Premium and Atrium Using EcoStruxure™ Control Expert

Ethernet Network Modules

User Manual

Original instructions

10/2019

35006192.20

www.schneider-electric.com

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

© 2019 Schneider Electric. All rights reserved.

Table of Contents

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER
DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

WARNING
WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

CAUTION
CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE
NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

BEFORE YOU BEGIN

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠ WARNING
UNGUARDED EQUIPMENT ● Do not use this software and related automation equipment on equipment which does not have point-of-operation protection. ● Do not reach into machinery during operation. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

START-UP AND TEST

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check be made and that enough time is allowed to perform complete and satisfactory testing.

⚠ WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:
- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

OPERATION AND ADJUSTMENTS

The following precautions are from the NEMA Standards Publication ICS 7.1-1995 (English version prevails):

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.
- Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Book

At a Glance

Document Scope

This manual describes the implementation of an Ethernet network on Premium and Atrium PLCs using Control Expert software.

Validity Note

This document is valid for EcoStruxure™ Control Expert 14.1 or later.

The technical characteristics of the devices described in the present document also appear online. To access the information online:

Step	Action
1	Go to the Schneider Electric home page *www.schneider-electric.com*.
2	In the **Search** box type the reference of a product or the name of a product range. ● Do not include blank spaces in the reference or product range. ● To get information on grouping similar modules, use asterisks (*).
3	If you entered a reference, go to the **Product Datasheets** search results and click on the reference that interests you. If you entered the name of a product range, go to the **Product Ranges** search results and click on the product range that interests you.
4	If more than one reference appears in the **Products** search results, click on the reference that interests you.
5	Depending on the size of your screen, you may need to scroll down to see the datasheet.
6	To save or print a datasheet as a .pdf file, click **Download XXX product datasheet**.

The characteristics that are presented in the present document should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the document and online information, use the online information as your reference.

Related Documents

Title of Documentation	Reference Number
Communication Services and Architectures, Reference Manual	35010500 (English), 35010501 (French), 35006176 (German), 35013966 (Italian), 35006177 (Spanish), 35012196 (Chinese)

You can download these technical publications and other technical information from our website at https://www.schneider-electric.com/en/download

Part I
Introduction to Ethernet Communication

Chapter 1
Communication via Ethernet Network

Overview

This chapter provides some general points about communication via Ethernet network and introduces the Ethernet services.

What Is in This Chapter?

This chapter contains the following topics:

General

Introduction

Premium PLCs can communicate with Ethernet networks using:
- modules TSX ETY 110 and TSX ETY 110 WS
- module TSX ETY 210
- modules TSX ETY 4103, TSX ETY PORT (TSX P57 1634/2634/3634), and TSX ETY5103
- Ethernet link of the TSX P57 6634/5634/4634 coprocessor

They have several types of interfaces.

TSX ETY 110

You can connect to an ETHWAY profile network that supports the following:
- common words *(see page 143)*
- UNI-TE messaging *(see page 78)*

You can connect to a TCP/IP profile network that supports the following:
- UNI-TE and Modbus messaging *(see page 85)*
- SNMP management *(see page 101)*

TSX ETY 110 WS

Connection can be made to an ETHWAY profile network supporting the following:
- common words *(see page 143)*
- UNI-TE messaging *(see page 78)*

Connection can be made to a TCP/IP profile network supporting the following:
- UNI-TE and Modbus messaging *(see page 85)*
- SNMP management *(see page 101)*
- with TCP direct access
- access to the HTTP Server user pages *(see page 141)*

TSX ETY 210

Connection can be made to an ETHWAY profile network supporting the following:
- common words *(see page 143)*
- UNI-TE messaging *(see page 78)*

Connection can be made to a TCP/IP profile network supporting the following:
- UNI-TE and Modbus messaging *(see page 85)*
- SNMP management *(see page 101)*
- specific to redundancy

TSX ETY 4103/PORT and TSX P57 6634/5634/4634

They allow connection to a TCP/IP profile network supporting the following:

- UNI-TE and Modbus messaging *(see page 85)*
- SNMP management *(see page 101)*
- electronic mail notification service (SMTP) *(see page 212)*
- input/output management (I/O scanner) *(see page 91)*
- IP address management (BOOTP/DHCP) *(see page 97)*
- Dynamic IP addressing *(see page 152)* (TSX ETY 4103/Port, version 3.2 or higher only)
- access to the built-in Web server *(see page 124)*
- common data exchange between stations (Global Data) *(see page 104)*
- diagnostics from Web pages *(see page 123)*

TSX ETY 5103

Connection can be made to a TCP/IP profile network, which is necessary when using FactoryCast and which supports the following:

- UNI-TE and Modbus messaging *(see page 85)*
- SNMP management *(see page 101)*
- electronic mail notification service (SMTP) *(see page 212)*
- time synchronization service (NTP) *(see page 204)*
- input/output management (I/O scanner) *(see page 91)*
- IP address management (BOOTP/DHCP) *(see page 97)*
- Dynamic IP addressing *(see page 152)* (version 3.2 or higher only)
- access to the built-in web server *(see page 124)*
- common data exchange between stations (Global Data) *(see page 104)*
- diagnostics from Web pages *(see page 123)*
- access to the HTTP Server user pages *(see page 141)*
- TCP direct access

TSX WMY 100

They allow connection to a TCP/IP profile network supporting the following:

- UNI-TE and Modbus messaging *(see page 85)*
- SNMP management *(see page 101)*
- access to the built-in web server *(see page 124)*
- diagnostics from Web pages *(see page 123)*

More Information

Elsewhere in this guide is a comparison of the available services for the different modules *(see page 24)*.

Details of Available Services

Selection Guide

The services available depend on the type of Ethernet module you select:

Service	TSX ETY 110	TSX ETY 110 WS	TSX ETY 210	TSX ETY 4103 / TSX ETY PORT	TSX ETY 5103	TSX P57 6634/5634/4634
Connection at 10 Mbits/s	Half/Full Duplex	Half/Full Duplex	Half/Full Duplex	Half/Full Duplex	Half/Full Duplex	Half/Full Duplex
Connection at 100 Mbits/s	-	-	-	Half/Full Duplex	Half/Full Duplex	Half/Full Duplex
TCP/IP	X	X	X	X	X	X
SNMP						
Standard MIB	X	X	X	X	X	X
MIB Ethernet Transparent Ready	-	-	-	X	X	X
I/O Scanner	-	-	-	X (1)	X	X
Address Server (BOOT/DHCP)	-	-	-	X (1)	X	X
UNI-TE messaging	X	X	X	X	X	X
Modbus Messaging	X	X	X	X	X	X
ETHWAY profile	X	X	X	-	-	-
Software loading via FTP (firmware)	X	X	X	X	X	X
Installed HTTP server	-	-	-	X	X	X
Global Data	-	-	-	X (1)	X	X
Diagnostics from Web pages	-	-	-	X	X	X
User WEB pages HTTP server	-	X	-	-	X	-
Redundancy	-	-	X	X	X	-
TCP direct access	-	X	-	-	X	-

Service	TSX ETY 110	TSX ETY 110 WS	TSX ETY 210	TSX ETY 4103 / TSX ETY PORT	TSX ETY 5103	TSX P57 6634/5634/4634
Electronic mail notification service	-	-	-	X	X	X
Time synchronization service	-	-	-	-	X	-
Legend						
X	Available					
-	Not available					

Installation Phase Overview

Introduction

The software installation of the application-specific modules is carried out from the various Control Expert editors:

- in offline mode
- in online mode

If you do not have a processor to connect to, Control Expert allows you to carry out an initial test using the simulator. In this case the installation *(see page 27)* is different.

The following order of installation phases is recommended but it is possible to change the order of certain phases (for example, starting with the configuration phase).

Installation Phases with Processor

The following table shows the various phases of installation with the processor:

Phase	Description	Mode
Declaration of variables	Declaration of IODDT-type variables for the application-specific modules and variables of the project.	Offline (1)
Programming	Project programming.	Offline (1)
Configuration	Declaration of modules.	Offline
	Module channel configuration.	
	Entry of configuration parameters.	
Association	Association of IODDTs with the channels configured (variable editor).	Offline (1)
Generation	Project generation (analysis and editing of links).	Offline
Transfer	Transfer project to PLC.	Online
Adjustment/Debugging	Project debugging from debug screens, animation tables.	Online
	Modifying the program and adjustment parameters.	
Documentation	Building documentation file and printing miscellaneous information relating to the project.	Online (1)
Operation/Diagnostic	Displaying miscellaneous information necessary for supervisory control of the project.	Online
	Diagnostic of project and modules.	
Key:		
(1)	These various phases can also be performed in the other mode.	

Implementation Phases with Simulator

The following table shows the various phases of installation with the simulator.

Phase	Description	Mode
Declaration of variables	Declaration of IODDT-type variables for the application-specific modules and variables of the project.	Offline (1)
Programming	Project programming.	Offline (1)
Configuration	Declaration of modules.	Offline
	Module channel configuration.	
	Entry of configuration parameters.	
Association	Association of IODDTs with the modules configured (variable editor).	Offline (1)
Generation	Project generation (analysis and editing of links).	Offline
Transfer	Transfer project to simulator.	Online
Simulation	Program simulation without inputs/outputs.	Online
Adjustment/Debugging	Project debugging from debug screens, animation tables.	Online
	Modifying the program and adjustment parameters.	
Key:		
(1)	These various phases can also be performed in the other mode.	

NOTE: The simulator is only used for the discrete or analog modules.

Part II
Ethernet Communication Hardware Installation

Aim of this Part

This Part describes Ethernet communication hardware installation for Premium and Atrium PLCs.

What Is in This Part?

This part contains the following chapters:

Chapter 2
Communication: TSX ETY 110 Module

Aim of this Chapter

This chapter deals with installing the TSX ETY 110 Ethernet network module in a Premium/Atrium PLC.

What Is in This Chapter?

This chapter contains the following sections:

Section 2.1
General Features of the TSX ETY 110

Introduction to the TSX ETY 110

Overview

Communication module **TSX ETY 110** is used to communicate in an Ethernet architecture. It is made up of a communication channel which offers two types of connections:

- connection to an ETHWAY network supporting common words and X-Way UNI-TE message-handling services on an ETHWAY profile
- connection to a TCP-IP network supporting the X-Way UNI-TE message-handling service

This module also ensures transparent routing of X-Way UNI-TE messages from a TCP-IP network to an X-Way network, and vice versa.

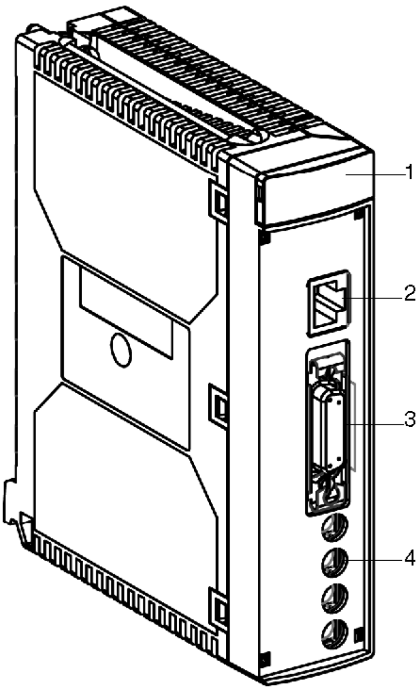
Please refer to the Ethernet reference manual for wiring an ETHWAY architecture.

Section 2.2
Physical Description of the TSX ETY 110

Physical Description of the TSX ETY 110

Illustration

The TSX ETY 110 module is a single (half size) module that is inserted in a rack slot of a Premium PLC station.



1 display panel indicating state of module
2 standard connector for 10baseT (RJ45) interface
3 standard connector for 10base5 (AUI) interface
4 thumbwheel to define station number and network number

Section 2.3
Ethernet Channel Characteristics of the TSX ETY 100

Characteristics of Ethernet channel

General

The module is made up of two standard interfaces for connecting to a network:
- One 10 BASE-T interface on front panel of the module, comprising an RJ45 connector, which is used for a point to point link via a linking cable made up of two twisted pairs of impedance 100 Ω ± 15 Ω.
- A 10 BASE-5 or AUI interface on front panel of module comprising a SUB-D 15-pin connector, used to link to network by branching. This interface is also used to supply active connection devices (Taps). It complies with the IEC 802 3 standard and is used to connect any device which complies with this standard.

The type of connection is recognized automatically as soon as connection is made to the network.

Services and operations supported by the module:

TCP/IP services	UNI-TE	• Client/server mode • Synchronous requests of 256 bytes • Asynchronous requests of 1 Kbyte
Ethway services	UNI-TE	• Client/server mode • Synchronous requests of 256 bytes • Asynchronous requests of 1 Kbyte
	Common words	• Shared database of 256 words
	Application to application	• Message exchange in point to point 256 bytes max.
Common services		• X-Way inter-network routing • X-Way /UNI-TE routing • Module diagnostics

NOTE: The Ethernet driver supports the Ethernet II and (LCC+SNAP) 802.3 formats on TCP-IP and LCC 802.3 on Ethway.

Section 2.4
Installing the TSX ETY 110 Module

Introduction

This section describes the installation of the TSX ETY 110 in a PLC.

What Is in This Section?

This section contains the following topics:

Installation Introduction

Overview

The TSX ETY 110 communication module is mounted in the rack slot of a Premium/Atrium PLC station. It can be installed in any available slot (except in the offset X Bus racks), on condition that the supply constraints of the rack are observed. Elsewhere in this guide are the electrical characteristics for the TSX ETY 110 *(see page 46)*.

Selecting the Type of Processor

Selection Guide

Selecting the processor to control the PLC station depends on the number of network connections required:

Processors	Maximum Number of Network Connections	Maximum Number of ETY 4103/5103 per Station (*)
TSX P57 104(1)	1	1
TSX P57 154(1)	1	1
TSX P57 204	1	1
TSX PCI 57 204	1	1
TSX P57 254(1)	1	1
TSX P57 2634	1	0
TSX H57 24M3)	1	3
TSX H57 44M(3)	1	3
TSX P57 2834(1)	1 2 (**)	0
TSX P57 304	3	3
TSX P57 354(1)	3	3
TSX P57 3634	3	2
TSX P57 454	4	4
TSX PCI 57 454(1)	4	4
TSX P57 4834(1)	4	3
TSX P57 554(1)	4	4
TSX P57 5634	4	3
TSX P57 4634	4	3
TSX P57 6634(2)	4	3

(*) Compatible with 5V power supply.
(**) Supports two network connections if the PLC is used in Warm Standby.
(1) Available for Unity Pro 2.0 or later.
(2) Available for Unity Pro 4.0 or later.
(3) Hot Standby processors *(see Premium using EcoStruxure™ Control Expert, Hot Standby, User Manual)*

Wiring/Unwiring the TSX ETY 110 with Power Switched On

The Module

Module TSX ETY 110 can be wired or unwired with power switched on without disrupting the operation of the station.

The module does not have a RAM internal backup memory function. The RAM is erased when power is switched off.

The module initializes itself when power is switched on. A communication break can be expected during this intervention.

The Link

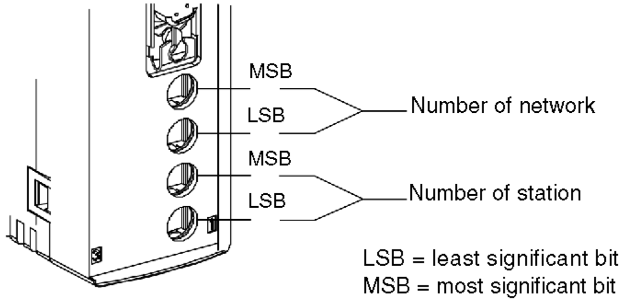
The 15-pin SUB-D connectors of the AUI interface and the RJ-45 connector of the 10 BASE-T interface can be connected or disconnected when power is on. A communication break can therefore be expected in the application in progress.

Station Address Coding

Thumbwheel Settings

⚠ CAUTION
UNINTENDED EQUIPMENT OPERATION
In an Ethernet network, there must only be one MAC address for each station. Before modifying these addresses you must check that they comply with the addressing plan of the carrier. If two devices have the same MAC address, information may be sent to the wrong destination.
Failure to follow these instructions can result in injury or equipment damage.

Four thumbwheels, which can be accessed from the front panel, are used to encode the network number and the station number.



Here is the range of possible coding values in hexadecimal:

Network Number	Station Number
0 to 7F	0 to 3F

For example:

Network 3: 16#03

Station 27: 16#1B

The thumbwheels are to be adjusted as follows:

0	PF
3	Pf
1	PF
B	Pf

Section 2.5
Connection via the AUI Interface

AUI interface Connection

General

The AUI interface is used to connect all types of devices which comply with the physical layer defined in the OSI 802.3 standard (10 BASE-5, 10 BASE-2, FOIRL, etc.) through a transceiver.

The TSX ETY 110 module can provide a remote power supply for the transceiver through the sub-D connector with the following characteristics:
- Imax = 0.5 mA
- 12 V-6%<Usupply<15 V+15%

The module is connected to the main cable via a transceiver and by the following branch cables:
- **TSX ETY CB 005**: 5 m length
- **TSX ETY CB 010**: 10 m length
- **TSX ETY CB 020**: 20 m length

The maximum length of a branch may be 50 m. This length can be achieved by connecting several branch cables end to end.

NOTE: Use TSX ETH ACC2 transceivers to connect two modules point to point.

Connector Pinouts

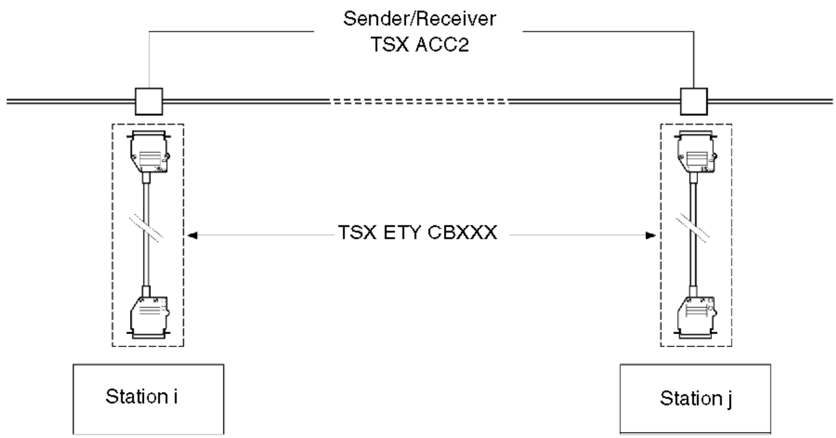
Sub-D 15 pins according to the OSI 802.3 standard:

Pin number	ISO 802.3 Designation	Use
1	CI-S (Control In Shield)	GND
2	CI-A (Control In A)	COLL+
3	DO-A (Data Out A)	TD+
4	DI-S (Data In Shield)	GND
5	DI-A (Data in A)	RD+
6	VC (Voltage Common)	GND
7	not used	
8	not used	
9	CI-B (Control In B)	COLL-
10	DO-B (Data Out B)	TD-
11	DO-S (Data Out Shield)	GND
12	DI-B (Date In B)	RD-

Pin number	ISO 802.3 Designation	Use
13	VP (Voltage Plus)	12 V
14	VS (Voltage Shield)	GND
15	not used	
Sub-D connector body	PG (Protective Ground)	Protective ground

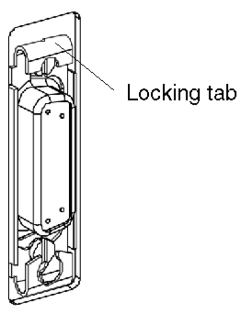
Topology

Illustration:



Locking Tab

The sub-D connector is equipped with a sliding lock system. The connector is locked by sliding the tab to the bottom. To ensure the module works properly in a disturbed environment, it is **essential** to carry out the locking procedure.



Section 2.6
10 BASE-T Interface

10 BASE-T interface

Overview

This interface has a standard type RJ45 connector. These connection cables are widely used in business.

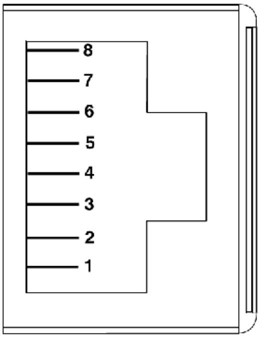
In an industrial environment, you must use a cable with the following characteristics:

- Shielded twisted double pair
- Impedance 100 Ω±15 Ω (from 1 to 16 MHz)
- Maximum attenuation 11.5 dB/100 meters
- Maximum length 100 meters

The 10 BASE-T connection is a point to point connection to form a star-shaped network. The stations are connected to concentrators or switches.

Pinouts

Illustration:



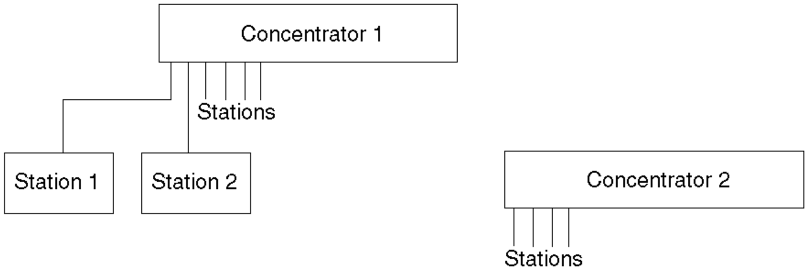
Pinout table:

Pin	Signal
1	TD+
2	TD-
3	RD+
4	not connected
5	not connected
6	RD-
7	not connected
8	not connected

Topology

This link is used to create a star-shaped network with connections in point to point. The stations are connected to a concentrator (Hub). The concentrators can also be connected in cascade to increase network size.

Illustration:

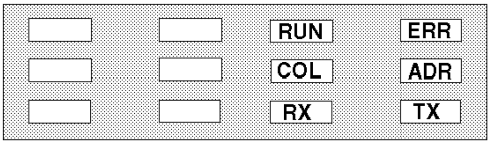


Section 2.7
Display Panel, Diagnostics

Diagnostics Display Panel

General

The display panel complies with the Premium standard



Diagnostics

Meaning of the diagnostics LEDs:

RUN	ERR	COL	ADR	TX	RX	Meaning
O	P	ns	ns	ns	ns	Module not operational.
O	F	O	O	O	O	Module not configured or configuration error.
F	F	O	O	O	O	Module running self-test.
P	O	O	O	F	O	Ethernet communication sending.
P	O	O	O	O	F	Ethernet communication receiving.
P	O	O	O	F	F	Ethernet communication in sending/receiving.
P	O	F	O	F	O	Module has detected collision.
P	O	O	P	O	O	Duplicate MAC address.
O	O	O	P	O	O	Network address beyond limits.
P = Permanently on, F = flashing, O = Off, ns = not significant						

Section 2.8
Electrical Features

TSX ETY 110 Electrical Characteristics

General

Module TSX ETY 110 can be inserted into any rack slot of a Premium/Atrium station (except an X Bus offset rack). The module consumption from the supply depends on the selection made from the transceiver remote power supply option.

Table of consumption:

Voltage	Current Consumed		Dissipated Power	
5 volts	Typical	Maximum	Typical	Maximum
with remote power supply (RJ45)	0.8 A	1.2 A	4 W	6 W
with remote power supply (AUI)	1.2 A	2.5 A	6 W	12.5 W

NOTE: TSX ETY 110 modules on 5 volts have high consumption when an AUI connection is used. Therefore, pay special attention to the types of devices in the rack before choosing the kind of supply.

NOTE:
The number of TSX ETY 110 modules that can be connected to a rack are listed:
- 2 modules with AUI connection
- 4 modules with RJ45 connection

Chapter 3
Communication: 10/100 MBits/s

About this Chapter

This chapter deals with hardware installation of the 10/100 MB/s Ethernet communication module via the **TSX ETY 4103/PORT, TSX WMY 100** and **TSX ETY 5103** modules, as well as the Ethernet 10/100 MB/s communication module integrated into the **TSX P57 6634/5634/4634** processors.

What Is in This Chapter?

This chapter contains the following sections:

Section 3.1
Introduction

10/100 Bit Communications

Premium PLCs can be integrated into an Ethernet communication architecture through:
- TSX ETY 4103/5103 modules
- TSX ETY PORT (TSX P57 1634/2634/3634) modules
- a TSX WMY 100 module
- the Ethernet channel integrated into the TSX P57 5634/4634 processor

The principal characteristics of the Ethernet connections are the following:
- connection to a TCP/IP network
- communication in half duplex and full duplex mode by automatic recognition
- transmission speed from 10 or 100 Mbits/s by automatic recognition
- connection to network by copper cable via an RJ45 connector

These modules are used to carry out the following functions:
- I/O Scanner service *(see page 137)* (except TSX WMY 100)
- Global Data *(see page 136)* (except TSX WMY 100)
- Web server *(see page 123)*
- Address Server *(see page 128)* (except TSX WMY 100)
- X-Way UNI-TE and Modbus messaging service on TCP/IP *(see page 85)*
- SNMP service *(see page 101)*
- electronic mail notification service (SMTP) *(see page 115)*
- time synchronization service (NTP) *(see page 204)*

NOTE: The TSX WMY 100 module behaves like the TSX ETY 4103 module, except for the I/O Scanning, Global Data, Address Server, and electronic mail notification services, which the TSX WMY 100 does not manage. For all other information concerning the TSX WMY 100 module, consult the relevant sections and chapters of TSX ETY 4103.

Section 3.2
Physical Description

About this Section

This section deals with the physical description of the **TSX ETY 4103/PORT**, **TSX WMY 100** and **TSX ETY 5103** modules and the Ethernet solution of the **TSX P57 6634/5634/4634** processor.

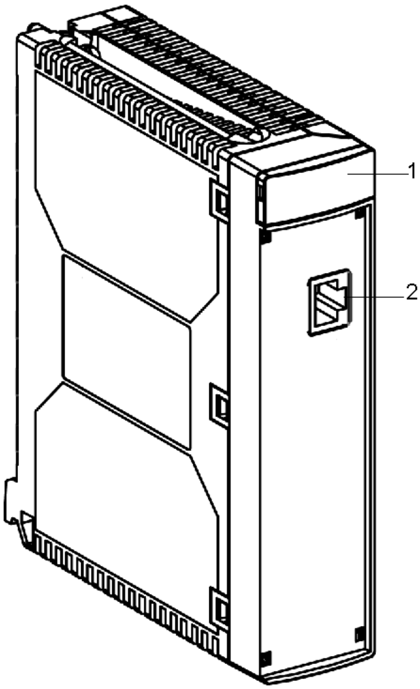
What Is in This Section?

This section contains the following topics:

The TSX ETY 4103/5103 Modules

The Module

The TSX ETY 4103/5103 modules are single-format modules that are inserted in a slot on the main or extension rack of a Premium PLC station. The TSX ETY PORT solution is a TSX ETY 4103 module built in to the processor and has the same characteristics as the TSX ETY 4103 module.



1 Display panel indicating module status:
2 Standard connector for 10/100 BASE-T (RJ45) interface.

The display panel LEDs are:
- **RUN** (green)
- **ERR** (red)
- **COL** (red)
- **STS** (yellow)
- **TX** (yellow)
- **RX** (yellow)

Elsewhere in this guide is a detailed explanation of these LEDs *(see page 45)*.

Physical Description of the TSX P57 6634/5634/4634 Processors

Illustration

The illustration below shows the different elements of a TSX P57 6634/5634/4634 processor:

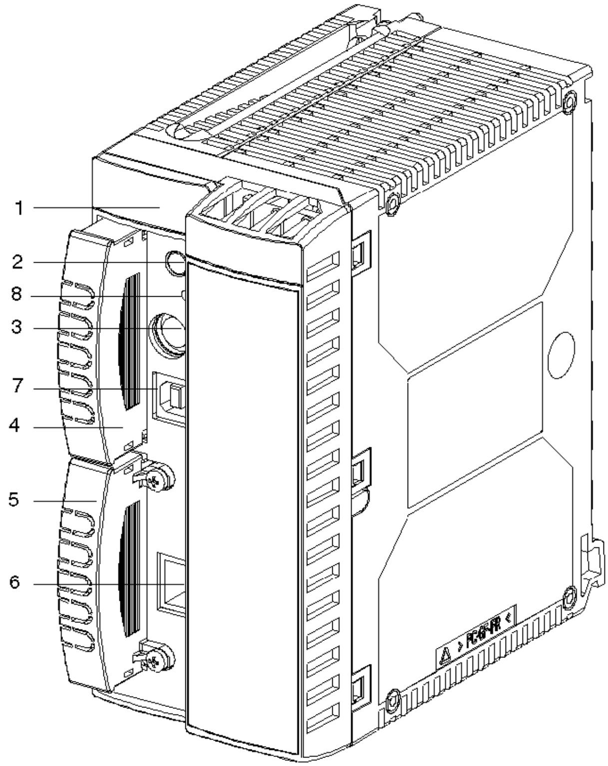


Table of Features

This table describes the elements of a processor module:

Number	Function
1	Display block consisting of 6 LEDs
2	Button for requesting removal of the PCMCIA SRAM card (and a DOS file or ATA in the future) This button must be pressed before removing the card; an LED shows the request status.
3	(**TER connector** (8-pin mini-DIN)) terminal port: This is used to connect an FTX or PC-compatible terminal, or to connect the PLC to the Uni-Telway bus via the TSX insulating unit TSX P ACC 01. This connector enables the peripheral connected to it to be supplied with a 5V current (within the limit of the available current provided by the power supply).
4	Slot for an extended memory card in PCMCIA type 1 format If there is no memory card, this slot is equipped with a cover that it advisable to leave in place to protect the connectors from dust or splashes.
5	Slot for a communication card in PCMCIA type 3 format enabling a Fipio Agent, Uni-Telway, series link, Modbus, Modbus Plus, etc. communication channel to be connected to the processor. This slot can also hold a SRAM data card or an ATA card in the future. If there is no communication card, this slot is equipped with a cover.
6	RJ45 connector for Ethernet connection
7	USB port
8	The **RESET** button activated with a pencil point that triggers a cold start of the PLC when used. ● **Processor operating normally:** cold start in **STOP** or in **RUN**, according to the procedure defined in the configuration. ● **Faulty processor:** forced start in **STOP**.

Section 3.3
Ethernet Channel Characteristics

Ethernet Channel Characteristics

Overview

The Ethernet modules have a standard interface for connecting to a 10/100BASE-T network and on the front panel there is a RJ45 connector for a pin-to-pin link via a link cable comprising two independent twisted pairs.

Functions supported by the modules include:

Support	Service	Protocol	Functions
TCP-IP Services	Messaging	UNI-TE	• Client/server mode • Synchronous requests of 256 bytes • Asynchronous requests of 1 Kbyte
		Modbus	• Data exchange
	I/O Scanner	Modbus	• Access to inputs/outputs
	Network management	SNMP	• Agent SNMP, MIB II, MIB Schneider
	Web	HTTP	• Preset, non-modifiable website on **TSX ETY 4103/PORT** • Website which can be modified and increased by increments within the limit of 7.5 Mb on **TSX ETY 5103**
	Management of IP addresses	BOOTP/DHCP	• Client and address server
	Global Data	UDP	• Exchange of data between stations
	Electronic Mail Notification Service	SMTP	• Reports alarms or events using emails • Define and update text and variable information
	Time synchronization service	NTP	• Synchronizes clocks over Internet to referenced time source • Event recording • Event synchronization • Alarm and I/O synchronization

Section 3.4
Installing the TSX ETY 4103/PORT/5103 Modules and the TSX P57 6634/5634/4634 Processor

About this Section

This section describes how to install the **TSX ETY 4103/PORT, TSX WMY 100**, and **TSX ETY 5103** modules and the **TSX P57 6634/5634/4634** processor with an integrated Ethernet port into a Premium PLC system.

What Is in This Section?

This section contains the following topics:

Introduction to Installation

Overview

TSX ETY 4103/PORT/5103 communication modules are mounted in the rack slot of a Premium/Atrium PLC. They can be installed in any available slot (except in an offset X Bus rack) only if the supply constraints of the rack are observed.

The TSX P57 6634/5634/4634 processors are mounted in slots 0 or 1 in the base rack (according to the power supply selected). They occupy two slots.

NOTE: When starting up a TSX P57 6634/5634/4634 processor, the CPU may send an address resolution protocol (ARP) request to verify the existence of a device using the IP address 192.168.2.1. The source IP address of this packet is the broadcast address of the CPU (the last IP address used in the PLC application, ending in 255).

Selecting the Type of Processor

Selection Guide

Selecting the processor to control the PLC station with one or more Ethernet modules will depend on the number of network connections required.

Processors	Maximum Number of Network Connections	Maximum Number of ETY 4103/5103 per Station (*)
TSX P57 104 (1)	1	1
TSX P57 154 (1)	1	1
TSX P57 204	1	1
TSX PCI 57 204	1	1
TSX P57 254 (1)	1	1
TSX P57 2634	1	0
TSX P57 2834 (1)	1 2 (**)	0
TSX P57 304	3	3
TSX P57 354 (1)	3	3
TSX P57 3634	3	2
TSX P57 454	4	4
TSX PCI 57 454 (1)	4	4
TSX P57 4834 (1)	4	3
TSX P57 554 (1)	4	4
TSX P57 5634	4	3
TSX P57 6634	4	3
TSX P57 4634	4	3
(*) Compatible with 5V power supply (**) Supports two network connections if the PLC is used in Warm Standby (1) Available for Unity Pro V2.0 or higher		

Wiring/Unwiring the TSX ETY 4103/PORT/5103 with Power Switched On

The Module

⚠ WARNING

LOSS OF APPLICATION

Wiring or unwiring while the TSX P57 5634/4634 processor is switched onis forbidden, as for the other processors.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The TSX ETY 4103/PORT/5103 modules can be wired or unwired when switched on without disrupting the operation of the station.

The module does not have a RAM internal backup memory function. The RAM is erased when power is switched off.

The modules reset when switched on. A communication break can be expected during these interventions.

The Link

The 10/100 BASE-T interface RJ45 connector can be connected or disconnected when power is on. A communication break can therefore be expected in the application in progress.

Section 3.5
10/100 BASE-T Interface

10/100BASE-T Interface

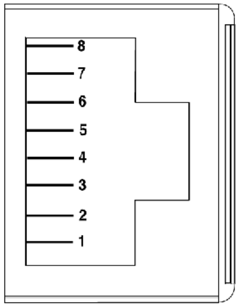
General

This interface has a standard type RJ45 connector.

Refer to the Ethernet reference manual for the connection accessories that comply with environmental circumstances the PLC requires in an industrial setting.

Pin Assignment

Illustration:



Reminder of pin assignment:

Pin	Signal
1	TD+
2	TD-
3	RD+
4	not connected
5	not connected
6	RD-
7	not connected
8	not connected

NOTE: If there is a connection via a shielded cable, the connector casing on the module is linked up to the ground connection.

Speed Line

The possibilities for the different speed lines for the TSX ETY 4103/PORT/5103 modules and the TSX P57 5634/4634 processor's integrated Ethernet channel are the following:

- 100 Mb in full duplex
- 100 Mb in half duplex
- 10 Mb in full duplex
- 10 Mb in half duplex

Speed Adaptation

The speed line cannot be configured by the user. Characteristics of self-adaptation are:

- Each unit diffuses its possibilities on the line.
- The chosen speed is the fastest of all entity possibilities on the line. In other words, speed is limited by the slowest entity on the line of which the speed possibility is the weakest.

Section 3.6
Diagnostics Display

Aim of this Section

This section deals with accessing **TSX ETY 4103/PORT**, **TSX WMY 100** and **TSX ETY 5103** module diagnostics using their display panel.

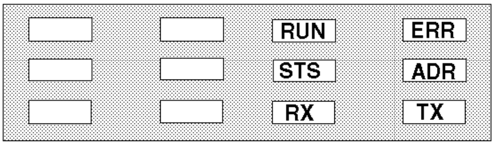
What Is in This Section?

This section contains the following topics:

Display Panel, Modules Diagnostics

Display Block

The display panel complies with the Premium standard



The **COL**, **RX** and **TX** LEDs are managed by the line's electronics; they indicate:

- **COL**: a collision
- **RX**: a reception
- **TX**: a transmission

Diagnostics

Meaning of the diagnostics LEDs:

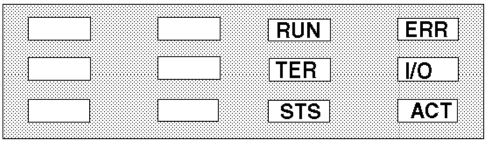
RUN	ERR	STS	COL	TX	RX	Meaning
O	O	O	ns	ns	ns	No supply to module.
O	O	P	ns	ns	ns	Module running self-test.
P	O	O	ns	ns	ns	Module ready.
O	P	O	ns	ns	ns	Module not operational.
O	P	P	ns	ns	ns	Software operation error. Temporary state causing module reinitialization.
O	F	P, F	ns	ns	ns	Module not configured or configuration in progress.
P	O	P	ns	ns	ns	Module configured, operational.
ns	ns	F	ns	ns	ns	Module configured. Diagnostics according to how the LEDs are flashing: ● 2 flashes: module has no MAC address. ● 3 flashes: Ethernet cable not connected on the module or Hub side ● 4 flashes: the module IP address is duplicated by another IP address on the network. Conflicting remote device flashing in the same way. ● 5 flashes: module configured as a BOOTP client and is waiting for a BOOTP server response. ● 6 flashes: invalid IP address. Module is set to its default IP address.
P	O	P	O	F	O	Ethernet communication sending.
P = Permanently on, F = flashing, O = Off, ns = not significant						

RUN	ERR	STS	COL	TX	RX	Meaning
P	O	P	O	O	F	Ethernet communication receiving.
P	O	P	O	F	F	Ethernet communication sending/receiving.
P	O	P	F	F	O	Module has detected collision.
P = Permanently on, F = flashing, O = Off, ns = not significant						

Display Panel, Ethernet Diagnostics for TSX P57 6634/5634/4634 Processors

Display Block

The display block for the **TSX P57 6634/5634/4634** processors complies with the Premium standard; it has two LEDs specific to the integrated Ethernet channel, the **STS** and **ACT** LEDs.



The dedicated Ethernet LEDs define:
- Line activity for **ACT**; this LED groups the indications of the two **RX** and **TX** LEDs for a standard TSX ETY •••• model.
- Module status for the **STS** LED.

Ethernet Channel Diagnostics

Meaning of the diagnostics LEDs:

I/O	STS	ACT	Meaning
O	O	O	No supply to module.
P	O	ns	Ethernet link not operational.
ns	F	ns	Module configured. Diagnostics according to how the LEDs are flashing: ● Steady flashing: Ethernet link awaiting configuration or configuration in process. ● 2 flashes: no MAC address. ● 3 flashes: Ethernet cable not connected on the module or Hub side ● 4 flashes: the IP address is duplicated by another IP address on the network. Module is set to its default IP address. Conflicting remote device flashing in the same way. ● 5 flashes: the Ethernet channel is configured as a BOOTP client and is waiting for a BOOTP server response. ● 6 flashes: Invalid IP address. Module is set to its default IP address. ● 7 flashes: the version of the Ethernet firmware is incompatible with the PLC processor firmware version (in cases where there are updates and user downloads).
O	P	ns	Ethernet link configured, operational.
O	P	F	Ethernet communication sending/receiving.
P = Permanently on, F = flashing, O = Off, ns = not significant			

Section 3.7
Electrical Characteristics

TSX ETY 4103/PORT/5103 Electrical Characteristics

Consumption and Dissipation Table

The TSX ETY 4103/PORT/5103 modules can be inserted in any rack slot of a Premium/Atrium station (except in the X Bus offset rack).

Table of consumption:

Voltage	Power Consumption		Power Dissipation	
5 volts	Typical	Maximum	Typical	Maximum
TSX ETY 4103/PORT/5103	360 mA	400 mA	1.8 W	2.1 W

NOTE: The electrical characteristics of the **TSX P57 5634/4634** Ethernet processors are in the processor presentation manual *(see Premium and Atrium using EcoStruxure™ Control Expert, Processors, racks and power supply modules, Implementation Manual)*.

Section 3.8
Standards

Norms and Standards

Compliance with Standards

The **TSX ETY 4103/PORT** and **TSX ETY 5103** modules, as well as the Ethernet link of the **TSX P57 5634/4634** processor comply with the following standards:

- UL 508
- CSA
- IEC 61131-2
- Marine classification

Section 3.9
Operating Conditions

Operating Conditions

Applicable Conditions

- **Operating Conditions:**
  - Temperature from 0 to +60° C
  - Relative humidity between 10% and 95% (without condensation) at 60° C
  - Altitude of between 0 and 4500 meters
  - Immunity to vibrations complies with the IEC 68-2-6 standard, Fc test
  - Immunity to shocks complies with the IEC 68-2-27 standard, Ea test
  - Immunity to free fall, hardware tested as per the IEC 68-2-32 standard, method 1
  - IP 20 protection index
- **Storage conditions:**
  - Temperature from -40° C to +85° C
  - Relative humidity between 0% and 95% (without condensation) at 60° C

Part III
Software Installation for Ethernet Communication

Aim of this Part

This part describes the software installation of communication on an Ethernet network using Control Expert.

What Is in This Part?

This part contains the following chapters:

Chapter 4
Services

Subject of this Chapter

This chapter introduces the main points of the different services used by the modules.

What Is in This Chapter?

This chapter contains the following sections:

Section 4.1
TCP/IP Messaging

Purpose

This section mentions the functions and characteristics of the TCP/IP profile.

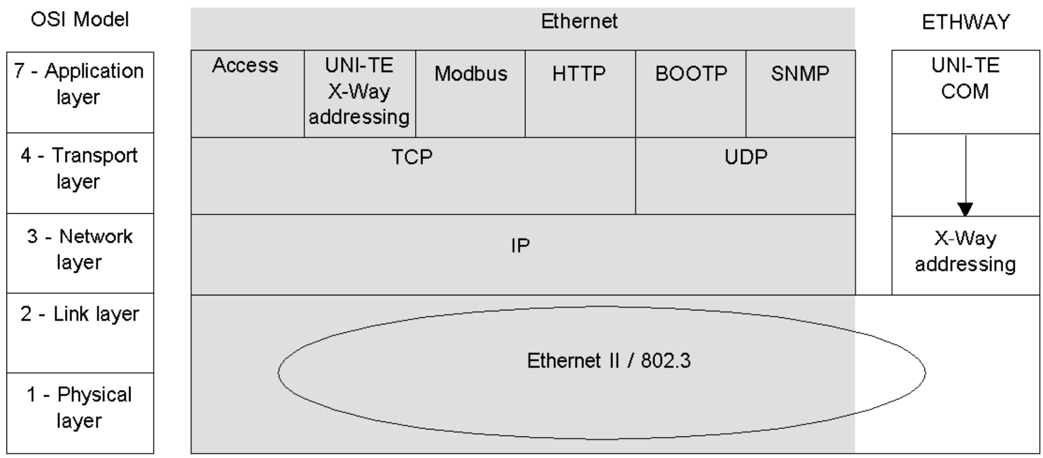
What Is in This Section?

This section contains the following topics:

TCP/IP

TCP/IP Communication Profile

The following diagram illustrates the make-up of a typical TCP/IP stack.



Software Port 502

The port reserved for the TSX ETY or TSX ETY PORT (TSX P57 1634/2634/3634) module or the Ethernet port of the TSX P57 6634/5634/4634 is TCP port 502. When a client wishes to access the server of these modules, it must send towards this port.

Timeout on TCP Connection

If a TCP connection cannot be established (when the destination is absent for example), the timeout error occurs after 80 seconds.

Each communication function timeout must be set to a value higher than 80 seconds if the first exchange was not successfully completed.

Keep Alive Frame

The TCP layer sends a "keep alive" frame almost every two hours so that breaks in connection can be detected (for example, cable disconnection, detection of power outage from the client by a server, etc.). Elsewhere in this guide is a discussion of broken connections *(see page 89)*.

Address Management for Ethernet Modules

Introduction

CAUTION

UNINTENDED EQUIPMENT OPERATION

If two devices have duplicate network addresses, you can not predict the operation of the equipment.

Failure to follow these instructions can result in injury or equipment damage.

You must carefully manage the modules' IP addresses because each device on the network requires a unique address.

MAC Address

General case

This address is unique for each Ethernet module. It is defined in the factory by the module manufacturer.

Exception

For the **TSX ETY 110** module, this address is derived from the X-Way address using the code selectors situated on the front panel of the module.

It is defined in the following way: `00.80.F4.00.<network number>.<station number>`

NOTE: Given the risk of possible duplicate addresses, you must ensure that it conforms to the company's addressing scheme.

IP Address

General case

You define this address yourself when configuring the module. On the same local network, this address must be unique.

Exception

For the TSX ETY 110 module, this address can be derived from the MAC address.

For the TSX ETY 110, TSX ETY PORT, and TSX ETY 5103 modules and the Ethernet link of the TSX 57 5634/4634 and, in the absence of confirmation by Control Expert, this address is, by default, derived from the MAC address.

X-Way Address

General case

All devices have an X-Way address linked to the IP address by the module configuration. This address must be unique within the entire X-Way architecture.

Special Cases

For the TSX ETY 110 module, the X-Way address is defined using the code selectors on the module. These selectors code the network number and the station number.

The Ethernet link built into the processors does not require an X-Way address.

IP Address

Overview

Each device connected to the network should have a unique IP address.

When the type of network environment is open, the uniqueness of the address is guaranteed by the authorized organism in the country where the network is located by assigning it a network identifier.

If the type of environment is closed, the uniqueness of the address is managed by the company's network manager.

The TSX ETY 4103/PORT/5103 modules and the Ethernet link of the TSX P57 6634/5634/4634 can have their address dynamically allocated by an address server or have their address configured by the user.

Address Composition

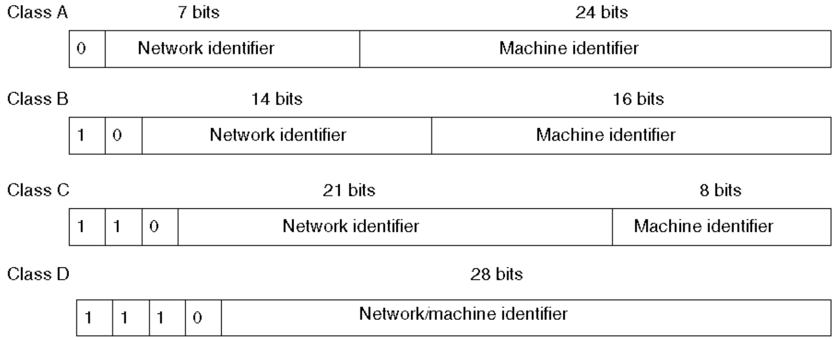
This address is made up of two identifiers, one of which identifies the network, the other identifies the connected machine.

An IP address is defined on 32 bits. It is made up from 4 decimal numbers, each coded on a byte (example: 140.186.90.3).

Depending on the network span, four address classes can be used:
- Class A applies to large span networks, which have a large number of connected stations.
- Class B applies to medium span networks, which have fewer connected stations.
- Class C applies to small span networks, which have few connected stations.
- Class D is used for multicast. A class D address must not be allocated to a module.

Structure

Depending on the class, an address is structured in the following way:



The following table displays the spaces reserved for the different IP address classes:

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255

Sub Addressing and Subnetwork Mask

Introduction

In an open environment, after a network identifier has been obtained from the accredited body, the local system administrator is able to manage several subnets.

This will allow local networks to be installed without changing anything for the outside world which will still only be able to see the network indicated by the network identifier.

Sub Addressing

This sub addressing function is possible by splitting the machine identifier into the following:

- a subnet identifier
- a machine identifier

Example: sub addressing for a class B address (IP address in question: 140.186.90.3)

16 bits	8 bits	8 bits
Network identifier = 140.186	Subnetwork identifier = 90	Machine identifier = 3

Mask

The subnet mask is used to find out the number of bits allocated respectively to the network identifier and the subnet indicator (bits to 1), and then to the machine identifier (bits to 0).

The value of the subnet mask must be chosen to comply with the IP address class. It will have the value (xxx: value chosen left up to the user):

- for a class A address: 255.xxx.xxx.xxx
- for a class B address: 255.255.xxx.xxx
- for a class C address: 255.255.255.xxx

Example: class C subnet mask (IP address in question :192.186.90.3)

16 bits	8 bits	8 bits
Network identifier = 192.186	Subnetwork identifier = 90	Machine identifier = 3

Subnetwork mask (24 bits to 1) = 255.255.255	Machine identifier (8 bits to 0)

NOTE: This division allows 254 possible subnets with 254 machines per subnet.

UNI-TE Communication

UNI-TE Messaging

Schneider Electric's Modicon and Telemecanique products use the UNI-TE protocol for Ethernet communications. UNI-TE on TCP/IP uses:

- the version of UNI-TE messaging that is applicable to the equipment (communication on the application layer)
- TCP/IP (communications on Ethernet)

Two data exchange services are offered. The type of service depends on the type of server used. There are two choices:

- synchronized data exchanges on the MAST task
- data exchanges performed as a background task in the following modes:
  - asynchronous server mode
  - asynchronous client mode

Synchronous Exchanges

Synchronous exchanges take place in one of two modes:

- **server mode**: All UNI-TE requests from the PLC are supported by the Ethernet module.
- **client mode**: This type of exchange enables UNI-TE requests to be sent using the functions:
  - READ_VAR
  - WRITE_VAR
  - DATA_EXCH
  - ...

Asynchronous Exchanges

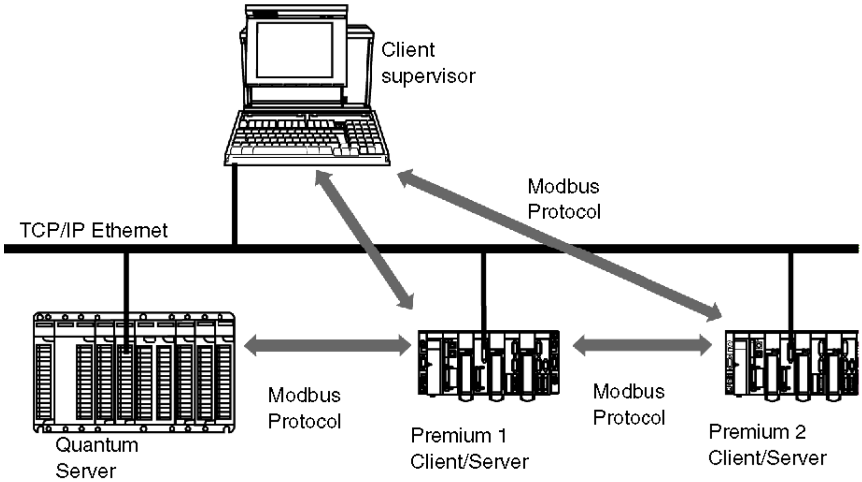
Asynchronous exchanges take place in one of two modes:

- **server mode**: The consistency of the written or read data can be guaranteed (guarantees that the request is sent in one cycle) by setting the system bit %S91 to 1. In this configuration, a Jitter phenomenon of 1.5 ms can appear on the MAST task.
- **client mode**: This service allows messages to be exchanged using the requests:
  - READ_ASYN: enables up to 507 words (%MW) or 8112 bits (%M) to be read through the asynchronous messaging channel.
  - WRITE_ASYN: enables up to 510 words (%MW) or 8160 bits (%M) to be written through the asynchronous messaging channel.

Modbus Communication on TCP/IP

Overview

Modbus on TCP/IP enables communication to be established through the Modbus protocol between a Premium PLC and a Quantum PLC or another Premium PLC and supervisor software on a PC or other device complying with the Modbus protocol.



The same module can communicate with a remote device in client mode (for example a Quantum PLC) and another remote device in server mode (for example a supervisor PC).

In the above figure, Premium PLC 1 is the client to the Quantum PLC. It opens the TCP/IP connection and sends Modbus messages to the Quantum.

Premium PLC 2 is the server to the supervisor. The supervisor has opened a TCP/IP connection for sending Modbus messages to Premium 2.

UNI-TE/Modbus Conflict

A UNI-TE and Modbus double profile is not supported on the same Premium remote station. In other words, station *A*, at a given moment, can not have both Modbus communication and Uni-TE communication toward station *B*.

