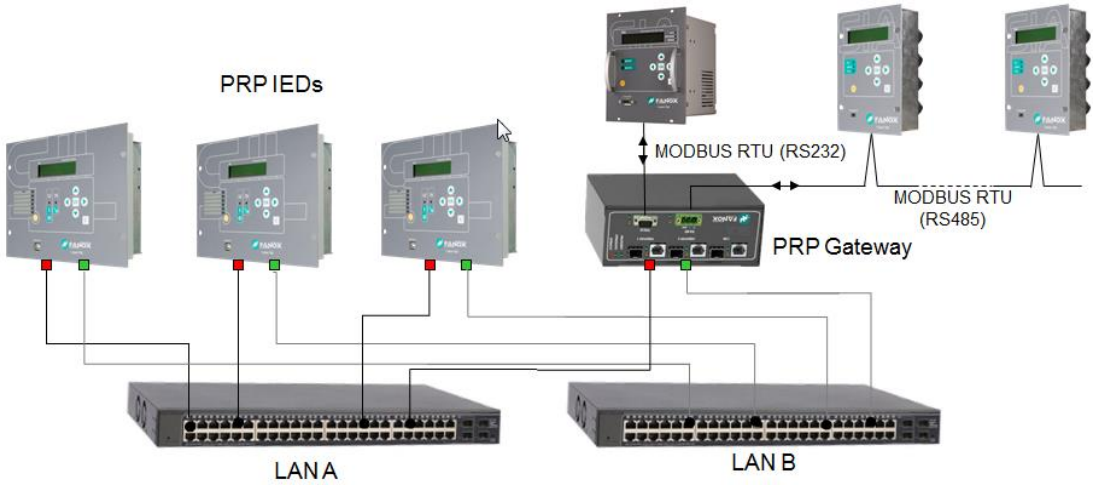

*Conexión de área local [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
763028 20.29916700 192.168.0.156 192.168.0.255 NBNS 92 Name query NB SRV-DOMAIN<20>
763029 20.29922300 192.168.0.156 192.168.0.255 NBNS 92 Name query NB SRV-DOMAIN<20>
763030 20.29962500 192.168.0.156 192.168.0.255 NBNS 92 Name query NB SRV-DOMAIN<00>
763031 20.29976600 Microchi_85:80:68 Iec_00:01:00 HSR/PRP 66 HSR Supervision
763032 20.29976800 Microchi_85:80:68 Iec_00:01:00 HSR/PRP 66 HSR Supervision
763033 20.29985100 192.168.0.156 192.168.0.255 NBNS 92 Name query NB SRV-DOMAIN<00>
763034 20.29992200 192.168.0.156 192.168.0.255 NBNS 92 Name query NB SRV-DOMAIN<20>
Frame 763032: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Microchi_85:80:68 (00:1e:c0:85:80:68), Dst: Iec_00:01:00 (01:15:4e:00:01:00)
High-availability Seamless Redundancy (IEC62439 Part 3 Chapter 5)
0001 .... = Path: 1
000. .... = Network id: 0
...1 .... = Lane id: Lane B (1)
.... 0000 0011 0100 = LSDU size: 52 [correct]
Sequence number: 1087
Type: Parallel Redundancy Protocol (PRP) and HSR Supervision (IEC62439 Part 3) (0x88fb)
HSR/PRP Supervision (IEC62439 Part 3)
0000 .... = Path: 0
.... 0000 0000 0001 = Version: 1
Sequence number: 18
TLV type: HSR Node (23)
TLV length: 6
Source MAC Address: Alfa_79:3d:64 (00:c0:ca:79:3d:64)
TLV type: Redundancy Box MAC Address (30)
TLV length: 6
RedBox MAC Address: Microchi_85:80:68 (00:1e:c0:85:80:68)
TLV type: End of TLVs (0)
TLV length: 0
0000 01 15 4e 00 01 00 00 1e c0 85 80 68 89 2f 10 34 ..N..... ...h./.4
0010 04 3f 88 fb 00 01 00 12 17 06 00 c0 ca 79 3d 64 .?..... .....y=d
0020 1e 06 00 1e c0 85 80 68 00 00 00 00 00 00 00 00 ....h ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 ..
HSR/PRP Supervision (IEC62439 Part 3) (hsr_...
Packets: 763034 · Displayed: ...
Profile: Default

7. SIC-A WORKING AS A REDUNDANT PROTOCOL GATEWAY

SIC-A device working as a Redundant protocol gateway takes advantage of the whole functionality of the equipment: protocol conversion + PRP/HSR redundancy.
This SIC-A variant works as the protocol gateway described in chapter 5. Please, refer to this chapter to configure it.
LAN port is disabled in order to enable the redundant ports.
The redundant protocol could be HSR or PRP. In the case of HSR, the expected behavior would be the same explained in chapter 6.



When PRP redundancy protocol is selected, SIC-A works attached to two independent networks of similar topology, which operate in parallel. A souce PRP device or SIC-A sends the same frame over both LANs and a destination device receives it from both LANs within a certain time, consumes the first frame and discards the duplicate.



The two LANs have no connection between them and are assumed to be fail-independent.
Redundancy can be defeated by single points of failure, such as a common power supply or a direct connection whose failure brings both network down.

Bizkaia Technology Park
Building, 604
Derio, 48160 Bizkaia SPAIN
T. +34 94 471 14 09
fds_fanox@wabtec.com
www.fanox.com