TSX ETY 100 Considerations

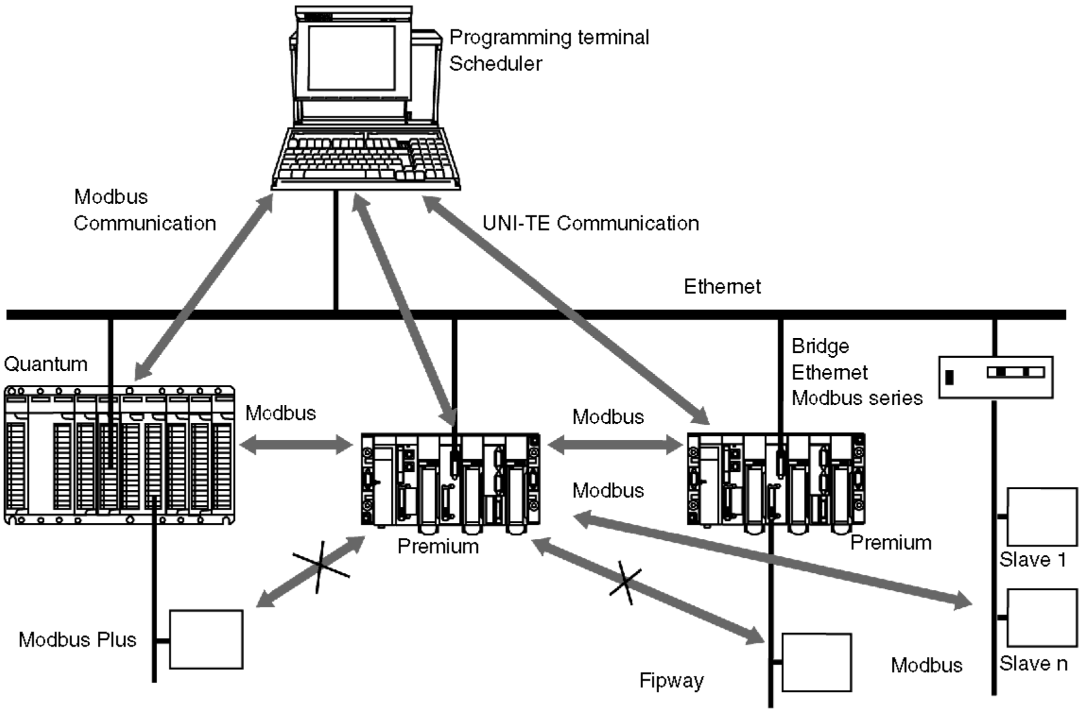
The client/server modes are exclusive to a given remote device in order to improve communication performance. PLC applications and network architectures must be designed so that switching from one mode to another between the same two devices is as rare as possible.

NOTE: Frequent mode switching could result in lost messages:
- If the Premium PLC communicates in server mode with a Quantum PLC that has opened the TCP/IP connection, the issuing of a message by the client Control Expert application will cause the server TCP/IP connection to close down after any server transactions in progress have been processed.
- f the Premium PLC that has opened the TCP/IP connection communicates in client mode with a Quantum PLC, a request to open the connection from the Quantum will cause the client TCP/IP connection to close down with the possible loss of any client transactions in progress.

Architecture Supported by Modbus Communication on TCP/IP

Introduction

The following figure shows the supported architecture:



Accessibility

The Modbus protocol provides interoperability between the Premium station and the Quantum station on a TCP/IP Ethernet network.

However, access from a Premium PLC to a Modbus Plus network connected to the Quantum PLC is not possible via TCP/IP.

The Modbus protocol cannot cross X-Way Premium bridges.

Communication between a Premium PLC on the Ethernet network with a remote device connected to a Modbus series bus is possible with a 174 CEV 300 10 serial-linked Ethernet/Modbus gateway.

Exception for the TSX ETY 110 Module

For a TSX ETY 110 module, communication between a Premium PLC on the Ethernet network with a device connected to the Modbus serial bus is not possible.

Modbus Messaging on the TCP/IP Profile

Introduction

The communication functions are the same as those described in the communication functions on Modbus.

Installation Principle

Although a remote Modbus station does not have an X-Way format address, each communication function will use an X-Way format address to designate a remote IP station.

For each remote Modbus station, you must configure the pair in the correspondence table (IP address, {network.station} X-Way) where:

- network: network number of the local X-Way station
- station: 100 to 164 = logical number of the X-Way station

For example, the X-Way address {2.108} is associated with the IP address 139.160.2.8.

This address will only be used by the local Premium module. It is not sent over the network.

In the case of a remote Premium station configured with the Modbus protocol, you should give an X-Way station address that takes the number of the local station and increments it by 100.

Sending Communication Functions

When the application sends communication functions to a remote device connected to Modbus via a serial-link Ethernet/Modbus gateway, the function address must be one of the following:

ADDR('{*network number*. *station number*}0.0.0.*Modbus destination address*')

where:

- *network number* and *station number* correspond to the X-Way address of the Ethernet/Modbus gateway
- *Modbus destination address* corresponds to the Modbus slave address

This syntax supports Modbus addresses in the range 0...253. On the Ethernet network, the Modbus TCP/IP frame will be sent to the gateway with the Modbus address coded in the Unit_Id field.

In the case the **Unit_Id** code is 254 or 255, for example to address TSX ETG100 gateway, the following syntax should be used:

ADDR('{*network number*. *station number*}0.0.254.255') to access the local variables of the TSX ETG100.

or

ADDR('{*network number*. *station number*}0.0.254.*Modbus destination address*').

Data Exchange

The following requests are addressed to the device with which you wish to perform variable read or write operations:

Modbus Request	Modbus Function Code	Equivalent UNI-TE Function
Read bits	16#01	`READ_VAR`
Read words (up to 125 registers)	16#03	`READ_VAR`
Write a bit or n bits	16#0F	`WRITE_VAR`
Write a word or n words	16#06 or 16#10	`WRITE_VAR`
Read input bits	16#02	`SEND_REQ`
Read input words	16#04	`SEND_REQ`

NOTE:
The timeout value for `READ_VAR` is user-configurable as follows:

- If you enter a 0 as the timeout value, the block will never timeout.
- If you enter a non-zero value, the block will timeout at the non-zero value you entered.

NOTE: In server mode only, an ETY module can support function code 16#16, allowing it to mask the writing of a specified word.

Correspondence of Object Types

This table describes object type correspondence between a Premium PLC and a Momentum or Quantum PLC:

Premium Objects	Quantum or Momentum Objects
%MW: internal words	4x... memory area
%M: internal bits	0x... memory area
%IW: input words	3x... memory area
%I: input bits	1x... memory area

Managing TCP Connections for X-Way UNI-TE and Modbus

Overview

The connection can be opened either by the local PLC or by a remote station which wants to communicate with the local PLC.

A connection is characterized by the pair:

(local TCP port, local IP address; remote TCP port, remote IP address)

NOTE: Managing the connections is transparent to the user.

Opening a Connection

Introduction

A connection can be opened by a request from:

- a remote device
- the local PLC

With a Remote Device

The module prepares for a connection coming from a remote device.

When the connection is received, verification of the IP address of the remote machine is done if and only if access check is activated. This test consists of checking that this address is on a list of remote machines authorized to connect.

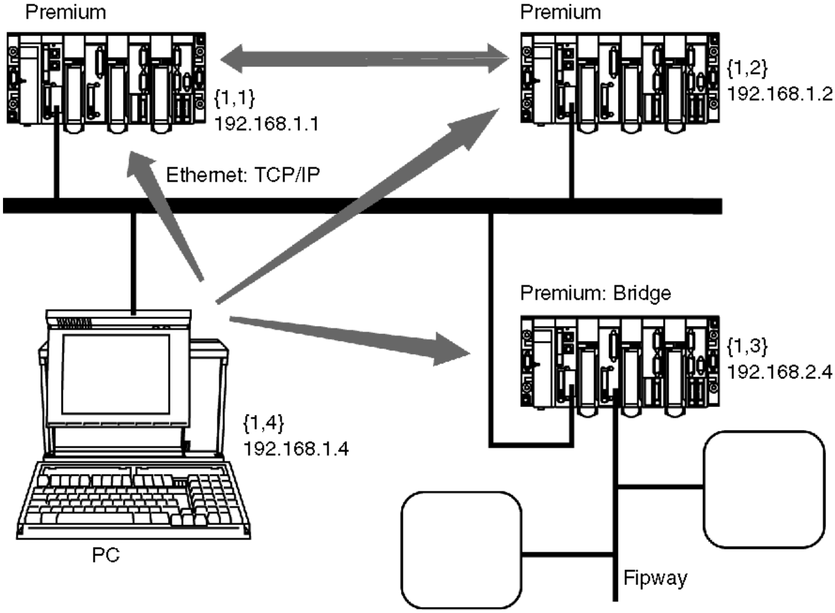
If the test is positive the connection is opened. If not the connection remains closed.

With a Local PLC

When a message is sent out by a communication function, if there is no connection with the remote device, this is opened automatically internally by the module to the remote 502 port.

Examples

Example of connections



In the example opposite, four TCP connections are open for communication between the terminal and the PLC stations or between two PLC stations.

The terminal is always able to open connections.

Either of two PLCs CANopen the connection between them (the client PLC).

Closing a TCP Connection

Overview

A TCP connection can be closed by one of the following:
- a remote station (which closes a connection by sending a TCP/IP connection closure message)
- the local PLC

When the Maximum Number of Connections are Open

If the PLC receives a request to open a new connection when the maximum number of connections has been reached, the PLC:
- closes an open but inactive connection
  - then -
- opens a new connection

To identify which connection to close, the PLC examines groups of connections for inactive open connections, in the following sequence:

1. non-referenced connections to devices that are not configured as part of the Control Expert application
2. client connections
3. server connections

If the PLC discovers one or more inactive connections in the first group, it closes the oldest inactive connection in that group then opens a new connection.

If no inactive connection is discovered in the first group, the PLC examines the second group of connections and, if it discovers one or more inactive connections in the second group, the PLC closes the oldest inactive connection in that group and opens a new connection.

If no inactive connection is discovered in the first and second groups, the PLC examines the third group and, if it discovers one or more inactive connections in the third group, the PLC closes the oldest inactive connection in that group and opens a new connection.

If the PLC fails to discover an inactive connection in any of the three groups, no open connection is closed and no new connection can be opened.

NOTE: Closure of a connection is indicated to the application by means of a status report (message refused) on any exchanges in progress.

Broken Connections

Introduction

There are two types of broken connections:
- physical problem with the network cable (cut or disconnected)
- disappearance of the remote device (break down, power cut, etc.)

Loss of connection is detected after 2 hours by the Keep Alive request.

If within this time the connection is re-established, restarting communications is different according to the type of break.

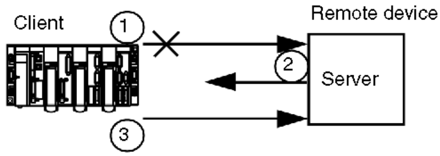
Reconnecting the Cable

In this case the break in connection is caused by a network cable but the two stations remain operational.

When the cable is reconnected communication between the ETY module and the remote device will start again on the TCP/IP connection that was opened previously.

Server Remote Device

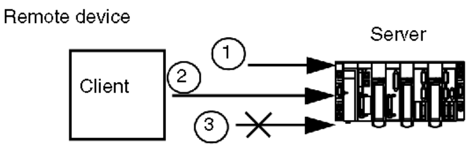
The remote device that disappeared was the server.



1 The client ETY module is still sending out data on the old connection (which remains half open).
2 The server receiving the information without associated connection sends out a Reset command and closes the old connection.
3 The client ETY module opens a new connection.

Client Remote Device

The remote device that disappeared was the client.



1 The client opens a new connection.
2 The server ETY module receives the request to open a new connection.
3 The server ETY module closes the old connection (if there is nothing in progress) and authorizes the new one.

Section 4.2
I/O Scanning Service

About this Section

This section presents some functions, characteristics, and configuration options for the I/O scanning service.

What Is in This Section?

This section contains the following topics:

I/O Scanning Service

At a Glance

The input/output scanner is used, periodically, to read or write remote inputs/outputs on the Ethernet network without specific programming. The I/O scanner is configured with Control Expert.

This service comprises the following essential elements:
- a read zone which groups together all the values of remote inputs
- a write zone which groups together all the values of remote outputs
- scanning periods which are independent of the PLC cycle and are specific to each remote device

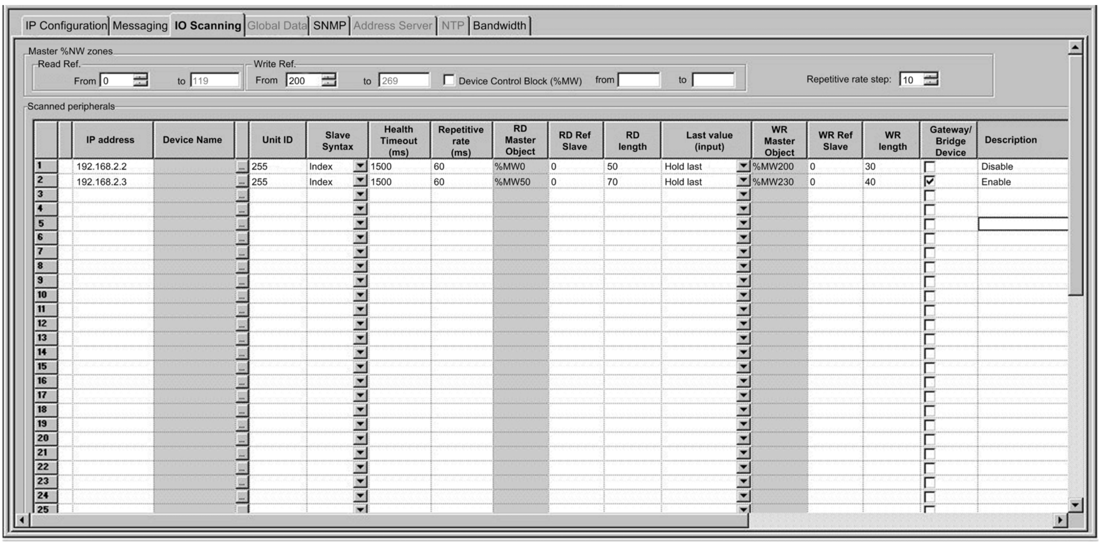
Recommendations for Use

Scanning is only performed when the PLC is in Run mode.

This service operates with all devices supporting Modbus communication on the TCP/IP profile in server mode.

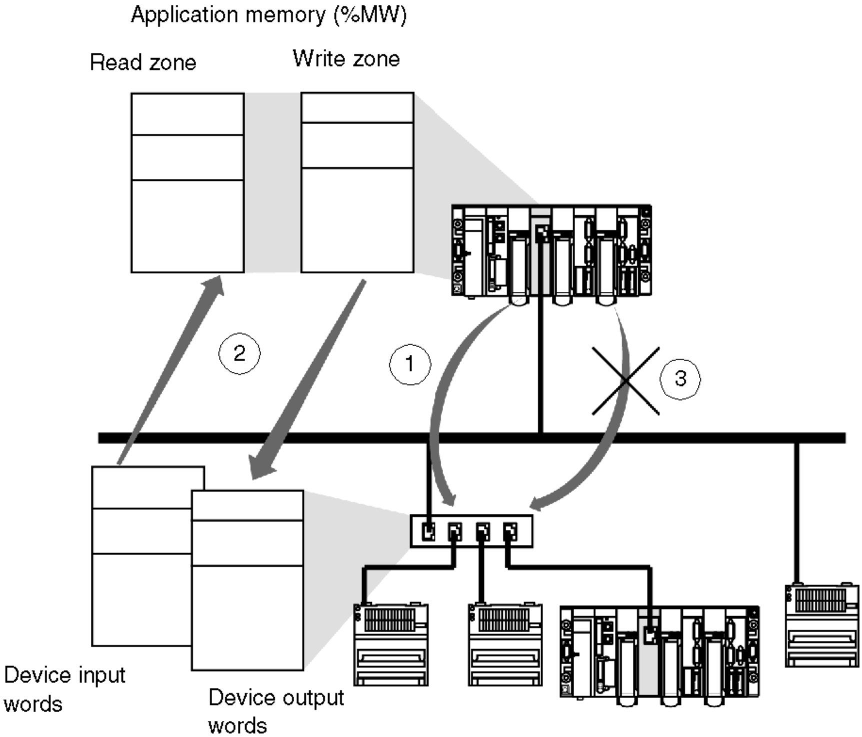
The exchange mechanism, which is transparent to the user, is carried out with the following requests:
- read requests
- write requests
- read and write requests

NOTE: If you use I/O scanning with gateway/bridge devices, select the check box in the **Gateway/Bridge Devices** column in the I/O scanner screen, as shown in the following illustration.



Operation

The following diagram shows how the scanning of remote inputs/outputs works.



1. As soon as the PLC switches to Run mode, the module opens up one connection for each scanned device (one connection for each line entered in the table of scanned elements).
2. Then the module periodically reads inputs words, and periodically writes output words for each device.
3. If the PLC switches to Stop mode, the connections to each device are closed.

Summary of Functionality

The I/O scanning service functionality is used to:
- manage the connection with each remote device (one connection per device scanned)
- scan the inputs/outputs of the device using Modbus read/write requests on the TCP/IP profile
- update the read and write zones in the application memory
- refresh the status bits for each remote device

Each I/O scanner device can be enabled/disabled.

For further configuration information for the I/O scanning functionality, see Configuration parameters for the IO Scanning service *(see page 156)*.

NOTE: These bits show whether the module's input/output words have been refreshed.

Read and Write Zones

The Zones

Within the application memory, the I/O scanning service defines:
- %MW word zone: reserved for reading inputs
- %MW word zone: reserved for writing outputs
- refresh periods: independent of the PLC scan

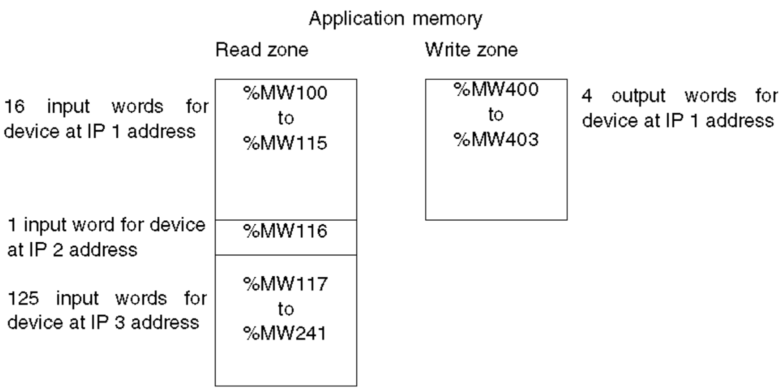
The read and write zones associated with the Ethernet module are tables of internal words (%MW) that contiguously group all input and output word values for connected remote devices. Remote input and output devices are supplied with:
- input words: used to send back the values of the inputs to the module
- output words: used to assign the value of the outputs to the remote device

NOTE: Refer to the documentation for each device for the number and details of input and output words to be managed.

Example

In this example, the Ethernet module scans three devices:
- a Momentum module at address IP1 (type 170 AA1 140 00: 16 analogue inputs; this module has 16 input words and 4 output words)
- a Momentum module at address IP2 (type 170 AA1 340 00: 16 discrete inputs; this module has one input word)
- a Premium PLC with 125 input words at address IP3

The read zone begins at %MW100 and the write zone at %MW400.



NOTE: The fields dedicated to remote devices must not have any overlap. Equally, the read and write zones must not have any overlap.

NOTE: Not all devices can be write-scanned by multiple modules. Check the remote device's documentation to see if it can be accessed by the I/O Scanner.

Scanning Period

At a Glance

Remote input/outputs are scanned periodically depending on the application requirements.

A scanning period is defined for each device through configuration, according to the update speed.

NOTE: The lower the scanning period, the faster the input/outputs are updated. However, this speed increases the network load.

NOTE: %SW8 and %SW9 do not stop remote station scanning, but inhibit the copying of I/Os to and from the application memory.

NOTE: If you configure a scanning period of 0, the request is sent immediately after the response to the previous request is received.

NOTE: The entry in the **Repetitive rate step** field should be a multiple of 10. Any other number will not work correctly.

Section 4.3
DHCP

Overview

This section describes the functions and characteristics of DHCP.

What Is in This Section?

This section contains the following topics:

Dynamic Assignment of Addresses

Introduction

The TSX ETY 4103/PORT/5103 module or the Ethernet link of the TSX P57 6634/5634/4634 can get addresses either through DHCP or BOOTP.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol that manages network parameters for network devices. Individual devices can get network IP addresses from a DHCP server through a request from this device.

The TSX ETY 4103/PORT/5103 module or the Ethernet link of the TSX P57 6634/5634/4634 can be configured as the DHCP server. They can also have their address configured by the user or dynamically allocated from an address server (configuration as BOOTP client).

NOTE: The DHCP server can also respond to the BOOTP protocol.

BOOTP Client

A module configured as a BOOTP client transmits requests on the network every second while it is starting up until it receives a reply from an address server.

The remote device acting as the BOOTP/DHCP server responds to this request and assigns the following to the client module. These must be configured correctly in order for BOOTP to work properly.

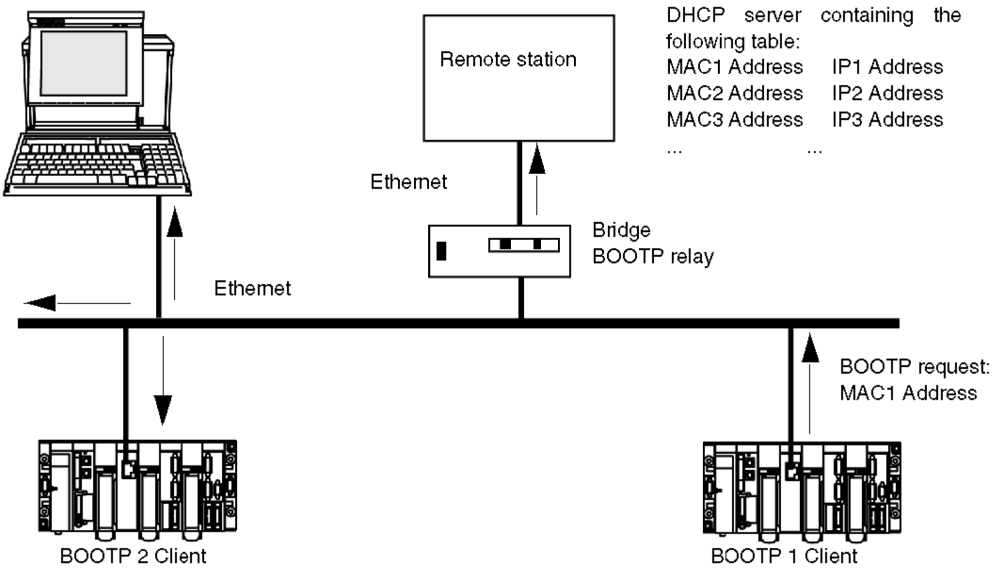
- IP address
- gateway IP address
- corresponding subnetwork mask

NOTE: The display of this information from a browser connected on the HTML pages of the rack display on the web server is sometimes inaccurate. Therefore, you must connect a Control Expert application on the PLC concerned in order to obtain the real values.

NOTE: If the absence of the address server or if there is no response, the client module does not start.

Example

The following diagram shows the routing of requests during start-up of a station on the network:



DHCP Servers

Overview

⚠ CAUTION
INCOMPLETE IP ADDRESSING Do not configure the PLC in automatic start in RUN mode else some stations such as the Momentum 170s may not obtain their IP address when the DHCP server restarts. **Failure to follow these instructions can result in injury or equipment damage.**

In this context, the module is used as a server for starting up client stations.

In listen mode, the server responds to the clients' requests and sends them their IP address configuration.

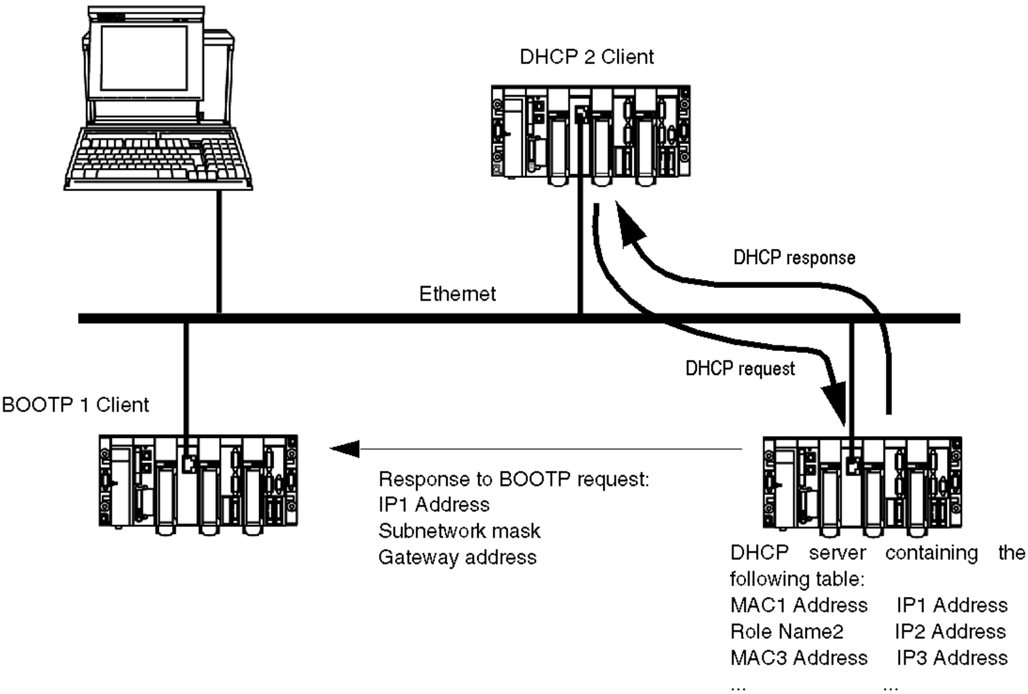
To do this, the server device has a table, which groups:
- Correspondence between the MAC addresses or the Names (Role Names) of the client stations and the IP addresses
- The Netmask and the Gateway
- The names and access paths to the parameter files (see *Replacing Faulty Remote Stations,* *page 107*)

NOTE: The server (present on the TSX ETY and TSX ETY PORT modules and the Ethernet link of the TSX P57 6634/5634/4634) only supplies network configuration data to client stations connected to the local area network.

When a module is used as a server for starting scanned stations *(see page 90)*, you must avoid configuring the PLC in **automatic start in RUN mode**. If you do not, there is a risk that stations such as the Momentum 170s will not be able to obtain their IP address when the DHCP server restarts.

Example of DHCP Server

The following diagram shows the routing of requests when responding to a start-up request from the server:



NOTE: The subnetwork mask and the address of the gateway belong to the DHCP server.

Section 4.4
SNMP Service

SNMP Communication on UDP/IP

Overview

The SNMP (Simple Network Management Protocol) standard defines network management solutions in terms of protocol and the exchange of supervised data.

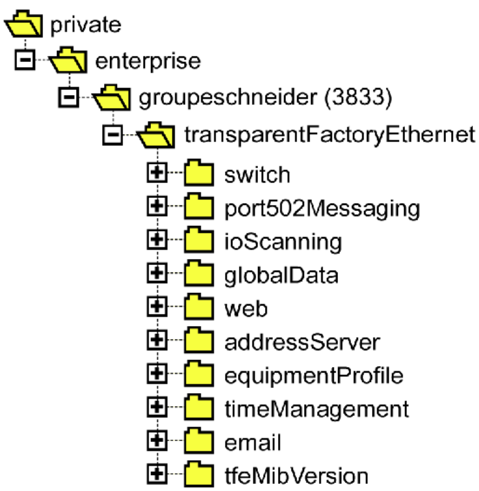
The SNMP structure relies on the following essential elements:

- The **Manager** allows entire or partial network supervision,
- One or more **Agents**. Each supervised device has a software module named **Agent** used by the SNMP protocol.
- A **MIB** (Management Information Base) is a data base or collection of objects.

The SNMP agent is implemented on the TSX ETY modules and on the Ethernet port of the processors. This allows a Manager to access MIB-II standardized objects from the agent TSX ETY via the SNMP protocol. The MIB-II allows management of TCP/IP communication layers.

On the TSX ETY 4103/PORT/5103 module and on the Ethernet port of the TSX P57 6634/5634/4634, it is also possible to access objects from the MIB Ethernet Transparent Factory, which provide specific information on Global Data, I/O Scanning and Messaging.

Branching view of the MIB Ethernet Transparent Factory:



The source file of the Ethernet Transparent Factory private MIB *(see page 415)* is available on the TSX ETY 4103/PORT/5103 module and on the Ethernet port of the TSX P57 6634/5634/4634. It can be downloaded from an internet navigator by clicking on the "Download MIB file" port on the HTTP server index page. This file may be compiled by the main SNMP Managers on the market.

The SNMP Protocol

The SNMP protocol defines 5 types of message between the agent and the manager. These messages are encapsulated in the UDP datagrams.

Messages from the manager to an agent:

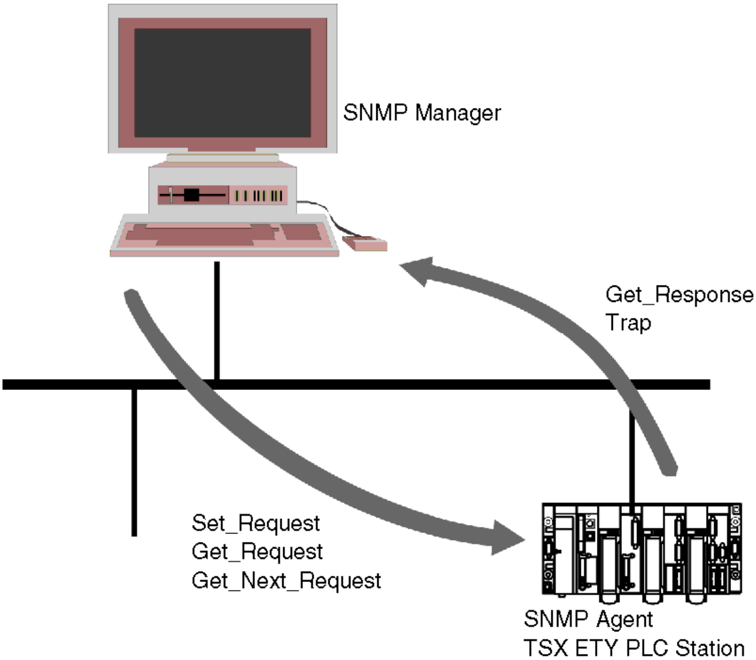
- `Get_Request`: message used to obtain the value of one or more variables.
- `Get_Next_Request`: obtains the value of the next variables.
- `Set_Request` : sets the value of a variable.

Messages from an agent to the manager:

- `Get_Response`: allows the agent to re-send the value of the requested variable.
- `Trap`: allows asynchronous event signaling by the agent.

SNMP Operations Example

The SNMP manager transmits read or write requests (`Set_Request`, `Get_Request`, `Get_Next_Request`, etc.) for objects defined in the MIB - II SNMP, and the SNMP agent of the TSX ETY module responds.



The module's SNMP agent transmits events (Traps) to the Manager. The managed Traps systems are as follows:

- `Coldstart Trap`:
  - For the TSX ETY 110 module, the event is transmitted following a module supply Reset.
  - For the TSX ETY 4103/PORT/5103 modules and the Ethernet port of the TSX P57 6634/5634/4634, the event is transmitted following a module supply Reset, or following a processor Reset, or following the downloading of an application to the PLC.
- `Authentication Failure Trap`: event transmitted following an authentication problem. The **Community Name** field in the received message is different to the one configured on the module. This trap can be enabled when configuring the module.

Section 4.5
Global Data

Global Data

Introduction

The aim of Global Data, which is supported by the TSX ETY 4103/PORT/5103 modules and the Ethernet link of the TSX P57 6634/5634/4634, is to provide an automatic data exchange for the coordination of PLC applications.

Operation

The communication modules are regrouped in a **Distribution Group** to exchange the variables used for PLC coordination.

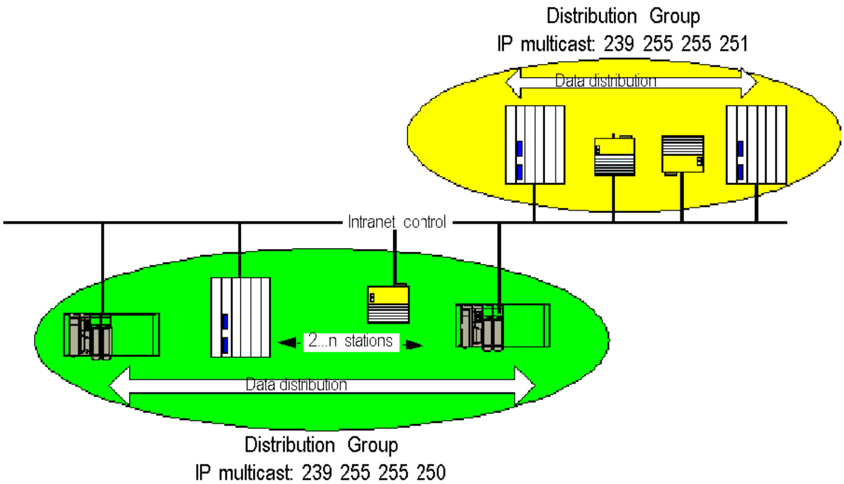
Each communication module **publishes** a local application variable for the other communication modules in the Distribution Group.

Each communication module can also **subscribe** to the application variables published by all other modules sharing the Distribution Group, whatever its location.

An **Application Variable** is a group of contiguous words from a PLC.

Through Global Data configuration you can define:
- the number of valid published and subscribed variables
- the group with which these variables are associated for the communications module.

Once the module is configured, exchanges between the communication modules sharing the same Distribution Group are automatically carried out when the PLC is in RUN mode.



A **Distribution Group** is a group of communication modules identified by the same multicast IP address. Exchanges in "multicasting" are used to distribute Global Data. Several independent Distribution Groups can co-exist on the same subnetwork with their own multicast address.

A publication/subscription protocol on UDP/IP is used for data distribution.

The publication of a variable is synchronized at the start of the PLC cycle.

Subscribed variables are copied in the PLC application memory at the end of the cycle.

The PLC memory zones that receive the various subscribed variables should not be recovered.

Health Bits

A **Health bit** (status bit) is associated to each application variable.

This status bit indicates the validity of each subscribed variable: it is 1 if the variable has been published and received in the configured validity time limit *(see page 304)*, otherwise it is 0.

Multicast Filtering

The global data service synchronizes several stations located in a distribution group. A distribution group is a set of stations identified by using the same IP multicast address for all stations in the group. By using the same IP address for multiple devices, multicast exchanges can be used to distribute global data. Several independent distribution groups can coexist on the same sub-network. Each distribution group possesses its own unique IP multicast address.

Early versions of switches treat multicast packets as a broadcast, thereby broadcasting to all nodes and suppressing all benefits of both switching and multicasting. Newer versions of switches provide automatic multicast filtering, and consequently only forward multicast traffic to ports that are connected to registered end stations.

The following multicast filtering protocols are supported by Ethernet modules for its global data service.

- GARP Multicast Registration Protocol (GMRP)
  GMRP provides a mechanism that allows bridges and end stations to dynamically manage the membership of multicast groups.
  NOTE: GMRP is defined in the IEEE 802.1D-1998 Standard, which is available as a free download at: http://IEEE802.org.
- Internet Group Management Protocol (IGMP)
  IGMP is a communications protocol used to manage the membership of internet protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

Operating Modes

The operating modes are as follows:

- Stopping the PLC **stops** Global Data exchanges.
- The use of the I/O forcing system bits (%S9,%SW8,%SW9) **does not stop** Global Data exchanges.

Limits

There are no theoretical limits for the number of stations sharing a Distribution Group. The main limitation is the number of variables exchanged in the Distribution Group (64 variables).

Section 4.6
Managing Faulty Devices

Replacing Faulty Remote Stations

Introduction

The objective of this service is to provide automatic recovery of remote I/O module parameters or intelligent modules connected to a Transparent Factory Ethernet sub-segment. When exchanging a faulty module with a functioning module.

Objective

The objective of this service is to:
- supply an IP address to a remote station from the Name given to this station (**Role Name**)
- give a remote station the capacity to store parameters and also to recover them, if required

Operation

This server requires the use of the DHCP server *(see page 99)* and the FTP/TFTP server of the TSX ETY 4103/PORT/5103 modules or the Ethernet link of the TSX P57 6634/5634/4634.

The following modules can configure up to 96 devices:
- TSX ETY 4103
- TSX ETY 5103
- ETY PORT

The following coprocessors can configure up to 128 devices:
- TSX P57 6634
- TSX P57 5634
- TSX P57 4634

Service operating principle:

Initially:
1. The valid remote station obtains an IP address from the name that has been given to it (Role Name).
2. The valid station gives its configuration parameters to the server.

Secondly:

This station breaks down. It is replaced with a non-configured device of the same type, which has the same name as the station it replaces:

1. It then transmits a DHCP request to the server.
2. It receives its configuration file, which was saved first on the server.
3. The remote station restarts automatically.

NOTE: The Role Name is limited to 16 characters in ASCII.

Section 4.7
Time Synchronization Service

About this Section

This section describes the time synchronization service, which establishes an accurate local clock by referencing a network time protocol (NTP) server via the network transfer protocol.

NOTE: The Control Expert configuration for the NTP service is available only with the TSXETY5103 module.

What Is in This Section?

This section contains the following topics:

Introducing the Time Synchronization Service

Overview

The time synchronization service established accuracy among computer clocks on an Ethernet system. For example, the time of one client may be synchronized either with another server or to a referenced time source such as a radio or satellite receiver.

Typical time service configurations use redundant servers and diverse network paths to establish high accuracy and reliability. Time service accuracy can be within a millisecond on LANs and within tens of milliseconds on WANs.

Use the time synchronization service for:

- event recording (for example, tracking a sequence of events)
- event synchronization (for example, triggering simultaneous events)
- alarm and I/O synchronization (for example, time stamping alarms)

Features of the Service

The time synchronization service offers:

- periodic time corrections obtained from the reference standard, for example, the NTP server
- automatic switchover to a backup time server if a problem occurs with the normal server system
- local time zone configurable and customizable (including daylight savings time adjustments)
- web page diagnostics for the time synchronization service

Controller projects use a function block to read the clock, a feature that allows events or variables in the project to be time stamped. Time stamping is accurate to:

- 5 ms for the TSX P57 4634/5634/6634 CPUs
- 10 ms for other CPUs

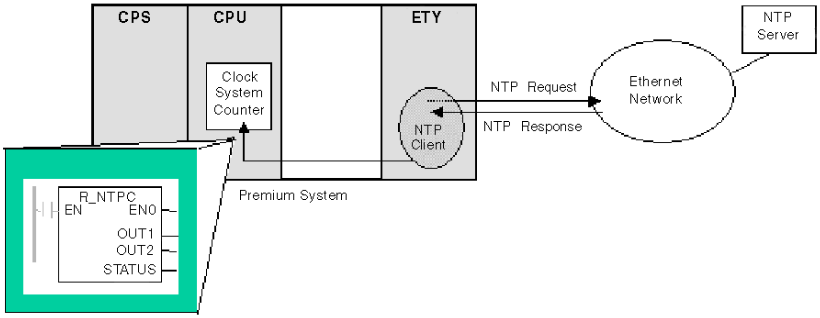
Time Synchronization and Time Stamps

The ETY Ethernet communications modules send a source time-synchronization signal to a CPU. The ETY's firmware includes an NTP client, which provides time synchronization. The synchronization process occurs as follows:

The NTP Client ...		Result
1	... requests a time synchronization signal from the NTP server over an Ethernet network.	The NTP server sends a signal.
2	... stores the time.	
3	... sends a message to the clock system counter in the CPU.	The CPU updates its internal clock at 1 ms for TSX P57 4634/5634/6634 CPUs or 5 ms for other CPUs.

Use the R_NTPC function block *(see page 113)* in either MAST, FAST or Interrupt sections to read the clock from the PLC application.

All the CPUs on an Ethernet network should be synchronized with the same NTP server.



Time Synchronization Terms

Term	Description of Service
local clock offset	Accurate local time adjustments are made via a local clock offset. The local clock offset is calculated as: `((T4 - T1) + (T3 - T2))2` where . . . ● T1 = time when NTP request is transmitted from the module ● T2 = time when NTP server receives the request (provided by the module in response) ● T3 = time when the NTP server transmits the response (provided to the module in the response) ● T4 = time when NTP response is received by the module
time accuracy	The local time error is < 10 ms compared to the referenced NTP server's time. ● typical: under 5 ms ● worst case: <10 ms
settling time	Maximum accuracy is obtained after 2 updates from the NTP server.
polling period dependency	Accuracy depends on the polling period. Less than 10 ms of error is guaranteed for polling periods of 120 s or less. To obtain the best possible accuracy (when your network bandwidth allows), reduce the polling period to a small value—e.g., a polling time of 5 s provides better accuracy than a time of 30 s.
time zone	The default format is universal time, coordinated (UTC). Optionally you may configure the service to use a local time zone—e.g., GMT+1 for Barcelona or Paris
daylight savings time	The module automatically adjusts the time change in the spring and fall.
leap second	To compensate for the deceleration of the earth's rotation, the module automatically inserts a leap second in the UTC time every 18 months via an international earth rotation service (IERS). Leap seconds are inserted automatically as needed. When needed, they are inserted at the end of the last minute in June or December, as commanded by the NTP server.

Using the Time Synchronization Service

Establishing Accuracy at Power Up

Before starting a system, the Ethernet network must be configured for a predefined interval within which the accuracy is established. Accuracy is established at power-up, when the Ethernet module boots and then obtains the time from the NTP server *(see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual)*.

Several updates may be required to achieve peak accuracy. Once an accurate time is obtained, the time synchronization service sets the STATUS *(see page 114)* in the associated time service register.

Obtaining and Maintaining Accuracy

The time service clock starts at 0 and increments until the Ethernet network time is fully updated from the module.

Model	Starting Date
Premium with Control Expert	January 1st 1980 00:00:00.00

Clock characteristics:
- Clock accuracy is not affected by issuing Stop/Run commands on the PLC
- Clock updates are not affected by issuing Stop/Run commands on the PLC
- Mode transitions do not affect the accuracy of the Ethernet network

Reinitializing the Time Service Register

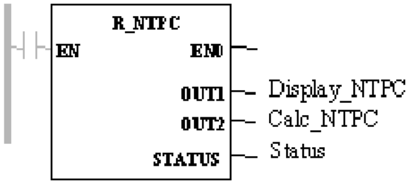
After a download or an NTP server swap, the status clock value associated with the time service register in the CPU is reinitialized.

Two polling periods elapse before an accurate time is reestablished.

Using the R_NTPC Block for Time Synchronization

R_NTPC Representation

The R_NTPC block reads Ethernet network system time and transfers it into specified parameters. The additional parameter EN should be configured.



The R_NTPC block has a 16-bit status word.

R_NTPC Parameter Description

Description of parameters:

<table>
<tr><th>Parameter</th><th>Data Type</th><th colspan="3">Description</th></tr>
<tr><td>Display_NTPC
(OUT1)</td><td>DT + INT</td><td colspan="3">NTP clock value displayed in:
year, month, day, hours, minutes, and seconds using the DT format
milliseconds as an INT</td></tr>
<tr><td>Calc_NTPC
(OUT2)</td><td>UDINT+INT</td><td colspan="3">NTP clock value displayed in:
seconds as an UDINT
fractions of a second as an INT</td></tr>
<tr><td rowspan="6">Status</td><td rowspan="6">INT</td><td>Low Byte</td><td>High Byte</td><td>Description</td></tr>
<tr><td>0</td><td>0</td><td>un-initialized state</td></tr>
<tr><td>1</td><td>0</td><td>illegal</td></tr>
<tr><td>0</td><td>1</td><td>the CPU is out of synchronization with the NTP server, but the clock has been updated at least once by an external server</td></tr>
<tr><td>1</td><td>1</td><td>normal operation</td></tr>
<tr><td colspan="3">The low byte is managed by the controller
Set = 0
clock value NOT available
date/time NOT updated within last two minutes
Set = 1
date/time updated within the last two minutes
date/time acceptable
The high byte is managed by the ETY
Set = 0
the NTP server clock value is not available
Set = 1
updated date/time received from server and sent to module (at least once)
within two minute time interval
acceptable (10 ms or less error)</td></tr>
</table>

Section 4.8
Electronic Mail Notification Service

About this Section

This section describes the electronic mail notification service, which uses SMTP to send e-mail messages.

What Is in This Section?

This section contains the following topics:

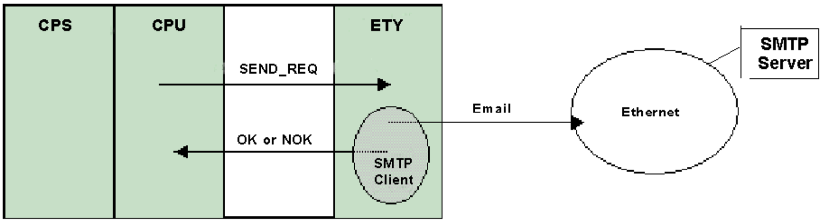
Introducing the Electronic Mail Notification Service

Introduction

The electronic mail notification service allows controller-based projects to report alarms or events. The controller monitors the system and dynamically creates an electronic mail message to alert local or remote users.

Mail Service Client

The TSX ETY 4103/5103 and the TSX P57 x634 modules include an SMTP client. When the module receives a specific request from the project, the module sends an email message to the mail server.



Mail System Types

SMTP provides two mechanisms for the transmission of email messages—direct connection and a relay system:

Mechanism	Condition	Result
Direct connection	sender and receiver are connected to the same transport service	Email messages are sent to host
Relay system	sender and receiver are connected to different transport services	Email messages are relayed from one server to another. The SMTP server must be supplied with the address of both the destination host and the destination mailbox.

Operating Modes and Sending Requests

Because the project sends the email request, a controller cannot send an email message either while in the stopped mode or while downloading a project. As soon as the controller is in run mode, the function block sends a request during the first project scan.

Diagnostic counters are reset to 0 after either a power-up, a project download, or a reconfiguration of the electronic mail notification service.

Using the Electronic Mail Notification Service

Configuring the Service

An authorized administrator may use the SMTP configuration web page to:
- configure the electronic mail notification service
- set the IP address of the mail server

NOTE:

- Configure the port specified by your local mail server *(see page 312)*. The default TCP port number for SMTP is 25.
- When configuring SMTP for an ETY 4103 or ETY 5103, use one of the following as an external email server:
  - Lotus Domino
  - Microsoft Exchange
  - Sendmail

Message Creation and Delivery

A user-defined event or condition triggers the SEND_REQ block to create a message *(see page 119)*. Each message uses one of three user-defined headers. Each message sent from the controller can contain text and variable information (up to a maximum of 238 bytes).

The project selects the appropriate header. Each header contains:
- sender name
- list of recipients
- subject

Header Examples

An authorized administrator can define and update the text and variable information via an embedded SMTP Configuration web page. Define mail headers to indicate different levels of importance. For example:
- header 1 could be *Urgent problem reported by PLC 10*
- header 2 could be *Notification from substation 10*
- header 3 could be *Info message from water system*

Listing different recipients in each of the three headers assures that information flows quickly to the right recipients. The project adds pertinent information such as the specific device, process or location. This information is added to the body of the mail message. Then the complete message is sent to an electronic mail server for distribution to recipients.

Recipients may be engineers, managers or process owners.

Security (Authentication)

An optional login (system ID) and password can be used to authenticate the connection to the SMTP mail server. The SMTP-supported authentication method is LOGIN.

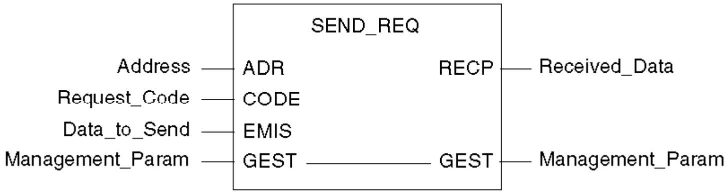
System Diagnostics

The SMTP diagnostic web page displays the status of the service. Diagnostic information is also available for remote management using the SNMP network management standard.

Using the SEND_REQ Block for Electronic Mail Notification

SEND_REQ Representation

To send an email message from the application, use a SEND_REQ block.



ADR

The ADR must use the following address format:

`{network.station}rack.module.channel.SYS`

For example, if an ETY module has the Xway address {10.1} and resides in slot 4 in the rack, its ADR would be:

`{10.1}0.4.0.SYS`

NOTE: An ADR of `{0.254}.0.4.0.SYS` also works, where `{0.254}` represents *my address*.

For the TSX P57 6634/5634/4634, use the ADR `{0.254}0.0.3.SYS`.

The ADR may be used to convert from the string format to the INT array expected by the block.

CODE

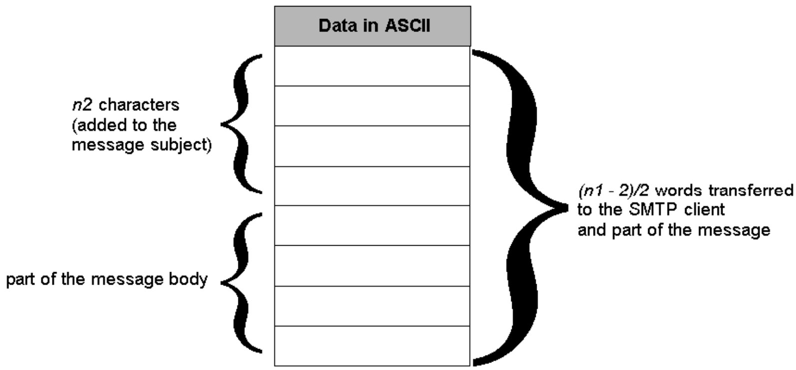
Use the write object request function code (0*x*37) for a SEND_REQ block. The expected success code is 0*x*FE, and the error code is 0*x*FD.

EMIS

The Data_to_Send contains the address of the buffer with the data to put in the body of the email. This information is preceded by a header with the following information:

Header Information	Value	Byte	Register
Segment	0x96	1	1
Type	0x15	2	
Address	N/A	3	2
		4	
Number (*n1*) of characters in the email	0	5	3
	≤ 240	6	
Mail header	{1, 2, 3}	7	4
	≤ (*n1* - 2)	8	

The following (*n1* - 2)/2 words (up to a maximum of 119)) contain the data in ASCII format that will be copied into the email message. The first *n2* characters are added to the configured email subject and the rest are part of the email body:



GEST

The fourth parameter of the management table must contain the size of the data buffer and must be set before you use the SEND_REQ block.

RECP

The Received_Data request does not return any data.

Reset Module Command

Parameter Usage for Reset Module Command

A Reset Module operation causes Premium ETY and ETY PORT communication modules to enter a cycle to reset its working environment. To program a SEND_REQ function block to perform a Reset Module command, use function code 37, subfunction code 10.

Parameter	Type	Value	Comment
`ADDRESS`	array [0...5] of INT	ADDR ('rack.slot.channel.SYS')	Example: ADDR (0.x.0.SYS') x = slot in which ETY module is installed
`REQUEST_CODE`	INT	16#37	
`Data_to_send`	array [0...1] of INT	byte 1: subfunction (10h)	high byte
		byte 2: subfunction (96h)	low byte
		bytes 3, 4: 0	reserved
`Manage_Param`	*word number*	*high byte*	*low byte*
	1	activity report	00
	2	operation report (see note)	communication report (see note)
	3	timeout (ms)	
	4	length: 4 (INT) (in this example)	
	NOTE: The following table gives details for Reset Module codes (successful and error).		

Reset Module Command Codes

Operation Report	Communication Report	Meaning
successful code		
FE (hex)	00 (hex)	SEND_REQ successfully reset module
error codes		
01 (hex)	FF (hex)	invalid request code value (e.g., not 16#37)
00 (hex)	07 (hex)	bad address mapping to the ETY
FD (hex)	00 (hex)	SEND_REQ did not reset module

Electronic Mail Notification Service Error Codes

Error Codes

The following codes are available only on the diagnostic screen for the electronic mail notification service:

Error Code (hex)	Description
5100	Internal error detected
5101	SMTP component not operational
5102	Mail header not configured
5104	Cannot connect to SMTP server
5105	Error detected during transmitting content of email body to SMTP server
5106	Closing SMTP connection with the server returned an error message
5107	SMTP HELO request unsuccessful
5108	SMTP MAIL request unsuccessful — SMTP server may require authentication
5109	SMTP RCPT request unsuccessful
510A	No recipient accepted by the SMTP server
510B	SMTP DATA request unsuccessful
510C	Send email request contains an invalid length
510D	Authentication unsuccessful
510E	A reset component request was received while the connection was open

Section 4.9
HTTP Onboard Server/Embedded Web Pages

About this Section

This section describes functions and characteristics of the onboard server or Embedded Web Pages. Web pages offer both configuration and diagnostic information. For more information, see the separate topics that discuss the diagnostics home page *(see page 135)* and service configuration *(see page 145)*.

What Is in This Section?

This section contains the following topics:

Embedded HTTP Server

Introduction

Some Ethernet modules include an embedded Web server, which allows:
- access to PLC data
- diagnostics to be carried out on the entire configuration

All the processor or module data is presented as standard Web pages in HTML format. Access Web pages with Internet Explorer 4.0 or higher running JRE 1.4.1_04 or higher.

None of the functions supplied by the Web site require any prior configuration or programming within the module.

The summary table below shows the various selections possible.

According to the type of module, the availability of these functions changes:

Function	TSX ETY 110	TSX ETY 110 WS	TSX ETY 4103 TSX ETY PORT TSX P57 6634/5634/4634	TSX ETY 5103	TSX ETY 210
Server	-	X	X	X	-
Predefined pages	-	-	X	X	-
Client pages	-	X	-	X	-
Client site size	-	1.2 Mb	-	6.5 Mb	-
Minimum FactoryCast version	-	V 3.0	-	V 3.01	-
Legend					
X	Available				
-	Not available				

Embedded Server Functions

The functions available on an embedded server are generally as follows:
- Statistics: This page shows the Ethernet network statistics.
- Security: This page is used to modify the user name and the password to access the site.
- Address Server: If the module is used as an address server, this page enables you to display and modify the server table.
- Displaying the Rack: This page enables you to display the configuration of the PLC which is controlling the module.
- Data Editor: This page allows you to display PLC data.
- Diagnostics Functions: These pages allow network diagnostics.

Connections to a TSX ETY Module

The module web-site shows static and dynamic pages (PLC data). To refresh dynamic pages, an X-Way connection is automatically created between the web browser and the module.

NOTE: The browser connection X-Way address is automatically derived from the module's address by taking the same network number and a station number between 54 and 63. It is therefore essential to leave at least one X-Way address free in this range of values.

The number of connections is regulated:

- It is not possible to connect several browsers on a given PC to the same TSX ETY module.
- Up to 10 PCs connected simultaneously to one module.
- On a TSX ETY 4103/PORT/5103 and on the Ethernet link of the TSX P57 6634/5634/4634, it is possible to connect a browser and another application (for example, an XIP driver).

HTTP Server Security Page

Introduction

This page can be used to modify the:

- user name and password for accessing the index page
- password for writing variables in the data editor

The size of the user name and passwords is a maximum of 16 characters in non-extended ASCII.

Accessing the Page

To access the security page from the index page:

Step	Action
1	Click the **Security** link.

Illustration

As an example, the security page of a TSX ETY 4103, a TX ETY PORT or the Ethernet link of the TSX P57 6634/5634/4634 is as follows:

Modifying HTTP Access Rights

To modify the HTTP access rights:

Step	Action
1	Enter the new **User** name.
2	Enter the new password.
3	Confirm the new password.
4	Confirm the modification using the **Change password** button. **Result:** An **Ethernet Configuration** page appears.
5	Click the **Reboot Device** button to recognize the modification in the module.

Modifying the Write Password

To modify the write password:

Step	Action	Comment
1	Enter the case-sensitive current password.	The default value of this field is: USER.
2	Enter the new password.	
3	Confirm the new password.	
4	Confirm the modification with the **Change password** button.	An **Ethernet Configuration** page appears to indicate that the password has been modified.

Address Server Page for the HTTP Server

Introduction

This page is used to display or modify the correspondence table between the MAC addresses or the Name (Role Name) and the IP addresses of the module if the latter is configured as a BOOTP server. Elsewhere in this guide is a detailed discussion of the Address Server *(see page 96)*.

This function is useful when replacing a failed remote device (for example, replacing a faulty Momentum module).

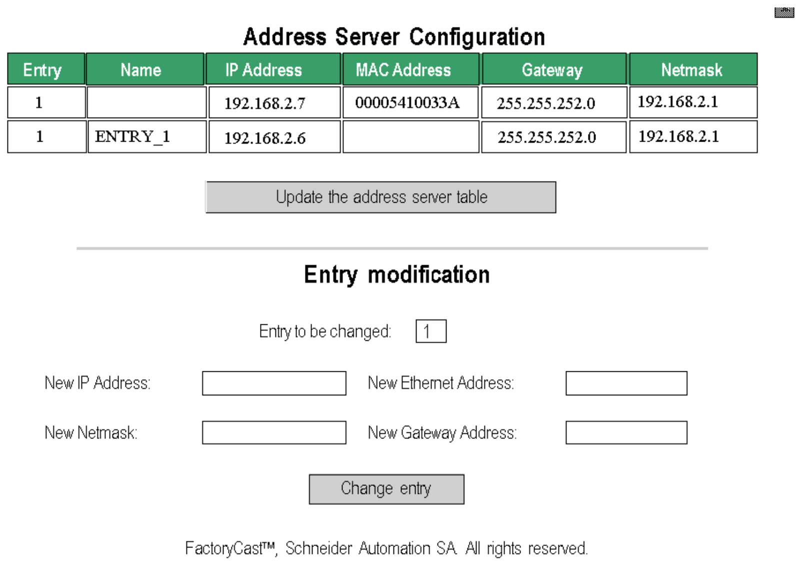
NOTE: This page does not allow the addition of new inputs, nor the modification of the Name (Role name) for a remote device.

Accessing the Address Server Page

Follow this procedure to access the Address server page from the index page:

Step	Action
1	Click on the **Setup** link.
2	Click on the **Address server** link.

The Address Server page of a TSX ETY4103, a TSX ETY PORT, or the Ethernet link of the TSX P57 6634/5634/4634 appears. Here is an example:



Modifying the Address Server Table

To modify entries in the Address Server Configuration window:

Step	Action
1	Enter the entry number to be modified in the field provided.
2	Enter the new IP address to be modified in the field provided.
3	Enter the new MAC address to be modified in the field marked: **New Ethernet Address**.
4	Is the server locked in run mode? ● **yes:** Enter the password associated to the address server then go to step 5. ● **no:** Go to step 5.
5	Confirm the modification with the **Change entry** button.
6	Click on the **Refresh Address server table** button to display the modification on the screen.

Recognition of Modifications

Configuration modifications are recognized either after a cold restart of the PLC, or on the next loading of the PLC application.

HTTP Server Rack Display Page

Introduction

This page allows you to carry out diagnostics on the modules in the local rack configuration that includes the Ethernet module.

By clicking on a module in the configuration, you obtain a set of diagnostic information on this module:

- LED status display
- the type and the version of the module as well as its position in the rack
- information specific to the functions of the module

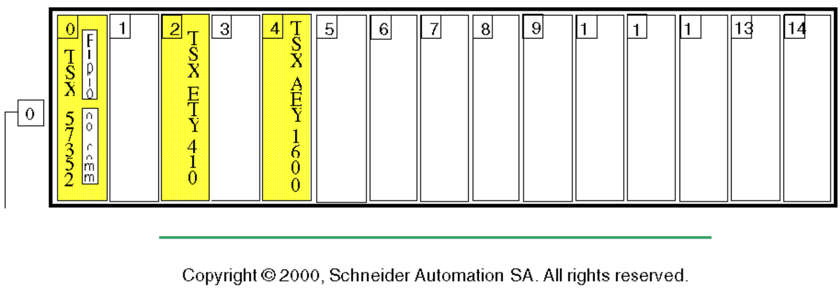
NOTE: For further information, refer to the FactoryCast User Guide.

Accessing the Server Rack Display Page

Follow this procedure to access the rack display page from the index page:

Step	Action
1	Click the **Diagnostics** link.
2	Click the **Rack Display** link.

The TSX ETY4103 rack display page apears. An example is shown below:



HTTP Server Data Editor Page

Introduction

This page is used to create animation tables containing lists of PLC variables to be displayed or modified.

Variables can only be accessed via addresses.

This function is useful when running diagnostics on an application.

NOTE: Write access is managed by password. For further information, refer to the FactoryCast User Guide documentation.

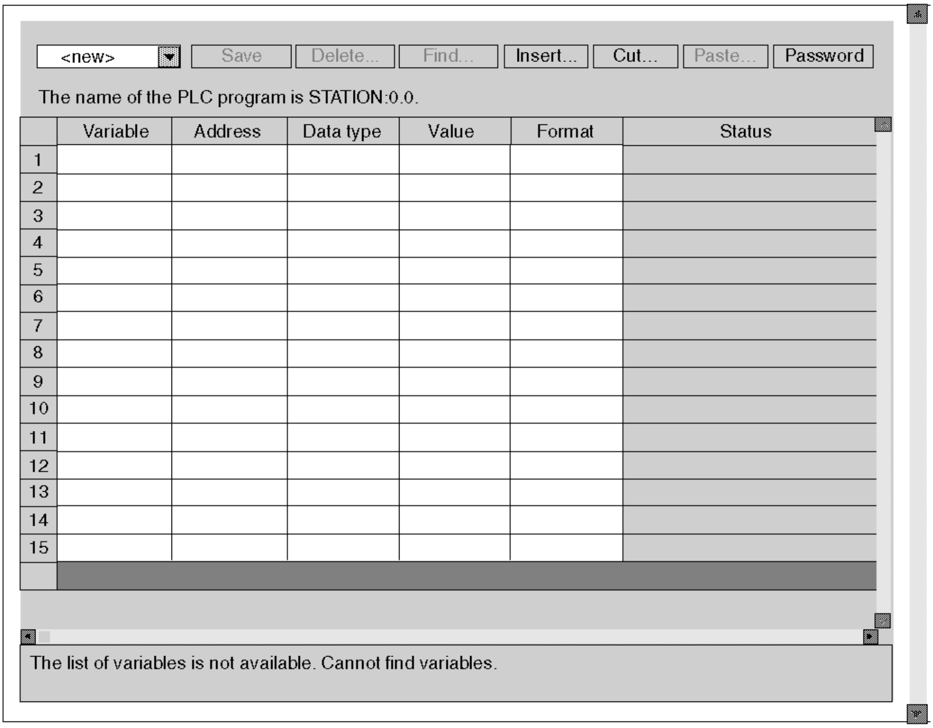
Accessing the Data Editor Page

Follow this procedure to access the data editor page from the index page:

Step	Action
1	Click on the **Monitoring** link.
2	Click on the **Data Editor** link.

Illustration

The Data Editor page of a TSX ETY 4103 or an TSX ETY PORT is presented below as an example.



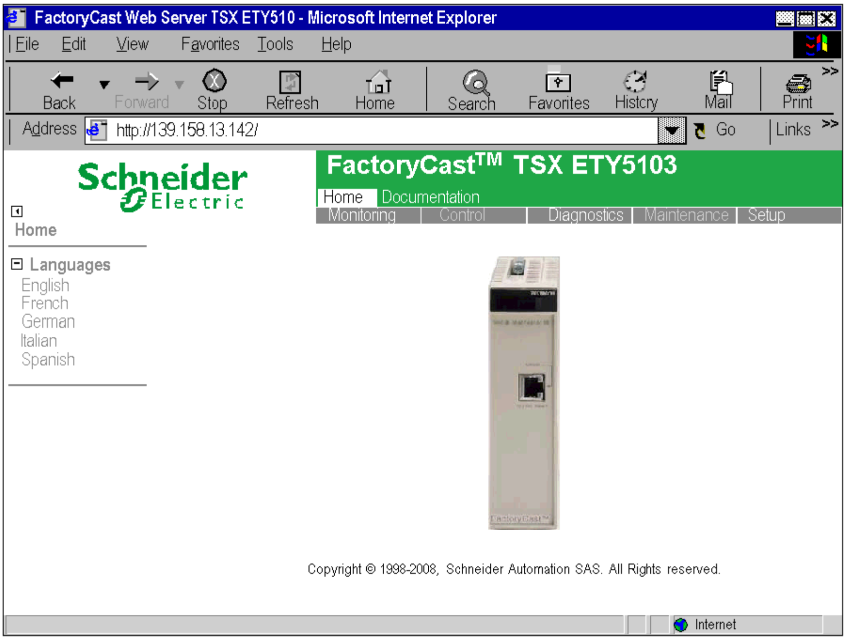
Premium Home Page

Overview

To access the Premium home page enter the IP address of the module in his web browser. No password is required to display this page.

Home Page

This Premium home page looks like this:



Links

From the Premium home page, you can access the following pages :

- Monitoring
- Diagnostics *(see page 135)*
- Setup
- Documentation
- Foreign language links exist for French, German, Italian and Spanish versions

Enter a user name and a password to access the services proposed in these pages.

Accessing Web Service Pages

Introduction

This topic discusses access to Web services from the Premium home page *(see page 133)*.

Access Web Services

The Premium home page has links to the following Web services:
- Monitoring *(see page 142)*
- Diagnostics *(see page 135)*
- Setup

To access the services:

Step	Action	
1	Click the service you want to access.	A window requesting the user name and password appears.
2	Enter the case-sensitive user name and password.	Default values for this field are: ● user name: USER ● password: USER
3	Click **OK**.	This confirms your choice.

Instructions for changing the user name and password can be found at HTTP Server Security Page *(see page 126)*.

Diagnostics Home Page

Home Page

This page lists the various services supported by the default Web site of the module and provides links for accessing the services you require.

Illustration

The **Diagnostics** home page looks like this:

Links

To access the service you require, click on a link:
- Rack Viewer *(see page 130)*
- Alarm viewer
- Ethernet *(see page 69)*

Ethernet Module Statistics Page

Home Page

The **Ethernet** menu contains a list of links for accessing the Ethernet module's different diagnostic pages:

- Global Data *(see page 104)*
- I/O scanning *(see page 137)*
- Messaging
- Bandwidth monitoring *(see page 142)*
- Ethernet module statistics

A link also allows the private MIB source file to be downloaded.

Click on a link to access the desired diagnostics page.

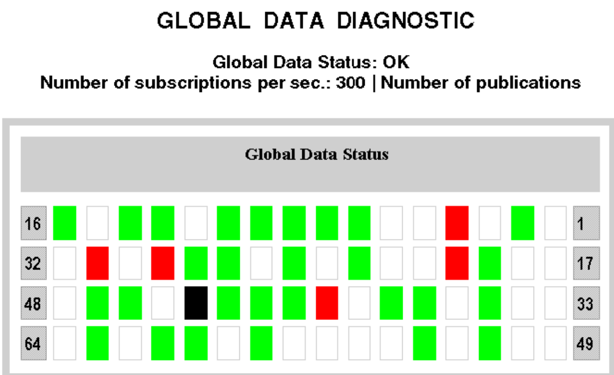
Global Data Page

If you click **Global Data** on the **Diagnostics** home page *(see page 135)*, the following information can be found:

- Status
- Number of publications per second
- Number of subscriptions per second

This page also shows a table of the published and subscribed variables in the same distribution group. The nature of each variable is identified by a color code:

- green: subscribed variables
- black: published variables
- white: unconfigured variables
- red: variables with detected communication faults



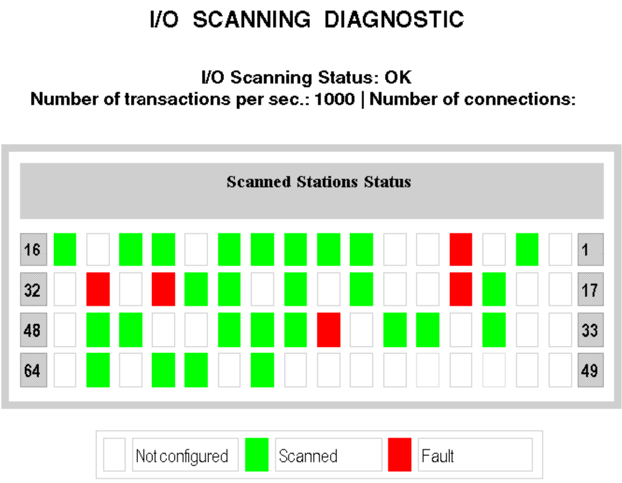
I/O Scanning Page

If you click **I/O scanning** on the **Diagnostics** home page *(see page 135)*, the following information can be found:

- Status
- Number of transactions per second
- Number of connections per second

This page also displays a summary of the status of modules with color coding:

- green for the scanned modules
- white for the unconfigured modules
- red for suspect modules
- black for the modules that are temporarily unscanned.



Messaging Page

The **Messaging** page provides current information on the open TCP connection on port 502.

MESSAGING DIAGNOSTIC

Number of Messages sent: 150 | Number of Messages received: 50

Conn.#	Remote addr.	Remote port	Local Port	Mess. sent	Mess. received	Err. sent.
1	192.160.10.20	1920	502	20	12	0
2	139.160.235.90	2020	502	0	30	02
3	192.160.10.21	502	300	3	60	0
4	139.160.234.20	1050	502	15	42	0
5	139.160.234.18	5120	502	0	39	1

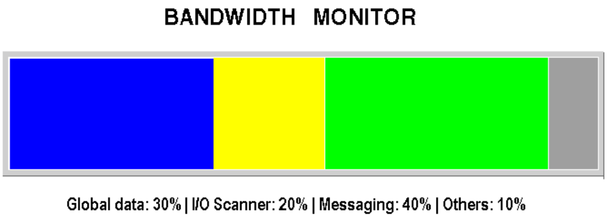
The number of sent/received messages on the port can be found at the top of this page. For each connection (numbered from 1 to 64), a table provides:

- the remote IP address (Remote addr.)
- the remote TCP port (Remote port:)
- the local TCP port (Local Port)
- the number of messages sent from this connection (Mess. sent)
- the number of messages received from this connection (Mess. received)
- the detected error number on this connection (Err. sent)

NOTE: Following a request to close a connection, the PLC may hold the connection open in its memory for a few minutes, during which the table will reflect the open connection.
Number of Messages received is not reset after a port 502 connection is closed. Therefore, the count indicates the total number of messages that have been received since the module was started.
The remote address ‘127.0.0.1’ is used as Private System Connection For Diagnostic Feature or SOAP Communications.

Bandwidth Monitoring Page

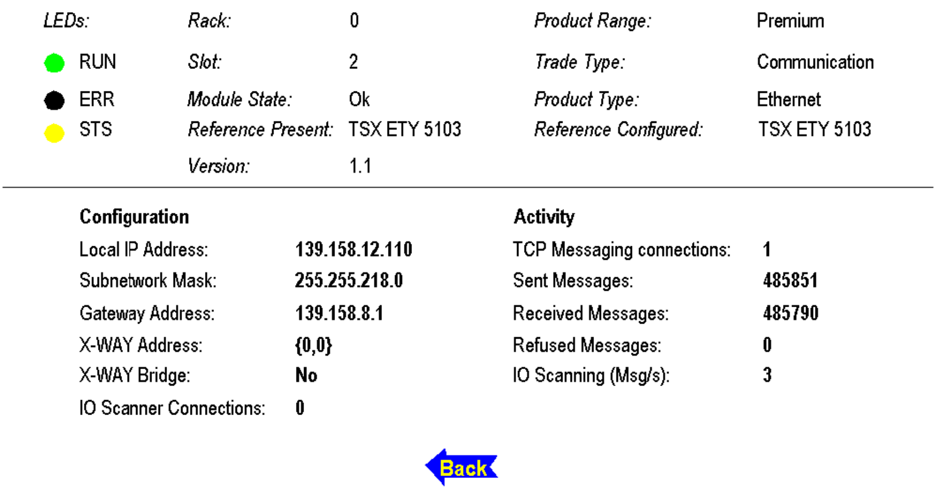
The **Bandwidth Monitoring** page shows the load distribution of the TSX ETY 4103/5103 module between the Global Data, I/O Scanning, Messaging and other services:



Statistics Page

When you click the Embedded Server module in the **Rack Viewer**, you reach the **Ethernet Module Statistics** page. This page provides up-to-date information about the status, configuration, and activity of the Embedded Server module.

Here is an example of an **Ethernet Module Statistics** page.



Dynamic Data

The LEDs in the upper left-hand corner of the screen provide a dynamic report on the Embedded Server module status.

LEDs	Color if On	Meaning if On	Meaning if Blinking	Meaning if Off
RUN	Green	Running normally	---	Power Off
ERR	Red	Module detected error	Not configured	Running normally
STS	Red	Invalid network address or station out of range	---	OK

Links

Clicking the back arrow takes you to the **Rack Viewer** page *(see page 130)* for this controller.

HTTP Server User Pages

Introduction

It is possible to create complete pages about certain modules. To do this, the FactoryCast software and a guide for creating and publishing user pages are delivered with these modules.

NOTE: The TSX ETY5103 module is delivered with the FactoryCast V3.01 (or above) CD and the accompanying guide for creating and publishing user pages.

There are two types of pages:
- pages that are protected by passwords
- pages that are not protected by passwords

Accessing Protected User Pages

Follow this procedure to access protected user pages from the home page:

Step	Action	Result
1	Click the **Monitoring** link.	
2	Click the **Protected user pages** link.	The dialog box for entering the password appears.
3	Enter your user name and password, then confirm.	The first branch page on the created site appears.

Accessing Unprotected User Pages

Follow this procedure to access unprotected user pages from the home page:

Step	Action	Result
1	Click the **Monitoring** link.	
2	Click the **unprotected user pages** link.	The first branch page on the created site appears.

Section 4.10
Bandwidth Monitoring

Bandwidth Monitoring

Introduction

Transparent Ready offers two types of services:
- real time: High-performance and predictable behavior are expected from services such as:
  - periodic services: I/O Scanner and Global Data
  - non-periodic services: Messaging on port 502 (Modbus)
- other: for Web and network management

After you configure the I/O Scanner, it is possible to estimate the load percentage of the module for this service.

The Bandwidth Monitoring function carries out this estimate during configuration.

The actual distribution of service loads is shown on the module's Control Expert diagnostics screen and on the diagnostics services bandwidth monitoring Web page.

Operation

In order to estimate this load, Control Expert asks you to supply two pieces of information during configuration:
- an estimate of the number of messaging transactions per second
- an estimate of the number of Global Data subscriptions received per second

Using this information, the software is able to display the load percentage of the module for:
- I/O Scanner *(see page 90)*
- Global Data *(see page 90)*
- messaging services *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*
- remaining services *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*

NOTE: During the configuration phase, these pieces of information are only estimates. The actual distribution is displayed in online mode.

Section 4.11
ETHWAY Service

ETHWAY Profile

Introduction

The ETHWAY profile offers the following data exchange capabilities:
- data exchanges synchronized on the MAST task
- or data exchanges in:
  - asynchronous server mode
  - asynchronous client mode
- or common data exchanges (common words)

Common data exchanges are described below. For a description of synchronous and asynchronous exchanges, see UNI-TE on TCP/IP *(see page 78)*.

Common Words

All common words represent a database distributed among all or part of the devices on the same network.

The maximum number of common words on a network depends on the number of stations issuing common words:
- 4 common words per station for 64 active stations
- 8 common words per station for 32 active stations
- 16 common words per station for 16 active stations
- 32 common words per station for 8 active stations
- 64 common words per station for 4 active stations

NOTE: Common words can take up a large part of the module's messaging bandwidth if there are many stations connected and if the configured PLC cycle time is very short. Common words are issued:
- on each PLC cycle if there are changes in status
- every 10 cycles if their value is not changed

You must not exceed the maximum capacity of the module.

Common words (%NW) are updated automatically. The application program simply involves writing or reading these words. For example:
- %NW1.7.0:= %MW10 (writing a value for sending)
- %MW50:=%NW1.8.2 (receiving a value)

Chapter 5
Configuration Parameters

Overview

This chapter introduces the configuration parameters for the different Ethernet services used by the modules.

What Is in This Chapter?

This chapter contains the following sections:

Section 5.1
Security Service Configuration Parameters

Security (Enable / Disable HTTP, FTP, and TFTP)

Security and HTTP, FTP, and TFTP Services

You can enhance security for your project by disabling the FTP/TFTP and HTTP services at times when you do not need to use them. The module uses the HTTP service to provide access to the embedded Web pages. The module uses the FTP and TFTP services to support various features including firmware upgrades, and FDR services.

The module's HTTP, FTP, and TFTP services can be disabled or enabled using the Control Expert **Network Editor** → **Security** screen.

On power up, these services are:

- disabled by default in projects created using Unity Pro 8.1 or later and one of the following modules:
  - TSX P57 1634M, firmware version 5.70 or later
  - TSX P57 2634M, firmware version 5.70 or later
  - TSX P57 3634M, firmware version 5.70 or later
  - TSX P57 4634M, firmware version 5.70 or later
  - TSX P57 5634M, firmware version 5.70 or later
  - TSX P57 6634M, firmware version 5.70 or later
  - TSX ETY 4103, firmware version 5.70 or later
  - TSX ETY 5103, firmware version 5.90 or later
- enabled by default in projects where:
  - the project was created using Unity Pro 8.0 or earlier, or
  - the communication module is not configured

You can use Control Expert to enable or disable HTTP, FTP, and TFTP services as described in the following procedure.

If the HTTP, FTP, or TFTP services have been enabled with Control Expert, they can also be enabled or disabled at run time using the DATA_EXCH block. (See the *Communication Block Library* for Control Expert.

Using Control Expert to Enable and Disable Firmware Upgrade, FDR and Web Access Services

Perform the following steps to enable or disable FTP/TFTP or HTTP services on the module.

Step	Action
1	In the Control Expert **Project Browser** → **Structural View**, double-click the desired Ethernet network in the **Communication** → **Networks** directory to open the **Network Editor**.
2	Click the **Security** tab.
3	On the **Security** screen, choose the appropriate setting: (**Enabled** or **Disabled**) for the service or services.

The edits will take effect when they are successfully downloaded from your PC to the CPU and from the CPU to the communication modules and network devices.

Section 5.2
TCP/IP Services Configuration Parameters

About this Section

This section introduces the configuration parameters linked to the TCP/IP Messaging services.

What Is in This Section?

This section contains the following topics:

Configuration Parameters Linked to the TCP/IP Service

Introduction

The TSX ETY modules of the Ethernet link of the TSX P57 6634/5634/4634 have configuration parameters linked to the TCP/IP service.

Depending on the Ethernet channel selected, some configuration parameters cannot be accessed on the configuration screen. They are either not shown on the screen or are grayed out.

Availability of Parameters

The following table shows the parameters that can be accessed from the configuration screen for each type of Ethernet channel and their associated values:

Parameters			TSX ETY 110	TSX ETY 4103/PORT/5103	TSX P57 6634/5634/4634
X-Way Address			By thumbwheels	By Control Expert	Optional
IP Address	Default IP address		X	X	X
	Configured	IP Address	X	X (dynamic)	X
		Subnetwork mask	X	X (dynamic)	X
		Gateway address	X	X (dynamic)	X
	Client/Server configuration		-	X	X
Connections	Connections which can be opened		from 1 to 32	-	-
	Access control		X	X	X
	Correspondence table	X-Way Address	X	X	X
		IP Address	X	X	X
		Protocol	UNI-TE or Modbus	UNI-TE or Modbus	UNI-TE or Modbus
		Access	X	X	X
		Mode	-	Mono- or Multi-connections	Mono- or Multi-connections
Ethernet	Ethernet II		X	X	X
	802.3		X	X	X
Key:					
X	Accessible				
-	Not accessible				

Configuration Parameters for IP Addresses

Introduction

This zone allows the IP address of a module to be defined in three distinct ways:

- either using a default configuration
- by manual configuration
- or by using a configuration supplied by a server device

Default IP Address

Selecting the **IP Address by default** field allows the module's IP address to be calculated from the code selectors *(see page 233)*.

In this instance, you must code the network and station numbers on the code selectors located on the front of the module.

With this coding, the IP address is automatically derived by the system and the **IP Address**, **Subnetwork mask**, and **Gateway Address** fields are not significant and are grayed out.

NOTE: The default parameters should not be selected when the module is connected to a closed or private network.

Configured IP Address

Selecting the **Configured** field allows manual configuration according to your own requirements:

- module IP address
- the subnetwork mask, which defines the part allocated to the subnetwork identifier in the IP address
- the IP address of the default gateway, to which messages for other networks are transmitted

NOTE: If the module is connected to an existing TCP/IP network, the IP addresses are administered globally, therefore the IP parameters must be configured. Otherwise there is a risk of disturbance on the existing network caused by possible double allocation of the IP addresses.

Dynamic Modification

You can change the IP parameters (IP address, subnet mask, and default gateway) of the ETY module with the SEND_REQ function block. (Refer to the Control Expert Communication Block Library documentation.) The dynamic Ethernet address function enables an ETY module (configured in a Unity 2.0-compatible PLC application) to dynamically assign itself new IP parameters.

The Premium ETY module’s dynamic Ethernet address facility allows you to:

- install a single common PLC application into multiple physical installations, reducing the need for multiple copies of similar programs or rebuilding the application for each location that uses a new IP address
- use the PLC application code to assign an IP address and associated parameters to an ETY

To ensure that the ETY module is ready for operation, allow the PLC to run (in run mode) for 15 seconds after the last stop mode before issuing the SEND_REQ function. After the user issues the `CHANGE IP PARAMETERS` command and the ETY module accepts the new parameters, the ETY module resets and begins operations with the new parameters.

NOTE: FDR clients that use the ETY module for a server must be rebooted after the ETY's IP address change is completed. Otherwise, these FDR clients can not update their parameter files on the FDR server (the ETY module).

NOTE: Constant words contain the original configuration parameters, not those that were updated after the IP address change.

NOTE: You can see the new configuration (IP parameters, subnet mask, and gateway address) in the Control Expert ETY debug screen *(see page 276)*. You can also see the newly assigned IP address in the Ethernet Module Statistics web page, however, you must be aware that the IP Address, Subnetwork mask, and Gateway data on this page reflect the old configuration.

Refer to the example for changing IP parameters with SEND-REQ *(see page 152)*.

Client/Server Configuration

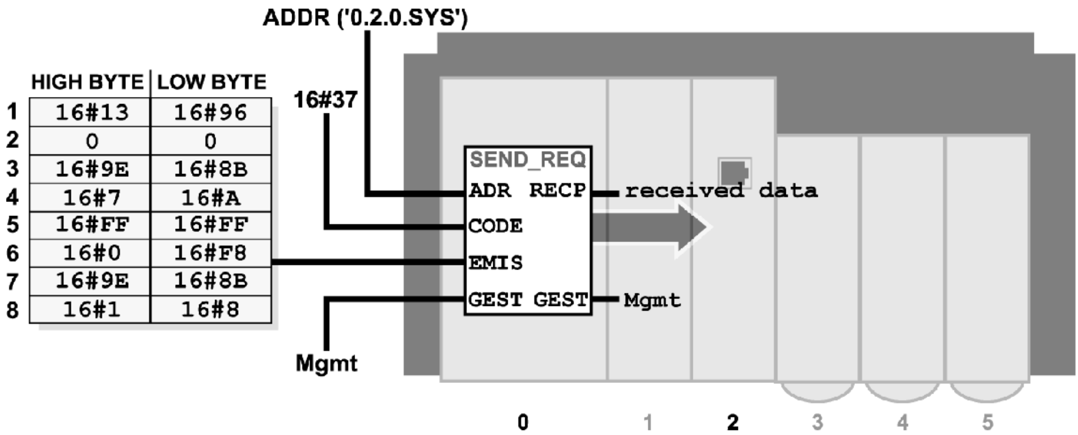
Selecting the **Client/Server configuration** field allows the module's IP address to be configured from a remote device acting as a BOOTP server *(see page 97)*.

In this instance, the **IP address**, **Subnetwork mask** and **Gateway Address** fields are not significant and are grayed out.

Changing IP Parameters with SEND_REQ (Example)

Illustration

The graphic shows you how to set IP parameters for the ETY module in slot 2 with the SEND_REQ block:



Note:
- ADR: reflects the ETY's position in slot 2.
- CODE: reflects the value of the REQUEST_CODE.
- EMIS: contains the IP parameters in Data_to_Send:
  - address (139.158.10.7)
  - subnet mask (255.255.248.0)
  - gateway (139.158.8.1)
- GEST: reflects Management_Param (management parameters).
  You have to assign a time to the third word of Management_Param. The fourth word should have the INT value 18.
- RECP: This parameter requires a minimum INT value of 1, even when no response message is returned, as in the case of an IP change request..

Connection Configuration Parameters

Introduction

This field is used to:
- configure the number of connections that can be opened by the module
- activate an access control service
- list the remote devices that can connect to the module according to a communication protocol

Connections Which Can be Opened

The **Connections which can be opened** field gives the maximum number of remote devices that can be connected to the module in parallel:
- The default value is 8 connections.
- The value is between 1 and 32 connections.

NOTE: You are recommended to set this parameter to a useful value in order to optimize the communication resources for each connection point.

Access Control

The **Access control** box is used to activate (or not) control of the remote devices trying to open a TCP connection to the module:
- If the box is checked, access control management is activated and the **Access** column of the table is active (no longer grayed out).
  Where the module operates in server mode, only remote devices selected by the **Access** box of the table are authorized to connect as clients before communicating.
- If the box is unchecked, access control management is inoperative and the **Access** column of the table is not active (grayed out).
  Where the module operates in server mode, remote third-party devices can connect as clients (before communicating with the module) without having to be declared in the table.

NOTE: Access control is only effective on the TCP/IP profile and assists module operations in server mode.

Correspondence Table

This table is used to:

- list the remote devices for which the local modules wish to open a TCP connection and for transmission (with the module operating in client mode)
- provide correspondence between the **X-Way** address {network, station} and the **IP address**
  - The network number must be less than or equal to 127.
  - The station number is between 0 and 63 for a UNI-TE connection or between 100 and 163 for a Modbus connection.
- specify the communication protocol during connection (using a drop-down menu) for each remote device of type **TSX ETY 110** or **TSX ETY 210**
  - **UNI-TE** (default value)
  - **Modbus**
- in the case of access control management, to designate the remote devices authorized to open a TCP connection and then to transmit to the local module (the module operating in server mode)
- for each remote IP address, to choose the connection **mode** using a drop-down menu:
  - **Mono-connection**: The module allows only one connection with the same remote IP address.
  - **Multi-connection**: The module allows only one connection in client mode with the same remote IP address and several connections in server mode with the same remote IP address.

X-Way Profile

This field is specific to the TSX P57 6634/5634/4634 and allows you to choose whether or not to use an X-Way profile.

Check the box and complete the X-Way network/station address. If the X-Way profile has not been checked, the station cannot participate in X-Way exchanges. It may however be connected to Control Expert or to Modbus applications.

Ethernet Frame Format

Introduction

The **Ethernet configuration** field on the IP Configuration tab *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)* is used to define the frame format for TCP/IP communications in accordance with those formats required by end devices (valid for configured IP addresses only). Options are:

- **Ethernet II:** The Ethernet II format complies with the RFC 894 standard (the most common standard).
- **802.3:** The 802.3 format complies with the RFC 1042 standard.

Section 5.3
I/O Scanning Configuration Parameters

About this Section

This section introduces the configuration parameters linked to I/O scanning.

What Is in This Section?

This section contains the following topics:

Configuration Parameters Linked to I/O Scanning

Parameter Table

The TSX ETY 4103/PORT/5103 modules and the Ethernet link of the TSX P57 6634/5634/4634 have configuration parameters linked to I/O scanning. These are given below.

		TSX ETY 4103/PORT/5103	TSX P57 6634/5634/4634
Parameters			
Master %MW zones	Read Ref.	x	-
	Write Ref.	x	-
	Device Control Block	X	X
	Repetitive rate	0...50000 ms	0...50000 ms
	Master RD ref.	automatic	x
	Slave RD ref.	x	x
	Read Length	x	x
	Input fallback	Fallback to 0/Maintain	Fallback to 0/Maintain
	Master WR ref.	automatic	x
	Slave WR ref.	x	x
	WR Length	x	x
Legend:			
X	Accessible		
-	Not accessible		

Configuring the General Parameters for I/O Scanning

Introduction

For configuring I/O scanning, the read and write zones are general at the remote inputs/outputs:

Master %MW Zones

This sub-window is used to define the ranges of internal words of the application memory (%MW) specific to the read and write zones.

To do this, you must complete:

- for the read zone, **Read Ref.** (the starting address in the table of internal words for reading inputs)
- for the write zone **Write Ref.** (the starting address in the table of internal words for writing outputs)

The length of tables has a maximum exchange capacity of:

- 2 Kwords for the read zone (ETY 4103/ETY 5103/ETY PORT)
- 4 Kwords for the read zone (TSX P57 6634/5634/4634)
- 2 Kwords for the write zone (ETY 4103/ETY5103/ETY PORT)
- 4 Kwords for the write zone (TSX P57 6634/5634/4634)

NOTE: The tables must not overlap and an overrun check is made on global validation.

Configuration of Scanned Peripheral Devices

Introduction

Scanned peripheral devices are configured in a table that is used to:
- list remote devices to be scanned, using the IP address
- specify the time out for each remote device
- specify the scanning period allotted to it for each remote device
- configure, for each device, the amount of space the input and output words take up in the read and write zones
- set the output fallback mode for each device
- add comments for each device

The IP Address and Unit ID Fields

The **IP Address** field is used to list the devices which must be scanned by the Ethernet module.

The **Unit ID** field is used to associate the slave address of the device connected to an Ethernet/Modbus gateway with the IP address:
- values are from 0 to 255
- the default value is 255

Refer to Architecture Supported by a Modbus Communication on the TCP/IP Profile *(see page 81)*.

Health Time Out

The **Health Time out** field is used to set the maximum interval between 2 responses from a remote device, from 1 to 50000 ms. Beyond this time limit, the **Health bit** switches to 0.

Repetitive Rate

The **Repetitive rate** field is used to associate an IP address with its scanning period *(see page 95)*, from 0 to 50000 ms.

Master RD Ref. and Master WR Ref.

These parameters give the addresses of the beginning of each range reserved for the device.

These parameters cannot be accessed. They are calculated automatically as the sum of:
- the address of the beginning of the **Read Ref.** table and the **Write Ref.** table
- the length of the **Read Length** and **Write Length** fields

Example

The Ethernet module scans two devices:
- a Momentum at the address IP1, which has 4 input words
- a Momentum at the address IP2, which has one input word

Furthermore, the read field address starts at %MW100.

In this case, **master RD ref.** for the address IP1 equals 100. The internal word range reserved for the address IP1 starts at %MW100 and is made up of 4 words.

Therefore, **master RD ref.** for the address IP2 equals 104. The internal word range reserved for the address IP2 starts at %MW104 (=%MW100 + 4 input words).

Slave RD Ref. and Slave WR Ref.

These fields correspond to the indices of the first word to be read and written for remote devices to be scanned.
- **slave RD ref.**: specifies the address of the first word to be read
- **slave WR ref.**: specifies the address of the first word to be written
- **Read Length** and **Write Length**

Input Fallback

This field is used to configure the behavior of inputs in the event of an access error in relation to the remote device (example: cut-off of the device, etc.):
- fallback to 0
- maintain

Description

This field is not used by the module. It is only used to locate the device in the configuration more easily.

It has a maximum size of 32 characters.

I/O Scanner Concepts

Introduction

An I/O Scanner resides in the TSX ETY 4103/5103 Ethernet modules and in the TSX P57 6634/5634/4634 CPUs. It transfers data between network devices and allows a CPU to regularly read data from and write data to scanned devices. The I/O Scanner needs to be configured with Control Expert.

I/O Scan List

An I/O scan list is a configuration table that identifies the targets with which repetitive communication is authorized. While the CPU is running, the Ethernet module transfers data to and from the CPU's registers as dictated by the I/O scan list.

I/O Scanner Parameters

Parameter	Value
Max. Number of Devices	64: TSX ETY 4103/5103
	64: TSX P57 1634/2634/3634 (ETY PORT)
	128: TSX P57 6634/5634/4634 CPUs
Max. Number of Input Words	4096 for TSX P57 6634/5634/4634 CPUs
	2048 for ETY modules and ETY port CPUs
Max. Number of Output Words	4096 for TSX P57 6634/5634/4634 CPUs
	2048 for ETY modules and ETY port CPUs
Health Timeout Value	User configurable (from 1...50000 ms) **Note:** The healthbits for Premium modules and CPUs are located in the IODDTs.
Last Value (Input)	User configurable (go to 0 or hold last value)
IP Address	User configurable IP address of scanned device (Slave IP)
Local and Remote Register Reference	User configurable
Repetitive Rate	User configurable
Unit ID	User configurable—only when you are using a bridge
Operation through a bridge	Modbus bridge supported
	Modbus Plus bridge supported

Use the I/O Scanner configuration dialog *(see page 163)* in Control Expert to set the scanner's operating parameters.

Using the I/O Scanner across a Network Router

The I/O Scanner can scan devices through an IP router with a TTL of 32.

Device Control Block

The device control block is a block of registers that supports either 8 words or 4 double words. The content of the registers is mapped in the CPU's memory. Each bit corresponds to an entry in the table.

Each I/O Scanner device can be disabled. To disable an individual scanner device:

Step	Action
1	Select the Device Control Block option in the I/O Scanner configuration dialog *(see page 163)*.
2	Put a check mark in the box.
3	Set the associated bit to 1. For example, %MD2:4

NOTE: A value of 0 in the device control block bit enables the device. A value of 1 in the device control block bit disables the device.

This table shows how the device control block bits are mapped to I/O Scanner entries:

Word																	
1	Table Entry #	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
	Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
2	Table Entry #	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
	Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
		Word 3 through Word 7															
8	Table Entry #	128	127	126	125	124	123	122	121	120	119	118	117	116	115	114	113
	Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Premium I/O Scanner Configuration

Introduction

Use the **I/O Scanner** to transfer data between master and slave devices.

NOTE: The **I/O Scanner** does not work if you enable the device control block with outdated versions of the firmware or software.

If you enable the device control block, you must have Unity Pro V2.0 or later and:

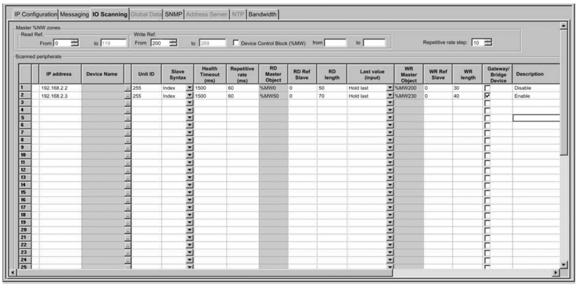
If you are using:	they must be at:
TSX ETY 4103 or -5103 Ethernet communications modules	version 3.1 or later
TSX P57 1634, -2634 or -3634 ETY ports	version 3.1 or later
TSX P57 4634, -5634 or -6634 CPUs	version 2.0 or later

I/O Scanner Configuration Dialog

Click the **I/O Scanner** tab on the Network Configuration screen to display the I/O Scanner configuration dialog. Set the desired configuration parameters by entering data in the appropriate fields.

I/O Scanner for an ETY Module

Illustration of an **I/O Scanner** screen for an ETY module:

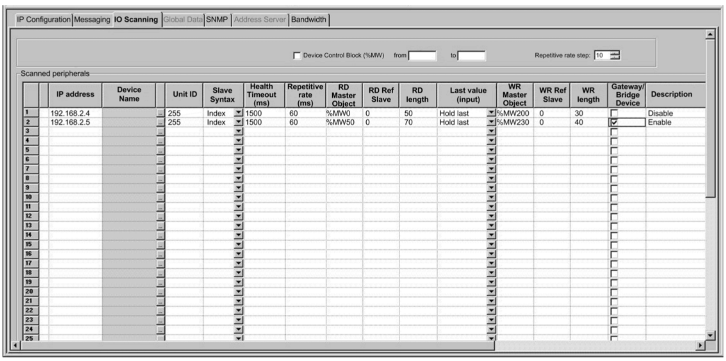


Master %MW zone parameters found only on the **ETY module** screen:

Parameter	Field	Description
Read Ref.	**From** and **to** data boxes	The values in these boxes define the range of destination address values in the CPU for the data read from each device. The addresses you enter here are displayed in the **RD Master Object** column of the dialog. In the example above, the **Read Ref.** values range from 0 to 599; notice that these values are displayed as %MW0, %MW599, etc. in the **Master Object** column.
Write Ref.	**From** and **to** data boxes	The values in these boxes define the range of source address values in the CPU. The address you enter here is displayed in the **WR Master Object** column. In the example above, values starting at %MW2000 are shown in the **WR Master Object** column.

I/O Scanner for a TSX P57 4634, TSX P57 5634 or TSX P57 6634 CPU

Illustration of an **I/O Scanner** screen for a CPU:



Common I/O Scanner Parameters above I/O Scanner Table

These parameters are common to both an ETY module and a CPU:

Parameter	Field	Description
Device Control Block	check box	If this box is checked, the device control block is enabled and the master can send requests to a slave. If the box is not checked, the device control block functionality is disabled and all I/O scanner table entries are active at all times.
	From and **to** data boxes	If a **Device Control Block** bit is disabled, the I/O scanner closes the connection and sets the health bit to an unhealthy state (bit value = 1).
Repetitive Rate Step	data box	The **Repetitive Rate Step** is set in multiples of 5 ms (the minimum) through 200 ms (the maximum). The **Repetitive Rate** column is where you enter a rate of time for how often you want the I/O scanner to send a query to the device after the rate has timed out. **NOTE:** The **Repetitive Rate** of the I/O scanner table is a multiple of the rate displayed in the **Repetitive Rate Step**. The real repetitive rate being executed by the I/O scanner service is shown in the **Repetitive Rate** column. **NOTE: Note:** An entry in the **Repetitive Rate** column is rounded up to the next multiple that was entered in the **Repetitive Rate Step** box if the entry is not a multiple of the **Repetitive Rate Step**. For example, if the entry in the **Repetitive Rate Step** is 5 and you enter a 7 in the **Repetitive Rate** column, the 7 is rounded up to 10; if you change the **Repetitive Rate Step** to 6 and enter a 7 in the **Repetitive Rate** column, the 7 is rounded up to 12.

NOTE: For more information, refer to the Contextual Menu for Copy/Cut/Paste topic *(see page 169)*.

NOTE: For more information, refer to the I/O Scanning with Multiple Lines topic *(see page 171)*.

Common I/O Scanner Table Parameters

These parameters are common to both an ETY module and a CPU:

Parameter	Description	Examples
Entry #	This is the first column; it has no name. Valid range: 1 ... 128 Each entry represents an I/O Scanning exchange on the network.	
IP Address	This is the IP address of the scanned Ethernet slave device.	192.168.1.100
Device Name	To configure a device (Advantys island or DTM), click the **...** button to open the **Property** box *(see page 183)* to start the device configuration software. For an introduction to this procedure for Advantys, go here *(see page 173)*. For an introduction to this procedure for DTMs, go to FDT Container *(see page 177)*. **NOTE:** While the **Property** box is open, **I/O scanning** cannot be edited.	MySTB1 or Master_PRM_DTM_10
Unit ID	This field associates the slave address of the device connected to an Ethernet/Modbus gateway with the IP address of that gateway: ● Value range: 1 to 255 ● Default value: 255 When using a bridge, enter the bridge index (1 to 255) in this field.	255
Slave Syntax	Use this drop-down menu to pick the way **RD Ref Slave** and **WR Ref Slave** values are displayed. The 4 choices are (with an example): ● Index: 100 ● Modbus: 400101 ● IEC 0: %MW100 ● IEC 1: %MW101	Index (default value)
Health Timeout (ms)	This field sets the maximum interval between the responses from a remote device. After this time period expires, the received data is invalid. The **Health Timeout** must be longer than the **Repetitive Rate** time (ms). For a Premium ETY Ethernet module, it must be longer than the CPU scan time. For the **Health Timeout**: ● Range: 1 ms to 50 seconds ● Interval: 1 ms	1500 ms

Parameter	Description	Examples
Repetitive rate (ms)	The rate at which data is scanned, from 0...50000 in multiples of the : ● If you are running Unity Pro V3.1 or earlier with the following firmware versions: ❍ ETY 4103/5103/Port (V4.0 or earlier): 10 ms ❍ TSX P57 4634/5634/6634 (V2.5 or earlier): 10 ms ● If you are running Unity Pro V4.0 or later with the following firmware versions: ❍ ETY 4103/5103/Port (V4.1 or later): 5 - 200 ms ❍ TSX P57 4634/5634/6634 (V2.6 or later): 5- 200 ms	60 ms (with a **Repetitive Rate Step** of 10 ms)
RD Master Object*	Destination address in the master PLC where, from each device, newly read information is stored	%mw10
RD Slave Ref.**	Source address index in the slave/remote device	The format of this value depends on the **Slave Syntax**: ● Index: 5 ● Modbus: 400006 ● IEC 0: %MW5 ● IEC 1: %MW6
RD length	Number of words to read	10
Last value (Input)	This field configures the behavior of inputs in the event of an access error in relation to the remote device (for example: inoperative network or device power supply, etc.): ● Set to 0: fall back to 0 ● Hold last: maintain last value	Hold last
WR Master Object*	Source address of the master PLC whose data is being written into the slave/remote device. Write operations are always performed at the word level.	%mw20
WR Slave Ref.**	The address of the first word written into the slave/remote device.	The format of this value depends on the **Slave Syntax**: ● Index: 1 ● Modbus: 400002 ● IEC 0: %MW1 ● IEC 1: %MW2
WR length	Number of words to be written	10

Parameter	Description	Examples
Gate-way/Bridge Device	To allow slower TCP/IP network devices (i.e., gateways and bridges) to be compatible with the I/O Scanner: ● Select the check box to enable this feature. Defines a new bit, and sets it to high (1). ● Deselect the check box to disable this feature (default). Defines a new bit, and sets it to zero (0).	Values: ● **Disable**: deselected check box ● **Enable**: selected check box
Description	Additional information	
*Master refers to the client PLC that makes the request. **Slave refers to the server from which data is read or to which data is written.		

I/O Scanning Contextual Menu for Copy/Cut/Paste

At a Glance

A right-click on a line in the **I/O Scanning** table opens the **I/O Scanning Contextual Menu**. Use this menu to perform common operations on the lines of the **I/O Scanning** table, such as, delete a device, copy & paste, cut & paste, insert a new line, etc.

Contextual Menu

The following illustration is the **I/O Scanning** contextual menu:

The following table describes the menu functions:

Menu Item	Description
Delete Device	For an ACS or PRA configuration, **Delete Device** permanently deletes the **Device Name** and all its data (and associated ACS symbols). For a **PRM Master DTM**, its link to the **I/O Scanning** table is deleted, **NOTE:** Deleting a **PRM Master DTM** link from the **I/O Scanning** table does not delete the corresponding DTM from the connectivity tree in the DTM Browser.
Cut line(s)	**Cut line(s)** copies and deletes the selected I/O Scanning lines. The lines are copied without the **Device Name** information. For an ACS or PRA configuration, it permanently deletes the **Device Name** and all its data (and associated ACS symbols). For a **PRM Master DTM**, the link between the DTM and the **I/O Scanning** line is removed.
Copy line(s)	**Copy line(s)** copies the selected lines, but without the **Device Name**.
Paste line(s)	**Paste line(s)** has 2 actions depending on its target line: ● If the line is empty, it fills the line with the copied line (without a **Device Name)** ● If the line is not empty, it replaces the line with the copied line (without a **Device Name**). Be careful, it also permanently deletes the **Device Name** link to the **I/O Scanning** table and, for an ACS or PRA configuration, all its data (and associated ACS symbols) of the old line before replacing it with the copied line.

Menu Item	Description
Insert copied line(s)	**Insert copied line(s**) inserts the copied line between the selected line and the line just above it. Be careful with ACS or DTM configurations, all the lines below the inserted line become desynchronized. To synchronize these lines, open and close the device configuration tool, then do an **Update** from the Property box *(see page 183)*.
Insert empty line	**Insert empty line** inserts an empty line above the line selected line. Inserting an empty line does not desynchronize the devices below the line, but using this line for a new device can, depending the number of words needed, desynchronize the devices below the line.
Pack all lines	**Pack all lines** removes any empty lines between the top of the **I/O Scanning** table and the last non-empty of the table.

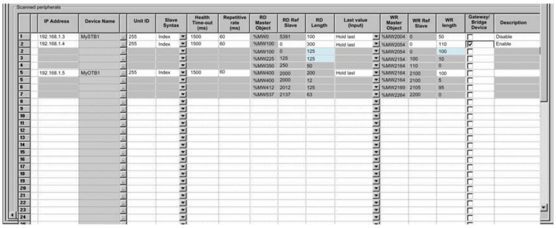
I/O Scanning with Multiple Lines

At a Glance

Modbus exchanges are limited to a maximum of 125 input words and 100 output words. If an application needs to exchange more than these limits for a device, more than one **I/O Scanning** line can be used: multiple lines for one device.

When the length is higher than the authorized limit for one Modbus exchange, the length is divided into 2 or more Modbus exchanges. New lines are created for each Modbus exchanges with the PLC.

The following **I/O Scanning** table is used for the multiple device lines example:



Scanned peripherals

	IP Address	Device Name	Unit ID	Slave Syntax	Health Time-out (ms)	Repetitive rate (ms)	RD Master Object	RD Ref Slave	RD Length	Last value (Input)	WR Master Object	WR Ref Slave	WR length	Gateway/ Bridge Device	Description
1	192.168.1.3	MySTB1	255	Index	1500	60	%MW0	5391	100	Hold last	%MW2004	0	50		Disable
2	192.168.1.4		255	Index	1500	60	%MW100	0	300	Hold last	%MW2054	0	110	✓	Enable
2							%MW100	0	125		%MW2054	0	100		
3							%MW225	125	125		%MW2154	100	10		
4							%MW350	250	50		%MW2164	110	0		
5	192.168.1.5	MyOTB1	255	Index	1500	60	%MW400	2000	200	Hold last	%MW2164	2100	100		
5							%MW400	2000	12		%MW2164	2100	5		
6							%MW412	2012	125		%MW2169	2105	95		
7							%MW537	2137	63		%MW2264	2200	0		
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															

NOTE: This example shows an Advantys island, but DTM and PRA devices work the same way.

Multiple Line Length Configuration Example

In this example, the *first* (the main) **I/O Scanning** line 2 contains all the information for the exchanges with the device including the totals for the **RD length** and **WR length**.

The *second* line 2 contains the specific word lengths (125 and 100) needed so that it can also be used for part of the exchanges.

Line 2 needs a **RD length** of 300 word and a **WR length** of 110 words. How many extra lines are needed?

- **RD length** = 300/125 = 2.72 = 3 lines needed
- **WR length** = 110/100 = 1.10 = 2 lines needed

The larger of the 2 numbers is used:

- Three lines are needed to accommodate the **RD length**: 125 words, 125 words, 50 words for a total of 300 words
- The 3 lines for the **WR length** are: 100 words, 10 words, 0 words for a total of 110 words

The *second* line 2, line 3, and line 4 correspond to the Modbus exchange queries.

When multiple lines are used, only the **RD length** and **WR length** columns of these new lines can be edited. In the case of Advantys or DTM, the software supplies the **RD length** and the **WR length**, and they cannot be changed in the **I/O Scanning** table.

NOTE: It is not necessary to have a **Device Name** defined to use multiple lines.

The total number of words allowed in an **I/O Scanning** table is:
- 4 KW for Premium extended and Quantum networks
- 2 KW for Premium ETY and M340 NOE modules

Line Length for Multiple Word Variables

When using variables with 2 or more words, adjust the **RD** and **WR lengths** so that a variable is not partly on one **I/O Scanning** line and partly on the next. Because the 2 newly created lines result in 2 independent Modbus exchanges that can be sent non-synchronized to the device. The variables can receive the wrong values (if the 2 parts are received at different times). It may be necessary to use a **RD length** < 125 and a **WR length** < 100 for some of the scanned lines, in order to get each variable on only one exchange line.

WARNING

UNEXPECTED SYSTEM BEHAVIOR

Verify that multiple word variables are completely on the same **I/O Scanning** line to avoid sending parts of a variable data in 2 non-synchronized **I/O Scanning** Modbus exchanges.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Introduction to Configuring Advantys from Control Expert

At a Glance

The Advantys Configuration Software (ACS) is integrated in Control Expert. This allows you to configure Advantys STB and OTB islands from the Control Expert **Ethernet I/O scanning** tab.

Configuring an Advantys Island

⚠ WARNING

UNEXPECTED SYSTEM BEHAVIOR

Always launch ACS from Control Expert in order to synchronize variables and data between Control Expert and ACS.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ WARNING

UNEXPECTED SYSTEM BEHAVIOR

Stop the PLC before transferring an ACS configuration and/or I/O scanning modifications.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The following procedure configures an Advantys STB or OTB island:

Step	Action	Results
1	Open the Ethernet network configuration screen.	
2	In the **Module Utilities** zone select **YES** for **IO Scanning**.	
3	Select the **I/O Scanning** tab.	**I/O Scanning** screen opens.
4	Enter, on a free line, the IP address for the connection you want to use to communicate with the Advantys island.	
5	Enter **RD length** and **WR length** on the same line. The lengths must be long enough for the expected Advantys configuration.	
6	Validate the **I/O Scanning** screen.	
7	Click on the **...** button (that is next to **Device Name** cell on the same line).	The **Property** box *(see page 183)* opens.
8	Select **STB** or **OTB** in the **Device Type** drop-down menu.	
9	Enter a **Device Name** (following the naming rules *(see page 186)*).	

<table>
<tr><th>Step</th><th>Action</th><th>Results</th></tr>
<tr><td>10</td><td>You have 2 choices:
1. If you want to go to ACS now to configure an island, click on the Launch Advantys Configuration Software button.
Click on Yes in the “Confirm device name and type” Message Box and go to Step 11.

2. If you want to configure the Advantys island later, click on the OK button.
Click on Yes in the “Confirm device name and type” Message Box.
To open the ACS later:
❍ Carry out Step 7.
❍ Click on the Launch Advantys Configuration Software button.</td><td>Results for both 1. and 2. are:
● A Control Expert message box opens: “The device name and device type won’t be modifiable. Do you want to confirm the device name and device type?”
● The Device Type and Device Name are verified and saved.
● The Property box closes.</td></tr>
<tr><td>11</td><td>After ACS opens, configure your Advantys island.

NOTE: While the ACS is open Ethernet screen is locked and cannot be edited, but the other Control Expert services can be edited.

NOTE: The <code>User Defined Label</code> must be filled in the <code>IO image</code>. If not, the Advantys varialble will no be added in the Control Expert Data Editor.</td><td></td></tr>
<tr><td>12</td><td>When your Advantys island has been built and validated, close ACS.</td><td>A Control Expert message box opens “Do you want to update your symbols now?”</td></tr>
<tr><td>13</td><td>You have 2 choices:
1. Click on Yes in the “update” Message Box and go to Step 14.

2. Click on No in the “update” Message Box.
You are returned to the I/O Scanning screen without carrying out the Yes results.
Later, when you want to update the Advantys symbols into Control Expert:
❍ Carry out Step 7
❍ In the Property box, click on the Update button and go to Step 14.</td><td>If you clicked on No:
● You are returned to I/O Scanning without carrying out the results in Step 14.
● The Device Name is displayed in the I/O Scanning in red. This indicates that the island configuration has not been synchronized with Control Expert.</td></tr>
</table>

Step	Action	Results
14	Your Advantys island configuration is being **synchronized** with Control Expert. After the synchronization is finished, you are returned to **I/O Scanning**. Verify that the **Device Name** is now displayed in black.	The results are: • The Advantys island modifications are synchronized with the Control Expert application. • The Advantys island symbols are imported into the Control Expert Data Editor. • The Advantys **Device Name** is displayed in the **I/O Scanning** in black. This indicates that the island configuration is synchronized.
15	Build your Control Expert application.	
16	STOP the PLC.	
17	Transfer: • Control Expert application to the PLC • STB or OTB configuration to the Advantys island using ACS	
18	RUN your application in the PLC.	

Copy an Existing Island

This following procedure copies an existing Advantys island file (*.isl) into a new Advantys island configuration:

Step	Action
1	From Control Expert, open a new Advantys island in ACS.
2	In ACS, select **File menu** → **Copy Island Contents**.
3	In the **Open island** window, select the island file (*.isl) to copy.
4	Click on **Yes** in the “Do you want to proceed?” message box.
5	The message “Island file has been saved.” in the **Log Window** verifies that the operation was successful.

Copy an Island File to a New Location

The following procedure copies an Advantys island file (*.isl) to a new directory:

Step	Action
1	In ACS, open an island configuration, for example, STB1.
2	Select **File** menu **=> Copy STB1 Contents**
3	In the **Copy STB1.isl to** window, select the target directory.
4	The message “A copy of the island file has been saved with another name.” includes in the **Log Window** verifies that the operation was successful. The name is new because its path has changed.

Introduction to Configuring the PRM Master DTM

At a Glance

The **PRM Bus Master** uses the Control Expert **I/O Scanner** to communicate with the CPU through an Ethernet port. This requires configuring the **PRM Master DTM** in the Control Expert Ethernet **I/O Scanning** tab.

Configuring a PRM Master DTM

The following procedure configures a **PRM Master DTM** in the **I/O Scanner**:

Step	Action
1	Install the **PRM Master DTM** on the Host PC. **NOTE:** After installing new DTMs, the **Hardware Catalog** must be updated.
2	Add a **PRM Master DTM** to the connectivity tree in the DTM Browser using the contextual **Device menu** service.
3	In the DTM Browser, select the **PRM Master** and use the contextual **Device menu** function to open the DTM **PRM Offline Parameter** screen.
4	In the **General Setting** part of this screen set the IP address of the **PRM device.**
5	Open the **I/O Scanning** configuration editor (tab).
6	In the **Module Utilities** zone select **YES** for **IO Scanning**.
7	Select the **I/O Scanning** tab. **Results: I/O Scanning** configuration editor opens.
8	Enter, on a free line, the IP address for the connection to be used to communicate with the **PRM Bus Master**.
9	Set correct values for the **Read Ref.** and **Write Ref.** parameters.
10	Enter **RD length** and **WR length** for the IP address line (within the **Read Ref.** and **Write Ref.** constraints). **NOTE:** The lengths must be long enough for the expected configuration **PRM Master DTM** and its subnode DTMs.
11	Validate the **I/O Scanning** screen.
12	Click on the **...** button (next to **Device Name** cell). Results: The **Property** box *(see page 183)* opens.
13	Select **DTM** in the **Device Type** drop-down menu.
14	Select the protocol in the **DTM Protocol** drop-down menu.
15	Select a **PRM Master DTM** in the **DTM Name** drop-down menu.
16	Click on **OK** to validate the choices you made. **Results:** ● The **Device Type**, **Device Protocol** and **Device Name** are verified and saved. ● The **Property** box closes.

Step	Action
17	Update the **I/O Scanning** line, refer to Updating I/O Scanning for a PRM Master DTM *(see page 178)*.
18	Build the Control Expert application.
19	Stop the PLC.
20	Transfer the Control Expert application to the PLC.
21	In the DTM Browser, right click on **PRM Master** and select the **Connect** function.
22	In the DTM Browser, right click on **PRM Master** and select the **Store data to device** function.
23	**Run** the application in the PLC.

Updating I/O Scanning for a PRM Master DTM

The following procedure updates the **I/O Scanning** information for a **PRM Master DTM**:

Step	Action
1	Configure and validate the **PRM Bus Masters** in the DTM Browser using the contextual **Device menu** function.
2	Open the **I/O Scanning** configuration editor (tab).
3	Click on the **...** button (that is next to the **Device Name** of the **PRM Master DTM** to update).
4	In the open **Property** box *(see page 183)*, click on the **Update** button. **Results:** ● The **PRM Master DTM** modifications are synchronized with the Control Expert application. ● The **PRM Master DTM** symbols are imported into the Control Expert Data editor. ● The **DTM Name** is displayed in the **I/O Scanning** configuration tab in black. This indicates that the PRM configuration is synchronized. ● The **Property** box closes.

Introduction to Configuring a BMX PRA 0100 from Control Expert

At a Glance

Control Expert allows configuration of BMX PRA 0100 modules through the Ethernet **I/O scanning** tab. The PRA device configuration is done in a **second** instance of Control Expert.

Configuring a PRA

The following procedure configures a PRA device:

Step	Action	Results
1	Open the Ethernet network configuration screen.	
2	In the **Module Utilities** zone select **YES** for **IO Scanning**.	
3	Select the **I/O Scanning** tab.	**I/O Scanning** screen opens.
4	Enter, on a free line, the IP address for the connection you want to use to communicate with the **PRA**. **NOTE:** The IP address in the **I/O Scanning** table must be the same as the IP address of the **PRA** device.	
5	Enter **RD length** and **WR length** on the same line.	
6	Validate the **I/O Scanning** screen.	
7	Click on the **...** button (that is next to **Device Name** cell on the same line).	The **Property** box *(see page 183)* opens.
8	Select **PRA** in the **Device Type** drop-down menu.	
9	Enter a **Device Name** (following the naming rules *(see page 186)*).	

<table>
<tr><th>Step</th><th>Action</th><th>Results</th></tr>
<tr><td>10</td><td>You have 2 choices:
1. If you want to now configure a PRA, click on the Launch PRA button.
Click on Yes in the “Confirm device name and type” Message Box and go to Step 11.

2. If you want to configure a PRA later, click on the OK button.
Click on Yes in the “Confirm device name and type” Message Box.
NOTE: The Device Name becomes red in the I/O Scanning table. This indicates that a PRA has not been configured for the table line that contains the Device Name

To configure a PRA later:
❍ Carry out Step 7.
❍ Click on the Launch PRA button.

NOTE: While the second PRA instance of Control Expert is running no changes can be made to the Ethernet Editor in the first (master) instance of Control Expert.</td><td>Results for both 1. and 2. are:
● A Control Expert message box opens: “The device name and device type won’t be modifiable. Do you want to confirm the device name and device type?”
● The Device Type and Device Name are verified and saved.
● The Property box closes.</td></tr>
<tr><td>11</td><td>After the second instance of Control Expert opens:
● File menu → Open
● Change the file type to .XEF
● Open the PRA application template, PRA_Template.XEF</td><td></td></tr>
</table>

Step	Action	Results
12	When your PRA application is configured: ● If desired, you can build the **PRA** application now. ● Save the application. **NOTE:** The **Save As** function is not available. To copy your PRA application use the Export or Save Archive function. ● Close this instance of Control Expert. **NOTE:** You are asked if you want to save the PRA application in the master application *.stu file. If you select **No**, all changes are lost. **NOTE:** Later you can build your **PRA** application by carrying out Step 7. Because the **PRA** application is saved (embedded) in the master application *.stu file, it is opened. You can then build the **PRA** application. **NOTE:** If there is no **PRA** application in the master *.stu, an empty application is opened (as happens the first time the **Launch PRA** button is used in the **Property** box)	
13	Build your Control Expert application.	
14	STOP the PLC.	
15	Transfer: ● Control Expert application to the PLC ● **PRA** configuration to the PRA device **NOTE:** There are no imported variables, the user must ensure the synchronization of the data exchange.	
16	RUN your application in the PLC.	

NOTE: When the second (**PRA**) instance of Control Expert is closed, there is no indication if the **PRA** application has been built or not.

Copy an Existing PRA Application

This following procedure copies an existing **PRA** application:

Step	Action
1	From the Control Expert **I/O Scanning** table using the **...** button, open an existing **PRA** application.
2	In the second Control Expert instance, save the existing **PRA** application with a new name as a *.sta or .xef file.
3	Close this second Control Expert instance.
4	In the Control Expert **I/O Scanning** table create a new **PRA** application on a new line.
5	Import or Open the *.xef or *.sta file previously saved.
6	If desired, build the new **PRA** application and transfer it to the **PRA** device.
7	Close the second Control Expert instance.

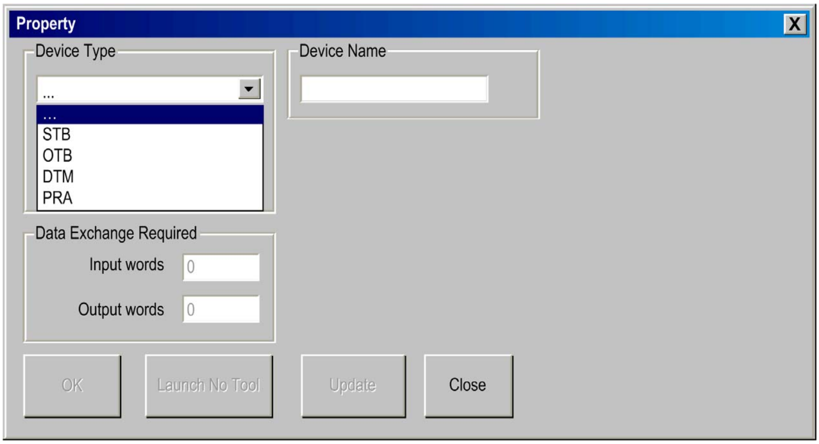
Property Box

At Glance

The **Property** box is the link between Control Expert and a device configuration tool. It is used to select and name a device and to launch the configuration tool for the device.

Property Box

The following illustration is the **Property** box before selecting the **Device Type**.

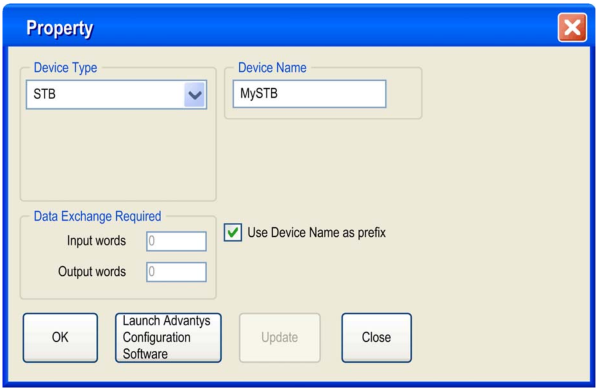


For details on how top use the **Property** box, refer to:
- Advantys *(see page 184)*
- DTM *(see page 187)*
- BMX PRA 0100 *(see page 185)*

Property Box for Advantys

This **Property** box allows you to choose the name and type of Advantys island to be configured using the Advantys Configuration Software (ACS).

The following illustration is the **Property** box for Advantys *after* **Device Type** and **Device Name** entered:



Property Box for Advantys Elements

The elements of the Advantys **Property** box are:

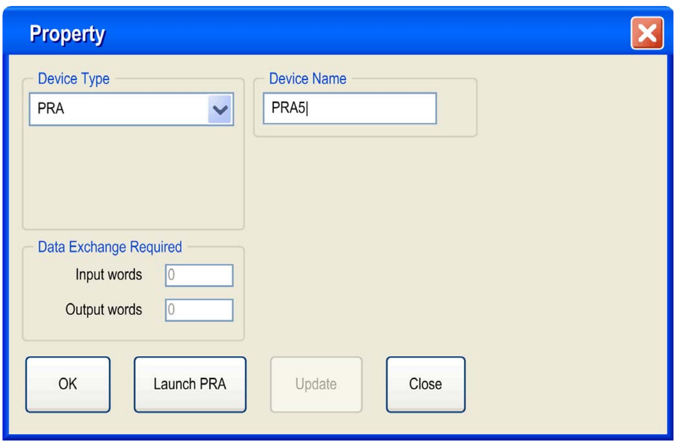
Element	Description
Device Type	Selection of a STB or OTB device is made from this drop-down list. After the first validation (using the **OK** or **Launch Advantys** button) the **Device Type** cannot be changed.
Device Name	The **Device Name** *(see page 186)* is used as a prefix to all variables created for an Advantys island in ACS. This allows unique variables for duplicated islands. After validation (using the **OK** or **Launch Advantys** button) the **Device Name** cannot be changed.
Data Exchange Required	These are the minimum number of words necessary for communication between the Control Expert module and the Advantys island. These values cannot be changed via the **Property** box. **NOTE:** Increasing the RD/WR lengths via the **I/O Scanning** tab leaves enough data exchange words for the future expansion of your Advantys island. Expanding an island that does not use the last line in the **I/O Scanning** table requires changing the values for all the lines below the line that needs the additional exchange words.
Use Device Name as prefix	If this checkbox is unchecked, the user is in charge of giving unique names to the variables and symbols in **all** Advantys islands. This checkbox is only available for ASC V5.5 or higher. For versions less than 5.5 the Device Name is automatically added to all variables and symbols in all Advantys islands.

Element	Description
OK	This button is only available after entering the **Device Type** and **Device Name**. When clicked, the **Device Type** and **Device Name** are checked to see if they are valid. If there is a problem, a message box opens explaining the why they were not valid. **OK** is only available during the first use of the **Property** box for a new island.
Launch Advantys Configuration Software	This button is only available if both: ● The **Device Type** and **Device Name** have been entered ● ACS is installed This button does two things: ● It carries out the action of the **OK** button ● If there is no problem during validation, it launches ACS
Update	When clicked, the ACS modifications are synchronized with your Control Expert application (after these modifications have been validated in ACS). It also imports and updates all ACS symbols and variables into the Control Expert variable manager. **NOTE:** All variables modified in ACS are deleted and rewritten in the Control Expert Data Editor. But they are not updated in the program.
Close	This button closes the **Property** box without saving anything.

Property Box for BMX PRA 0100

This **Property** box allows you to choose the name for the PRA module to be configured.

The following illustration is the **Property** box for the PRA *after* **Device Name** validation:



Property Box for PRA Elements

The elements of the PRA **Property** box are:

Element	Description
Device Type	Selection of the PRA device is made from this drop-down list. After the first validation (using the **OK** or **Launch PRA** button) the **Device Type** cannot be changed.
Device Name	The **Device Name** *(see page 186)* is the name of PRA application.
Data Exchange Required	This is not used when configuring a PRA device.
OK	This button is only available after entering the **Device Type** and **Device Name**. When clicked, the **Device Type** and **Device Name** are checked to see if they are valid. If there is a problem, a message box opens explaining why they are not valid. **OK** is only available during the first use of the **Property** box for a new PRA configuration.
Launch PRA	This button is only available if the **Device Type** and **Device Name** has been entered. This button does two things: ● It carries out the action of the **OK** button ● If there is no problem during validation, it launches another instance of Control Expert, which is used to do the actual configuration of the PRA.
Close	This button closes the **Property** box without saving anything.

Valid Name

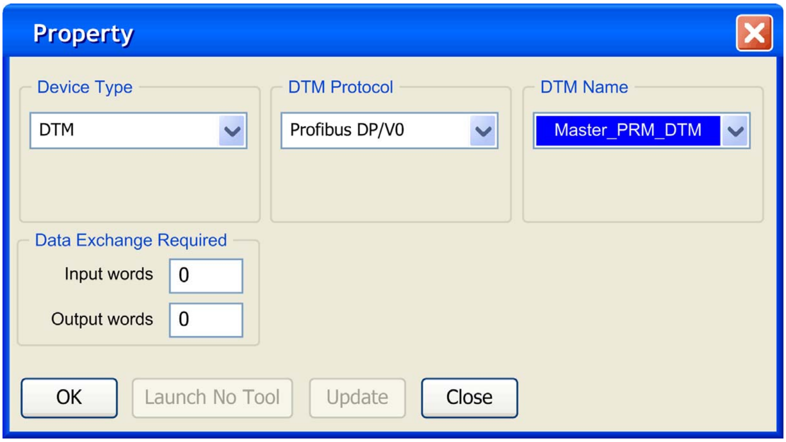
A valid **Device Name** for a configuration:

- Does not already exist in the application
- Is not a empty name
- Starts with a letter
- Has a maximum of 8 characters
- Only ASCII characters, not Unicode characters
- Has no spaces
- Follows the Windows file naming conventions: no slashes, question marks, etc.
- Follows Control Expert variable naming conventions

Property Box for a PRM Master DTM

This **Property** box allows you to choose the type and protocol for a **PRM Master DTM**:

The following illustration is the **Property** box *after* selecting the **Device Type**, **DTM Protocol** and **DTM Name**:



Property Box PRM Master DTM Elements

The elements of the DTM **Property** box are:

Element	Description
Device Type	Selection of DTM device type is made from this drop-down list.
DTM Protocol	Select the protocol to be used from this drop-down list. This list contains the DTM protocols of all the DTMs in the DTM Browser that can be linked with I/O Scanning.
Device Name	Select a **PRM Master DTM** from this drop-down list.This list uses the DTM Browser Alias names. This list contains all the **PRM Master DTMs** in the DTM Browser that support the selected DTM Protocol. To validate the choices, click on the **OK** button.
Data Exchange Required	These are the minimum number of words necessary for communication between Control Expert and the **PRM Master DTMs**. These values cannot be changed via the **Property** box. **NOTE:** Increasing the RD/WR lengths via the **I/O Scanning** tab leaves enough data exchange words for the future expansion of your DTM topology tree. Expanding a tree that does not use the last line in the **I/O Scanning** table requires changing the values for all the lines below the line that needs the additional exchange words.

Element	Description
OK	The **OK** button is only available after selecting the **Device Type**, **DTM Protocol** and **DTM Name**. When clicked, the **DTM Protocol** and **DTM Name** are checked to see if they are valid. If there is a problem, a message box opens explaining the why they were not valid. The **OK** button is only available during the first use of the **Property** box for a new **PRM Master DTM**.
Launch No Tool	This button is never available for **PRM Master DTMs**.
Update	Use the **Update** button after validating or changing the configuration of the linked **PRM Master DTM**. Refer to Update I/O Scanning for a PRM Master DTM *(see page 178)*.
Close	The **Close** button closes the **Property** box without saving anything.

Saving an Advantys Configuration in an Control Application

At a Glance

ACS saves an island configuration in an *.isl file. To add the island to an application, it is necessary for Control Expert to know the location of the island configuration information.

Saving the Configuration

The recommended way to save your island configuration information is to save your Control Expert application as a *.stu or *.sta file. The *.isl file is automatically included in these files.

Uploading or Importing

There are 2 situations where the information contained in the *.isl file is not available:

1. Uploading the application running in the PLC
2. Importing an *.xef file

In these 2 cases, if ACS is launched from the **Property** box *(see page 183)*, it automatically tries to open the latest **Device Name**.isl file the Control Expert **General Path => Project Path** directory:

- If the same PC is used for the import (upload) and export (download) and the Control Expert **Project Path** has not changed, the island configuration is synchronized with ACS.
- If the same PC is not used for the import (upload) and export (download) or if the Control Expert Project Path has changed, either:
  - Create a new island
  - Use the **File** menu => **Copy Island Contents** function
    NOTE: The new **Device Name**.isl file is copied to the **Project Path** directory.

Managed Variables

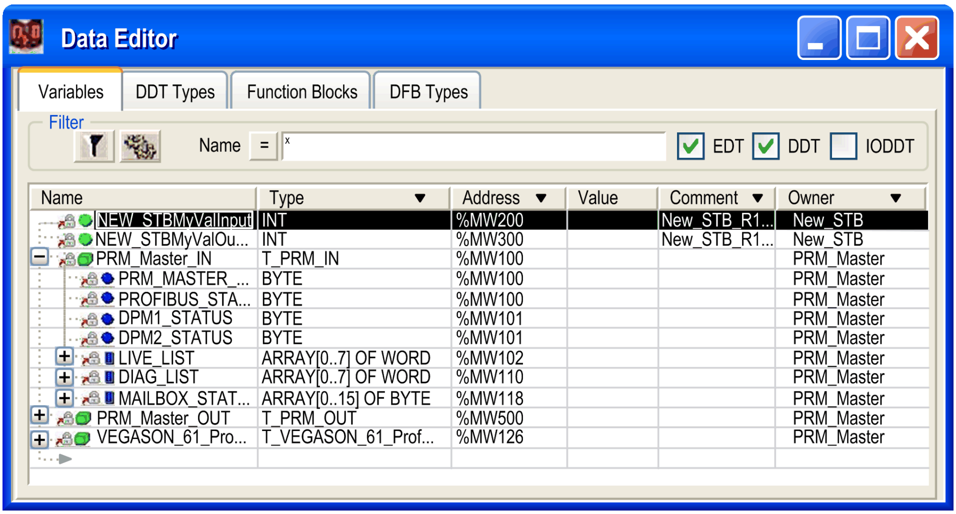
At a Glance

Variables of devices that are linked to Control Expert through **I/O Scanning** or **DTM** are *managed variables*. They are created by the device configuration tool or by the DTM and are imported into Control Expert. They are named as a concatenation of the Property box *(see page 183)* **Device Name** + device symbol name.

Managed Variables in the Data Editor

Advantys symbols become managed variables when imported into Control Expert. An Advantys managed variable name is a concatenation of:
the Advantys island name + Advantys symbol name.

This **Data Editor** illustration shows managed variables with their device name **prefixes** and their **Owner** attributes:



Managed variables follow the usual rules for Control Expert and ACS or DTM naming.

The optional **Owner** column lists the owner attribute of the managed variables. This allows you to filter the variables according to their **Device Name**.

The Control Expert managed variables are locked and cannot be modified through the **Data Editor**. You have to use the device configuration tool (ACS or the DTM) to modify these variables.

Importing Managed Variables from a Device (Advantys, DTM)

Using the **Update** button on the Property box *(see page 183)* imports the device Symbols into the Data Editor as Control Expert managed variables.

In the case of a conflict between an device Symbol and an existing variable in the Data Editor:

- If the Control Expert variable *is not* managed, a message box allows you to replace this variable with the managed variable coming from the ACS- or DTM-controlled device).
- If the Control Expert variable *is already* managed, the update is cancelled.

For an already managed variable, there are 2 options, either:

1. Use the device configuration tool (ACS or the DTM) to rename the variable.
2. Delete the old managed variable using the tool that manages the variable, then use the tool to perform an Update.

After performing one of these options, use the **Update** button again on the device being updated to complete the import without a conflict.

Permanent Deletion of a Managed Variable

Managed variables cannot be deleted directly from the Data Editor.

Removing a managed variable from a configuration must be done from the tool (ACS or the DTM) that manages the device (either delete the device using the DTM or delete the Symbol using the ACS).

NOTE: During an **Update**, all managed variables are deleted and recreated during synchronization between Control Expert and the device.

Partial Import of a Managed Variable

Starting with Unity Pro V5.0, the managed variables become *unmanaged* during a partial import from an .XSY file. This allows deletion of the variables if the linked device is not also imported.

NOTE: Unity Pro is the former name of Control Expert for version 13.1 or earlier.

After importing variables from an .XSY file, an **Update** is needed to resynchronize the managed variables linked to a device. During this **Update**, a conflict box appears to allow validation of the replacement managed variables.

Section 5.4
Address Server Configuration Parameters

About this Section

This section describes the configuration parameters linked to the DHCP address server.

What Is in This Section?

This section contains the following topics:

Configuration Parameters Linked to the Address Server

Introduction

The TSX ETY 4103/PORT/5103 modules and the Ethernet link of the TSX P57 6634/5634/4634 have configuration parameters linked to the address server.

These parameters are given below.

List of Parameters

The following table shows the parameters that can be accessed from the configuration screen and the values that they can have:

Parameters	
HTTP modification	Locked when executing
	Password
Client/server address table	

Configuration of the Address Server

Introduction

Parameters linked to the address server are divided into two categories:
- rights to modify the service via the HTTP server
- the client/server address table

HTTP Modification

This field is used to define the access rights to the address table via the HTTP server.

The access rights are configured by two parameters:
- the **Locked in operation** check box: which activates or deactivates access control to the table
- the **Password** field: the table is accessed via the HTTP server by means of a password of no more than 8 ASCII characters

Address Tables

The address table can be used:
- to list, by the MAC address or by their name (16 ASCII characters), the remote stations that need the DHCP server to start up
- to provide a correspondence between the MAC address or the Name and the IP address of the remote station, the subnetwork mask and the Gateway

Section 5.5
SNMP Configuration Parameters

About this Section

This section introduces the configuration parameters linked to SNMP.

What Is in This Section?

This section contains the following topics:

Configuration Parameters Linked to SNMP

Introduction

The TSX ETY modules or the Ethernet port of the TSX P57 6634/5634/4634 have configuration parameters linked to SNMP.

Depending on the Ethernet channel selected, some configuration parameters cannot be accessed on the configuration screen. They are either not shown on the screen or are grayed out.

Availability of Parameters

The following table shows, for each Ethernet module, the parameters that can be accessed from the configuration screen.

Parameters		TSX ETY 110	TSX ETY 4103/PORT/5103 TSX P57 6634/5634/4634
IP Address Managers		X	X
Agent	Location (SysLocation)	X	X
	Contact (SysContact)	X	X
	SNMP Manager	-	X
Community names	Set	X	X
	Get	X	X
	Trap	X	X
Security	Enable "Authentication Failure" trap	X	X
Legend:			
X	Accessible		
-	Not accessible		

SNMP Configuration Parameters

Introduction

Parameters on the SNMP configuration tab *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)* are divided into four categories:

- the IP addresses of SNMP manager devices
- SNMP agents
- the community names
- security

NOTE: Only 7-bit ASCII characters can be used in the character string entry fields.

IP Address Managers

This zone allows you to complete the IP addresses of the SNMP managers. The modules authorize a maximum of two managers.

These addresses are used during possible transmission of events (TRAP). The transmission of supervised data is detailed at the topic SNMP *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Agent

This zone allows the localization and identification of an agent from the SNMP manager.

It comprises two fields:

- The **Location (SysLocation)** field: indicates the physical location of the device (32 characters maximum).
- The **Contact (SysLocation)** field: indicates the person to contact for device management and the method of contact (strings of 32 characters maximum).
- If you prefer to have this information assigned by an SNMP Manager tool for network management, check the **SNMP Manager** box.

Community Name

This zone is used to define community names for the Set, Get and Trap utilities. It comprises three fields:

- The **Set** field defines the community name for the Set utility (strings of 16 characters maximum). The default value of the field is *Public*.
- The **Get** field defines the community name for the Get utility (strings of 16 characters maximum). The default value of the field is *Public*.
- The **Trap** field defines the community name for the Trap utility (strings of 16 characters maximum). The default value of the field is *Public*.

The purpose of these fields is to define the access rights for the MIB objects of the SNMP agent (local module) in relation to requests sent by the manager.

Example: If the manager sends a SetRequest request with the community name *Test* and the module has the community name *Public*, the request is not executed.

Security

⚠ CAUTION
UNEXPECTED NETWORK BEHAVIOR - SNMP PARAMETERS RESET
The SNMP manager is able to modify the value of certain configurable parameters(Enabling "Authentication failure," Location, Contact. etc.).
the **SNMP Manager** box is not checked and there is a cold start, warm restart, or application download, the initially configured values are restored.
Failure to follow these instructions can result in injury or equipment damage.

This zone contains the **Enable "Authentication Failure" trap** check box.

Checking this box allows you to validate the transmission of an authentication failure event (TRAP) from the SNMP agent to the configured manager.

In this way, the agent warns the manager that the request has been refused following an identification error (community name configured in the manager is different from the one configured in the agent).

Section 5.6
Global Data Configuration Parameters

About this Section

This section introduces the configuration parameters linked to Global Data.

What Is in This Section?

This section contains the following topics:

Configuration Parameters Linked to Global Data

Introduction

The TSX ETY4103/PORT/5103 modules and the Ethernet link of the TSX P57 6634/5634/4634 have configuration parameters linked to Global Data:

Parameters	
Global Data configuration	Group address
	Group name
	Distribution Period
	Validity time out
	Multicast Filtering

NOTE: Elsewhere in this guide is detailed information about configuring Global Data General Parameters *(see page 201)*.

Publish/Subscribe Variables

Association between Global Data variables (network variables) and application variables is carried out in the Control Expert variable editor.

Each application variable published or subscribed (**Global Data** field) in a Distribution Group (**Group** field) is link to a Global Data item (network variable).

Each Global Data item has a unique identification (**Data ID**) within a Distribution Group. The rank of the status bit in the HealthBit zone of Global Data corresponds to the identifier (**Data ID**) of the Global Data.

Properties

The following table provides Global Data properties.

Type	Value
Max. number of publications	1
Size of a variable at publication	1 to 512 words
Max. number of subscriptions	64
Maximum variable size at subscription	Total of 2K words

Configuring the General Parameters for Global Data

At a Glance

The following parameters can be entered in the Global Data Configuration zone of the configuration *(see page 302)* screen:

- group address
- group name
- distribution period
- health time out
- multicast filtering

Group Address

This zone is used to enter the multicast IP address (class D) for the group to which the station belongs. The value 239.255.255.255 is the default value.

Group Name

This field is used to fill in the group name associating a variable from the variable editor with a module.

Distribution Period

This zone is used to select the distribution period of the publication. The publication is synchronized with the PLC master task. The publication period can be configured from 1 scan to 50 scans.

Health Time Out

This zone is used to adjust the health "time-out" value.

An associated status bit (%IW zone) is linked to each Global Data item and is used to monitor whether the data has been published and received by the end of the time indicated in this window. If yes, the value is 1, otherwise the bit is set to 0.

Multicast Filtering

The multicast filtering drop down list allows you select the following:

- None: disable both GMRP & IGMP
  (Data will be sent to all end devices in the network.)
- GMRP
  Make sure your client, server and switches, and routers support and endable GMRP.
- IGMP V1
  Make sure your client, server and switches, and routers support and endable IGMP.

Note: The following modules support IGMP V1:

- TSX ETY 4103/5103 V4.3 or later
- TSX ETY PORT (TSX P57 1634/2634/3634): V4.3 or later
- TSX P57 4634/5634/6634 V2.8 or later

This function is used to reduce data flow on large networks.

Configuration of the Variables Table

At a Glance

The Global Data variables table is configured in the Control Expert data editor.

Three fields are specifically used for Global Data:
- Global Data
- group
- data ID

Global Data Field

This column enables you to choose the type of each variable:
- **NO**: variable that is neither published nor subscribed
- **PUB**: published variable
- **SUB**: subscribed variable

Group Field

This column contains the name of the Distribution Group to which the variable belongs.

Data ID Field

This column contains the Global Data identifier in the same Distribution Group (numbered from **1 to 64**).

Section 5.7
Time Synchronization Service Configuration Parameters

About this Section

This section introduces the configuration parameters linked to the time synchronization service, which uses NTP.

What Is in This Section?

This section contains the following topics:

Configuration Parameters Linked to the Time Synchronization Service (NTP)

List of Parameters

Configure or change the following parameters on the NTP Configuration page.

1. **IP address of primary NTP server**
   - Enter a valid IP address
2. **IP address of secondary NTP server**
   - Enter a valid IP address
3. **Polling Period (in seconds)**
   Enter a value
   - min = 1 sec
   - max = 120 sec
   - default = 5 sec
4. **Time Zone**
   - Select from drop-down menu
     Universal Time, Coordinated (GMT) = default
   - Custom time zone
5. **Automatically adjust clock for daylight saving change**
   - Parameter is selected by default (check mark appears) if daylight saving time is chosen.

Time Zones Available

Select a time zone the from drop-down menu.

Time Zone	Description	DST Available
Custom		Yes
(GMT-12:00)	Dateline Standard Time [Eniwetok Kwajalein]	No
(GMT-11:00)	Samoa Standard Time [Midway Is Samoa]	No
(GMT-10:00)	Hawaiian Standard Time [Hawaii Honolulu]	No
(GMT-09:00)	Alaskan Standard Time [Anchorage]	Yes
(GMT-08:00)	Pacific Standard Time [Los Angeles Tijuana]	Yes
(GMT-07:00)	Mexican Standard Time [Chihuahua La Paz Mazatlan]	Yes
(GMT-07:00)	Mountain Standard Time [Arizona Phoenix]	No
(GMT-07:00)	Mountain Standard Time [Denver]	Yes
(GMT-06:00)	Central Standard Time [Chicago]	Yes
(GMT-06:00)	Mexico Standard Time [Tegucigalpa]	No
(GMT-06:00)	Canada Central Standard Time [Saskatchewan Regina]	No
(GMT-06:00)	Central America Standard Time [Mexico_city]	Yes

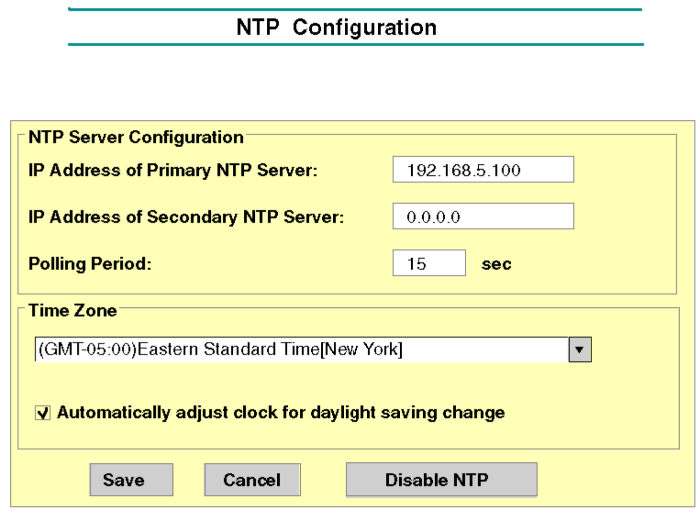
Time Zone	Description	DST Available
(GMT-05:00)	SA Pacific Standard Time [Bogota Lima Quito]	No
(GMT-05:00)	Eastern Standard Time [New York]	Yes
(GMT-05:00)	Eastern Standard Time [Indiana (East)] [Indianapolis]	No
(GMT-04:00)	SA Western Standard Time [Caracas La Paz]	No
(GMT-04:00)	Pacific SA Standard Time [Santiago]	Yes
(GMT-03:30)	Newfoundland Standard Time [Newfoundland St Johns]	Yes
(GMT-03:00)	E. South America Standard Time [Brasilia Sao_Paulo]	Yes
(GMT-03:00)	SA Eastern Standard Time [Buenos Aires Georgetown]	No
(GMT-02:00)	Mid-Atlantic Standard Time [South_Georgia]	No
(GMT-01:00)	Azores Standard Time [Azores Cape Verde Island]	Yes
(GMT)	Universal Coordinated Time [Casablanca, Monrovia]	No
(GMT0)	Greenwich Mean Time [Dublin Edinburgh Lisbon London]	Yes
(GMT+01:00)	Romance Standard Time [Amsterdam CopenHagen Madrid Paris Vilnius]	Yes
(GMT+01:00)	Central European Standard Time [Belgrade Sarajevo Skopje Sofija Zagreb]	Yes
(GMT+01:00)	Central Europe Standard Time [Bratislava Budapest Ljubljana Prague Warsaw]	Yes
(GMT+01:00)	W. Europe Standard Time [Brussels Berlin Bern Rome Stockholm Vienna]	Yes
(GMT+02:00)	GTB Standard Time [Athens Istanbul Minsk]	Yes
(GMT+02:00)	E. Europe Standard Time [Bucharest]	Yes
(GMT+02:00)	Egypt Standard Time [Cairo]	Yes
(GMT+02:00)	South Africa Standard Time [Johannesburg Harare Pretoria]	No
(GMT+02:00)	FLE Standard Time [Helsinki Riga Tallinn]	Yes
(GMT+02:00)	Israel Standard Time [Israel Jerusalem]	Yes
(GMT+03:00)	Arabic Standard Time [Baghdad]	Yes
(GMT+03:00)	Arab Standard Time [Kuwait Riyadh]	No
(GMT+03:00)	Russian Standard Time [Moscow St. Petersburg Volgograd]	Yes
(GMT+03:00)	E. Africa Standard Time [Nairobi]	No
(GMT+03:30)	Iran Standard Time [Tehran]	Yes
(GMT+04:00)	Arabian Standard Time [Abu Dhabi Muscat]	No
(GMT+04:00)	Caucasus Standard Time [Baku Tbilisi]	Yes
(GMT+04:00)	Afghanistan Standard Time [Kabul]	No
(GMT+05:00)	Ekaterinburg Standard Time [Ekaterinburg]	Yes

Time Zone	Description	DST Available
(GMT+05:00)	West Asia Standard Time [Islamabad Karachi Tashkent]	No
(GMT+05:30)	India Standard Time [Bombay Calcutta Madras New Delhi]	No
(GMT+06:00)	Central Asia Standard Time [Almaty Dhaka]	Yes
(GMT+06:00)	Sri Lanka Standard Time [Columbo]	No
(GMT+07:00)	SE Asia Standard Time [Bangkok Hanoi Jakarta]	No
(GMT+08:00)	China Standard Time [Beijing Chongqing Hong Kong Urumqi]	No
(GMT+08:00)	W. Australia Standard Time [Perth]	No
(GMT+08:00)	Singapore Standard Time [Singapore]	No
(GMT+08:00)	Taipei Standard Time [Taipei]	No
(GMT+09:00)	Tokyo Standard Time [Osako Sapporo Tokyo]	No
(GMT+09:00)	Korea Standard Time [Seoul]	No
(GMT+09:00)	Yakutsk Standard Time [Yakutsk]	Yes
(GMT+09:30)	Cen. Australia Standard Time [Adelaide]	Yes
(GMT+09:30)	AUS Central Standard Time [Darwin]	No
(GMT+10:00)	E. Australia Standard Time [Brisbane]	No
(GMT+10:00)	AUS Eastern Standard Time [Canberra Melbourne Sydney]	Yes
(GMT+10:00)	West Pacific Standard Time [Guam Port Moresby]	No
(GMT+10:00)	Tasmania Standard Time [Hobart]	Yes
(GMT+10:00)	Vladivostok Standard Time [Vladivostok]	Yes
(GMT+11:00)	Central Pacific Standard Time [Magadan Solomon Is New Caledonia]	Yes
(GMT+12:00)	New Zealand Standard Time [Auckland Wellington]	Yes
(GMT+12:00)	Fiji Standard Time [Fiji Kamchatka Marshall Is]	No

Configuration of the Time Synchronization Service (NTP)

Configuring the Time Service with the NTP Configuration Page

You must use the module's embedded Web page to configure the time service for all TSX ETY modules, except the TSX ETY 5103 module. For the TSX ETY 5103 module, you may configure the NTP service via Control Expert as long as the module is version 4.6 or later. For any earlier version, you must configure the NTP service via the module's embedded Web page *(see page 209)*.



Time Service Command Buttons

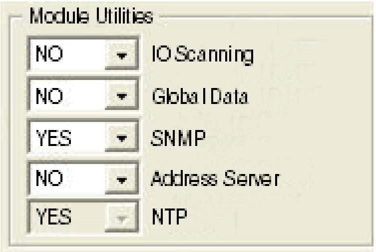
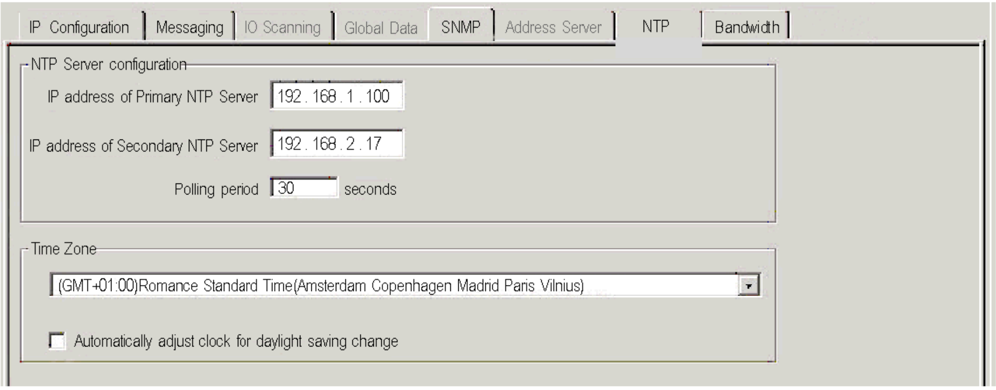
Execute the following commands:

Command Button	Description
Save	Stores new NTP (time service) configuration. Previous configuration is no longer valid.
Cancel	Cancels new NTP (time service) configuration. Previous configuration is valid.
Disable NTP	IP of Primary and Standby set = 0. NTP server not polled. Time in controller not updated.

Configuring the Time Service via the NTP Tab in Control Expert

NOTE: You can configure the NTP service via Control Expert with a Premium platform. The TSX ETY 5103 module must be version 4.6 or later. For any earlier version, you must configure the NTP service via the module's embedded Web page.

The following procedure shows you to access the **NTP** tab from the index page:

Step	Action
1	Access the module configuration screen.
2	In the **Module Utilities** field, select **YES** in the **NTP** menu. The other options are **NO** for no NTP configuration and **WEB** for NTP configuration through the module Web pages. 
3	Select the **NTP** tab. 

Changing Time Service Parameters

To make any changes to the time synchronization service:

Step	Action
1	Enter changes in the appropriate field on the NTP Configuration page for one or all of the configurable parameters.
2	Click **Save**.

Important Information about the Time Service

NOTE:
About the time service:

1. **Enable/disable daylight savings time parameter**
   If the **Enable/Disable** check box is selected, the module automatically corrects the local time to account for daylight savings time. Therefore, no action is required, as the daylight savings time start and end are automatically changed each year.
2. **Polling time parameter**
   The time (in seconds) is the time between time updates from the NTP server. The default is 5 seconds.
3. **Storing the time service configuration**
   The last time service configuration is saved internally in the Ethernet module.
4. **Replacing the Ethernet module**
   If the Ethernet module has to be replaced, the stored configuration is lost, and the system returns to the default configuration.

Customizing Time Zone Parameters

If you want a time zone not listed in the time zone table:

Step	Action	Comment
1	Write the text rules for the custom time zone.	
2	Using an FTP client, store your rules in the file: /FLASH0/wwwroot/conf/NTP/customrules user ID: ntpupdate password: ntpupdate	Root directory to store 'customrules' is set by the FTP server as /FLASH0/wwwroot/conf/NTP
3	When the rules are written, choose the drop down menu on the NTP Configuration web page, and configure (or reboot) the module by selecting Time Zone = Custom	The NTP component looks for customrules, calls the tz compiler and generates a new file called 'tz_custom'. This file is binary file and should not be edited. If the tz compiler detects a syntax error in customrules, the error is logged in the file: /FLASH0/wwwroot/conf/NTP/error.log 1. NTP component is not launched. 2. NTP Status field in diagnostic web page displays NOT OK.
4	If you want more information, the syntax to write those rules along with a few examples are found in the module in: /FLASH0/wwwroot/conf/NTP/instructions.txt	

Section 5.8
Electronic Mail Notification Service Configuration Parameters

About this Section

This section introduces the configuration parameters linked to the electronic mail notification service, which uses SMTP.

What Is in This Section?

This section contains the following topics:

Configuration Parameters for the Electronic Mail Notification Service (SMTP)

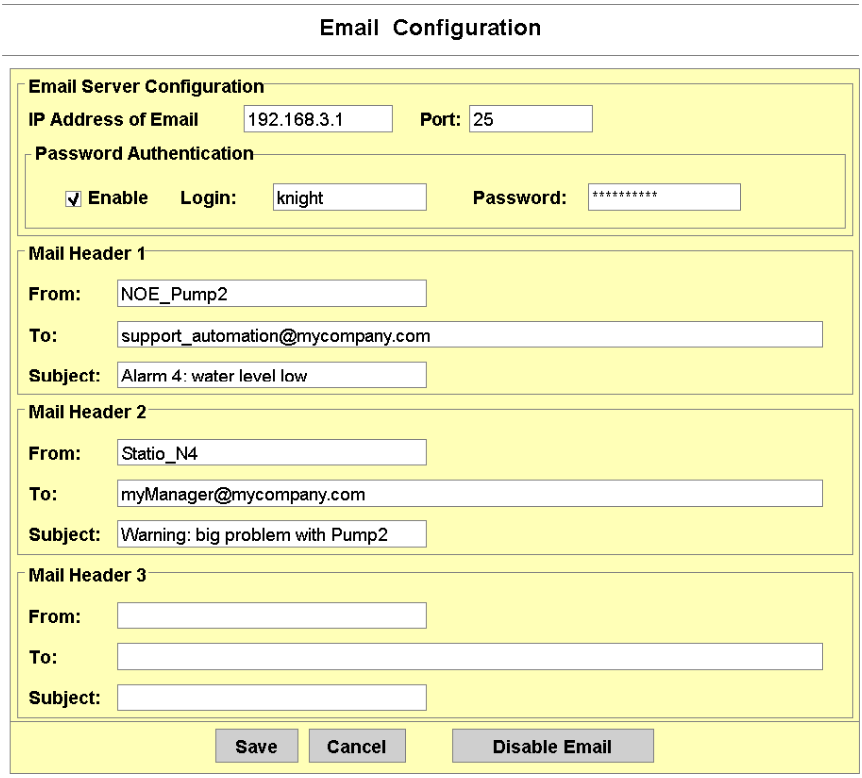
Configurable Mail Service Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>IP Address of Email</td><td>Enter a valid IP address. (This parameter identifies the SMTP server.)</td></tr>
<tr><td>Port</td><td>Default = 25 (If necessary, enter a new value.)</td></tr>
<tr><td>Password Authentication</td><td>If security is needed, enable Password Authentication by entering a check mark in the box.
Enter values for:
Login
Any printable character allowed
64-character maximum
Password
Any printable character allowed
64-character maximum</td></tr>
<tr><td>3 Mail Headers</td><td>Each header must contain:
Sender’s ID in the From field
32-character maximum (no spaces)
List of recipients in the To field
Separate each email address with a comma.
128-character maximum
Fixed part of message in the Subject field[1]
32-character maximum</td></tr>
<tr><td colspan="2">1. The Subject field consists of two parts:
Fixed (32-character maximum)
Dynamic (206-character maximum)</td></tr>
</table>

Configuration of the Electronic Mail Notification Service (SMTP)

Configuring the Mail Service with the Email Configuration Page

You must use the module's embedded Web page to configure the electronic mail notification service. No other method is available.



Mail Service Command Buttons

Mail service configuration buttons

Command Button	Description
Save	Saves the new Email configuration. Note: Previous configuration is not valid. Previous configuration is not stored.
Cancel	Cancels the entries in the fields. Previous configuration is valid.
Disable Email	Clears the stored configuration, and disables the email service. Note: Next time the service is enabled, a new configuration is required.

Section 5.9
ETHWAY Profile Configuration Parameters

About this Section

This section introduces the configuration parameters linked to the ETHWAY profile.

What Is in This Section?

This section contains the following topics:

Configuration Parameters Linked to the ETHWAY Profile

Introduction

The TSX ETY110 modules have configuration parameters linked to the ETHWAY profile:

<table>
<tr><th colspan="3">Parameters</th></tr>
<tr><td rowspan="9">ETHWAY data (common words)</td><td colspan="2">None</td></tr>
<tr><td colspan="2">Common read words</td></tr>
<tr><td colspan="2">Common read/write words</td></tr>
<tr><td rowspan="5">Word size/station</td><td>4</td></tr>
<tr><td>8</td></tr>
<tr><td>16</td></tr>
<tr><td>32</td></tr>
<tr><td>64</td></tr>
<tr><td colspan="2">Network address</td></tr>
</table>

Configuration of ETHWAY Data

Introduction

The ETHWAY data parameters are used to configure the common words by:
- selecting the type of service supported
- the number of words allocated per station
- the network address of the local station

None

The selection of this field invalidates the management of common words in the application.

The module does not manage the common database.

Common Reading Words

The application has read only access to the common words *(see page 143)*.

Common Reading/Writing Words

The application has read and write access to the common words *(see page 143)*.

Size of Words/Station

This field can be accessed when selecting **Common reading words** or **Common reading/writing words**.

Filling in this field configures the number of common words managed by the local module.

NOTE: The size of common words must be the same for each network station.

Network Address

This field can be accessed when selecting **Common reading words** or **Common reading/writing words**.

Filling in this field identifies the network which supports the common words service.

Chapter 6
Method for Programming an Ethernet Network

Aim of this Section

This chapter describes the method for creating an Ethernet network on Premium PLCs.

What Is in This Chapter?

This chapter contains the following topics:

Configuration Methodology for an Ethernet Network

Introduction

Creation and configuration of an Ethernet network involves four major stages:

Stage	Description
1	Creation of an Ethernet logic network (see note 1)
2	Configuration of an Ethernet logic network (see note 1)
3	Declaration of the module (see note 2)
4	Association of the module with the logic network (see note 2)
Note 1: Run from the project browser	
Note 2: Run from the hardware configuration editor	

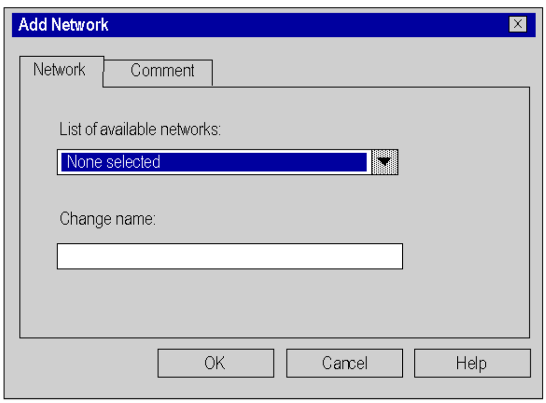
These four stages are described in the remainder of this documentation for an Ethernet TSX ETY 4103 module. These stages are also necessary for the Ethernet channels integrated in the processors.

NOTE: The benefit of this method is that from the second step onwards, you can design your communication application (you do not have to have the hardware to start working) and use the simulator to test its operation.

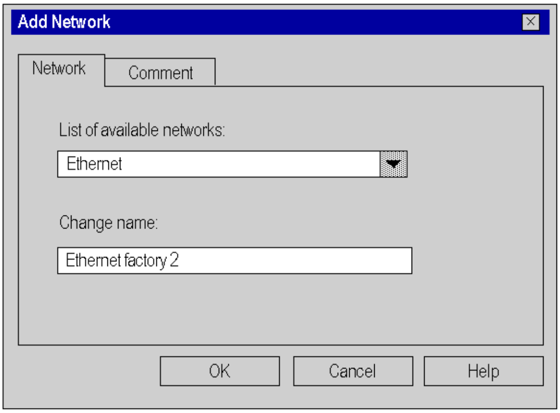
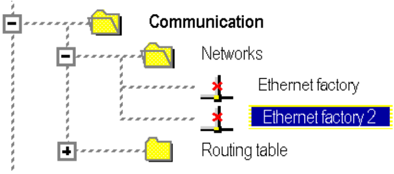
Create a Logical Ethernet Network

To create a logical Ethernet network:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Right-click the Network subdirectory of the Communication directory in the Project browser, and select the Add Network option. The Add Network screen appears:

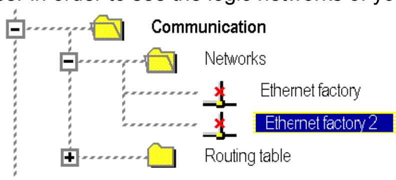
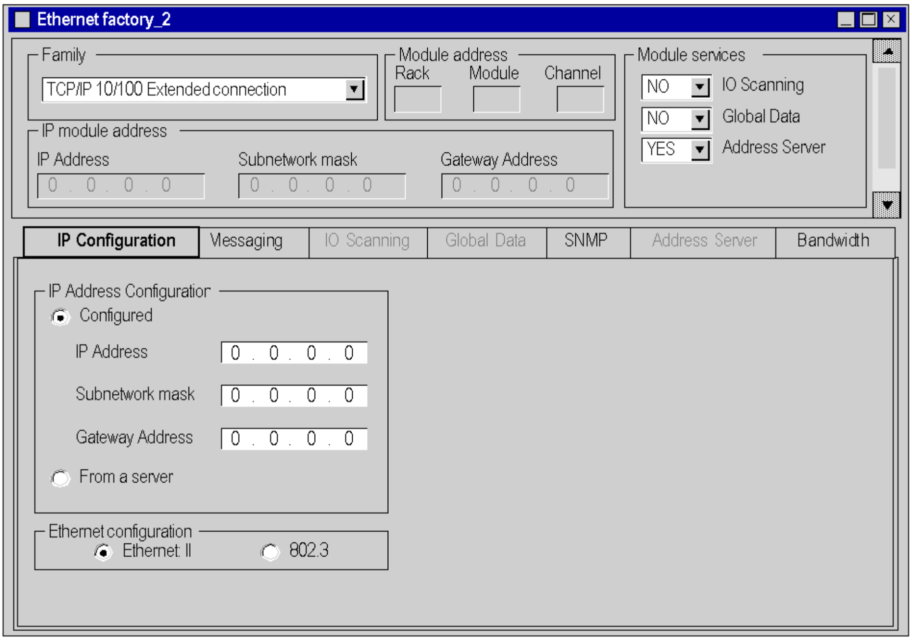


</td></tr>
</table>

Step	Action
2	Choose **Ethernet** in the list of available networks and choose a meaningful name for your selection:  **Note**: If desired, a comment may be added by clicking on the **Comment** tab.
3	Click **OK**, and a new logic network is created. The new Ethernet network appears in the project browser.  **Note**: As you can see, a small icon indicates that the logical network is not associated with a PLC device.

Access the Logical Ethernet Network Configuration

To access the logical Ethernet network configuration:

Step	Action
1	Open the project browser in order to see the logic networks of your application. 
2	Right-click the Ethernet logic network to be configured, and select **Open**. The Ethernet configuration screen is displayed. 
3	Choose the model family of your network. (To help you, a popup menu appears when you place your mouse over the selection menu.) **Note**: The network can then be configured following the instructions given in the rest of this document by consulting the chapters describing the configuration procedures for each module type.

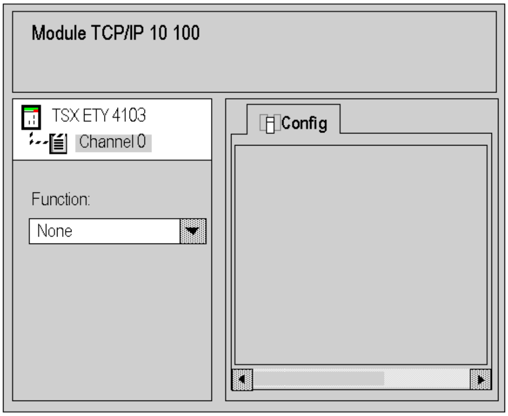
Declare the Module

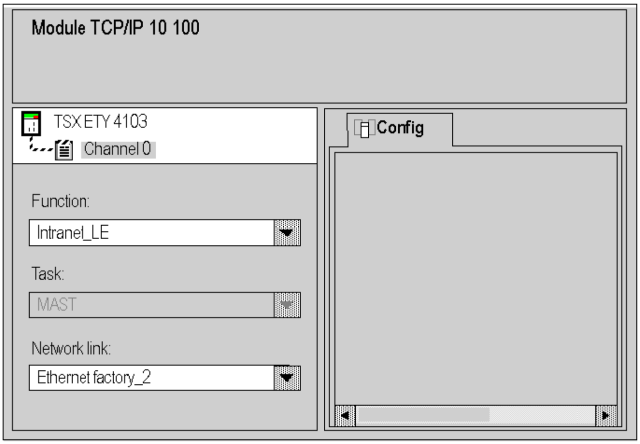
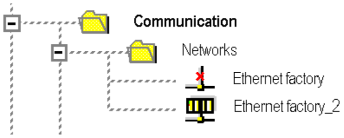
To declare an Ethernet module:

Step	Action	Result
1	Open the hardware configuration editor.	
2	Click twice on the empty slot in which you wish to place the module.	The module catalog window appears.
3	Choose the **Communication** family.	
4	Choose the desired Ethernet module from the list of **Communication** family modules.	The module appears in the rack (see note).
Note: In the case of Ethernet solutions integrated in the processors, the Ethernet communication channel is automatically declared when a processor is chosen.		

Associate the Module with the Network

To associate the logical Ethernet network with the module you have just declared:

Step	Action
1	Open the hardware configuration editor.
2	Click twice on the module slot. 

Step	Action
3	In the **Function** zone, select the network to be associated with the card. Then, in the **Network link** zone, select the logic network you wish to associate with the Ethernet channel of the module. 
4	Confirm your choice and close the window. The **Ethernet factory_2** logic network is associated with the Ethernet TSX ETY 4103 module. The module address is written in the logic network's configuration window. The icon associated with this logic network changes and indicated the links with a PLC. 

Choosing a Logical Network Family

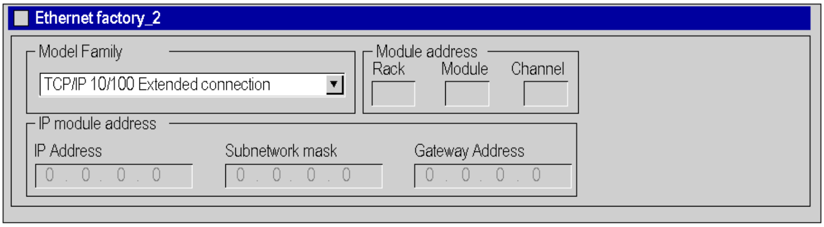
Network Families

Unlike other networks, during the configuration phase of a logical Ethernet network it is necessary to choose the module family to be attached to the logical network in order to access the different available services.

There are three Premium PLC families:

- **TCP/IP 10 and ETHWAY** for ETY 110 and 110 WS
- **TCP/IP 10/100 extended connection** for TSX P57 6634/5634/4634
- **TCP/IP 10/100 standard connection** for TSX ETY 4103/5103 and ETY PORT (TSX P57 1634/2634/3634)

The figure below shows the family selection window:



Chapter 7
TSX ETY 110 Module

Subject of this Chapter

This chapter describes the implementation of a TSX ETY 110 module.

What Is in This Chapter?

This chapter contains the following sections:

Section 7.1
General Points (TSX ETY 110)

About this Section

This section introduces Ethernet communication from the TSX ETY 110 coupler and its characteristics.

What Is in This Section?

This section contains the following topics:

TSX ETY 110 Module: General

Introduction

The communication channel of the Ethernet TSX ETY 110 module offers two connection types:

- connection to an ETHWAY network with common-word and X-Way UNI-TE messaging on an ETHWAY profile
- connection to a TCP/IP network with X-Way UNI-TE and Modbus messaging on a TCP/IP profile

Because it functions as an SNMP agent, the module can be supervised by one or two SNMP managers.

Architectures

The TSX ETY 110 can be used in three different architectures:

- in a closed proprietary ETHWAY architecture
- in a proprietary ETHWAY architecture connected to a TCP/IP network by an intermediate gateway
- in open TCP/IP architecture via direct connection to the network

The recommended uses differ according to the architecture *(see page 241)*.

NOTE: When the Ethernet network load passes 30%, you should use:

- the TCP/IP profile instead of the ETHWAY profile
- switch-type accessories and routers to reduce the load

Characteristics (TSX ETY 110)

Messaging

The TSX ETY 110 module supports:
- maximum 32 parallel connections on TCP/IP
- only one connection to a remote device

The maximum frame size depends on the type of transaction:
- In synchronous messaging, the maximum frame size is 256 bytes.
- In asynchronous messaging, the maximum frame size is 1 Kbyte.

The number of communication functions handled simultaneously depends on the type of profile:
- where a TCP/IP profile is used, maximum 16 simultaneous messages
- where an ETHWAY profile is used, maximum 16 simultaneous messages

Maximum Capacity of the Module

The module provides the following capacities:
- in the case of ETHWAY messaging : 130 messages per second
- in the case of X-Way messaging on TCP/IP : 140 messages per second
- in the case Modbus messaging on TCP/IP : 100 messages per second

NOTE:
A message can be:
- sending a communication function
- the response to a communication function

Common Words

A common word message is equivalent to 0.5 data messages.

Example of application dimensioning :

Five stations exchange common words every 100 ms and X-Way messaging on TCP/IP.

The flow of common words received by each module is:
- 50 messages per second of common words
- around 25 messages per second on TCP/IP

So the remaining maximum capacity on each module on TCP-IP is:

140 – 25 + 115 messages per second

Elsewhere in this guide is a detailed discussion of common words *(see page 143)*.

Module Performance (TSX ETY 110)

Sample Performance Data

The performance data below are given for a communication between two PLCs equipped with TSX 57-30 processors.

The values are expressed in ms and represent an average duration of the time described in the table:

Opening time of a TCP/IP connection	10 ms
Transaction time of a 128-byte UNI-TE request in periodic mode of 50 ms (MAST task)	150 ms
Transaction time of a 128-byte UNI-TE request in cyclic mode of 4 ms (MAST task)	80 ms
Transfer time of common words (out/in) in periodic mode 50 ms	250 ms
Module crossing time	15 to 30 ms

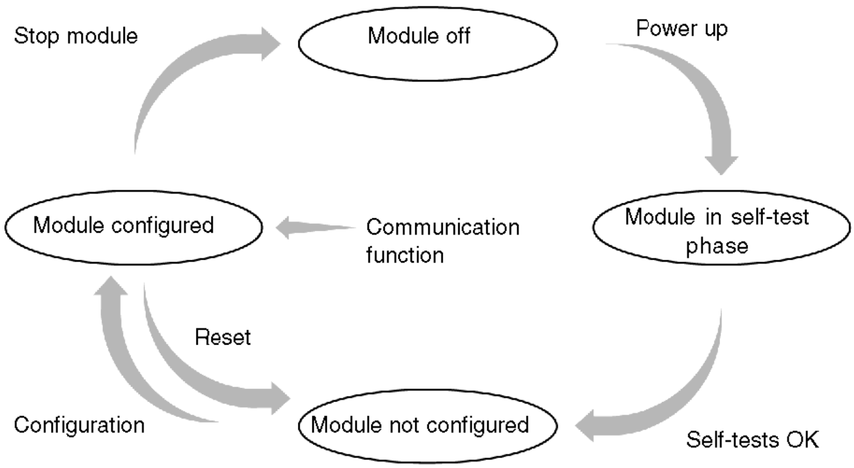
The transaction time takes into account the time to send the message and to receive the response.

Operating Modes of the TSX ETY 110 Module

At a Glance

The following diagram describes the operating modes of the TSX ETY 110 module.

General Diagram



Operation

- After power-up, the module carries out self-testing. During this phase, the LED indicators blink.
- The module does not operate with a default configuration. It must be sent this configuration by the Control Expert application with a terminal connected to the terminal port of the PLC containing the module.
  The configuration values are given in the list of language objects %KW.
  The network, station address is given by the thumbwheels on the front panel.
- When the configuration is received, the module resets the current communication to zero before configuring itself (terminates current exchanges, shuts down TCP connections).

Common Functions on the ETHWAY and TCP/IP Profile

Duplicate MAC Address

Detecting a duplicate MAC address (defined by the code selector) between stations that have a Schneider MAC address is done when the device is switched on.

So that this detection is operational, the connection cable to the network must be plugged in before being switched on.

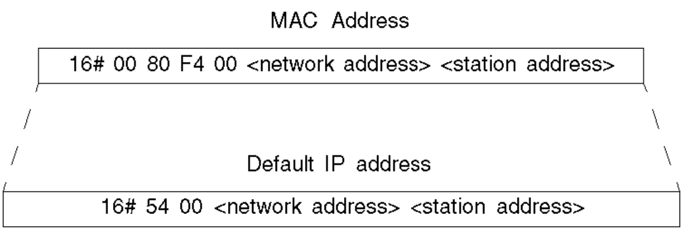
The RUN and ADR LEDs light up on the front panel of the module when a duplicate is detected.

Managing IP Parameters

In a closed architecture you may choose not to configure IP parameters and to keep the default values.

In an open TCP/IP architecture, the IP parameters (IP address, subnet mask, gateway address) must be configured.

The default value of the local IP address is derived from the MAC address (its uniqueness is not guaranteed in an open TCP/IP architecture). It is a class A IP address.



The default value of the subnet mask is 0.0.0.0 (no subnet knowledge).

The default value of the default gateway is 0.0.0.0 (no IP gateway knowledge).

Section 7.2
TSX ETY 110 Configuration

About this Section

This section describes the implementation of the TSX ETY 110 module during its configuration.

What Is in This Section?

This section contains the following topics:

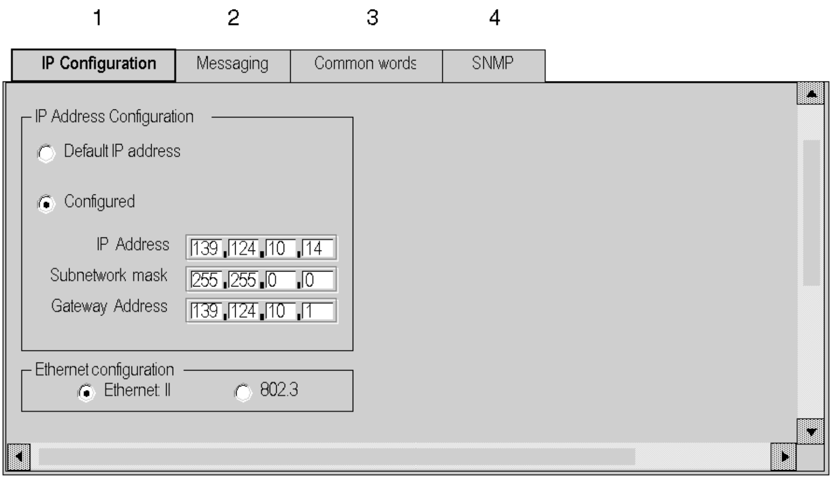
Module Configuration Screen

Introduction

This screen, separated into six zones, is used to declare the communication channel and to configure the necessary parameters for an Ethernet port.

Figure

The screen dedicated to Ethernet communication is displayed as follows:



Elements and Functions

This table describes the various zones that make up the configuration screen:

Tab	Function
1	Enables the configuration of IP addresses *(see page 150)* and configuration of the type of Ethernet frame *(see page 155)*
2	Enables the configuration of TCP/IP connections *(see page 153)*
3	Configures common words
4	Configures SNMP *(see page 197)*

Type of Communication According to Chosen Configuration

Introduction

Depending on the configuration of the TSX ETY 110 module, you can carry out messaging:

- on the ETHWAY profile
- on the TCP/IP profile

Module in Client Mode

When the module is the client, the ETHWAY or TCP/IP profile is fixed by the configuration of stations in the module's connection table.

The following table specifies which profile is used according to the configuration of the table.

	If the address of the remote station is …	
	referenced in the table	**not referenced in the table**
Communication profile	TCP/IP	ETHWAY

NOTE: If no station is recorded in the table, the communication profile is ETHWAY.

Module in Server Mode

When the module is the server, the ETHWAY or TCP/IP profile is fixed according to the client device :

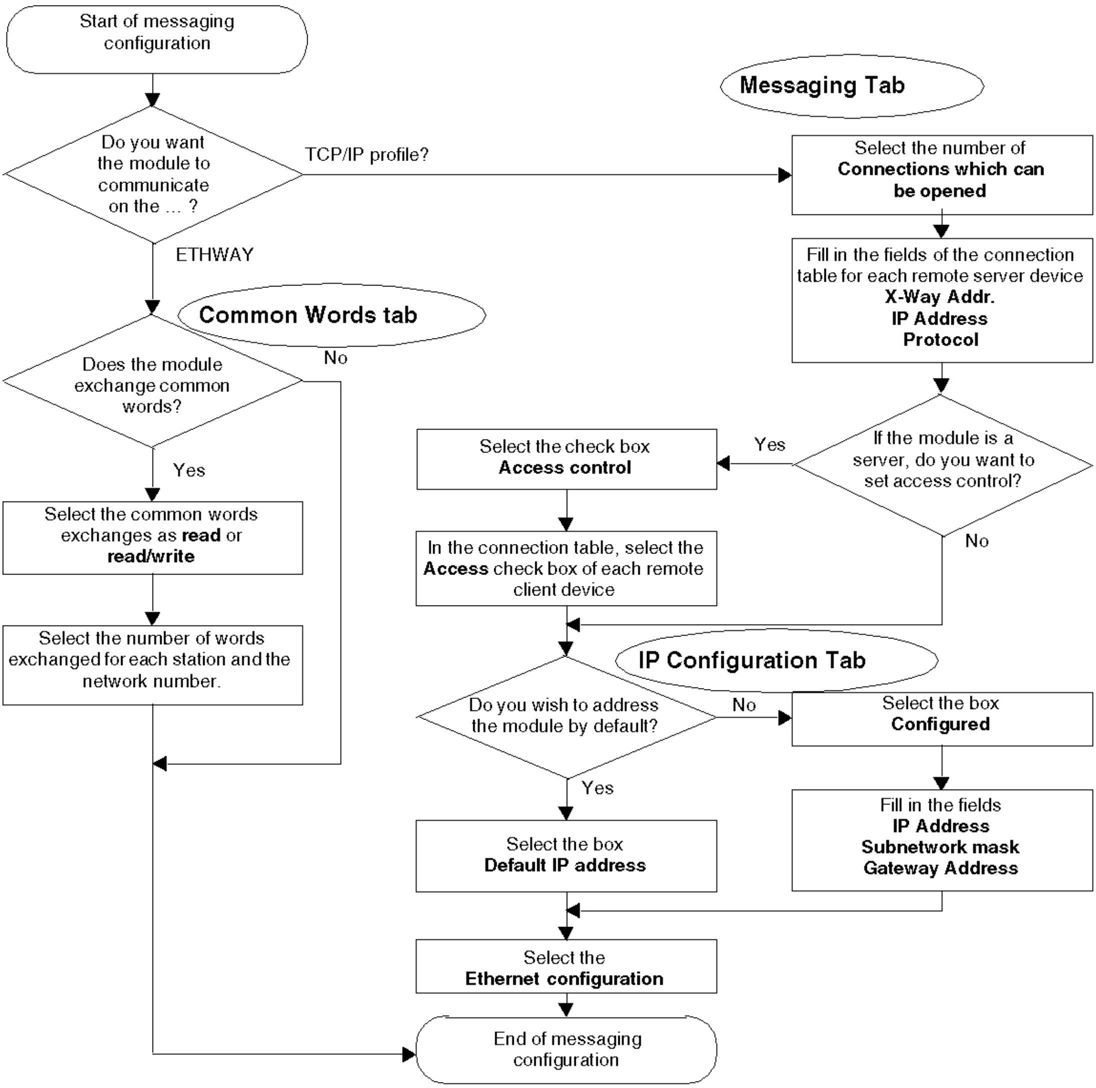
- If the client transmits on the ETHWAY profile, the module responds on the ETHWAY profile.
- If the client transmits on the TCP/IP profile, the module responds on the TCP/IP profile.

NOTE: Where access control is activated, compatibility must be ensured between the client and server's connection tables. If the client's address is referenced in the server's table, the client must communicate on the TCP/IP profile.

Configuration of Messaging on the TCP/IP Profile or the ETHWAY Profile

Module Configuration

You must set the configuration parameters to use the TSX ETY 110 for Ethernet communications. Before configuring the module, access the configuration screen and click on the various tabs corresponding to your choices.



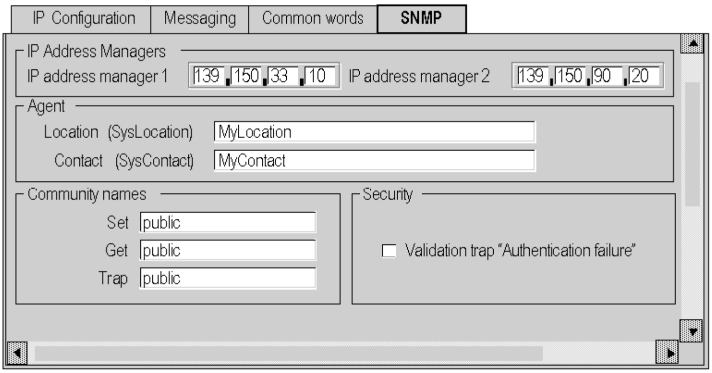
Configuration of SNMP (TSX ETY 110)

Introduction

In order to use the TSX ETY 110 module as an SNMP agent, it is necessary to set the SNMP configuration parameters.

Access the SNMP

To access the configuration parameters for SNMP:

Step	Action
1	Access the configuration screen module (Network directory in the Project browser).
2	Click the **SNMP** tab. **Result:** The following window appears: 

Configuring SNMP

To configure SNMP:

Step	Action
1	Enter the SNMP manager addresses: ● **Manager 1 IP addresses** ● **Manager 2 IP addresses**
2	Fill in the fields: ● **Location (SysLocation)** ● **Contact (SysLocation)**.
3	If you want to set access rights, fill in the community names: ● **Set** ● **Get** ● **Trap**
4	If you want to activate transmission of an event to the module, check the **Activate "Authentication Failure" trap** box.

Configuration of the Bridge Function (TSX ETY 110)

Introduction

The TSX ETY 110 module can be used as an X-Way bridge station. This guarantees transparent communication between various networks.

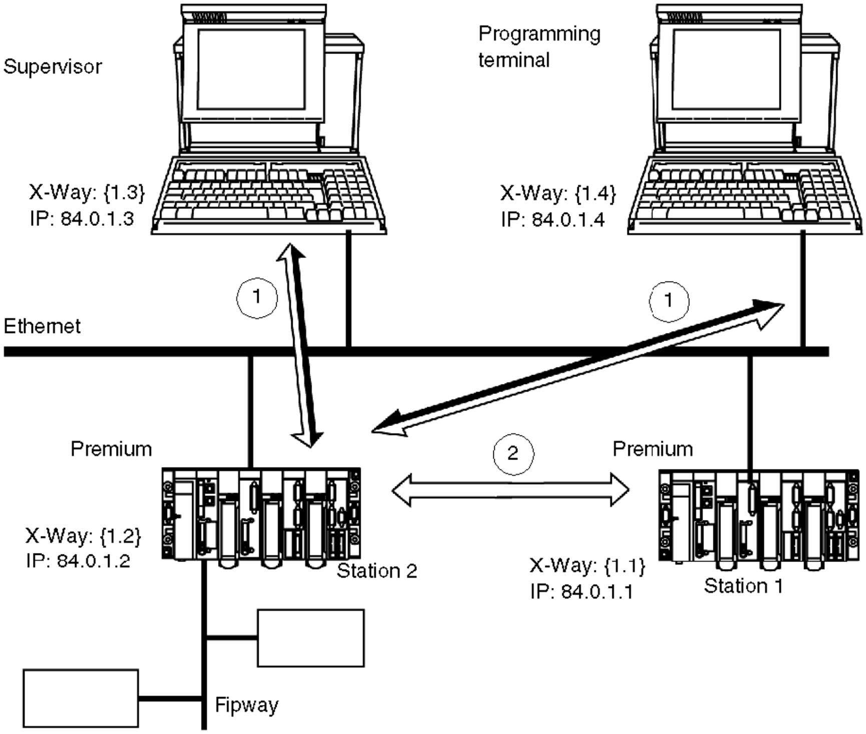
NOTE: For detailed information on configuring X-Way routing, refer to:

- Premium, Atrium and Quantum using Unity Pro Communication, services and architectures reference manual (35006173)

Example: a TSX ETY 110 in an ETHWAY Private Architecture

Overview

The following figure shows a TSX ETY 110 module in an ETHWAY private architecture:



1 ETHWAY or TCP/IP communication
2 ETHWAY communication

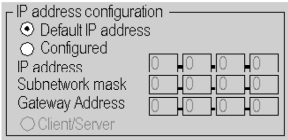
Recommended Operating Mode

- IP addressing is not managed (default value). It is taken from the values displayed on the thumbwheels of the module.
- Inter-PLC communication uses the ETHWAY services (COM, UNI-TE).
- Communication between the PLC and the supervisor or the programming terminal uses ETHWAY services or UNI-TE on TCP/IP.
- The frame format used is Ethernet II.

NOTE: In the following examples, it is assumed that the communication with the terminals is done on TCP/IP.

Configuration of the Local Address of the Module at Station 2

In a closed environment, it is possible to not manage the IP addresses, the **Default IP address** mode is selected.



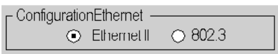
Configuration of the Connections of the Module at Station 2

The field to be entered is the X-Way address of the remote stations with which dialog is to be established (X-Way address 1.3); the other fields are automatically initialized. Access protection is inhibited by default and the maximum number of connections is 32.

NOTE: Since the PLC is still the server vis-à-vis the programming terminal, the latter does not have to be declared.

Ethernet Configuration of the Module at Station 2

The Ethernet frame format selected for TCP/IP is **Ethernet II** because, in the example, the terminals use this format.



Configuration of the Common Words of the Module of Station 2

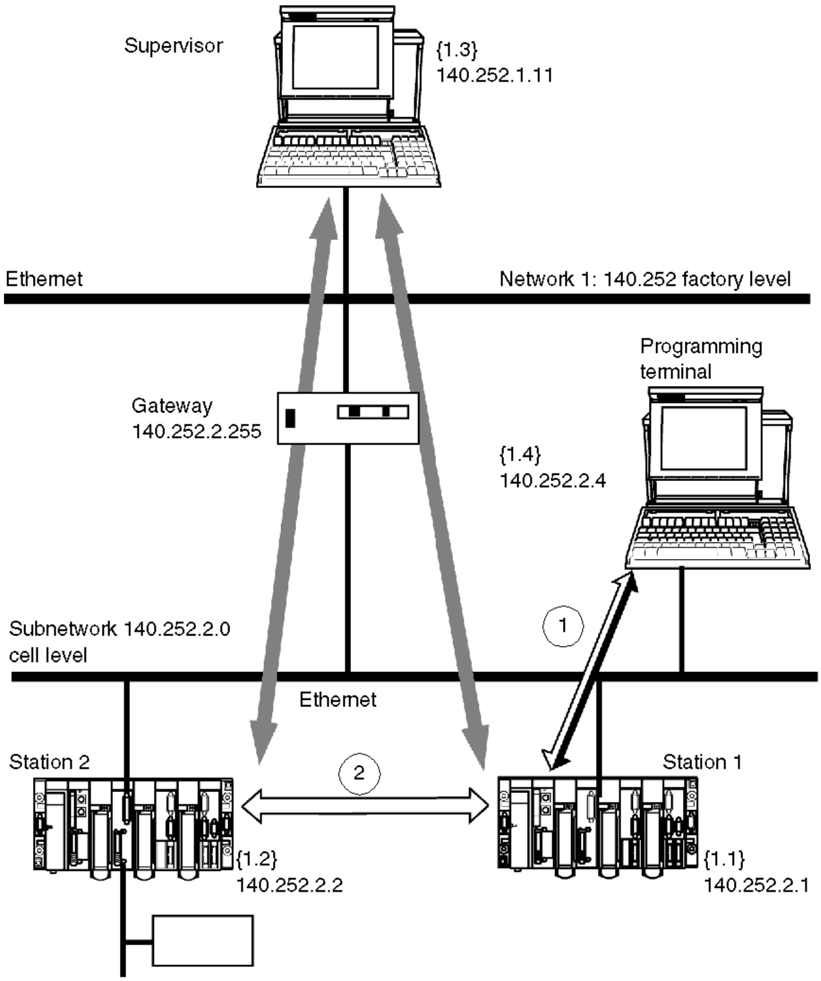
Station 2 exchanges 16 common write/read words with the other PLCs connected to the network.

Therefore you need to configure the:
- type of service
- size of common words
- network number

Example of ETHWAY Type Architecture Connected to TCP/IP

Overview

The following figure shows the installation of a TSX ETY 110 module in an ETHWAY architecture connected to a TCP/IP network.



1 ETHWAY or TCP/IP communication
2 ETHWAY communication

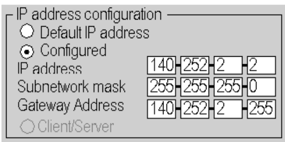
Recommended Operating Mode

- IP addressing is globally managed because connection is made to an existing TCP/IP factory network.
- At cell level, inter-PLC communication uses the ETHWAY services (COM, UNI-TE).
- Communication between the PLC and the supervisor or the programming terminal, at cell level, uses ETHWAY services or UNI-TE on TCP/IP.
- Communication between the PLC and the supervisor uses the UNI-TE services on TCP/IP.
- The frame format used is Ethernet II.

NOTE: Cell-level ETHWAY services are the same as the services described in the previous example. This example only describes communication between the factory-level supervisor and a Premium PLC at cell level.

Configuration of the Local Address of the Module on Station 2

As the IP addresses must be managed, the configured IP address mode is selected.



You must enter the IP parameters given above. These values are taken from the installation global addressing plan managed by the network manager.

The network manager can ensure their uniqueness by having their network ID (140.252) allocated by an authorized body.

The cell network is an IP subnetwork. This enables a unique network ID (140.252) to be allocated for the whole architecture. The subnetworks are then defined by the user of the subnetwork mask 255.255.0.0.

The address class chosen (in this case class B) depends on the number of machines and the number of installation networks.

Configuration of the Connections of the Module on Station 2

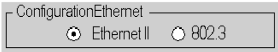
You must enter both the X-Way address and the IP address of the devices with which the module must communicate.

Click on the **Access control** button to activate this control, then check the corresponding box in the **Access** column.

The maximum number of connections in the application can be adjusted.

Ethernet Configuration of the Module on Station 2

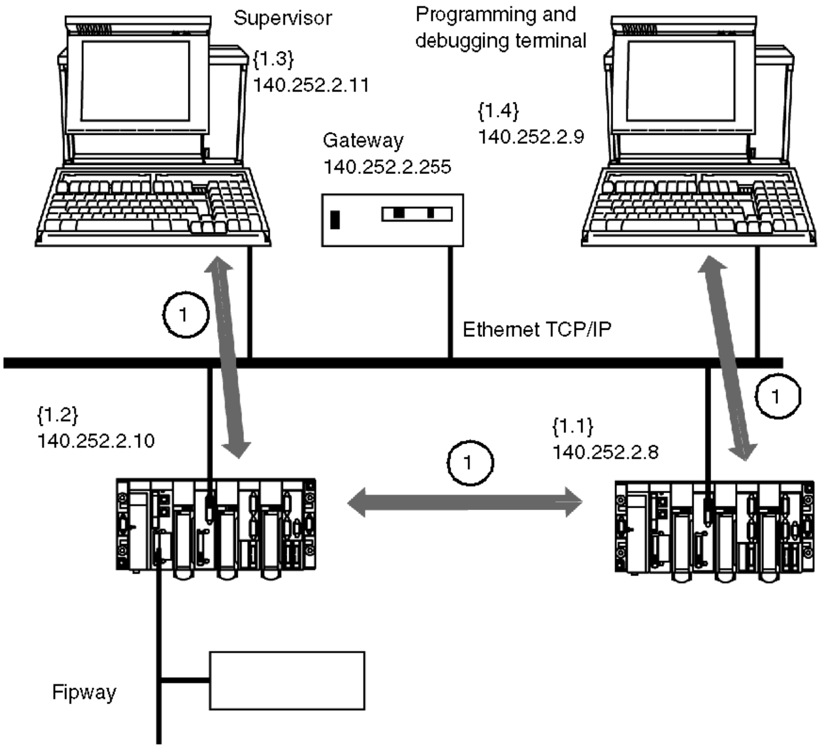
The Ethernet frame format selected for TCP/IP is **Ethernet II** because, in the example, the terminals use this format.



Example of Connection to a Non-Private TCP/IP Network

Overview

The following figure shows the installation of a TSX ETY 110 connected to an existing TCP/IP network.



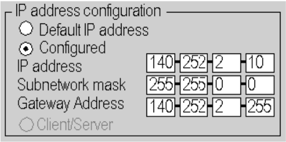
1 TCP/IP Communication

Recommended Operating Mode

- IP addressing must be managed because connection is made to a non-private TCP/IP network.
- Inter-PLC communication uses UNI-TE on TCP/IP.
- Communication between the PLC and the supervisor or the programming terminal uses UNI-TE on TCP/IP.
- The frame format used is Ethernet II.

Configuration of the Local Address of the Module

The IP addresses must be managed, the **Configured IP address** mode is selected, you must enter the IP parameters.



Configuration of the Connections of the Module

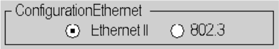
You must enter both the X-Way address and the IP address of the devices with which the module must communicate.

Click on the **Access control** button to activate this control, then check the corresponding box in the **Access** column.

The maximum number of connections which can be opened in the application can be adjusted.

Ethernet Configuration of the Module

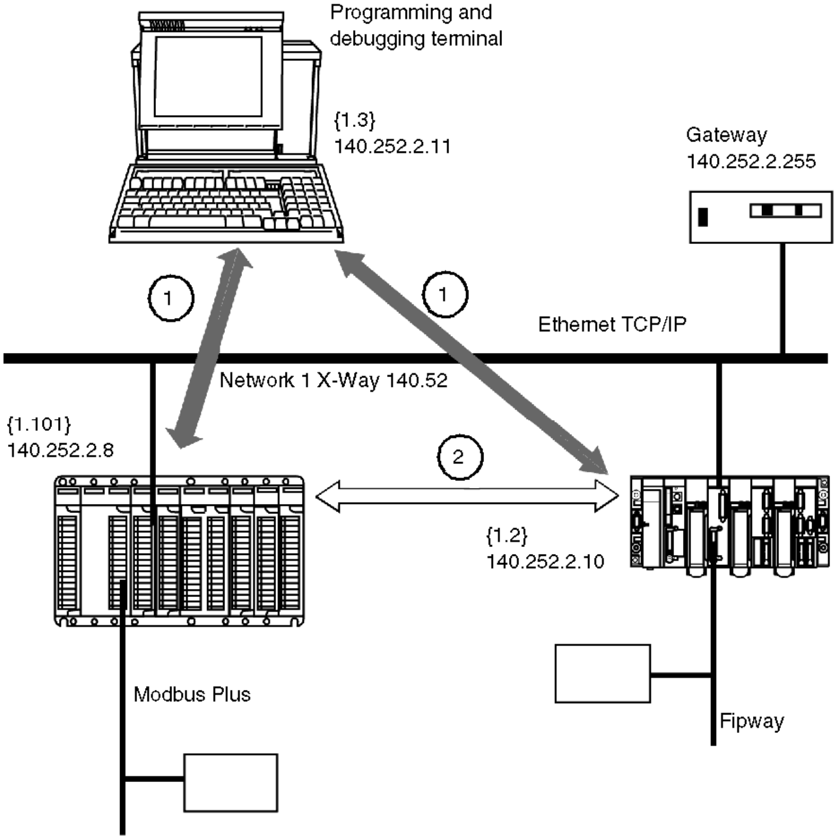
The Ethernet frame format selected for TCP/IP is **Ethernet II** because, in the example, the terminals use this format.



Example: Communication between Premium and Quantum

Overview

The following figure shows the installation of a TSX ETY 110 in a Premium system for communicating with a Quantum PLC:

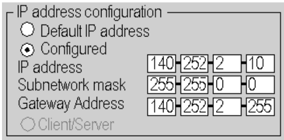


Recommended Operating Mode

- IP addressing is managed due to the risk of duplicating IP addresses with default values.
- Inter-PLC communication uses Modbus on TCP/IP.

Configuration of the Module's Local Address

The IP addresses must be managed, the **Configured IP address** mode is selected, you must enter the IP parameters.



Configuration of the Module Connections

You must enter both the X-Way address and the IP address of the devices with which the module must communicate.

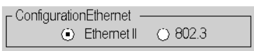
Click on the **Access control** button to activate this control, then check the corresponding box in the **Access** column.

The maximum number of connections in the application can be adjusted.

NOTE: Communication with the Quantum PLC requires the Modbus protocol to be configured.

Ethernet Configuration of the Module

The Ethernet frame format selected for TCP/IP is **Ethernet II** because, in the example, the terminals use this format.



Section 7.3
Debugging (TSX ETY 110)

About this Section

This section describes the debugging for the TSX ETY 110 module.

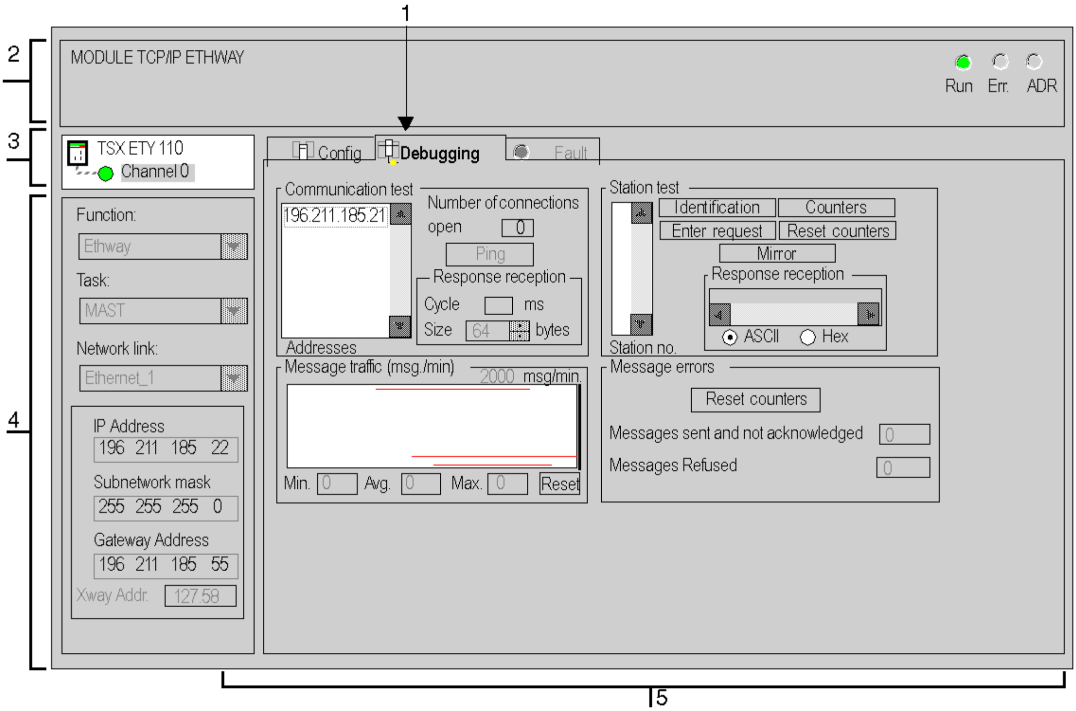
What Is in This Section?

This section contains the following topics:

Module Debugging Screen

The Screen

The five-zone screen allows for the debugging of an Ethernet link:



This table describes the zones in the configuration screen:

Number	Zone	Function
1	Tab	Debug tab
2	Module	Module description zone
3	Channel	Channel selection zone
4	General parameters	General parameters zone
5	General parameters	Debug zone containing the different parts described hereafter.
	Message traffic	allows the graphical display of the number of messages processed by the module
	Message errors	allows the display of the number of unacknowledged or refused messages.
	Communication tests	allows: • display of TCP/IP utilities configuration • communication testing of the TCP/IP profile
	Station tests	allows: • display of ETHWAY utilities configuration • communication testing of the ETHWAY profile

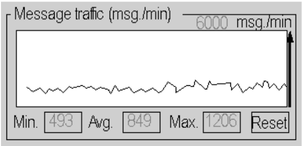
General Debugging Parameters

Introduction

The general debugging parameters are grouped into two windows:
- the **Message traffic** window
- the **Message errors** window

Message Traffic

The **Message traffic** window looks like this:



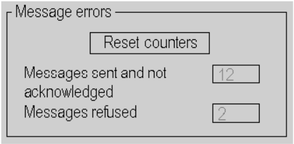
It graphically shows the number of messages per minute handled by the module (sent and received).

This number can be compared to the maximum flow rate offered by the module (7800 or 8400 messages at 128 bytes per minute) in order to determine whether the latter is working in a normal use range or in overload.

The **Reset** button resets the three counters, **Min.**, **Av.** and **Max** to 0.

Message Errors

The **Message errors** window looks like this:



The message errors window shows the number of unacknowledged messages on ETHWAY and the number of refused messages on ETHWAY or TC/IP.

You can reset these counters to zero by clicking the **Init counters** button.

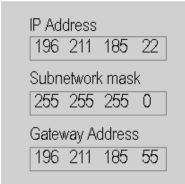
Debugging Parameters for TCP/IP

Introduction

The debugging parameters for the TCP/IP services are grouped together in two windows:
- the **IP Address** window
- the **Communication test** window

IP Address

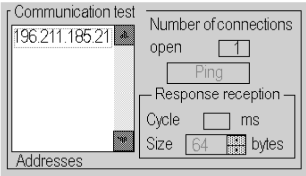
The window is displayed as below:



It specifies the configuration data of the IP address:
- **IP Address**
- **Subnetwork mask**
- **Gateway Address**: address of the gateway

Communication Test

The window is displayed as below:

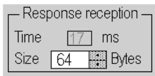


This window allows you to test IP communication towards another declared station in the remote devices grid.

Testing TCP/IP Communications with a Ping Request

Initiating a Ping Request

To test the routing information between two devices with a Ping request:

Step	Action
1	Select the address of the station to be interrogated with the help of the **Addresses** field.
2	Select the number of bytes to be transmitted using the **Size** field. This specifies the length of the message to be sent between 64 and 1472 bytes.
3	Press the button **Ping**. **Result:** The reply appears in the field **Time**.  The time returned corresponds to the turnaround time for the message in ms.

Responses

The following table groups together the different types of response to the Ping request:

If the response is…	then …
positive	The window indicates the turnaround time for the message in ms.
negative	• A window with the message **Timeout** specifies the absence of response from the remote device. • A window with the message **Host unreachable** specifies that the remote device has not been reached in the network architecture.

Debugging Parameters for Ethway Utilities

Introduction

The debugging parameters for the TCP/IP utilities are grouped together in two windows:

- the **Station Address** window
- the **Station test** window

Station Address

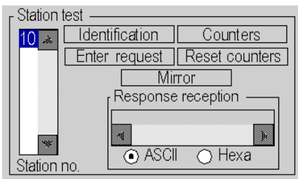
The window is displayed as below:

It recalls the configuration data:

- **Addr. X-Way** : X-Way address of the station

Station Test

The window is displayed as below:



This window is used to test a communication channel by sending a request to one of the stations present on the network.

Requests Available for the Communication Channel Test

Introduction

This page describes the different possibilities for testing a communication channel from the debugging screen.

Test Conditions

Sending a request to an unconnected station results in an error message.

Available Requests

Window **Test station** allows the following requests:

- **Identification**: Prompts the Identification request to be sent to the designated remote station.
- **Counters**: Prompts the sending of the request for the Reading of the error counters to the designated station.
- **Counters**: Prompts the designated station’s error counters to be reset to zero.
- **Request input**: Allows a UNI-TE request, other than those provided by the command buttons, to be sent to the designated station. The choices available in this function give access to a screen that allows you to select the parameters that are specific to the request (request code must be coded in hexadecimal).
- **Mirror**: Allows a mirror request to be sent to the designated station. Selecting this function gives access to a screen that allows you to select the length of the character string to be sent (a maximum of 80 characters). The PLC then sends this character string (ABCD….) to the destination device. This automatically sends the character string that was received back to the sender.

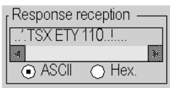
Testing a Channel with Identification and Mirror Requests

Introduction

This topic indicates the procedure to follow to test a communication channel by means of Identification and Mirror requests.

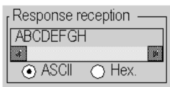
Identifying a Station

The following procedure allows the identification of a designated station.

Step	Actions
1	Select the address of the station to be interrogated with the help of the field **Station**.
2	Click the **Identification** button. **Result**: The response appears in the **Receive Response** window. 

Sending the Mirror Request

The following procedure allows the sending of the Mirror request and thus tests the routing of information between two devices.

Step	Action
1	Select the address of the station to be interrogated with the help of the field **Station**.
2	Click the **Mirror** button. **Result**: The following window appears. 
3	Input the length of data to be sent (maximum 80 characters).
4	Click the **Send** button. **Result**: The response appears in the **Receive Response** window.  The response contains the character string ABCDEFGH that corresponds to the length of data sent 8.

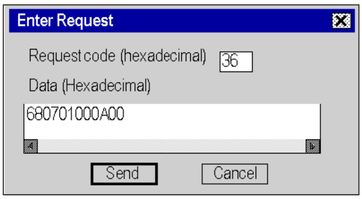
Testing Channels with Requests

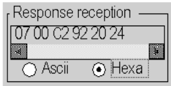
Introduction

This topic describes the procedure for testing a communication channel from the debugging screen through different requests.

Sending a Request

The following procedure allows a request, other than those provided by the command buttons, to be sent to a designated station. In this example, the request sent is used to read 10 words (from %MW1 to %MW10).

Step	Action
1	Select the address of the station to be interrogated with the help of the field **Station**.
2	Click the **Input Request** button. **Result**: The following window appears.  The data sent in this example is coded on 6 bytes.
3	Input the function code (coded in hexadecimal on one byte), corresponding to the request that you want to send. For this example the read request code is 16#36.
4	Input the data to be sent by coding all the data in hexadecimal. The data is sent non-stop without any time intervals between them. When the data is coded on one word, the most significant and least significant bytes are reversed. For this example the data is as follows: ● 16#68: on one byte, defines the segment (internal data) ● 16#07: on one byte, defines the object type (words) ● 16#0100: on one byte, defines the first word to read ● 16#0A00: on one byte, defines the number of words to read

Step	Action
5	Click the **Send** button. **Result**: The response appears in the **Receive Response** window.  The response from the example has data on 21 bytes: ● 16#07: corresponds to object type (words) ● 16#00C2: corresponds to the value of the first word (the most significant and least significant bytes are reversed, its value is 16#C200) ● ...

Chapter 8
Ethernet Modules TSX ETY 4103, TSX ETY PORT, TSX WMY 100, and TSX ETY 5103

About this Chapter

This chapter describes the installation of the TSX ETY 4103, TSX ETY PORT (TSX P57 1634/2634/3634), TSX WMY 100, and TSX ETY 5103 Ethernet modules.

What Is in This Chapter?

This chapter contains the following sections:

Section 8.1
Ethernet Communications

About this Section

This section introduces Ethernet communication from TSX ETY 4103, TSX ETY PORT, TSX WMY 100, and TSX ETY 5103 Ethernet modules and their properties.

What Is in This Section?

This section contains the following topics:

Introduction to Ethernet Communications

Communications Overview

The communication channel of the Ethernet TSX ETY 4103/PORT/5103 module offers connection to a TCP/IP network supporting the UNI-TE and Modbus messaging on a TCP/IP profile.

The three modules, TSX ETY 4103, TSX ETY PORT, and TSX ETY 5103 also offer the following services:

- Thanks to their SNMP agent functionality, the modules can be supervised by one or two SNMP managers.
- They are able to perform the role of DHCP server or the BOOTP client.
- Because of its I/O Scanning facility, they can drive remote inputs/outputs on the Ethernet network.
- They integrate an embedded HTTP server.
- With Global Data, the modules allow the exchange of data between IEC standard PLC stations.
- Bandwidth monitoring, which allows the repair of the module services to be verified.
- Replace faulty device allows the device configuration to be saved in the module. In case of breakdown, another installed blank module can be restarted with the configuration parameters of the previous one.
- Electronic Mail Notification Service, which sends alarms and events messages from controller to designated recipient.
- Time synchronization service, which updates controller clocks with Universal Time, Coordinated (UTC) from a referenced source.
  NOTE: The Control Expert configuration for the NTP service is available only with the TSX ETY 5103 module.

In addition, the TSX ETY 5103 module offers the option of creating user Web and TCP Open pages.

TSX ETY 4103/PORT/5103 Characteristics

Maximum Capacity of the Module

The maximum frame size depends on the type of transaction:
- In synchronous messaging, the maximum frame size is 256 bytes.
- In asynchronous messaging, the maximum frame size is 1 Kbyte.

The modules TSX ETY 4103, TSX ETY PORT and TSX ETY5103 allow you:
- to manage 64 TCP connections using port 502 messaging
- to scan up to a maximum of 64 devices using I/O scanning
- to be the DHCP server for a maximum of 96 devices requiring this utility

In conjunction with a processor dedicated to this sort of handling, the module can be used:
- for X-Way synchronous messaging on TCP/IP (UNI-TE server):
  - with a TSX 57-454 processor: 800 messages per second
  - with a TSX 57-354 processor: 490 messages per second
- in the case of asynchronous X-Way messaging on TCP/IP:
  - between 600 and 1200 messages per second (number varies depending on the size of the messages, the number of clients and the time it takes to run the application)

I/O Scanning

The module can scan a maximum of 64 remote devices.

For the same station, the application can process:
- a maximum total volume of inputs to be scanned of 2K words
- a maximum total volume of outputs to be scanned of 2K words

NOTE: When using I/O scanning, the PLC cycle is impacted by about 1 ms per volume of 512 I/O words scanned.

In the same way, the size of the application is impacted by 6 Kbytes for each configured TSX ETY 4103/PORT/5103 module.

Global Data

The user interface is a %MW zone defined in configuration.
- Each module can issue a variable of between 1 and 512 words.
- Each module can subscribe from 1 to 64 variables. The total data cannot exceed 2Kwords.

Replace Faulty Equipment

The module reserves a 512 kbyte zone for this function.
- Up to 96 remote devices can be configured in the DHCP address server.
- The 96 remote devices must share the 512 kb reserved for their parameters.

Type of Connections Supported

Introduction

This topic discusses the maximum number of connections that the TSX ETY 4103 or TSX ETY PORT and TSX ETY 5103 modules support.

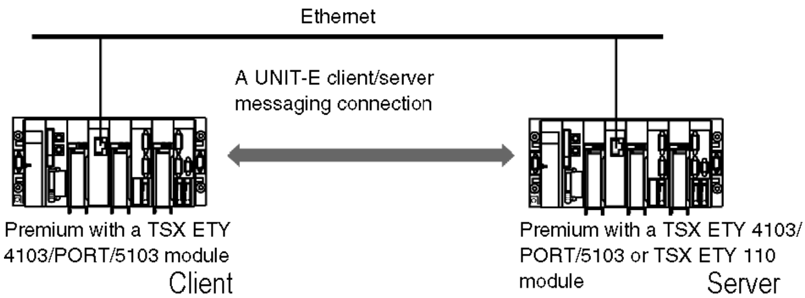
Maximum Parallel Connections

The table shows the maximum number of parallel connections for each module type:

Module	HTTP Connections	TCP/IP Connections
TSX ETY 4103	8	64
TSX ETY 5103	16	64
TSX ETY PORT	8	64

Connection to a Premium

Between two Premium PLCs using UNI-TE messaging on the TCP/IP profile, the TSX ETY 4103/PORT/5103 module only allows one connection in client/server mode.

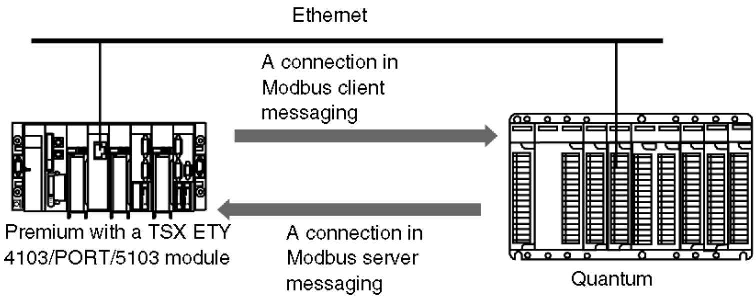


Connection to a Quantum

Between a Premium PLC and a Quantum PLC using Modbus messaging on the TCP/IP profile, the TSX ETY 4103/PORT/5103 module allows:

- a single connection in Modbus client mode
- a single connection in Modbus server mode

Example:

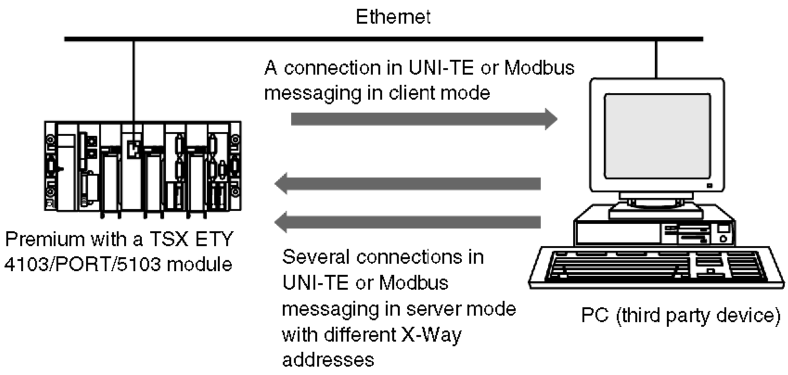


Connection to a Third Party Device

Between a Premium PLC and a third party device, the TSX ETY 4103/PORT/5103 module allows:

- a single connection in UNI-TE or Modbus client mode
- several connections in UNI-TE or Modbus server mode

Example:



Performance of I/O Scanning

Introduction

The performance data presented below are those of the module TSX ETY 4103/PORT/5103 while using I/O scanning *(see page 156)*.

Restart Time for an I/O Scanning Configuration

This time corresponds to the time between the power up of the complete configuration and the moment when all the remote inputs/outputs become operational (the status bits are activated, the word bits %IWr.M.c.1 to %IWr.m.c.4 = 1).

Values are given in seconds:

- T= 35 s, if the TSX ETY 4103/PORT/5103 module is used as a BOOTP server to connect the scanned devices
- T = 17 s, if the scanned devices use another BOOTP/DHCP server

Input/Output Restart Time

This time corresponds to the time between the power up of the remote input/output and the moment when all the status bits are activated (word bits %IWxy.i.l to %IWxy.i.4 = 1).

The value is given in seconds:

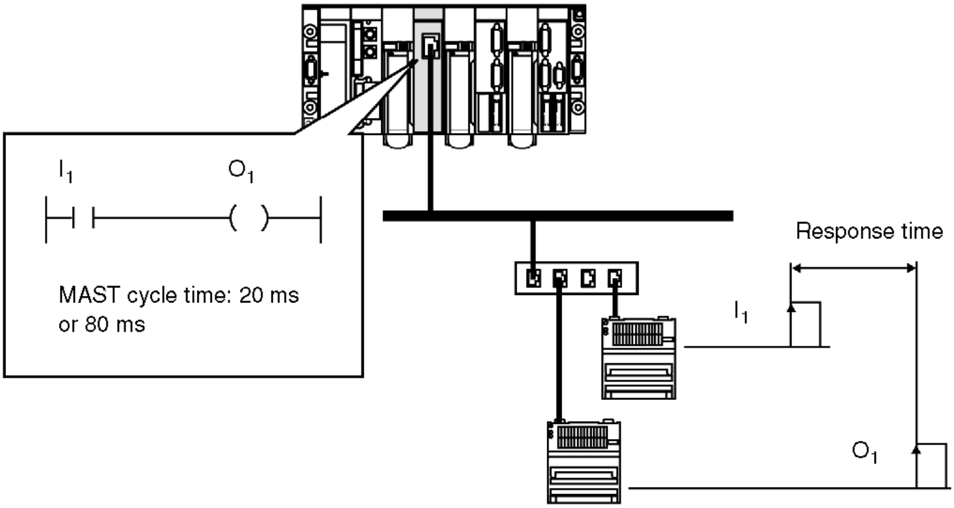
- T = 5 s

Application Response Time

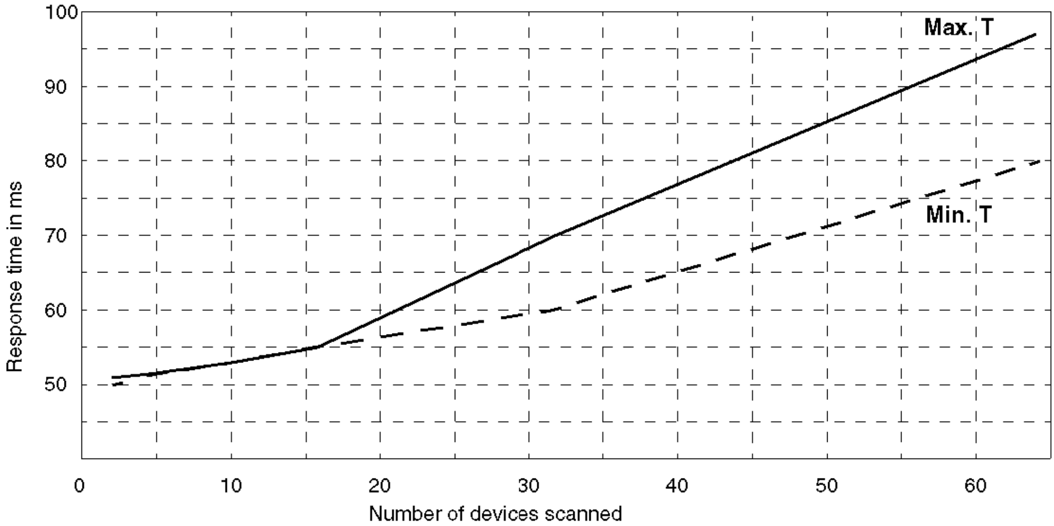
This time corresponds to the elapsed time between the acquisition of a remote input and the positioning of a remote output.

This is a logic response time, which does not take filtering time and actuator and sensor interface response times into account.

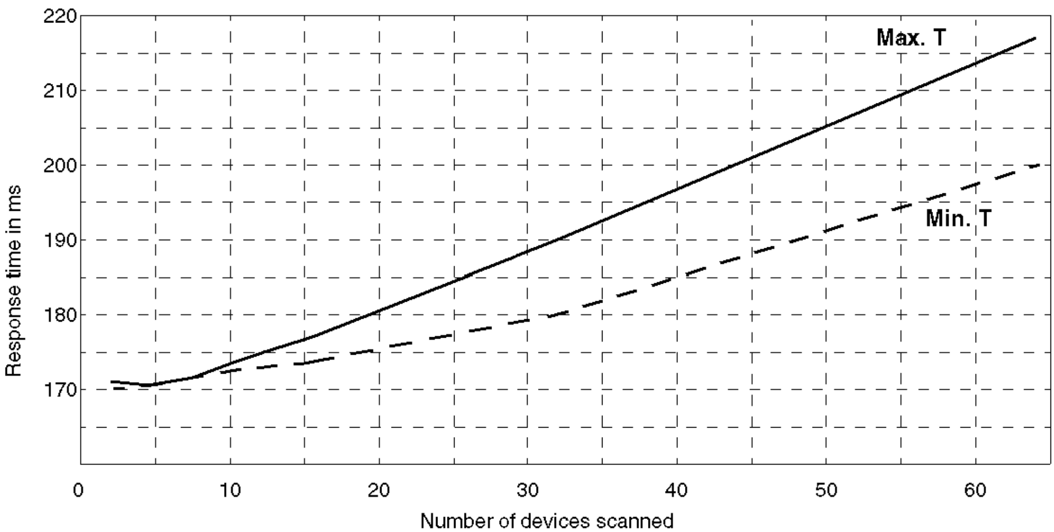
This is an example of time elapsed from acquiring an input to the positioning of an output:



Response time with a cycle of 20 ms



Response time with a cycle of 80 ms



Global Data Performances

Introduction

The topic discusses Global Data performance.

Definition

Global Data return time:

This time corresponds to the elapsed time between the publication of a variable value by the local PLC application, the subscription by a remote PLC application, the publication of the same value by the remote PLC application, and the subscription by the local PLC application.

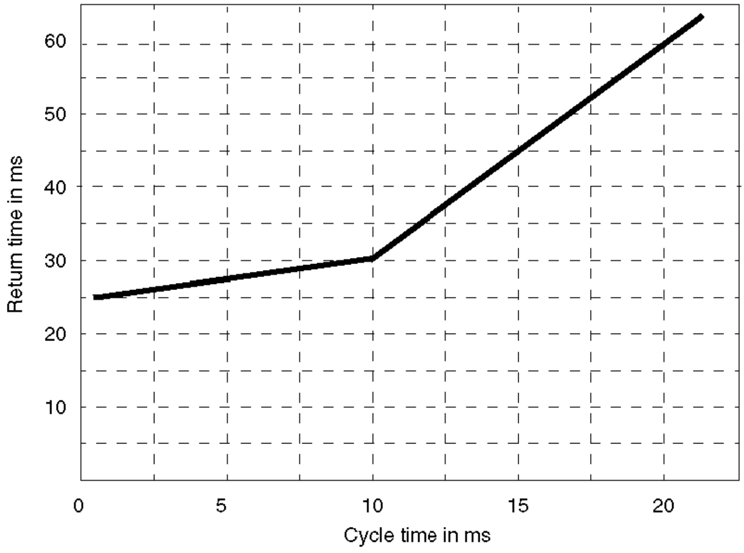
Values

Measurement conditions:
- The cycle time for local and remote PLC applications are identical.
- Only one variable is exchanged in each direction.

Result:

PLC cycle time	Return time
>= 10 ms	3 times the PLC cycle time
= 5 ms	5 to 6 times the PLC cycle time

Illustration:

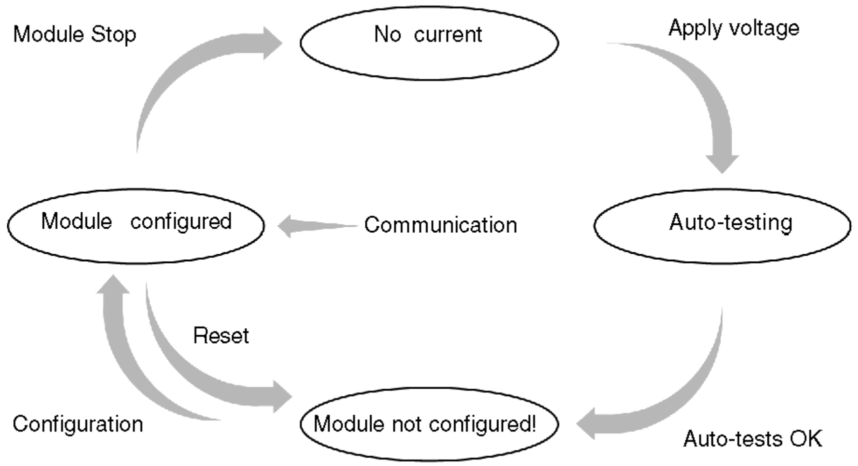


TSX ETY 4103/PORT/5103 Operating Modes

Introduction

The following diagram describes the operating modes of the TSX ETY 4103/PORT/5103 module.

General Diagram



Operation

- After power-up, the module carries out self-testing. During this phase, the STS LED is lit. After the self tests, the RUN LED lights up.
- The module does not operate with a default configuration. It must be sent this configuration by the application of the local PLC.
  The configuration values are given in the list of language objects %KW and in particular provide the IP address and the X-Way address of the module.
  The configuration is retransmitted upon every PLC restart (warm or cold).
- When the configuration is received, the module resets the current communication to zero before configuring itself (terminates current exchanges, shuts down TCP connections).
  The module is now operational. The RUN and STS LEDs are lit up.
- The I/O Scanning and Global Data functions start when the PLC transfers to RUN mode. They stop when it switches to STOP mode.

Special Cases

If a TSX ETY 4103/PORT/5103 module is not configured in the Control Expert application (RUN LED off and ERR LED blinking), it takes the IP address built from its MAC address:

085.016.xxx.yyy where xxx and yyy are the last two numbers of the MAC address.

Example

The module's MAC address is (in hexadecimal): 00 80 F4 01 12 20

In this case the default IP address is (in decimal): 085.016.018.032

The module also transmits BOOTP/DHCP requests to obtain another IP address. These requests are sent until a BOOTP/DHCP server responds or until configuration by Control Expert.

If the module detects a duplicated IP address, the STS LED flashes 4 times during one minute (the same applies for the module that has the same IP address).

Section 8.2
Debugging Ethernet Modules

About this Section

This section describes the debugging options for TSX ETY 4103, TSX ETY PORT, TSX WMY 100, and TSX ETY 5103 Ethernet modules.

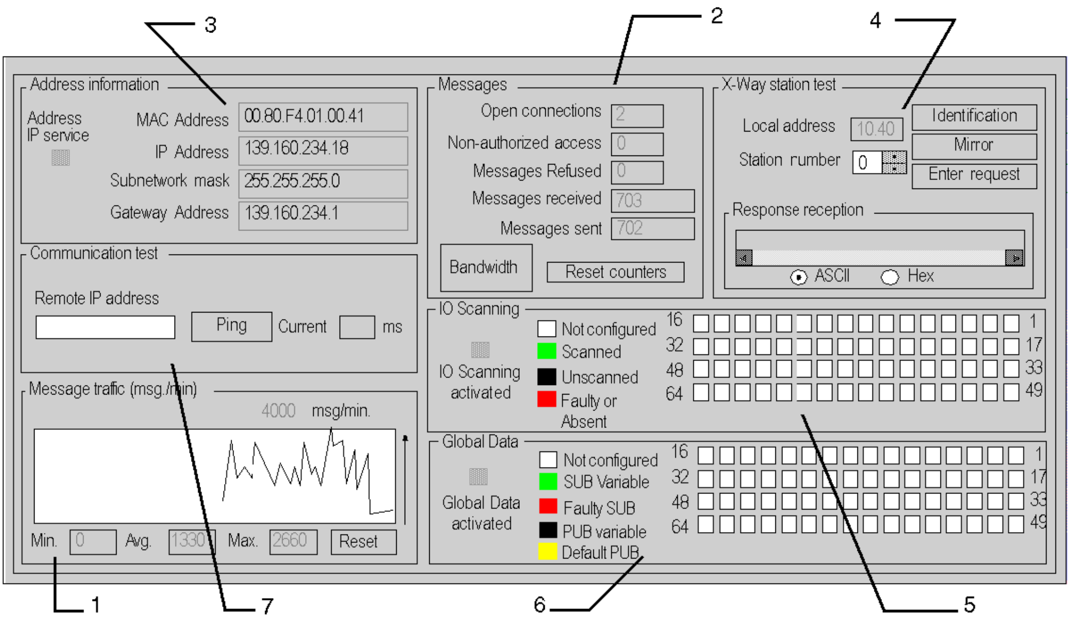
What Is in This Section?

This section contains the following topics:

Module Debugging Screen

Figure

The eight-zone debugging screen is dedicated to Ethernet communications:



Elements and Functions

This table describes the different zones that make up the debugging screen:

Number	Zone	Function
1	Message traffic	Allows the graphical display of the number of messages processed by the module
2	Messages	Allows you to view the number of connections and unacknowledged or rejected messages. The counter values can be reset using the **Reset Counters** button. A **Bandwidth** button is used to access bandwidth diagnostics.
3	Address information	Allows: ● display of TCP/IP services configuration ● communication testing of the TCP/IP profile
4	X-Way station test	Allows UNI-TE communication testing on the TCP/IP profile
5	IO Scanning	Allows display of the status for each remote input/output module
6	Global Data	Allows display of the status for Global Data variables
7	Communication test	Performs a communication test

General Debugging Parameters

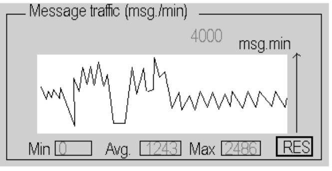
Introduction

The general debugging parameters are grouped together in two windows:

- the **Message traffic** window
- the **Messages** window

Message Traffic

The window is displayed as below:

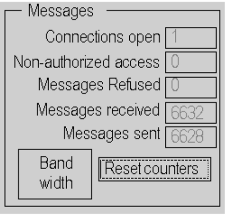


It indicates graphically the number of messages per minute processed by the module (send and receive). For better display, the scale automatically adapts to the flow rate.

The **Reset** button resets the three counters **Min.**, **Av.** and **Max.** to zero.

Messages

The window is displayed as below:



This window relates to TCP/IP messaging, and displays:

- the number of connections opened
- the number of unauthorized accesses
- the number of messages refused, received, and sent

To reset the counters to zero, simply click on the **Reset counter** button. To view the bandwidth status click on the **Bandwidth** button.

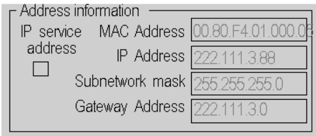
Debugging TCP/IP Parameters

Introduction

The debugging parameters for the TCP/IP services are grouped together in two windows:
- the **Address information** window
- the **Communication test** window

Address Information

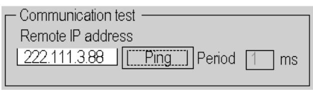
The window is displayed as below:



It specifies the following IP address configuration data:
- the MAC address, which is unique fixed address for a module
- the IP address
- the subnetwork mask
- the gateway address

Communication Test

Once the **Ping** button has been pressed, the window is displayed as follows:



This window is used to test IP communication towards another station.

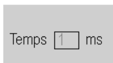
Testing TCP/IP Communications with the Ping Request

Introduction

This topic discusses indicates the procedure for testing TCP/IP communication with a **Ping** request.

Procedure

To send the Ping request to test the correct routing of information between two devices:

Step	Action
1	From the main screen, click the **Ping** button.
2	Enter the address of the station to be queried using the **Remote IP address** field.
3	Press the **Ping** button. The response appears in the **Time** field.  The returned time corresponds to the time it takes the message to be sent and return in ms.

Response Type

The following table groups together the various types of possible responses to the Ping request.

If the response is	then
positive	The windows records the time it takes the message to be sent and return in ms. A window appears with the message **Exchange successful**.
negative	A window with the message **Exchange incorrect** specifies that the remote device was not reached in the network architecture.

Communication Channel Testing

Introduction

This topic discusses the different possibilities for testing a communication channel from the debugging screen. Remember:

- Sending a request to an unconnected station results in an error message.
- The test applies to stations belonging to the same local area network.

Available Requests

The **X-Way station test** window allows the following requests:

- **Identification**: Prompts the Identification request to be sent to the designated remote station.
- **Mirror**: Allows a mirror request to be sent to the designated station. Selecting this function gives access to a screen that allows you to select the length of the character string to be sent (a maximum of 80 characters). The PLC then sends this character string (ABCD...) to the destination device. This device automatically returns the string of characters received to the sender.
- **Request input**: Allows a UNI-TE request, other than those provided by the command buttons, to be sent to the designated station. If this function is chosen, a screen appears allowing you to select the parameters specific to the request (the request code must be coded in hexadecimal).

NOTE: The first two requests are sent to the UNITE server of the TSX ETY module. The third is sent to the server of the processor.

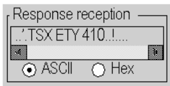
Testing Communication Channels with the Identification and Mirror Requests

Introduction

This topic discusses the procedure for testing a communication channel using the Identification and Mirror requests.

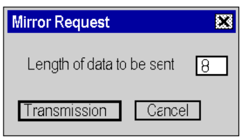
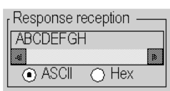
Identifying a Station

To identify a designated station:

Step	Actions
1	Select the address of the station to be queried using the **Station number** field.
2	Press the **Identification** button. The response appears in the **Receive Response** field. 

Sending the Mirror Request

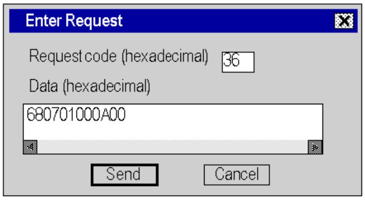
To send the Mirror request to test the correct routing of information between two devices:

Step	Action
1	Select the address of the station to be queried using the **Station** field.
2	Press the **Mirror** button. The following window appears. 
3	Enter the length of the data to be sent (maximum 80 characters).
4	Press the **Send** button. The response appears in the **Receive Response** field.  The response contains the character string ABCDEFGH corresponding to a length of data sent of 8.

Testing a Channel with Requests

Sending a Request

You can test a communication channel from the debugging screen through different requests.. The following procedure allows a request, other than those provided by the command buttons, to be sent to a designated station. In this example, the request sent is used to read 10 words (from %MW1 to %MW10).

Step	Action
1	Select the address of the station to be interrogated with the help of the field **Station**.
2	Click the **Input Request** button. The following window appears.  The data sent in this example is coded on 6 bytes.
3	Input the function code (coded in hexadecimal on one byte), corresponding to the request that you want to send. For this example the read request code is 16#36.
4	Input the data to be sent by coding all the data in hexadecimal. The data is sent non-stop without any time intervals between them. When the data is coded on one word, the most significant and least significant bytes are reversed. For this example the data is as follows: ● 16#68: on one byte, defines the segment (internal data) ● 16#07: on one byte, defines the object type (words) ● 16#0100: on one byte, defines the first word to read ● 16#0A00: on one byte, defines the number of words to read
5	Click the **Send** button. The response appears in the **Receive Response** window.  The response from the example has data on 21 bytes: ● 16#07: corresponds to object type (words) ● 16#00C2: corresponds to the value of the first word (the most significant and least significant bytes are reversed, its value is 16#C200) ● ...

I/O Scanning Debugging Parameters

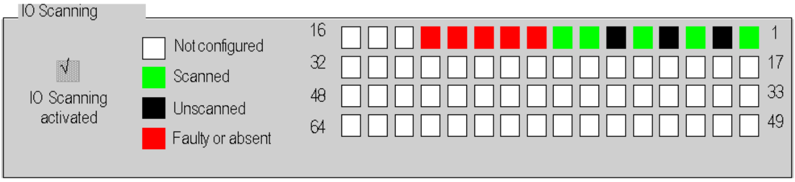
Introduction

When I/O scanning is activated, the status of each configured device is displayed on the screen.

NOTE: There is no I/O scanning for the TSX WMY 100.

I/O Scanning Dialog

The window is displayed as below:



A device referenced in the I/O scanning configuration tab can have the following states:

- **Scanned**: green
- **Not configured**: white
- **Unscanned**: black (caused by I/O scanning not being activated, none selected in configuration)
- **Faulty or absent**: red

NOTE: In the cases of **Not configured** and **Unscanned**, no Modbus request is generated towards the device.

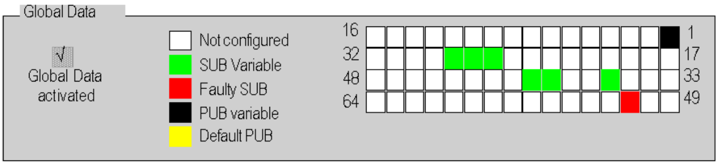
Global Data Debugging Parameters

Introduction

When Global Data is activated, the status of a Global Data variable is displayed on the screen.

Global Data

The window is displayed as below:



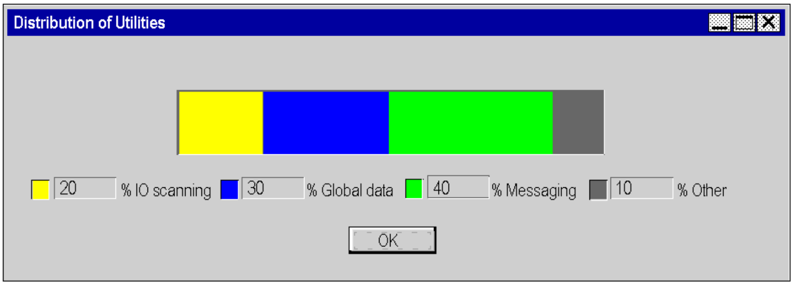
A Global Data variable can have the following status:

- **Not configured**: white
- **SUB variable**: subscribed variable received in the health timeout limit, green
- **Faulty SUB**: subscribed variable not received in the health time out limit, red
- **PUB variable**: published variable, green
- **Default PUB**: published variable not updated within the allotted period, yellow

Bandwidth Control Diagnostic Parameters

Bandwidth Control Window

When bandwidth control is activated, the load of module TSX ETY 4103/PORT/5103 is displayed on the screen:



This graphic displays the actual load distribution, between I/O Scanning, Global Data, Messaging and other services:

- %IO Scanning (yellow)
- % Global Data (blue)
- % Messaging: (green)
- % Other: (gray)

If you wish to modify this distribution, return to configuration *(see page 314)*.

Section 8.3
Ethernet Module Configuration

About this Section

This section describes the implementation of TSX ETY 4103, TSX ETY PORT, TSX WMY 100, and TSX ETY 5103 modules during configuration.

What Is in This Section?

This section contains the following topics:

Module Configuration Screen

Configuring an Ethernet Network

Use the two-zone Ethernet network configuration screen to declare the communication channel and to configure the necessary parameters for an Ethernet link.

Elements and Functions

This table describes the various zones that make up the configuration screen:

Zone	Area	Function
common	Header	Common part of the Ethernet communication configuration screens. This part enables you to choose the network family to be configured. When the network is associated with a module, the module address appears in the **Module address** zone.
specific	Module Services	Allows selection of the services used by the module
	IP Module Address	Displays the module address
	Security tab	Allows enabling and disabling of FTP, TFTP, and HTTP *(see page 293)*.
	IP Configuration tab	Enables the configuration of TCP/IP services *(see page 148)*
	Messaging tab	Allows the configuration of Access Control for the module.
	IO Scanning tab	Allows configuration of I/O Scanning *(see page 156)*
	Global Data tab	Allows configuration of Global Data *(see page 199)*
	SNMP tab	Allows configuration of SNMP *(see page 195)*
	Address Server tab	Allows configuration of the address server *(see page 192)*
	Bandwidth tab	Allows you to check that the services configured are compatible with the processing capacity of the Ethernet channel *(see page 314)*
	NTP tab	Allows configuration of Time Service *(see page 204)*
	Mail Service web page	Allows configuration of Mail Service *(see page 212)*

NOTE: In the Control Expert software, the TSX WMY 100 module is set in the TCP/IP Regular Network family, although it belongs to the TCP/IP FactoryCast network family. So, the services listed above (I/O scanning, Global Data, address server, Bandwidth monitoring) are not supported by the module. However, they can be selected in the TCP/IP regular network configuration in Control Expert. (Even if they are configured, those services won't work with the module.)

Type of Communication According to Connection Configuration

Introduction

Depending on the connection configuration of the TSX ETY 4103/PORT/5103 module, you can carry out messaging:

- in mono-connection
- in multi-connection

There is more information at Connection Configuration Parameters *(see page 153)*.

According to the type of protocol and access control management, multi-connection mode requires a specific configuration of the correspondence table.

NOTE: In the following, only examples of multi-connection will be dealt with. Furthermore, the emphasis is placed on communication between the module and a remote PC device containing several applications.

Configuration Rules

Several connections can be configured with the same IP address. They must be defined with the same protocol, the same access rights, and the same connection mode.

In the case of a Modbus connection, only two connections can be configured with the same IP address. Addresses associated with these connections are:

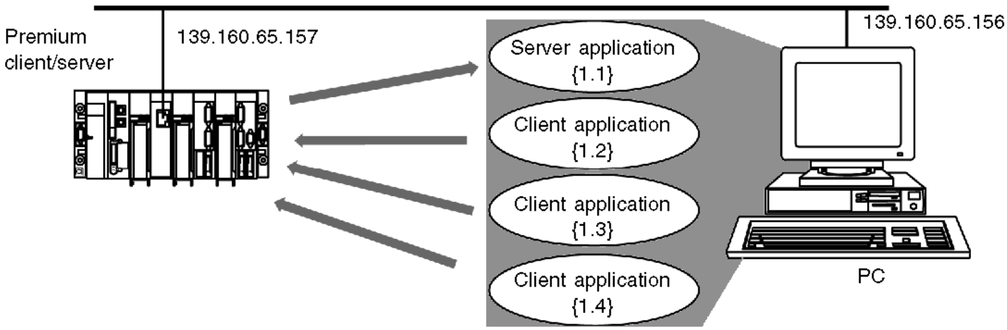
- an X-Way address (for example: {2.103}) for the Modbus client connection
- an X-Way address equal to {x.x} for Modbus server connections

Multi-Connection in UNI-TE Protocol with Access Management

In this example, the PC contains four applications with a unique X-Way address and one single IP address:

- The module opens a connection and communicates with the server application with the address {1.1}.
- Each of the other client applications with the address {1.2}, {1.3}, {1.4} is authorized to open a connection and communicate with the module.

Exchanges are carried out according to the UNI-TE protocol and the module's access control utility is enabled.



In order to implement this example, you must:

- activate connection management by checking the module's **Access control** box
- configure communication from the module to the PC's server application in the table:
  - **X-Way address**: 1.1
  - **IP address**: 139.160.65.156
  - **Protocol**: UNI-TE
  - **Access**: authorized (cell checked)
  - **Mode**: Multi
- configure communication of each of the PC's client applications to the server module in the table:
  - **X-Way address**: 1.2 and 1.3 and 1.4
  - **IP address**: 139.160.65.156
  - **Protocol**: UNI-TE
  - **Access**: authorized (cell checked)
  - **Mode**: Multi

Multi-Connection in UNI-TE Protocol without Access Management

This example is the same as the previous one, except that access control is not configured.

In this case, if the application {1.1} is the only server application, the module's correspondence table only contains the following line:

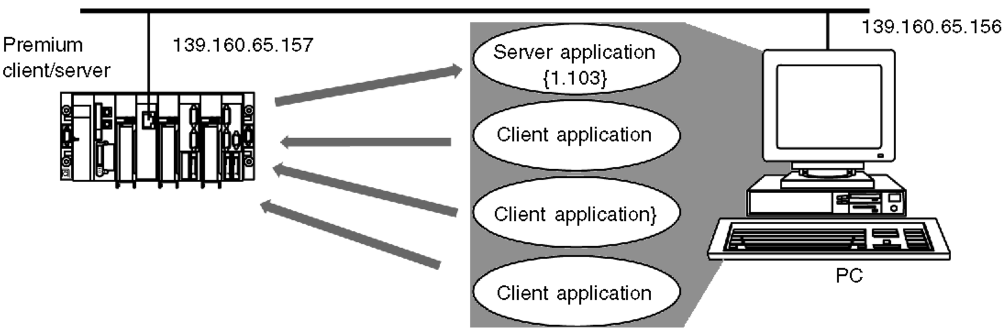
- **X-Way address**: 1.1
- **IP address**: 139.160.65.156
- **Protocol**: UNI-TE
- **Access**: the cell is grayed out
- **Mode**: Multi

Multi-Connection in Modbus Protocol with Access Management

In this example, the PC contains four applications. The server application has an imaginary X-Way address and the other client applications do not need an X-Way address:

- The module opens a connection and communicates with the server application with the imaginary address {1.103}.
- Each of the client applications has no address but is authorized to open a connection and communicates with the module.

Exchanges are carried out according to the Modbus protocol and the module's access control utility is enabled.



In order to implement this example, you must:

- activate connection management by checking the module's **Access control** box
- configure communication from the module to the PC's server application in the table:
  - **X-Way address**: 1.103 (address between 100 and 163)
  - **IP address**: 139.160.65.156
  - **Protocol**: Modbus
  - **Access**: the cell is grayed out
  - **Mode**: Multi
- configure communication of all the PC's client applications to the server module in the table:
  - **X-Way address**: x.x (this address allows you to specify that other applications exist for the same IP address)
  - **IP address**: 139.160.65.156
  - **Protocol**: Modbus
  - **Access**: authorized (allows you to specify that other applications are authorized to connect and communicate)
  - **Mode**: Multi

NOTE:
If you want to prevent connection by client applications you must configure:

- **X-Way address**: x.x (this address allows you to specify that other applications exist for the same IP address)
- **IP address**: 139.160.65.156
- **Protocol**: Modbus
- **Access**: not authorized (cell unchecked)
- **Mode**: Multi

NOTE: When using Modbus protocol and Access Control, it is necessary to configure the Xway address of each device that will be polling the unit (the IP of the client) as 255.255 in the Connection Configuration field of the Messaging dialog.

Multi-Connection in Modbus Protocol without Access Management

This example is the same as the previous one, except that access control is not configured.

In this case, if the application {1,103} is the only server application, the module's correspondence table only contains the following line:

- **X-Way address**: 1.103
- **IP address**: 139.160.65.156
- **Protocol**: Modbus
- **Access**: the cell is grayed out
- **Mode**: Multi

Security (Enable / Disable HTTP, FTP, and TFTP)

Security and HTTP, FTP, and TFTP Services

You can enhance security for your project by disabling the FTP/TFTP and HTTP services at times when you do not need to use them. The module uses the HTTP service to provide access to the embedded Web pages. The module uses the FTP and TFTP services to support various features including firmware upgrades, and FDR services.

The module's HTTP, FTP, and TFTP services can be disabled or enabled using the Control Expert **Network Editor → Security** screen.

On power up, these services are:

- disabled by default in projects created using Unity Pro 8.1 or later and one of the following modules:
  - TSX P57 1634M, firmware version 5.70 or later
  - TSX P57 2634M, firmware version 5.70 or later
  - TSX P57 3634M, firmware version 5.70 or later
  - TSX ETY 4103, firmware version 5.70 or later
  - TSX ETY 5103, firmware version 5.90 or later
- enabled by default in projects where:
  - the project was created using Unity Pro 8.0 or earlier, or
  - the communication module is not configured

You can use Control Expert to enable or disable HTTP, FTP, and TFTP services as described in the following procedure.

If the HTTP, FTP, or TFTP services have been enabled with Control Expert, they can also be enabled or disabled at run time using the DATA_EXCH block. (See the *Communication Block Library* for Control Expert.

Using Control Expert to Enable and Disable Firmware Upgrade, FDR, and Web Access Services

Perform the following steps to enable or disable FTP/TFTP or HTTP services on the module.

Step	Action
1	In the Control Expert **Project Browser → Structural View**, double-click the desired Ethernet network in the **Communication → Networks** directory to open the **Network Editor**.
2	Click the **Security** tab.
3	On the **Security** screen, choose the appropriate setting: (**Enabled** or **Disabled**) for the service or services.

The edits will take effect when they are successfully downloaded from your PC to the CPU and from the CPU to the communication modules and network devices.

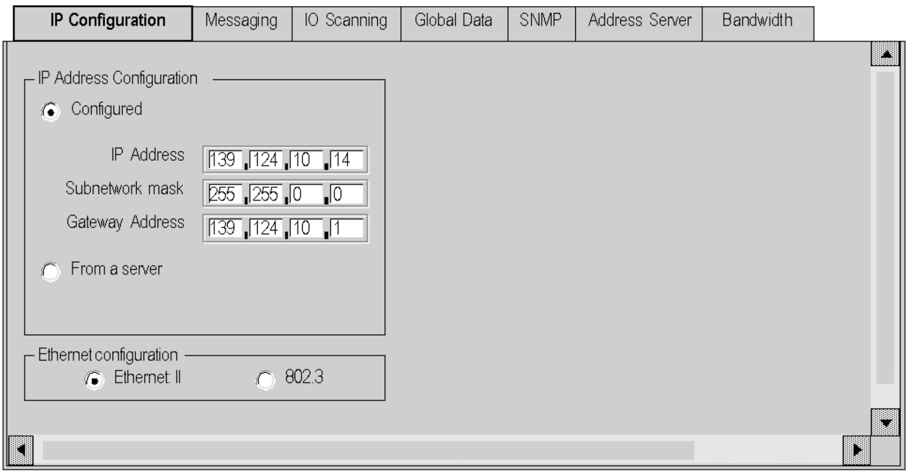
Configuration of TCP/IP Messaging

Introduction

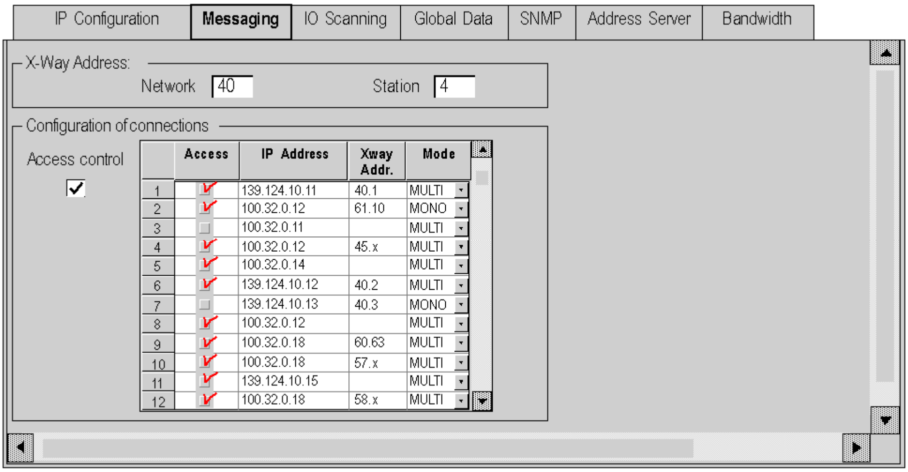
In order to use the TSX ETY 4103/5103 module to communicate on Ethernet, it is necessary to set the *Configuration Parameters Linked to the TCP/IP Service,* *page 149*.

Access Messaging

Messaging is configured in the two windows accessible by the tabs: **IP Configuration** and **Messaging**.To access configuration parameters for TCP/IP services:

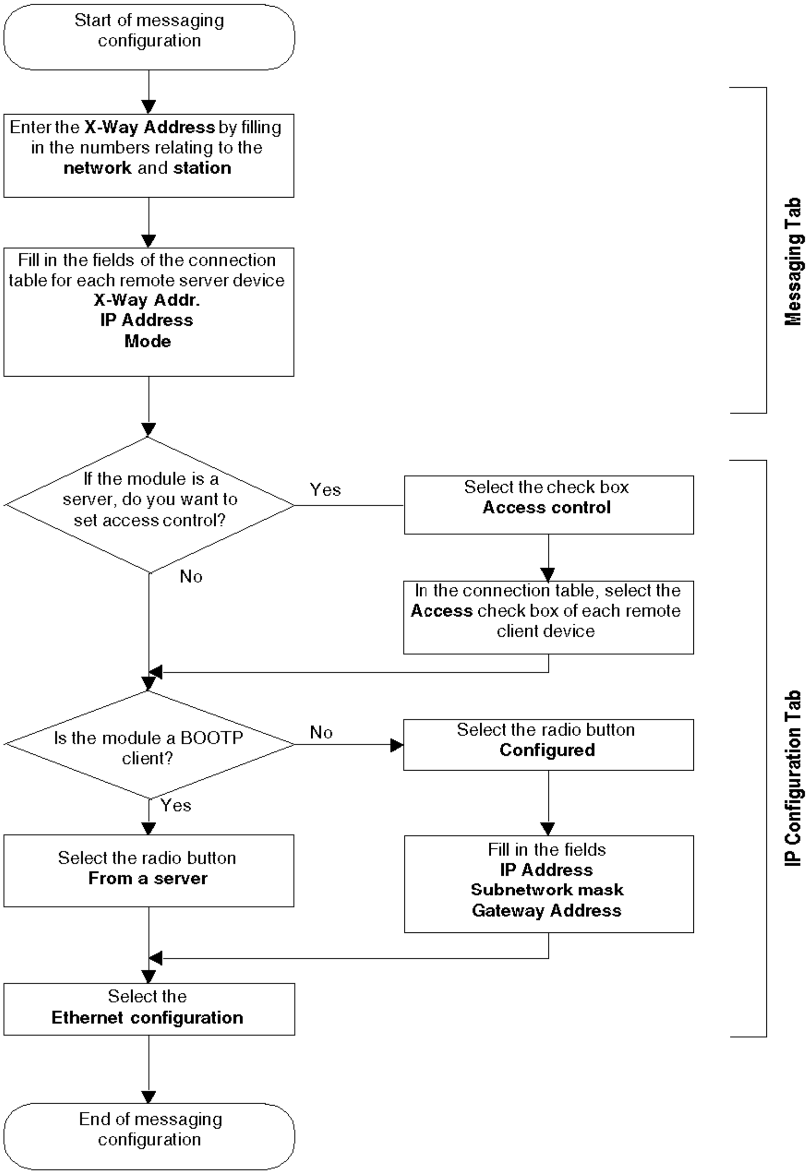
Step	Action
1	Access the module configuration screen.
2	Select the **IP Configuration** tab: 

Step	Action
3	Select the **Messaging** tab:



Configure Messaging

The following procedure gives the configuration principle.



I/O Scanning Configuration

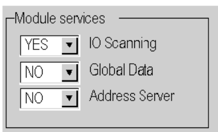
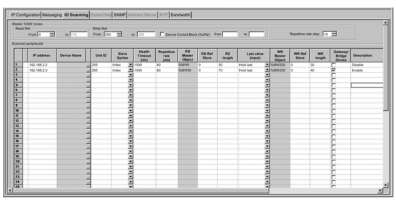
Introduction

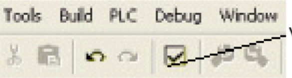
In order to use the TSX ETY 4103/5103 modules and the TSX P57 1634/2634/3634 CPUs to control remote I/Os, it is necessary to set the **I/O Scanning** configuration parameters *(see Premium and Atrium using EcoStruxure™ Control Expert, Asynchronous Serial Link, User Manual)*.

The **I/O scanning** service is used to:
- transfer data between network devices
- allow a CPU to regularly read data from and write data to scanned devices

Accessing I/O Scanning

The following procedure accesses configuration parameters for I/O scanning:

Step	Action
1	Open Control Expert on your PC.
2	Configure or open an application using one of the modules or CPUs mentioned above.
3	In the **Project Browser**, open **Communication** → **Networks**.
4	Select an Ethernet device to access the device IP configuration screen.
5	In the **Module services** dialog, select **YES** for **IO Scanning**:  **Result**: The **IO Scanning** tab is enabled (no longer grayed out).
6	Select the **IO Scanning** tab: 
7	Enter the parameter settings in each column as described in the following I/O Scanning Parameters topic *(see page 298)*.

Step	Action
8	Select the validate check box in the upper tool bar to confirm the I/O scanning parameter settings: 

Configuring I/O Scanning

Follow these steps to configure I/O Scanning:.

Step	Action
1	Only use this step if you are configuring an ETY module. For CPUs, go directly to step 2. Set the address of the beginning of the internal words (in the application memory), which are dedicated to I/O scanning: ● **Read** zone ● **Write** zone
2	For each device, enter the **IP Address**.
3	To configure a device (Advantys island or DTM), click the **...** button to open the **Property** box *(see page 183)* to start the device configuration software. For an introduction to this procedure for Advantys, click here *(see page 173)*. **NOTE:** While the **Property** box is open, **I/O scanning** cannot be edited.
4	Enter the **Unit ID** Modbus slave address for each device, if necessary.
5	Enter a **Health Timeout** value in ms, if required.
6	Enter the **repetition periods** of the remote device (scanning period of the slave).
7	Only use this step if you are configuring a CPU. For ETY modules go directly to step 8. For each device, enter the address of the master PLC variables in the **RD Master Object**.
8	For each device, enter the address of the variables read in each slave **Slave Ref. (read)**. Choose the syntax of this value using the **Slave Syntax** for this line.
9	For each device, enter the number of words to be sent in read format in **Length (read)**.
10	Select the input fallback mode in **Fallback value (read)**.
11	Only use this step if you are configuring a CPU, for ETY modules go directly to step 12. For each device, enter the address of the master PLC variables in the **WR Master Object**.
12	For each device, enter the address of the variables written in each slave **Slave Ref. (write)**.

Step	Action
13	For each device, enter the number of words to be sent in write format in **Length (write)**.
14	To allow slower TCP/IP network devices (i.e., gateways and bridges) to be compatible with the I/O scanner: ● Select the check box in the **Gateway/Bridge Device** column to enable this feature. Defines a new bit, and sets it to high (1). ● Deselect the check box in the **Gateway/Bridge Device** column to disable this feature (default). Defines a new bit, and sets it to zero (0).
15	For each device enter, if necessary, a comment in **Description**.

Configuring a Specific Read and Write Scenario

When scanned, certain devices, such as TSX ETY modules, do not support simultaneous read/write requests. In this case, to read/write inputs/outputs, the following procedure must be performed:

Step	Action
1	Enter the **IP address** of the device.
2	If necessary, enter the device’s **Unit ID** Modbus slave address.
3	Select the scanning period of the slave.
4	Enter the address of the read variables of the slave **Slave Ref. (read)**.
5	Enter the number of words to be sent in read format in **Length (read)**.
6	Enter **0** in **Slave Ref. (write)** (if the **Slave Syntax** is set to **Index**).
7	Enter **0** in **Length (write)**.
8	On the following line, enter the same **IP address**.
9	Enter the same **Unit ID** Modbus slave address, if necessary.
10	Select the same period.
11	Enter **0** in **Slave Ref. (read)** (if the **Slave Syntax** is set to **Index**).
12	Enter **0** in **Length (read)**.
13	Enter the write destination address in **Slave Ref. (write)**.
14	Enter the number of words to be sent in read format in **Length (write)**.

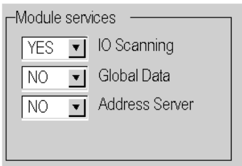
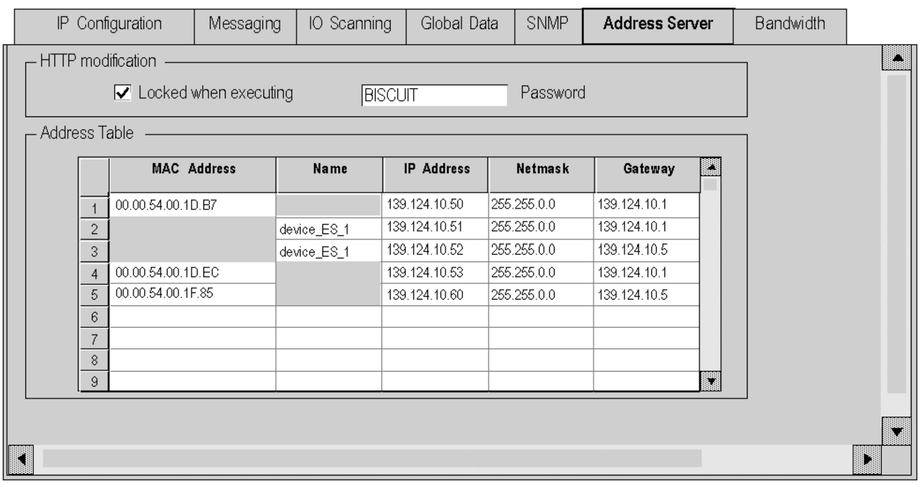
Address Server Configuration

Introduction

In order to use the TSX ETY 4103/PORT/5103 module as an address server, it is necessary to set the configuration parameters of the address server *(see page 192)*.

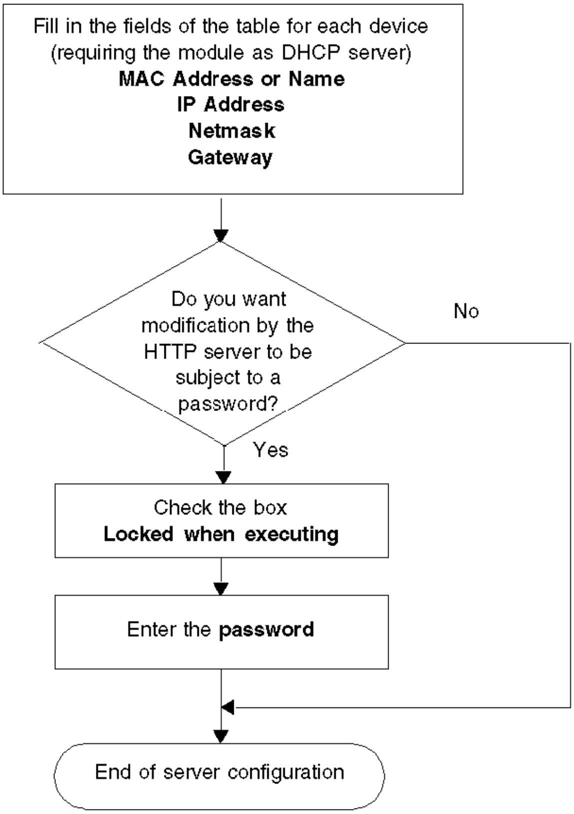
Accessing the Address Server

To access the configuration parameters of the address server:

Step	Action
1	Access the module configuration screen.
2	In the **Module utilities** zone, select the **Address Server** check-box:  The **Address Server** tab is no longer grayed out.
3	Select the **Address Server** tab: 
4	Fill in all the fields with information on the devices. **Note**: The MAC address is coded on 6 bytes and is of the form: 00 00 54 F6 E3 2F.

How to Configure the Server

The following procedure gives the server configuration principle.



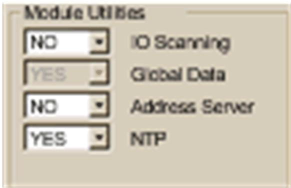
Configuring Global Data

Introduction

In order to use the TXS ETY 4103/PORT/5103 module to use Global Data, it is necessary to set the configuration parameters *(see page 200)*.

Access the Global Data

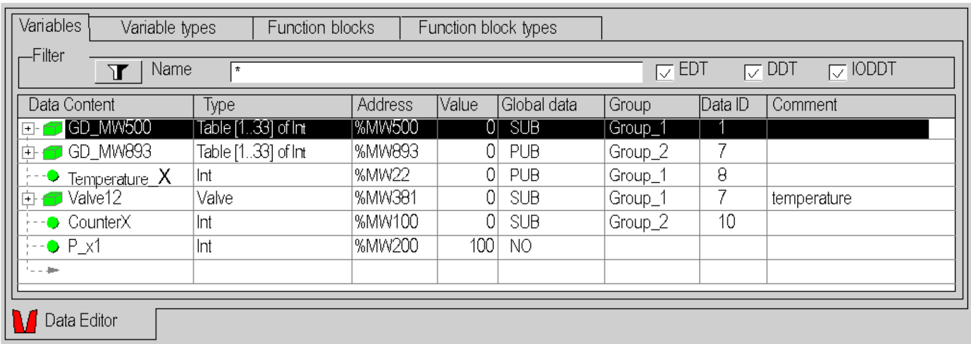
To set Global Data:

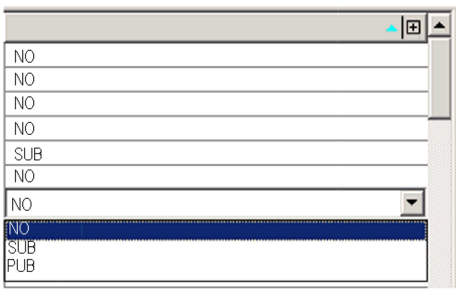
Step	Action
1	Access the module configuration screen.
2	In the Module utilities zone, select the **Global Data** check box:  The **Global Data** tab is no longer grayed out.
3	Select the **Global Data** tab: 

NOTE: The **IGMP** and **None** features are available only in Unity 4.1 or later.

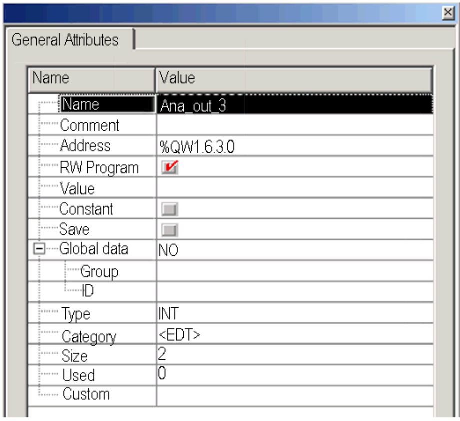
Table of Variables

To configure the Global Data variables, you must use the Control Expert **variable editor**:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Go to the Control Expert variable editor:


</td></tr>
<tr><td>2</td><td>For each Global Data variable, define whether it is published (PUB) or subscribed (SUB) in the Global data field. To do this, double click the Global data column for the variable you want to define, and then select an option from the menu, as shown below.


</td></tr>
</table>

Step	Action
3	Click the column for each variable that you want to configure, and then right click the column to display the **Data Properties** box for the variable you selected. In the **Name** column, expand **Global data**. 
4	Give the Global Data group a name in the **Group** field.
5	Fill in the **ID** field: identifier of a remote station in a distribution group.

NOTE: The Global data column in the variable editor does not display by default. If the Global data column is not visible when you open the variable editor, right click in any column in the editor, and select **Customize Column...** When the **Column Configuration** dialog box appears, select the check box next to **Global data**, then click **OK**. The Global data column is now visible in the variable editor.

Configuring Global Data

To configure Global Data, follow these steps in the **Global data configuration** zone:

Step	Action
1	Indicate the Distribution **Group Address** to which the station belongs, between 224.0.0.0 and 239.255.255.255.
2	Adjust the **Distribution Period** to between 1 and 50 PLC cycles.
3	Fill in the **group name** defined in the Control Expert data editor (see above).
4	Select which multicast protocol *(see page 106)* you require: ● None ● GMRP ● IGMP
5	Define the **Health time out**. This value can be adjusted from 50 to 15000 ms (in increments of 50 ms).

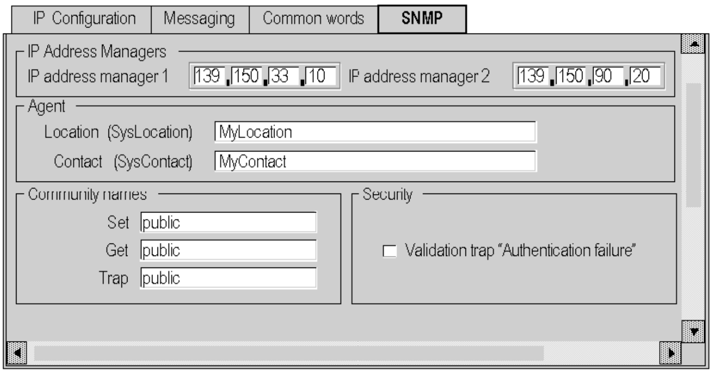
SNMP Configuration

Introduction

In order to use the TSX ETY 4103/PORT/5103 module as an SNMP agent, it is necessary to adjust the configuration parameters of SNMP *(see page 195)*.

Accessing SNMP

To access configuration parameters for SNMP:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Access the module configuration screen.</td></tr>
<tr><td>2</td><td>Select the SNMP tab:

</td></tr>
</table>

Configuring SNMP

The following procedure gives the configuration principle for SNMP.

Step	Action
1	Enter the SNMP manager addresses: ● **Manager 1 IP addresses** ● **Manager 2 IP addresses**
2	Fill in the fields: ● **Location (SysLocation)** ● **Contact (SysLocation)**. Or alternatively check the **SNMP Manager** box to indicate that the information will be completed by the SNMP Manager.
3	If you want to set access rights, fill in the community names: ● **Set** ● **Get** ● **Trap**
4	If you want to activate transmission of an event to the module, check the **Activate "Authentication Failure" trap** box.

Configuring the Time Synchronization Service

Configuring the Time Service

You can configure the time service using either the module's NTP Configuration page in Control Expert or the embedded Web page.

Configurable Time Service Parameters

Configure or change the following parameters on the **NTP Configuration** page.

1. IP address of primary NTP server
   - Enter a valid IP address
2. IP address of secondary NTP server
   - Enter a valid IP address
3. Polling Period (in seconds)
   Enter a value
   - min = 1sec
   - max = 120sec
   - default = 5 sec
4. Time Zone
   - Select from drop-down menu
     Universal Time, Coordinated (GMT) = default
   - Custom time zone
5. Automatically adjust clock for daylight saving change
   - Parameter is selected by default (check mark appears) if daylight saving time is chosen.

Time Service Command Buttons

Execute the following commands:

Button	Description
Save	Stores new NTP (time service) configuration. Previous configuration is no longer valid.
Cancel	Cancels new NTP (time service) configuration. Previous configuration is valid.
Disable NTP	IP of Primary and Standby set = 0. NTP server not polled. Time in controller not updated.

Changing Time Service Parameters

To make any changes to the time synchronization service:

Step	Action
1	Enter changes in the appropriate field on the NTP Configuration page for one or all of the configurable parameters.
2	Click **Save**.

Important Information about the Time Service

NOTE: About the time service:
1. **Enable/Disable Daylight Savings Time parameter**: If the Enable/Disable check box is selected, the module automatically corrects the local time to account for daylight savings time. Therefore, no action is required, since the daylight saving time start and end are automatically changed each year.
2. **Polling Time Parameter**: The time (in seconds) is the time between time updates from the NTP server. The default is 5 seconds.
3. **Storing the Time Service Configuration**: The last time service configuration is saved internally in the Ethernet module.
4. **Replacing the Ethernet Module**: If the Ethernet module has to be replaced, the stored configuration is lost, and the system returns to the default configuration.

Customizing Time Zone Parameters

If you want a time zone not listed in the time zone table:

Step	Action	Comment
1	Write the text rules for the custom time zone.	
2	Using an FTP client, store your rules in the file: /FLASH0/wwwroot/conf/NTP/customrules user ID: ntpupdate password: ntpupdate	Root directory to store 'customrules' is set by the FTP server as: /FLASH0/wwwroot/conf/NTP
3	When the rules are written, choose the drop down menu on the **NTP Configuration** web page, and configure (or reboot) the module by selecting Time Zone = Custom	The NTP component looks for customrules, calls the tz compiler and generates a new file called 'tz_custom'. This file is binary file and should not be edited. If the tz compiler detects a syntax error in customrules, the error is logged in the file: /FLASH0/wwwroot/conf/NTP/error.log 1. NTP component is not launched 2. NTP Status field in diagnostic web page displays NOT OK.
4	If you want more information, the syntax to write those rules along with a few examples are found in the module in: /FLASH0/wwwroot/conf/NTP/instructions.txt	

Time Zone Parameters

Select a time zone from the drop-down menu.

Time Zone	Description	DST Available
Custom		Yes
(GMT-12:00)	Dateline Standard Time [Eniwetok Kwajalein]	No
(GMT-11:00)	Samoa Standard Time [Midway Is Samoa]	No
(GMT-10:00)	Hawaiian Standard Time [Hawaii Honolulu]	No
(GMT-09:00)	Alaskan Standard Time [Anchorage]	Yes
(GMT-08:00)	Pacific Standard Time [Los Angeles Tijuana]	Yes
(GMT-07:00)	Mexican Standard Time [Chihuahua La Paz Mazatlan]	Yes
(GMT-07:00)	Mountain Standard Time [Arizona Phoenix]	No
(GMT-07:00)	Mountain Standard Time [Denver]	Yes
(GMT-06:00)	Central Standard Time [Chicago]	Yes
(GMT-06:00)	Mexico Standard Time [Tegucigalpa]	No
(GMT-06:00)	Canada Central Standard Time [Saskatchewan Regina]	No
(GMT-06:00)	Central America Standard Time [Mexico_city]	Yes
(GMT-05:00)	SA Pacific Standard Time [Bogota Lima Quito]	No
(GMT-05:00)	Eastern Standard Time [New York]	Yes
(GMT-05:00)	Eastern Standard Time [Indiana (East)] [Indianapolis]	No
(GMT-04:00)	SA Western Standard Time [Caracas La Paz]	No
(GMT-04:00)	Pacific SA Standard Time [Santiago]	Yes
(GMT-03:30)	Newfoundland Standard Time [Newfoundland St Johns]	Yes
(GMT-03:00)	E. South America Standard Time [Brasilia Sao_Paulo]	Yes
(GMT-03:00)	SA Eastern Standard Time [Buenos Aires Georgetown]	No
(GMT-02:00)	Mid-Atlantic Standard Time [South_Georgia]	No
(GMT-01:00)	Azores Standard Time [Azores Cape Verde Island]	Yes
(GMT)	Universal Coordinated Time [Casablanca, Monrovia]	No
(GMT0)	Greenwich Mean Time [Dublin Edinburgh Lisbon London]	Yes
(GMT+01:00)	Romance Standard Time [Amsterdam CopenHagen Madrid Paris Vilnius]	Yes
(GMT+01:00)	Central European Standard Time [Belgrade Sarajevo Skopje Sofija Zagreb]	Yes
(GMT+01:00)	Central Europe Standard Time [Bratislava Budapest Ljubljana Prague Warsaw]	Yes
(GMT+01:00)	W. Europe Standard Time [Brussels Berlin Bern Rome Stockholm Vienna]	Yes
(GMT+02:00)	GTB Standard Time [Athens Istanbul Minsk]	Yes
(GMT+02:00)	E. Europe Standard Time [Bucharest]	Yes

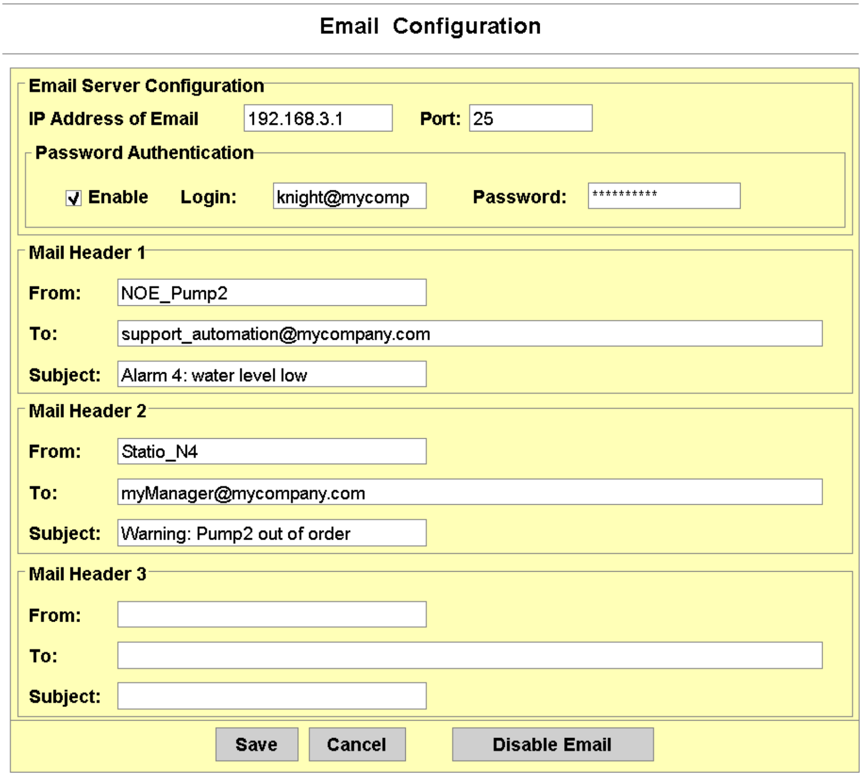
Time Zone	Description	DST Available
(GMT+02:00)	Egypt Standard Time [Cairo]	Yes
(GMT+02:00)	South Africa Standard Time [Johannesburg Harare Pretoria]	No
(GMT+02:00)	FLE Standard Time [Helsinki Riga Tallinn]	Yes
(GMT+02:00)	Israel Standard Time [Israel Jerusalem]	Yes
(GMT+03:00)	Arabic Standard Time [Baghdad]	Yes
(GMT+03:00)	Arab Standard Time [Kuwait Riyadh]	No
(GMT+03:00)	Russian Standard Time [Moscow St. Petersburg Volgograd]	Yes
(GMT+03:00)	E. Africa Standard Time [Nairobi]	No
(GMT+03:30)	Iran Standard Time [Tehran]	Yes
(GMT+04:00)	Arabian Standard Time [Abu Dhabi Muscat]	No
(GMT+04:00)	Caucasus Standard Time [Baku Tbilisi]	Yes
(GMT+04:00)	Afghanistan Standard Time [Kabul]	No
(GMT+05:00)	Ekaterinburg Standard Time [Ekaterinburg]	Yes
(GMT+05:00)	West Asia Standard Time [Islamabad Karachi Tashkent]	No
(GMT+05:30)	India Standard Time [Bombay Calcutta Madras New Delhi]	No
(GMT+06:00)	Central Asia Standard Time [Almaty Dhaka]	Yes
(GMT+06:00)	Sri Lanka Standard Time [Columbo]	No
(GMT+07:00)	SE Asia Standard Time [Bangkok Hanoi Jakarta]	No
(GMT+08:00)	China Standard Time [Beijing Chongqing Hong Kong Urumqi]	No
(GMT+08:00)	W. Australia Standard Time [Perth]	No
(GMT+08:00)	Singapore Standard Time [Singapore]	No
(GMT+08:00)	Taipei Standard Time [Taipei]	No
(GMT+09:00)	Tokyo Standard Time [Osako Sapporo Tokyo]	No
(GMT+09:00)	Korea Standard Time [Seoul]	No
(GMT+09:00)	Yakutsk Standard Time [Yakutsk]	Yes
(GMT+09:30)	Cen. Australia Standard Time [Adelaide]	Yes
(GMT+09:30)	AUS Central Standard Time [Darwin]	No
(GMT+10:00)	E. Australia Standard Time [Brisbane]	No
(GMT+10:00)	AUS Eastern Standard Time [Canberra Melbourne Sydney]	Yes
(GMT+10:00)	West Pacific Standard Time [Guam Port Moresby]	No
(GMT+10:00)	Tasmania Standard Time [Hobart]	Yes
(GMT+10:00)	Vladivostok Standard Time [Vladivostok]	Yes
(GMT+11:00)	Central Pacific Standard Time [Magadan Solomon Is New Caledonia]	Yes

Time Zone	Description	DST Available
(GMT+12:00)	New Zealand Standard Time [Auckland Wellington]	Yes
(GMT+12:00)	Fiji Standard Time [Fiji Kamchatka Marshall Is]	No

Mail Service Configuration

Configuring the Mail Service with the Email Configuration Page

Use the module's embedded Web page to configure the Electronic Mail Notification service. No other method is available.



Mail Service Command Buttons

Button	Description
Save	Saves the new Email configuration. **Note**: The previous configuration is no longer valid and it is not stored.
Cancel	Cancels the entries in the fields. The previous configuration is valid.
Disable Email	Clears the stored configuration, and disables the email service. **Note**: The next time the service is enabled, a new configuration is required.

Configurable Mail Service Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>IP address of Email</td><td>Enter a valid IP address. (This parameter identifies the SMTP server.)</td></tr>
<tr><td>Port</td><td>Default = 25 (If necessary, you may enter a new value.)</td></tr>
<tr><td>Password Authentication</td><td>If you want to restrict access, enable Password Authentication by entering a check mark in the box.
Enter values for:
● Login:
❍ Any printable character allowed
❍ 64 character maximum
● Password:
❍ Any printable character allowed
❍ 64 character maximum</td></tr>
<tr><td>3 mail headers</td><td>Each header contains:
● sender’s ID in the From: field
❍ 32 character maximum; no spaces
● list of recipients in the To: field
❍ Separate each email address with a comma.
❍ 128 character maximum
● fixed part of message in the Subject: field
❍ (32 character maximum)</td></tr>
<tr><td colspan="2">The Subject field consists of two parts:
1. Fixed (32 character maximum)
2. Dynamic (206 character maximum)</td></tr>
</table>

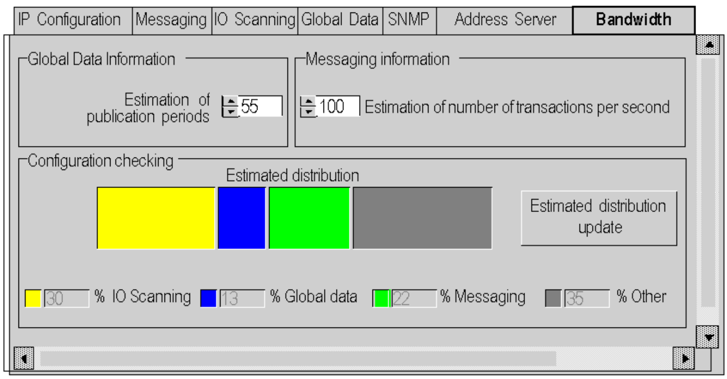
Bandwidth Checking

Introduction

The TSX ETY 4103/PORT/5103 module offers a utility for checking the bandwidth used.

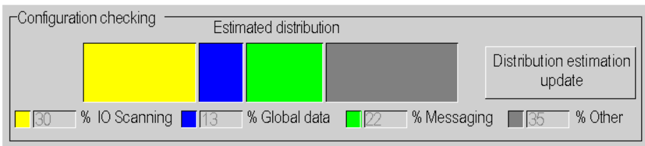
Accessing Bandwitdh Checking

The procedure for accessing the configuration parameters of bandwidth checking is as follows.

Step	Action
1	Access the module configuration screen.
2	Select the **Bandwidth** tab: 

Using Bandwidth Checking

To use Bandwidth checking, proceed in the following way:

Step	Action
1	Once you have configured I/O scanning and Global Data, enter the estimated number of transactions per second in the **Messaging data** zone.
2	In the **Global Data information** zone, indicate the **estimated publication periods**. The value entered must be the estimated average publication frequency of the distribution group stations (local and remote stations). **Example**: Your application publishes the variable 5 and subscribes variables 12 and 15, published by a PLC 1 and a PLC 2. Your publication is configured at 150 ms. PLC 1 publishes variable 12 every 100 ms. PLC 2 publishes variable 15 every 200 ms. The value to be entered is 150 ms: arithmetic mean (150+100+200)/3.
3	To view the bandwidth distribution estimation, click the **Update distribution estimation** button. 
4	If the module load overflows, the message **Module load cannot exceed 100%** appears. Repeat steps 1 to 3 to adjust the configuration parameters until the module load is correct.

Bridge Function Configuration

Bridge Communications

The TSX ETY 4103/PORT/5103 module can be used as an X-Way bridge station. This guarantees transparent communication between various networks.

NOTE: The installation of this function is described in the manual Communication Architecture and Services.

Chapter 9
Ethernet Coprocessor

About this Chapter

This chapter discusses the software installation of the Ethernet channel built in to the TSX P57 6634/5634/4634 processors.

What Is in This Chapter?

This chapter contains the following sections:

Section 9.1
Introduction to Ethernet Coprocessors

About this Section

This section describes the built-in Ethernet communications of coprocessors.

What Is in This Section?

This section contains the following topics:

Ethernet Communication Channels in Processors

Overview

The Ethernet communication channel built in to the processors concerns the following references:
- TSX P57 1634 M (ETY PORT)
- TSX P57 2634 M (ETY PORT)
- TSX P57 3634 M (ETY PORT)
- TSX P57 4634 M (Copro Premium)
- TSX P57 5634 M (Copro Premium)
- TSX P57 6634 M (Copro Premium)

The characteristics of the Ethernet channel of the first three processors (called **TSX ETY PORT** in the previous sections) are the same as those of the Ethernet channel of the module **TSX ETY 4103** *(see page 263)*.

Ethernet Channel for TSX P575634/4634

The Ethernet channel of the **TSX P57 6634/5634/4634** processor offers connection to a TCP/IP network supporting the UNI-TE and Modbus messaging services on a TCP/IP profile.

It also offers the following services:
- SNMP: allows the module and system to be monitored by one or two SNMP managers
- Address server: for clients on the local network
- I/O scanning: allows control of inputs/outputs on an Ethernet network
- HTTP server: allows information to be deployed via web pages
- Global Data: allows data to be auto-exchanged between PLCs
- Bandwidth monitoring: verifies the balance of resources used by the different services
- Replace Faulty Device: allows the client device configuration to be saved in the PLC module. In case of breakdown, a new client device can be restarted with the configuration parameters of the previous one.
- SMTP: enables a controller’s project to send e-mail messages

Characteristics of Ethernet Coprocessors (TSX P57 6634/5634/4634)

Maximum Capacity

The maximum Ethernet frame size depends on the type of transaction. The maximum frame size is:

- 256 bytes in synchronous messaging
- 1 Kbyte in asynchronous messaging

The Ethernet channel of the TSX P57 4634/5634/6634 can:

- manage 64 TCP connections using port 502 messaging
- scan up to a maximum of 128 devices using I/O scanning
- be the address server for a maximum of 128 devices

The processor is used:

- for X-Way synchronous messaging on TCP/IP (UNI-TE server):
  - 800 messages per second
- in the case of asynchronous X-Way messaging on TCP/IP:
  - between 600 and 1200 messages per second (number varies depending on the size of the messages, the number of clients and the application execution time)

I/O Scanning

The Ethernet channel of the TSX P57 4634/5634/6634 can scan a maximum of 128 remote devices. For the same station, the application can process:

- a maximum total input volume to be scanned of 4K words
- a maximum total output volume to be scanned of 4K words

Global Data

The user interface is a PLC variable zone defined in configuration. The Ethernet port can:

- publish a variable of between 1 and 512 words
- subscribe between 1 and 64 variables (The total data cannot exceed 2 Kwords.)

Replace Faulty Equipment

The coprocessor reserves a 512 Kbytes zone for this function.

- Up to 128 remote devices can be configured in the DHCP address server.
- The 128 remote devices should share the 512 kb reserved for their parameters.

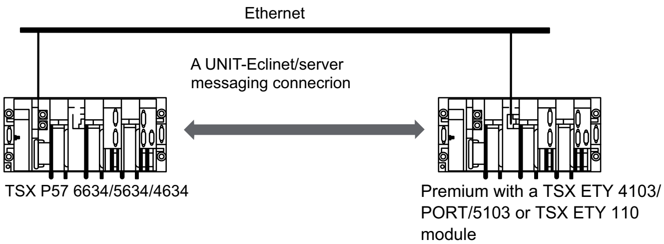
Type of Connections Supported

Overview

The Ethernet channel of the TSX P57 6634/5634/4634 authorizes a maximum of 16 HTTP connections in parallel and a maximum of 64 connections in parallel over TCP/IP.

Connection to Premium

Between two Premium PLCs using UNI-TE messaging on the TCP/IP profile, the channel of the TSX P57 6634/5634/4634 allows only one connection in client/server mode:

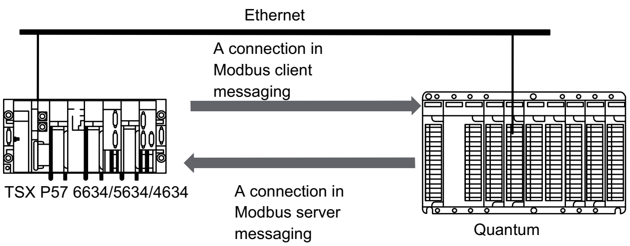


Connection to a Quantum

Between a Premium and a Quantum PLC using Modbus messaging on the TCP/IP profile, the Ethernet channel of the TSX P57 6634/5634/4634 allows a single connection in one of the following modes:

- Modbus client
- Modbus server

Example:

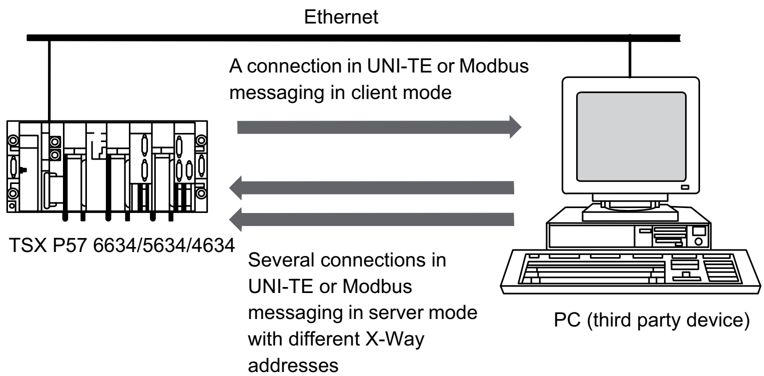


Connection to a Third-Party Device

Between a Premium PLC and a third-party device, the Ethernet channel of the TSX P57 6634/5634/4634 allows:

- a single connection in UNI-TE or Modbus client mode
- several connections in UNI-TE or Modbus server mode

Example:



NOTE: It is optional to give an X-Way address to the Ethernet port of the TSX P57 6634/5634/4634:
Without an X-Way address, the module cannot participate in message exchanges with other X-Way stations. It can nevertheless be connected to Control Expert and receive Modbus messaging.

Performance of I/O Scanning

Introduction

The performance data given below are those of the Ethernet channel of the **TSX P57 6634/5634/4634** when using I/O scanning.

Restart Time for an I/O Scanning Configuration

This time corresponds to the time between the power up of the complete configuration and the moment when all the remote inputs/outputs become operational (the status bits are activated, the word bits %IWr.m.c.l to %IWr.m.c.4 = 1).

Values are given in seconds:

- T= 35 s, if the module the channel is used as a DHCP server to connect the scanned devices
- T = 17 s, if the scanned devices use another DHCP server

Input/Output Restart Time

This time corresponds to the time between the power up of the remote input/output and the moment when all the status bits are activated (word bits %IWr.m.c.l to %IWr.m.c.4 = 1).

The value is given in seconds:

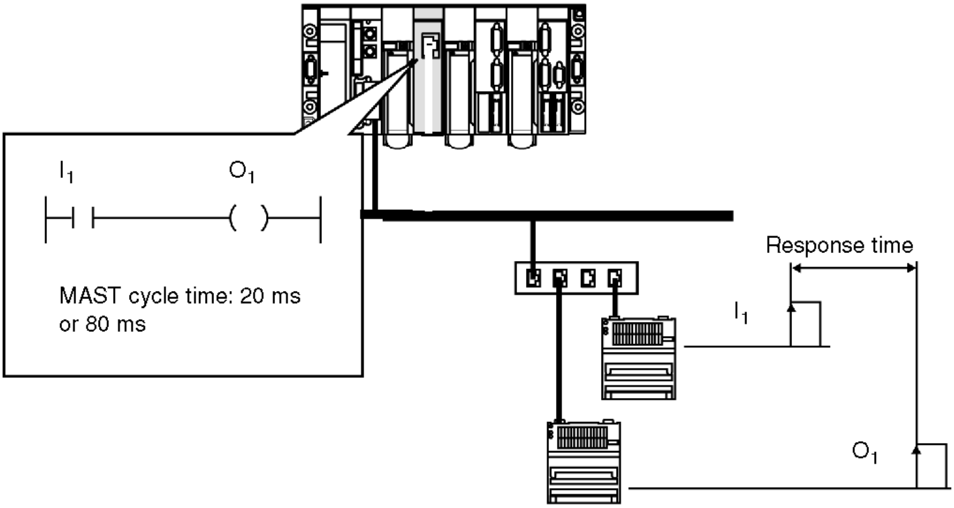
- T = 5 s

Application Response Time

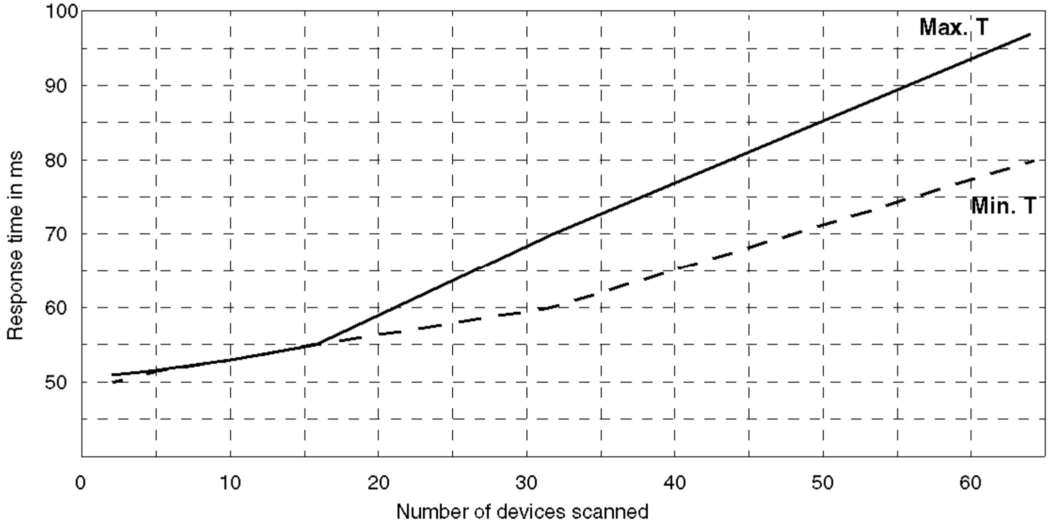
This time corresponds to the elapsed time between the acquisition of a remote input and the positioning of a remote output.

This is a logic response time, which does not take filtering time and actuator and sensor interface response times into account.

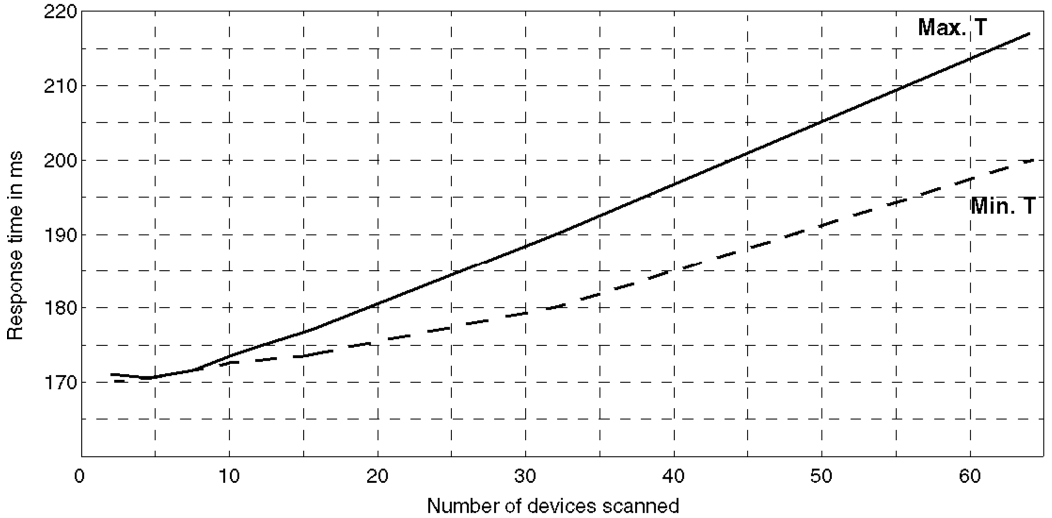
This is an example of time elapsed from acquiring an input to the positioning of an output:



Response time with a cycle of 20 ms



Response time with a cycle of 80 ms



Global Data Performances

At a Glance

The values shown below evaluate Global Data performance on the Ethernet channel of the TSX P57 6634/5634/4634.

Definition

Global Data return time:

This time corresponds to the elapsed time between the publication of a variable value by the local PLC application, the subscription by a remote PLC application, the publication of the same value by the remote PLC application, and the subscription by the local PLC application.

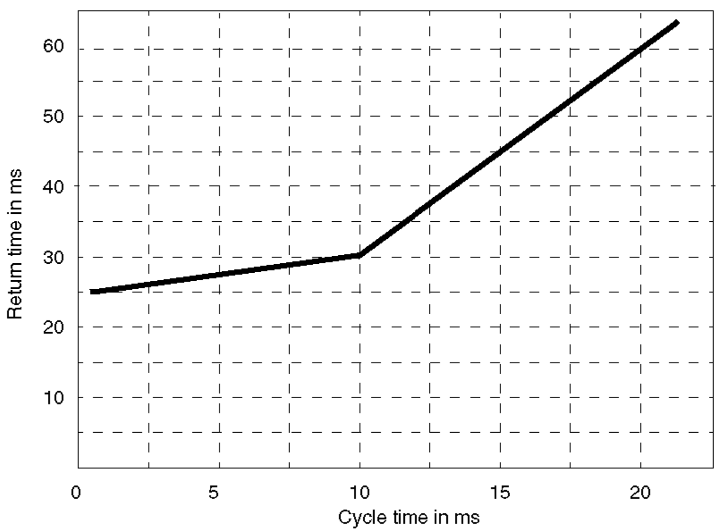
Values

Measurement conditions:
- The cycle times for local and remote PLC applications are identical.
- Only one variable is exchanged in each direction.

Result:

PLC cycle time	Return time
>= 10 ms	3 times the PLC cycle time
= 5 ms	5 to 6 times the PLC cycle time

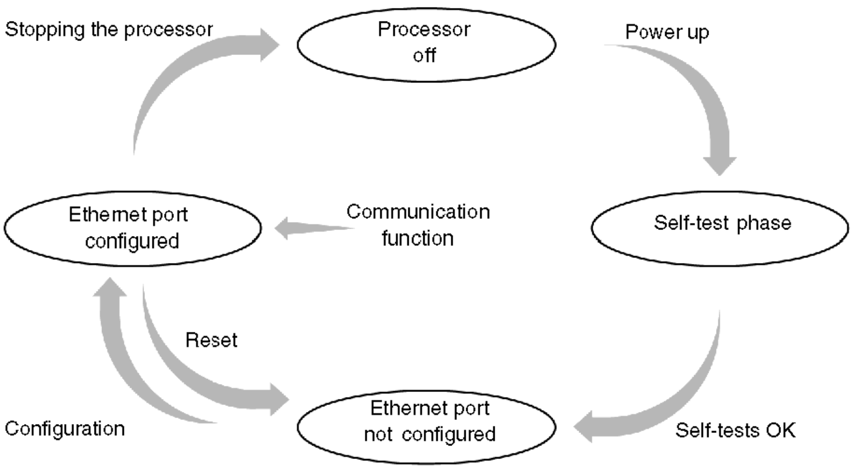
Illustration:



Operating Modes of the Ethernet Channel of the TSX P57 6634/5634/4634

Operating Mode Diagram

The following diagram describes the operating modes of the Ethernet channel of the TSX P57 6634/5634/4634:



Operation

- After power-up, the coprocessor performs self-tests. During this phase, the STS LED is lit. After the self-tests, the STS LED switches off.
- When the configuration is received, the Ethernet channel resets the current communication to 0 before configuring itself (terminates current exchanges, shuts down TCP connections). The channel is then operational. The STS LED is lit.
- The I/O Scanning and Global Data functions start when the PLC switches to RUN mode and stop when the PLC switches to STOP mode.

Special Cases: Channel Not Configured

If the Ethernet channel is not configured in the Control Expert application, it takes the IP address built from its MAC address:

085.016.xxx.yyy where xxx and yyy are the last two numbers of the MAC address.

Example

The MAC address is (in hexadecimal): 00 80 F4 01 12 20

In this case the default IP address is (in decimal): 085.016.018.032

The channel also transmits BOOTP requests to obtain another IP address. These requests are sent until a DHCP server responds or until Control Expert provides a new configuration.

An unconfigured Ethernet channel allows you to receive:
- a connection from Control Expert (loading application, etc.)
- Modbus messaging

If the STS LED flashes five times, then the IP address of the Ethernet channel is taken from the MAC address.

If the STS LED stays permanently on, then an IP address has been served by another network device. This IP address can be read in the channel's IP address language objects.

Section 9.2
Ethernet Channel Configuration

About this Section

This section describes the installation of the Ethernet channel of the TSX P57 6634/5634/4634 during configuration.

What Is in This Section?

This section contains the following topics:

Ethernet Channel Configuration Screen (TSX P57 6634/5634/4634)

Elements and Functions

This table describes the various zones that make up the Ethernet channel configuration screen:

Zone	Area	Function
common	Header	This common part of the Ethernet communication configuration screens enables you to choose the network family to be configured. When the network is associated with a module, the module address appears in the **Module address** field.
specific	IP Module Address	Allows the display of the module address
	Module Services	Allows selection of the services used by the module
	Security tab	Supports enabling/disabling of FTP, TFTP, and HTTP *(see page 146)*.
	IP Configuration tab	Enables the configuration of TCP/IP services *(see page 148)*
	IO Scanning tab	Allows configuration of I/O scanning *(see page 156)*
	Address Server tab	Allows configuration of the address server *(see page 192)*
	Module Services	Allows selection of the services used by the module
	SNMP tab	Allows configuration of SNMP *(see page 195)*
	Global Data tab	Allows configuration of Global Data *(see page 199)*
	Bandwidth tab	Allows you to check that configured services are compatible with the processing capacity of the Ethernet channel

Type of Communication According to Connection Configuration

Overview

Depending on the connection configuration *(see page 153)* of the Ethernet channel of the **TSX P57 6634/5634/4634**, you can carry out messaging.

- in mono-connection
- in multi-connection

According to the type of protocol and access control management, multi-connection mode requires a specific configuration of the correspondence table.

NOTE: In the following, only examples of multi-connection are shown. Furthermore, emphasis is placed on communications between the coprocessor and a remote PC device containing several applications.

Configuration Rules

Several connections can be configured with the same IP address. They must be defined with the same protocol, the same access rights, and the same connection mode.

In the case of a Modbus connection, only two connections can be configured with the same IP address. Addresses associated with these connections are:

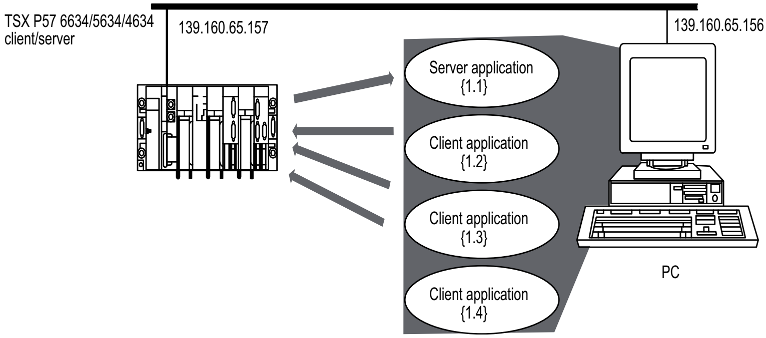
- an X-Way address greater than 100 (for example: {2.103}) for the Modbus client connection
- no X-Way address for the server Modbus connections

Multi-Connection in UNI-TE Protocol with Access Management

In this example, the PC contains four applications with a unique X-Way address and one single IP address:

- The coprocessor opens a connection and communicates with the address server application {1.1}.
- Each of the other client applications with the address {1.2}, {1.3}, {1.4} is authorized to open a connection and communicate with the coprocessor.

Exchanges are carried out according to the UNI-TE protocol when the coprocessor's access control utility is enabled.



In order to implement this example, you must:

- activate connection management by checking the coprocessor's **Access control** box
- configure communication from the coprocessor to the PC's server application in the table
  - **X-Way address**: 1.1
  - **IP address**: 139.160.65.156
  - **Access**: authorized (cell checked)
  - **Mode**: multi
- configure communication of each of the PC's client applications to the server coprocessor in the table:
  - **X-Way address**: 1.2 and 1.3 and 1.4
  - **IP address**: 139.160.65.156
  - **Access**: authorized (cell checked)
  - **Mode**: multi

Multi-Connection in UNI-TE Protocol without Access Management

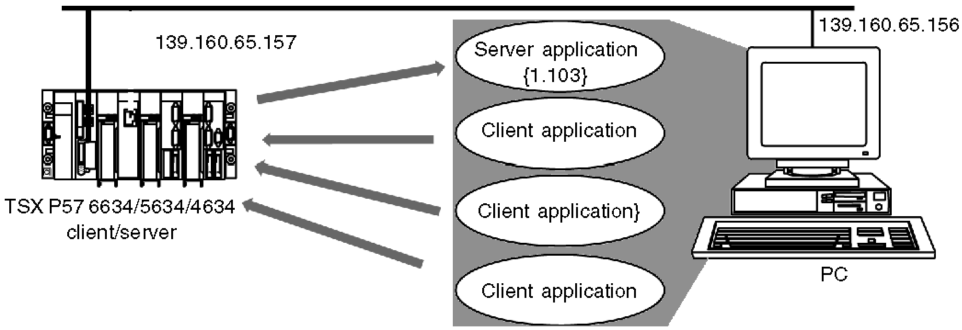
This example is the same as the previous one, except that access control is not configured.

In this case, if the application {1.1} is the only server application, the coprocessor's correspondence table only contains the following line:
- **X-Way address**: 1.1
- **IP address**: 139.160.65.156
- **Access**: the cell is grayed out
- **Mode**: multi

Multi-Connection in Modbus Protocol with Access Management

In this example, the PC contains four applications. The server application has an imaginary X-Way address and the other client applications do not need an X-Way address:
- The coprocessor opens a connection and communicates with the server application with the imaginary address {1.103}.
- Each client application has no address but is authorized to open a connection and communicate with the Ethernet channel of the **TSX P57 5634/4634**.

Exchanges are carried out according to the Modbus protocol when the coprocessor's access control utility is enabled.



In order to implement this example, you must:

- activate connection management by checking the coprocessor's **Access control** box
- configure communication from the coprocessor to the PC's server application in the table
  - **X-Way address**: 1.103 (address between 100 and 163 for the Modbus protocol)
  - **IP address**: 139.160.65.156
  - **Access**: the cell is grayed out
  - **Mode**: multi
- configure communication of all of the PC's client applications to the server coprocessor in the table:
  - **X-Way address**: empty
  - **IP address**: 139.160.65.156
  - **Access**: authorized (allows you to specify that other applications are authorized to connect and communicate)
  - **Mode**: multi

NOTE: If you want to prevent connection by client applications you must configure

- **X-Way address**: empty
- **IP address**: 139.160.65.156
- **Access**: not authorized (cell unchecked)
- **Mode**: multi

Multi-Connection in Modbus Protocol without Access Management

This example is the same as the previous one, except that access control is not configured.

In this case (where the application {1.103} is the only server application), the coprocessor's correspondence table only contains the following line:

- **X-Way address**: 1.103 (address between 100 and 163 for the Modbus protocol)
- **IP address**: 139.160.65.156
- **Access**: the cell is grayed out
- **Mode**: multi

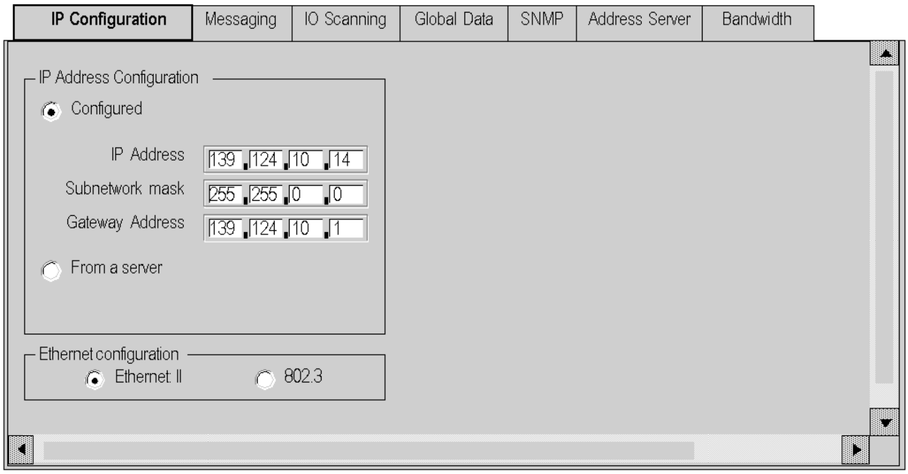
Configuration of TCP/IP Messaging (TSX P57 6634/5634/4634)

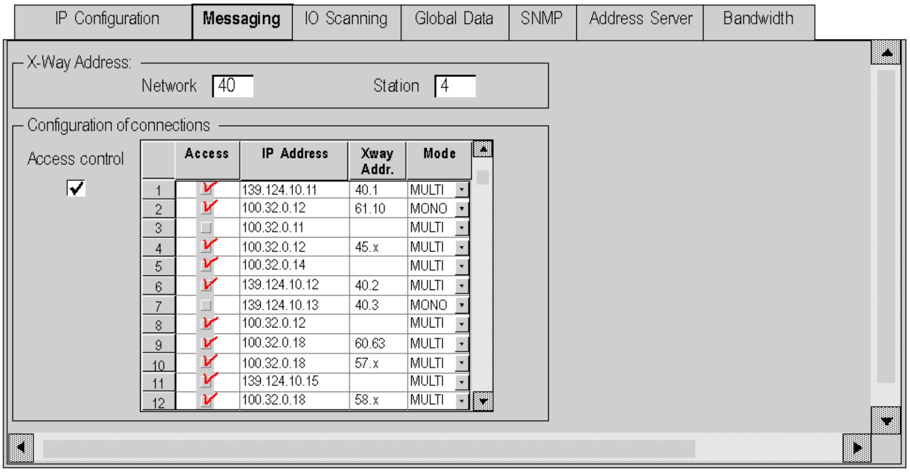
Introduction

In order to use the channel of the TSX P57 6634/5634/4634 module to communicate on Ethernet, it is necessary to set the messaging configuration parameters *(see page 149)*.

Accessing Messaging

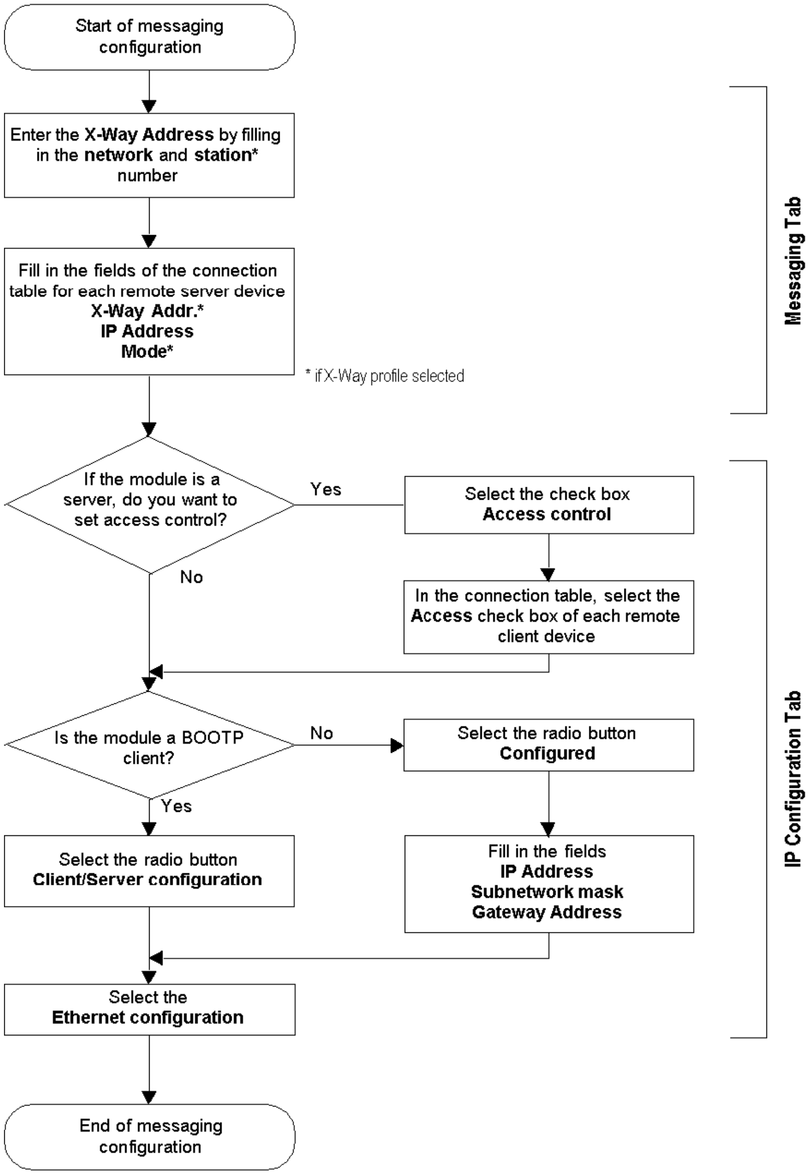
Messaging is configured in the two windows accessible by the tabs: **IP Configuration** and **Messaging**. To access the configuration parameters for TCP/IP services:

Step	Action
1	Access the module configuration screen.
2	Select the **IP Configuration** tab: 

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>3</td><td>Select the Messaging tab:

</td></tr>
</table>

Configuring Messaging

The following procedure gives the configuration principle:



I/O Scanning Configuration

Introduction

To see the procedure on how to use an Ethernet coprocessor go here *(see page 297)*.

Configuration of the Other Services of the TSX P57 6634/5634/4634

Services

The other available Ethernet channel services for the TSX P57 6634/5634/4634 are configured using screens that are the same as those of the TSX ETY 4103/5103 and the TSX P57 1634M/2634M/3634M modules. These services are:

- Security *(see page 293)*
- Address Server *(see page 300)*
- Global Data *(see page 302)*
- SNMP *(see page 305)*
- Bandwidth monitoring *(see page 314)*

Section 9.3
Ethernet Channel Debugging

About this Section

This section describes the installation of the Ethernet channel of the TSX P57 6634/5634/4634 during its debugging.

What Is in This Section?

This section contains the following topics:

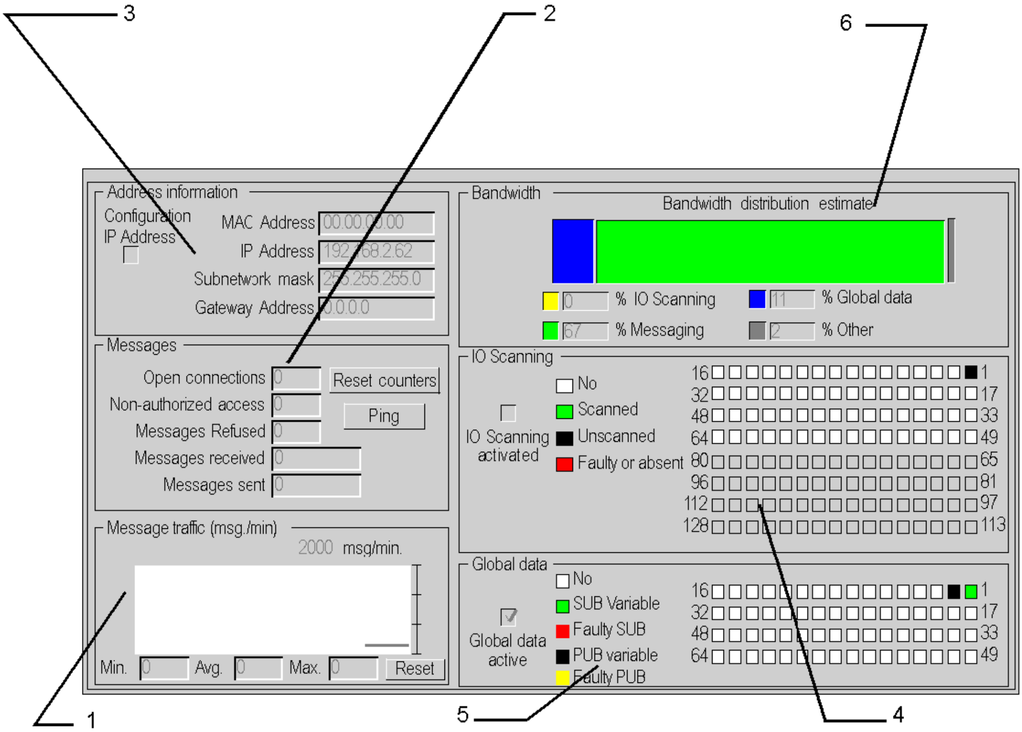
Ethernet Channel Debugging Screen

Introduction

This screen, separated into six zones, allows debugging via an Ethernet port.

Figure

The screen dedicated to Ethernet communication is displayed as follows:



Elements and Functions

This table describes the different zones that make up the debugging screen:

Number	Zone	Function
1	Message traffic	Allows the graphical display of the number of messages processed by the module
2	Messages	Allows the display of the number of unacknowledged or refused messages and connections. The counter values can be reinitialized using the **Init Counters** button. A **Ping** button is used to access the communication test.
3	Addresses	Displays the various TCP/IP addresses
4	IO Scanning	Allows display of the status for each remote input/output module
5	Global Data	Allows display of the status for Global Data variables
6	Bandwidth	Displays the Bandwidth diagnostics

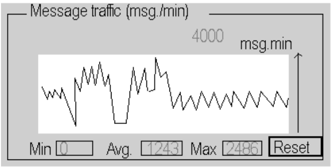
General Debugging Parameters

Introduction

The general debugging parameters are grouped together in two windows:
- the **Message traffic** window
- the **Messages** window

Message Traffic

The window is displayed as below:

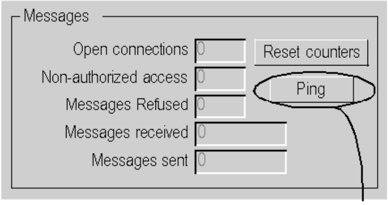


It indicates graphically the number of messages per minute processed by the module (send and receive). For better display, the scale automatically adapts to the flow rate.

The **Reset** button resets the three counters **Min.**, **Av.** and **Max.** to zero.

Messages

The window is displayed as below:



This window relates to TCP/IP messaging:
- the number of connections opened
- the number of unauthorized accesses
- the number of messages refused, received, and sent

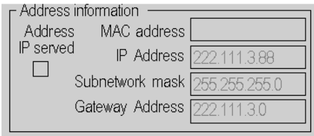
You can reset these counters to zero by clicking on the **Init counter** button.

The **Ping** *(see page 345)* button is used to access the communication test.

TCP/IP Address Information

At a Glance

The window is displayed as below:



It specifies the configuration data of the IP address:

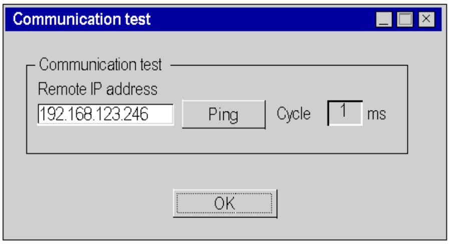
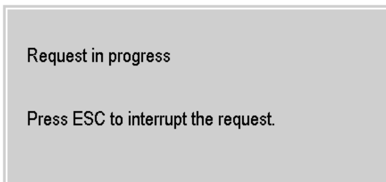
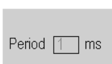
- **MAC address**: unique fixed address for a module
- **IP Address**
- **Subnetwork mask**
- **Gateway Address**: address of the gateway

A box indicates if the IP address is served or configured.

Testing TCP/IP Communications with the Ping Request

Procedure

Use this procedure to validate TCP/IP communications between two devices with a Ping request:

Step	Action
1	From the main screen, click the **Ping** button. The following window appears: 
2	Click the **Ping** button, and enter the address of the station to be queried using the **Remote IP address** field.
3	Press the **OK** button. The following window appears:  **Result**: If the exchange is successful, the following window appears:  Also, the message's send/return time (in ms) appears in the **Period** field: 

Response Type

The following table groups together the various types of possible responses to the Ping request.

If the response is	then
positive	The windows records the time (ms) it takes the message to be sent and returned. A window appears with the message **Exchange successful**.
negative	A window with the message **Exchange incorrect** specifies that the remote device was not reached in the network architecture.

Debugging Parameters for I/O Scanning

At a Glance

When I/O scanning is activated, the status of each configured device is displayed on a screen tab.

I/O Scanning

A device referenced in the **IO Scanning** configuration tab can have the following states:

- **Scanned**: green
- **Not configured**: white
- **Unscanned, Faulty or absent**: red

NOTE: In the cases of **Not configured** and **Unscanned**, no Modbus request is generated towards the device.

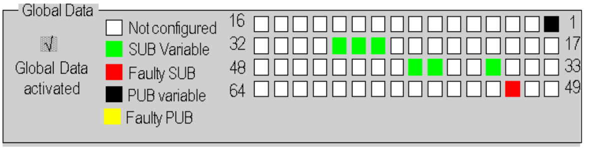
Debugging Parameters for Global Data

Introduction

When Global Data is activated, the status of a Global Data variable is displayed on the screen.

Global Data

The window is displayed as below:



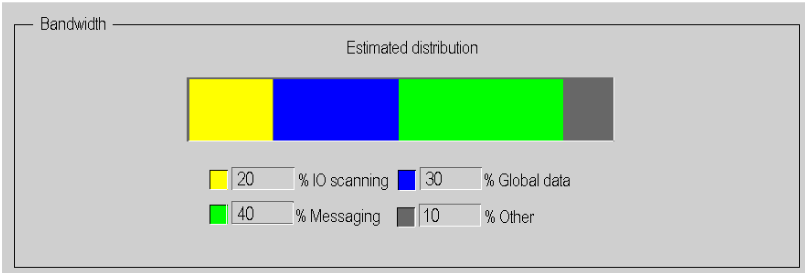
A Global Data variable can have the following status:

- **Not configured**: white
- **SUB variable**: subscribed variable received in the health timeout limit, green
- **Faulty SUB**: subscribed variable not received in the health time out limit, red
- **PUB variable**: published variable, green
- **Faulty PUB**: published variable not updated within the allotted period, yellow

Bandwidth Control Diagnostic Parameters

Bandwidth Screen

When bandwidth control is activated, the load of the coprocessor is displayed on the screen:



This graphic displays the actual load distribution, between I/O scanning, Global Data, Messaging and other services:
- %IO Scanning: yellow
- % Global Data: blue
- % Messaging: green
- % Other: gray

You can modify this distribution with bandwidth checking *(see page 314)*.

Chapter 10
Hot Standby and TSX ETY 4103/5103

At a Glance

This chapter provides an overview of Premium Hot Standby with Control Expert, focusing on the role of the TSX ETY 4103/5103 in the system. It includes:

- descriptions of Hot Standby topology
- ETY configuration with Hot Standby
- IP address assignment
- ETY operating modes
- address swap times
- network effects of Premium Hot Standby

NOTE: For a complete explanation of the operation of a Premium Hot Standby System, refer to the *Premium Hot Standby with Unity Manual*.

What Is in This Chapter?

This chapter contains the following sections:

Section 10.1
Overview of Premium Hot Standby Systems

Overview of the Premium Hot Standby System

Overview

Hot standby systems deliver high availability through redundancy. They are used when downtime can not be tolerated. A Hot Standby PLC system may consist of a single rack configuration.

Components in a Hot Standby System

The mandatory redundant component requirements per rack are:

- Standard Premium rack
- a TSX H57 24M or TSX H57 44M Hot Standby processor
- a power supply module
- one TSX ETY 4103/5103 TCP/IP Ethernet communication module (minimum firmware version 4.0)
- a CPU sync link cable
- an ETY sync link cable

The optional redundant components are:

- a TSX REY 200 Bus X remote rack master module
- other TSX ETY 4103/5103 TCP/IP Ethernet communication modules (minimum firmware version 4.0)
- Modbus communication module TSX SCP 114 in TSX SCY 21601
- discrete/analog input modules
- discrete/analog output modules

The two Hot Standby PLCs are configured with identical hardware and software. One of the Hot Standby processor TSX H57 24M or TSX H57 44M’s acts as the *primary* PLC, and the other acts as the *standby* PLC.

The Sync Link Cables

The CPU sync link is a point-to-point cable dedicated to application data exchange from the primary PLC to the standby PLC and to Hot Standby system diagnostics. Do not connect any other Ethernet devices on this link.

An ETY sync link cable runs between the two monitored ETY modules. A monitored ETY is used to diagnose the hot standby configuration and the communication between ETYs over the ETY sync link cable.

The Primary and Standby PLCs

The primary PLC:

- executes the full application program
- controls the Ethernet I/O and in-rack I/O
- updates the standby PLC after every scan (program cycle); if the primary PLC fails, the standby PLC takes control within one scan.

The standby PLC:

- executes only the first section of the full application program
- checks the health of the primary PLC
- does not control the in-rack or Ethernet I/O

NOTE:
- Redundant in-rack I/O modules are connected in parallel between the 2 PLCs via specific connection blocks.
- Local in-rack I/O modules are not connected in parallel.

The primary and the standby PLCs can manage local in-rack I/O with some restrictions.

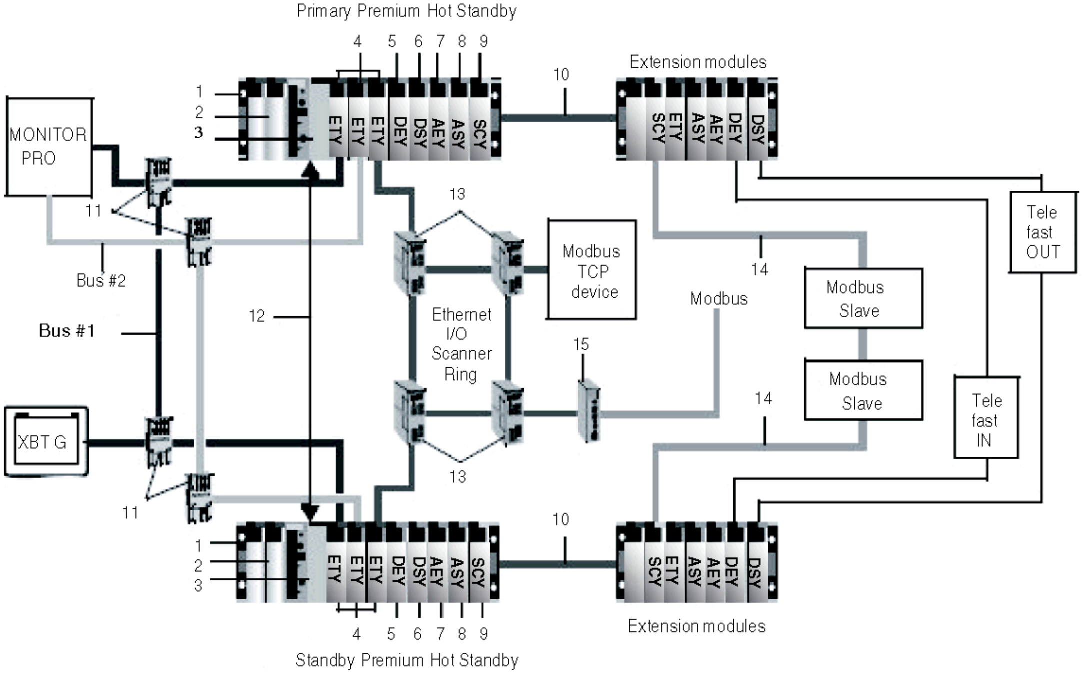
Switchover

At any moment, either of the two PLCs may be the primary or standby PLC—primary and standby states are interchangeable.

Switchover can only occur if one of the two PLCs is functioning as the primary PLC and the other one is in standby mode.

The Ethernet I/O and the redundant in-rack I/O are always controlled by the primary PLC.

System Components



1 Main rack with line terminator
2 Power supply
3 PLC processor (TSX H57 24M or TSX H57 44M)
4 Ethernet modules (TSX ETY 4103/5103, minimum firmware version 4.0) with monitored ETY managing an I/O scanner ring
5 Discrete input module (i.e. TSX DEY 64D2K)
6 Discrete output module (i.e. TSX DSY 64T2K)
7 Analog input module (i.e. low level isolated inputs, thermocouples, temperature probes, TSX AEY 414)
8 Analog output module (i.e. isolated output, TSZ ASY 410)
9 Communication module (TSX SCY 21601 with Modbus PCMCIA TSX SCP 114))
10 Bus X
11 Ethernet switch
12 CPU sync-link
13 Ethernet ring switch
14 Modbus RS485 cable
15 Modbus gateway (i.e. TSX ETG 1000)

Modbus Components

A Modbus TCP device can be any of the following:

- STB
- OTB
- Momentum I/O
- ATV61
- XBT G
- XBT GT
- Premium

A Modbus slave device can be any of the following:

- STB
- OTB
- ATV31
- TeSys U

Section 10.2
Hot Standby Topology

Introduction

In order for a Premium Hot Standby System to function correctly, the PLCs and ETY modules must be configured correctly. This section describes how to configure these parts of the hot standby system.

What Is in This Section?

This section contains the following topics:

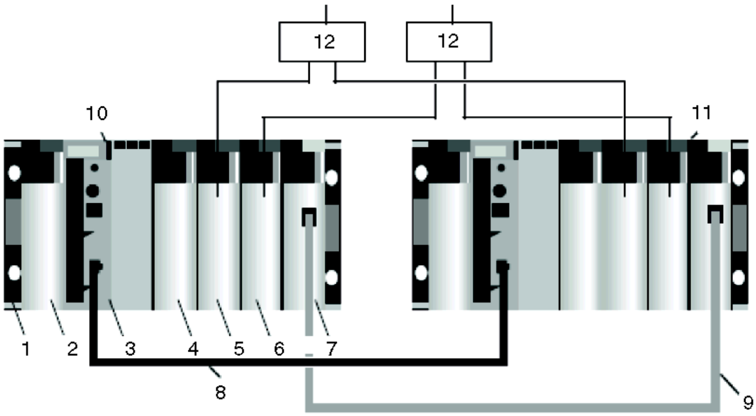
Hot Standby Topology

Overview

A Premium Hot Standby system can be configured in many ways. Below are two examples of Premium Hot Standby topology.

Connecting the ETY Modules

The illustration below displays a simple Premium Hot Standby configuration two ETY modules connected by an Ethernet cable; no switches are used.



1 Premium rack with line terminators
2 Power supply
3 Hot Standby processor (TSX H57 24M or TSX H57 44M)
4 Communication module (TSX SCY 21601 with Modbus PCMCIA TSX SCP 114)
5 Discrete output module (i.e. TSX DSY 64T2K)
6 Discrete input module(i.e. TSX DEY 64D2K)
7 ETY 4103/5103 (minimum firmware version 4.0)
8 CPU sync link cable
9 ETY sync link cable
10 Primary PLC (A)
11 Standby PLC (B)
12 Connection block

The link between the two ETY modules is called the *ETY-sync link*. The two ETYs are called *monitored* ETYs. Monitored ETY modules manage:

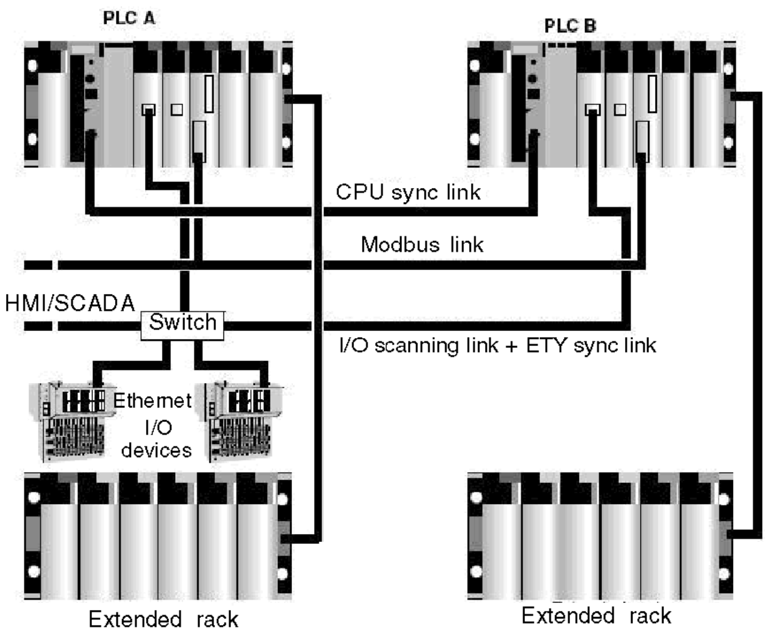
- only diagnostic information in the case of exclusive Bus-X configuration
- diagnostic information and I/O Scanning if Ethernet I/O devices are connected on the link
- diagnostic information, I/O Scanning, and other Ethernet services

NOTE: In the above Premium hot standby configuration, the two monitored ETYs are linked with a crossover cable. No Ethernet devices are connected to the ETY-sync link. A failure on this link does not generate a switchover because the ETY-sync link is not part of the I/O or messaging process.
On the contrary, when Ethernet I/O devices or other equipment are connected to the ETY-sync link, it is necessary to generate a switchover when a cable failure appears on the primary side.

Example of Configuration

The following configuration is:

- PLC A and PLC B with the following modules:
  - Power supply
  - Hot standby processor in slot 0
  - Monitored ETY module in slot 2
  - Modbus communication (SCY with SCP 114) in slot 4
  - In-rack discrete module (DIS IN and DIS OUT) in slots 5 and 6
- One switch for simplified schema to connect between Ethernet I/O scanner and SCADA or HMI
- A CPU sync link cable between the two CPUs *(see page 352)*



Connecting Ethernet I/O

The link between the two monitored ETY modules, the ETY sync link cable, transfers information to diagnose the Hot Standby system and manages Ethernet I/O devices and/or other PLCs by configuring Ethernet I/O Scanning and/or Global Data in each monitored ETY.

You can use either of the following architectures:

- a low-level architecture, which comprises two Ethernet switches connected together and each ETY connected to one of the switches
- a high-level architecture, where several Ethernet ring switches are connected to the Ethernet devices and/or PLCs

For using hubs or switches in different network topologies, such as star, tree, or ring topologies, refer to the ConneXium catalog and the *Transparent Ready User Guide*.

ETY Configuration and Hot Standby

Overview

Because a user can configure several ETY modules in each PLC, the monitored ETY modules that are dedicated to the ETY sync link *(see page 352)* must be configured in Control Expert.

NOTE: Only one ETY module can be dedicated to the ETY sync link in each PLC.

Description of the Hot Standby Solution

⚠ CAUTION

RISK OF INCREASE OF TIME TO SWAP

TSX ETYs must communicate with each other in order to swap IP addresses. Whenever possible, use of a switch (not a hub) to connect the TSX ETYs to each other or to the network. Schneider Electric offers switches. Contact a local sales office for more information.

Failure to follow these instructions can result in injury or equipment damage.

ETY Hot Standby allows automatic IP address swapping.

The TSX ETYs coordinate the swapping of IP addresses. After closing both the client and the server connections, the TSX ETY sends a swap UDP message to its peer TSX ETY. The sending TSX ETY then waits for a specified time-out (50 ms) for the peer swap of UDP messages. Either after receiving the messages or after a time-out, the TSX ETY changes its IP address.

NOTE: TSX ETYs must communicate with each other in order to swap IP addresses. Schneider Electric recommends that you connect the primary and standby TSX ETYs to the same switch for two reasons:

- Communication failures between the TSX ETYs increases the time to swap
- Connecting two TSX ETYs to the same switch minimizes the probability of a communication failure.

Actions of the ETY in the Premium Hot Standby System

⚠ WARNING

UNEXPECTED APPLICATION BEHAVIOR

Design your application so that unmonitored ETYs support communication only to noncritical parts of the application.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The TSX ETY waits for either a change in the controller's Hot Standby state or the swap of UDP messages. Then the TSX ETY performs one of two Hot Standby actions.

If the TSX ETY...	It then...
Detects that the new Hot Standby state is either primary or standby	changes the IP address.
Receives a swap UDP message	transmits a Swap UDP message and swaps the IP address.

All client/server services (I/O Scanner, Global Data, Messaging, FTP, SNMP, and HTTP) continue to run after the switchover from the old to the new primary TSX ETY.

The failure of a monitored primary ETY module triggers a switchover. The failure of an unmonitored primary ETY module does not trigger a switchover.

Section 10.3
Configuration of the Monitored ETY Module

Configuration of the Monitored ETY Module

Overview

Premium Hot Standby enables the switching of Ethernet services and automatic IP address swapping between the primary and standby TSX ETY modules.

NOTE: The Global Data Publish/Subscribe Service is disabled in Control Expert when configuring Premium Hot Standby systems.

Position of the ETY

The position of the ETY is unrestricted in the Premium configuration (main rack or extension rack). However, both PLCs must have identical firmware, configurations, and module positions. ETY modules are linked either through the Ethernet switches (one switch per ETY) or an Ethernet crossover cable. By using an Ethernet transceiver, you have an optical connection for longer distances.

Configuration of the Module

To configure the monitored ETY module in Control Expert, set the topology address of the monitored ETY module by selecting the address from a list of existing ETY card addresses in the combo box on the Hot Standby tab of the CPU screen.

ETY Modules and I/O Scanners

The Ethernet port for I/O scanning should be connected to the monitored ETY. If a fault appears on this module (e.g., module hardware failure, broken wire, or cable disconnection) switchover is automatic. If a fault appears on any unmonitored ETY modules, switchover is not automatic; you must design your application to request a manual switchover.

For better performance and more predictable time at switchover, any other required Ethernet services (e.g., Global Data, HTTP server, FTP/TFTP) should be configured in unmonitored ETY modules. These services should not be configured in the monitored ETYs.

If the ETY Module Fails

For a switchover to occur when an ETY-sync link failure appears in the primary system, one of the two Ethernet services (I/O Scanning or Global Data) must be configured in the monitored ETY. If neither service is configured in the monitored ETY, an ETY-sync link failure does not generate a switchover.

If the monitored ETY module fails, the CPU sends a state change command to all configured ETY modules present on the X-BUS (in the main and extended racks). All ETY modules present in the Hot Standby PLC then swap IP addresses.

Section 10.4
IP Address Assignment

IP Address Assignment

Overview

The ETY TCP/IP address must be configured in Control Expert. Since the primary and standby controllers must have an identical configuration, the configured IP addresses will be the same. The ETY's IP address is either the configured IP address or the configured IP address + 1.

The IP address is determined by the current local Hot Standby state. In the offline state *(see page 369)*, the IP address is determined by whether or not the standby PLC is in transition to the primary state. In a Premium Hot Standby System, the two IP addresses are consecutive.

Address Assignments

The following table shows the IP address assignments.

Hot Standby State	IP Address
Primary	Configured IP address
Standby	Configures IP address + 1
Transition from primary to offline	Configured IP address, if peer PLC does not go to primary
Transition from standby to offline	Configured IP address + 1.

NOTE: Offline results depend on whether or not the PLC is detected to be in transition into the primary state. If the current IP is the configured IP address and the other PLC is in transition to primary, then the IP address changes to IP address + 1.

Restrictions

- Do not configure the ETY module to obtain an IP address from a server.
- Assign IP addresses that are in the same network and subnetwork to the primary and the standby ETY modules.

NOTE: Duplicate IP address checking is performed only at power-up of the hot standby PLC. It is not performed during a switchover or after the removal or replacement of the ETY Ethernet cable.

IP Address Transparency

⚠ CAUTION

UNEXPECTED EQUIPEMENT OPERATION

For a Premium Hot Standby configuration:

- Do not use consecutive IP addresses for consecutive ETY modules configured.
- Do not configure the primary address as *nnn.nnn.nnn.*254. This causes the standby IP address to be: *nnn.nnn.nnn.*255. The ETY would then return the diagnostic code **Bad IP configuration**.

Failure to follow these instructions can result in injury or equipment damage.

For continued Ethernet communication, the new primary ETY must have the same IP address as the former primary ETY. The IP address in the standby ETY is the primary IP address + 1.

The ETYs integrated into the Premium Hot Standby configuration coordinate this IP address swapping with the management of Ethernet services used.

If the ETY detects a duplicate IP address when it powers up, the PLC goes to its offline state and the ETY's IP address goes to its default setting.

Section 10.5
ETY Operating Modes

Introduction

This section describes ETY operating modes with Premium Hot Standby Systems.

What Is in This Section?

This section contains the following topics:

ETY Operating Modes and Premium Hot Standby

Overview

There are 4 ETY operating modes:

- *Primary mode*, where all client/server services are active
- *Standby mode*, where all server services are active except I/O scanning
- *Standalone mode*, which occurs when the ETY is in a nonredundant system or when the CPU module is not present or is not healthy
- *Offline mode*, where the CPU is stopped or the CPU module is in offline mode

ETY and the Premium Hot Standby System Synchronization

The Premium Hot Standby and the ETY operating modes are synchronized by the conditions described in the following table.

CPU Module Status	HSBY State	ETY Operating Mode
Not present or unhealthy	N/A	Unassigned
Present and healthy	Primary	Primary
Present and Healthy	Standby	Standby
Present and Healthy	Offline	Offline

Any one of four events will affect the ETY operating mode. They occur when

- the ETY is powered-up
- an ETY executes a Hot Standby switchover
- an ETY goes to offline mode
- a new application is downloaded to the ETY

If the ETY detects a duplicate address when it powers up, the PLC goes to its offline state and the ETY's IP address goes to its default address.

Power-up and IP Address Assignment

An ETY obtains its IP address assignment at power-up as follows:

If the HSBY ETY mode is ...	Then the IP address assigned is ...
Standalone	from the ETY configuration table.
Primary	the configured primary IP address from the ETY configuration table.
Standby	the configured primary address from the ETY configuration table + 1.
Not powered to powered up	determined by which controller powers up first (after check remote, the second ETY takes IP address + 1), or if powered at the same time, by a resolution algorithm: ● Lower copro MAC address: IP address/primary state ● Higher copro MAC address: IP address + 1/standby state

Offline Event Table

If the HSBY ETY mode is ...	Then the IP Address assigned is ...
Primary to Offline	the configured IP address from the ETY configuration table if the peer controller does not go to Primary state
Standby to Offline	the configured primary address from the ETY configuration table + 1.

When the CPU stops, the HSBY ETY goes to the Offline mode. The IP address remains the same if the peer controller does not go to Primary state.

Power-up and Ethernet Services

The following table shows how the status of an ETY service is affected by the Premium Hot Standby state.

HSBY State	Status of ETY Services					
	Client Services	Client/Server Services	Server Services			
	I/O Scanner	Modbus Messaging	FTP	SNMP	HTTP	DHCP
Not powered up to power-up	Run	Run	Run	Run	Run	Run
Primary	Run	Run	Run	Run	Run	Run
Standby	Stop	Run	Run	Run	Run	Run
Offline	Stop	Run	Run	Run	Run	Run

Address Swap Times

The following table shows the swap time for each of the Ethernet services. It also describes what occurs during an address swap, e.g., closing connections, swapping IP addresses, and reestablishing connections.

Service	Typical Swap Time	Maximum Swap Time
Swap IP Address	6 ms	500 ms
I/O Scanning	1 initial cycle	500 ms + 1 initial I/O scanning cycle
Client Messaging	1 CPU scan	500 ms + 1 CPU scan
Server Messaging	1 CPU scan + the time for the client to reestablish the connection	500 ms + the time for the client to reestablish the connection
FTP/TFTP Server	The time for the client to reestablish the connection	500 ms + the time for the client to reestablish the connection
SNMP	1 CPU scan	500 ms + 1 CPU scan
HTTP Server	the time for the client to reestablish the connection	500 ms + the time for the client to reestablish the connection

Section 10.6
Connecting Two Premium Hot Standby PLCs

Introduction

This section describes how to connect two Premium Hot Standby PLCs.

What Is in This Section?

This section contains the following topics:

Connecting Two Premium Hot Standby PLCs

Overview

To work properly, the primary and standby PLCs must be linked in a specific way.

Which Connections Are Required?

⚠ CAUTION
IMPROPER SYSTEM BEHAVIOR To prevent double primary PLCs when the two links are broken, route the two cables as far away from each other as possible. **Failure to follow these instructions can result in injury or equipment damage.**

Two sync link connections *(see page 352)* are required between the two Premium Hot Standby PLCs:

- a CPU sync link between the two CPUs
- an ETY sync link between the two monitored ETY modules

If these two links do not work properly, the two PLCs function as standalone units.

Which Cables May be Used?

The following cable type may be used in sync link connections:

- twisted pair copper cable

In-rack I/O and Ethernet I/O Notes

Remember three things when you connect in-rack and Ethernet I/O modules to a Premium Hot Standby System.

- Only in-rack discrete and analog I/O modules can be used with Premium Hot Standby Systems. They are considered part of the redundant system.
- Ethernet I/O modules are not considered part of the redundant system.They are shared between the two PLCs.
- The primary PLC manages both the redundant in-rack and the Ethernet I/O modules.

Mapping the Backplane Extension

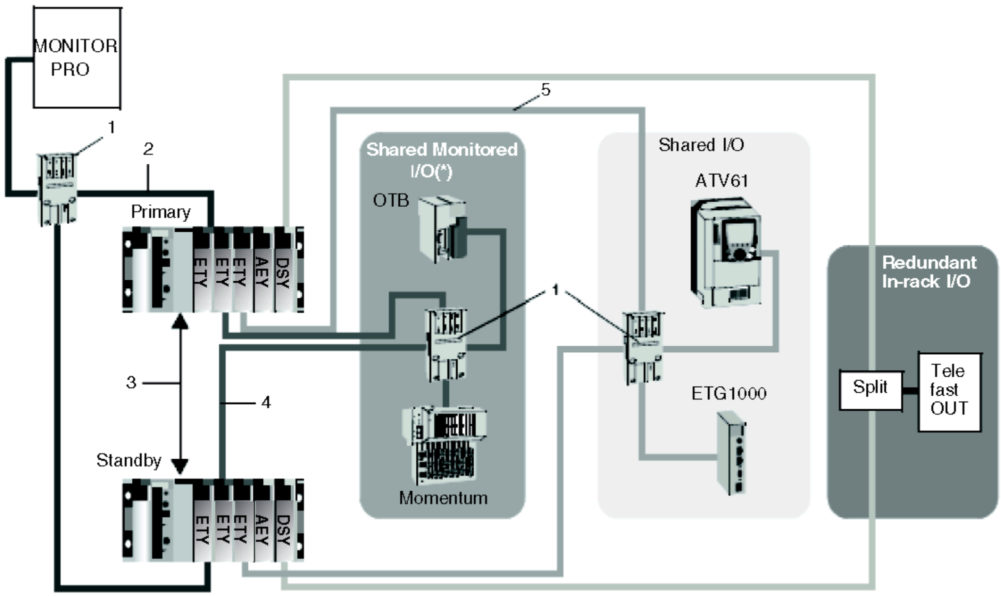
Overview

Two backplanes must be configured with identical hardware, software, and firmware, and the modules must be positioned identically in the backplanes. Either PLC may function as a primary or a standby PLC.

NOTE: Refer to the *Premium and Atrium using EcoStruxure™ Control Expert, Processors, racks and power supply modules, Implementation Manual* and *Electrical installation guide* for more information.

Multiple I/O with Scanning ETY

The following graphic shows an architecture example with 2 ETYs configured of I/O scanning.



1 Ethernet switch
2 Ethernet TCP/IP
3 CPU sync link
4 Ethernet I/O scanner #1
5 Ethernet I/O scanner #2

NOTE: Ethernet I/O scanner # 1 is a monitored ETY with an ETY sync link connection *(see page 352)*.

Section 10.7
Operating Requirements and Restrictions

Network Effects of Premium Hot Standby

Overview

Hot standby is a powerful feature in itself, and ETYs are a key part of the feature. It increases the reliability of your installation. Hot Standby uses a network, and using the Hot Standby feature over a network can affect the behavior of:

- Browsers
- Remote and local clients
- I/O scanning service
- Global Data service
- FTP/TFTP service

You may encounter issues with each of these while using the Premium Hot Standby. Below are some possible issues and resolutions.

NOTE: The Global Data Publish/Subscribe Service is disabled in Control Expert when configuring Premium Hot Standby systems.

Browsers

If a browser requests a page and during the process of downloading that page an IP address swap occurs, the browser will either hang or time out. Click the **Refresh** or the **Reload** button.

Remote Clients

Hot Standby swaps affect remote clients.

An ETY will reset under the following conditions:

- Remote Connection Request During Hot Standby Swap
  If a remote client establishes a TCP/IP connection during a Hot Standby swap, the server closes the connection using a TCP/IP reset.
- Hot Standby Swap during Remote Connection Request
  If a remote client makes a connection request and a Hot Standby swap occurs during the connection request, the server rejects the TCP/IP connection by sending a reset.
- Outstanding Request
  If there is an outstanding request, the ETY will not respond to the request, but will reset the connection.

The ETY will perform a Modbus logout if any connection has logged in.

Local Clients

During a swap, the ETY will reset all client connections using a TCP/IP reset.

I/O Scanning Service

⚠ CAUTION
UNEXPECTED EQUIPMENT OPERATION - DEVICES GO TO THEIR FALLBACK STATES DURING SWITCHOVER
Configure Ethernet output devices to their Hold Last Value fallback state whenever possible. This configuration has to be done with the configuration tool that is provided with the Ethernet device. Output devices that support only a Set to Zero fallback state may produce a pulse during switchover.
Failure to follow these instructions can result in injury or equipment damage.

I/O Scanning provides the repetitive exchange of data with remote Ethernet I/O devices. While the PLC is running, the primary ETY sends Modbus Read/Write requests to remote I/O devices and transfers data to and from the PLC memory. In the standby controller, the I/O scanning service is stopped.

When the Hot Standby swap occurs, the primary ETY closes all connections with I/ O devices by sending a TCP/IP reset. The I/O scanning service in this ETY is in Standby mode.

After the swap, the new primary ETY re-establishes the connection with each I/O device. It restarts the exchange of data with these reconnections.

The TSX ETY 4103/5103 provides the I/O scanning feature. Configure it with the Control Expert software.

If you are using the Ethernet I/O scanning service for critical applications, the following important issues regarding switchover must be considered:

- If a communication function block is used for TCP/IP, the block will not complete its transaction.
- While the ETY is in the process of performing the transaction, a new communication function block may become active.
- The PLC will use the state configured in the last value option in the I/O scanning table of the ETY module (in the Control Expert software) as the input state for the scanned Ethernet I/O devices.
  These two states are one of the following:
  - Set to 0
  - Hold last value

NOTE: When the I/O Scanning service is configured in the monitored ETY, an ETY-sync link failure on the primary side will generate a switchover.

FTP/TFTP Service

The File Transfer Protocol/Trivial File Transfer Protocol (FTP/TFTP) service is available as soon as the module receives an IP address. Any FTP/TFTP client can log on to the module. Access requires the correct user name and password. Premium Hot Standby allows only one active FTP/TFTP client session per ETY module.

When the Hot Standby swap occurs, the primary and standby ETYs close the FTP/ TFTP connection. If a user sends an FTP/TFTP request during the swap, the communication is closed.

Whenever you re-open communication, you must re-enter a user name and a password.

Chapter 11
Ethernet Language Objects

Purpose

This chapter describes the language objects associated with the Ethernet communication modules.

What Is in This Chapter?

This chapter contains the following sections:

Section 11.1
Language Objects and IODDT of Ethernet Communication

Aim of this Section

This section provides a general overview of language objects and IODDT of Ethernet communication

What Is in This Section?

This section contains the following topics:

Description of Language Objects for Ethernet Communication

General

Ethernet communication has four IODDTs:
- `T_COM_ETY_1X0` specific to the modules ETY_110 and ETY_120
- `T_COM_ETY_210` specific to the module ETY_210
- `T_COM_ETYX103` specific to the module ETY_4103/PORT/5103
- `T_COM_ETHCOPRO` specific to the Ethernet channel of the processor TSX P 57 5634

NOTE: IODDT variables can be created in two different ways:
- Using the **I/O objects** *(see EcoStruxure™ Control Expert, Operating Modes)* tab
- Data Editor *(see EcoStruxure™ Control Expert, Operating Modes)*

Types of Language Objects

Each IODDT has a set of language objects that is used to control and check the operation of the IODDT.

There are two types of language objects:
- **implicit exchange objects**, which are exchanged automatically on each cycle turn of the task associated with the module
- **explicit exchange objects**, which are exchanged at the request of the application ,using explicit exchange instructions

Implicit exchanges concern the states of modules, communication signals, slaves, etc.

Explicit exchanges are used to set parameters and diagnose the module.

Details of T_COM_EIP IODDT

Exchange Objects of the IODDT

The T_COM_EIP IODDT supports both implicit and explicit exchange objects:
- Implicit exchange objects are automatically exchanged at each cycle of a task associated with the channel.
- Explicit exchange objects can be reached via explicit messaging controlled either by program logic, or by operator commands.

Exchange objects are %I, %IW, %M and %MW.

The tables below presents the various implicit and explicit exchange objects of IODDT T_COM_EIP, as supported by the TSX ETC 101 communication module.

The parameters r, m, and c shown in the following-tables represent the topological addressing of the module. Each parameter has the following signification:
- r represents the rack (or station) number
- m represents the module (or slot) number
- c represents the channel number

Implicit and Explicit Exchange Objects of the T_COM_EIP IODDT

The T_COM_EIP IODDT presents the following implicit communication objects:

Standard symbol	Type	Access	Description	Address
CH_ERROR	BOOL	R	Channel detected error bit	%Ir.m.c.ERR
STS_ETH_SERVICES	INT	R	Status of Ethernet services:	%IWr.m.c.0
			Bit 0: EIP Scanner (0 = OK, 1 = NOK)	
			Bit 1: EIP Adapter (0 = OK, 1 = NOK)	
			Bit 2: EIP Client (0 = OK, 1 = NOK)	
			Bit 3: EIP Server (0 = OK, 1 = NOK)	
			Bit 4: Modbus scanner (0 = OK, 1 = NOK)	
			Bit 5: Modbus TCP Client (0 = OK, 1 = NOK)	
			Bit 6: Modbus TCP Server (0 = OK, 1 = NOK)	
			Bit 7: FDR Server (0 = OK, 1 = NOK)	
			Bit 8–Bit 15: (reserved)	

Explicit Exchange Objects of the T_COM_EIP IODDT

The T_COM_EIP IODDT presents the following explicit communication objects:

Standard symbol	Type	Access	Description	Address
EXCH_STS	INT	R	Exchange Status:	%MWr.m.c.0
STS_IN_PROGR	BOOL	R	Bit 0: Status parameter read in progress	%MWr.m.c.0.0
CMD_IN_PROGR	BOOL	R	Bit 1: Command parameter write in progress	%MWr.m.c.0.1
ADJ_IN_PROGR	BOOL	R	Bit 2: (Not used)	%MWr.m.c.0.2
EXCH_RPT	INT	R	Channel report	%MWr.m.c.1
STS_ERR	BOOL	R	Bit 0: Error detected while reading channel status	%MWr.m.c.1.0
CMD_ERR	BOOL	R	Bit 1: Error detected while sending a command on the channel	%MWr.m.c.1.1
ADJ_ERR	BOOL	R	Bit 2: (Not used)	%MWr.m.c.1.2
CH_FLT	INT	R	Channel faults detected	%MWr.m.c.2
NO_DEVICE	BOOL	R	Bit 0: (Reserved)	%MWr.m.c.2.0
ONE_DEVICE_FLT	BOOL	R	Bit 1: (Reserved)	%MWr.m.c.2.1
BLK	BOOL	R	Bit 2: (Reserved)	%MWr.m.c.2.2
TO_ERR	BOOL	R	Bit 3: (Reserved)	%MWr.m.c.2.3
INTERNAL_FLT	BOOL	R	Bit 4: Internal error detected: channel inoperative	%MWr.m.c.2.4
CONF_FLT	BOOL	R	Bit 5: Hardware or software configuration error detected	%MWr.m.c.2.5
COM_FLT	BOOL	R	Bit 6: X-bus communication error detected	%MWr.m.c.2.6
APPLI_FLT	BOOL	R	Bit 7: Application configuration error detected	%MWr.m.c.2.7
ETH_GLOBAL_STS	INT	R	Ethernet global status	%MWr.m.c.3
	BOOL	R	Bit 0: Configuration error detected	
	BOOL	R	Bit 1: (Reserved)	
	BOOL	R	Bit 2: duplicate IP address detected	
	BOOL	R	Bit 3: Ethernet link is disconnected	
	BOOL	R	Bit 4: (Reserved)	
	BOOL	R	Bit 5: The module is in the process of obtaining an IP address (BOOTP or in duplicate IP address)	
IP_ADDR	DINT	R	IP address	%MWr.m.c.4

Implicit Exchange Language Objects Associated with the Application-Specific Function

At a Glance

An integrated application-specific interface or the addition of a module automatically enhances the language objects application used to program this interface or module.

These objects correspond to the input/output images and software data of the module or integrated application-specific interface.

Reminders

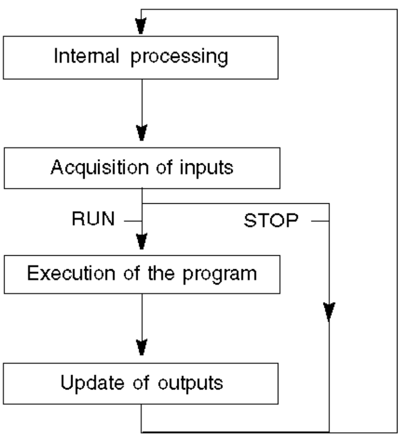
The module inputs (`%I` and `%IW`) are updated in the PLC memory at the start of the task, the PLC being in RUN or STOP mode.

The outputs (`%Q` and `%QW`) are updated at the end of the task, only when the PLC is in RUN mode.

NOTE: When the task occurs in STOP mode, either of the following are possible, depending on the configuration selected:
- outputs are set to fallback position (fallback mode)
- outputs are maintained at their last value (maintain mode)

Figure

The following diagram shows the operating cycle of a PLC task (cyclical execution).



Explicit Exchange Language Objects Associated with the Application-Specific Function

Introduction

Explicit exchanges are performed at the user program's request using these instructions:

- READ_STS (read status words)
- WRITE_CMD (write command words)
- WRITE_PARAM (write adjustment parameters)
- READ_PARAM (read adjustment parameters)
- SAVE_PARAM (save adjustment parameters)
- RESTORE_PARAM (restore adjustment parameters)

For more details about instructions, refer to *EcoStruxure™ Control Expert, I/O Management, Block Library*.

These exchanges apply to a set of %MW objects of the same type (status, commands or parameters) that belong to a channel.

These objects can:

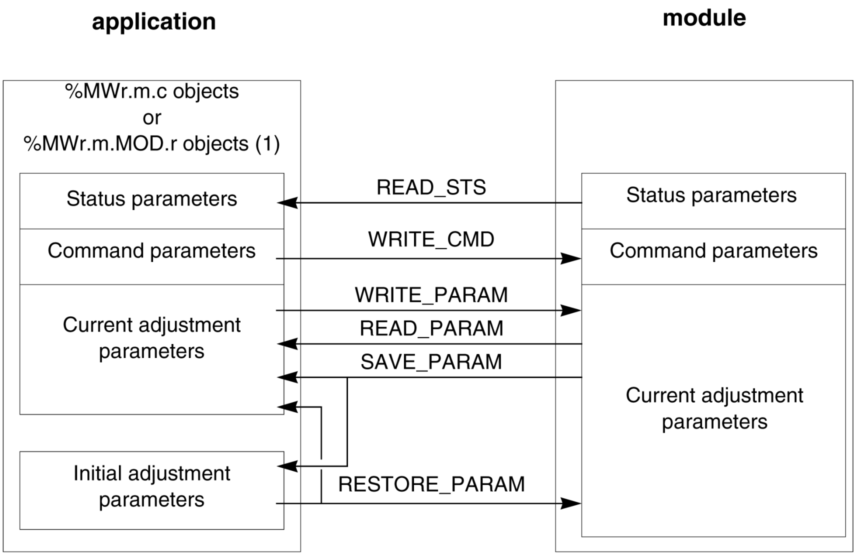
- provide information about the module (for example, type of error detected in a channel)
- have command control of the module (for example, switch command)
- define the module’s operating modes (save and restore adjustment parameters in the process of application)

NOTE: To avoid several simultaneous explicit exchanges for the same channel, it is necessary to test the value of the word EXCH_STS (`%MWr.m.c.0`) of the IODDT associated to the channel before calling any EF addressing this channel.

NOTE: Explicit exchanges are not supported when X80 analog and digital I/O modules are configured through an eX80 adapter module (BMECRA31210) in a Quantum EIO configuration. You cannot set up a module's parameters from the PLC application during operation.

General Principle for Using Explicit Instructions

The diagram below shows the different types of explicit exchanges that can be made between the application and module.



(1) Only with READ_STS and WRITE_CMD instructions.

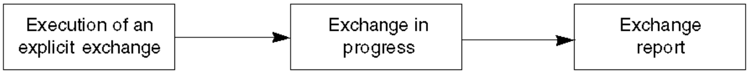
Managing Exchanges

During an explicit exchange, check performance to see that the data is only taken into account when the exchange has been correctly executed.

To do this, two types of information is available:

- information concerning the exchange in progress *(see Unity Pro S, I/O Management, Block Library)*
- the exchange report *(see EcoStruxure™ Control Expert, I/O Management, Block Library)*

The following diagram describes the management principle for an exchange.



NOTE: In order to avoid several simultaneous explicit exchanges for the same channel, it is necessary to test the value of the word EXCH_STS (`%MWr.m.c.0`) of the IODDT associated to the channel before calling any EF addressing this channel.

Section 11.2
Language Objects and Generic IODDT Applicable to Communication Protocols

About this Section

This section presents the language objects and generic IODDT applicable to all communication protocols except Fipio and Ethernet.

What Is in This Section?

This section contains the following topics:

Details of IODDT Implicit Exchange Objects of Type T_COM_STS_GEN

Introduction

The following table presents the IODDT implicit exchange objects of type `T_COM_STS_GEN` applicable to all communication protocols except Fipio and Ethernet.

Error Bit

The table below presents the meaning of the detected error bit `CH_ERROR` (`%Ir.m.c.ERR`).

Standard Symbol	Type	Access	Meaning	Address
CH_ERROR	EBOOL	R	Communication channel error bit.	%Ir.m.c.ERR

Details of IODDT Explicit Exchange Objects of Type T_COM_STS_GEN

Introduction

This section presents the `T_COM_STS_GEN` type IODDT explicit exchange objects applicable to all communication protocols except Fipio and Ethernet. It includes the word type objects whose bits have a specific meaning. These objects are presented in detail below.

Sample Variable Declaration: `IODDT_VAR1` of type `T_COM_STS_GEN`

Observations

- In general, the meaning of the bits is given for bit status 1. In specific cases an explanation is given for each status of the bit.
- Not all bits are used.

Execution Flags of an Explicit Exchange: EXCH_STS

The table below shows the meaning of channel exchange control bits from channel `EXCH_STS` (`%MWr.m.c.0`).

Standard Symbol	Type	Access	Meaning	Address
STS_IN_PROGR	BOOL	R	Reading of channel status words in progress.	%MWr.m.c.0.0
CMD_IN_PROGR	BOOL	R	Current parameter exchange in progress.	%MWr.m.c.0.1
ADJ_IN_PROGR	BOOL	R	Adjustment parameter exchange in progress.	%MWr.m.c.0.2

Explicit Exchange Report: EXCH_RPT

The table below presents the meaning of the exchange report bits `EXCH_RPT` (`%MWr.m.c.1`).

Standard Symbol	Type	Access	Meaning	Address
STS_ERR	BOOL	R	Reading error for channel status words.	%MWr.m.c.1.0
CMD_ERR	BOOL	R	Error during command parameter exchange.	%MWr.m.c.1.1
ADJ_ERR	BOOL	R	Error during adjustment parameter exchange.	%MWr.m.c.1.2

Standard Channel Faults, CH_FLT

The table below shows the meaning of the bits of the status word `CH_FLT` (`%MWr.m.c.2`). Reading is performed by a `READ_STS` (`IODDT_VAR1`).

Standard Symbol	Type	Access	Meaning	Address
NO_DEVICE	BOOL	R	No device is working on the channel.	%MWr.m.c.2.0
1_DEVICE_FLT	BOOL	R	A device on the channel is inoperative.	%MWr.m.c.2.1
BLK	BOOL	R	Terminal block not connected.	%MWr.m.c.2.2
TO_ERR	BOOL	R	Time out exceeded anomaly.	%MWr.m.c.2.3
INTERNAL_FLT	BOOL	R	Internal detected error or channel self-testing.	%MWr.m.c.2.4
CONF_FLT	BOOL	R	Different hardware and software configurations.	%MWr.m.c.2.5
COM_FLT	BOOL	R	Interruption of the communication with the PLC.	%MWr.m.c.2.6
APPLI_FLT	BOOL	R	Application detected error (adjustment or configuration).	%MWr.m.c.2.7

Section 11.3
The Language Objects and IODDTs Associated with Ethernet Communication

Purpose

This section shows the language objects and IODDTs associated with Ethernet communication.

What Is in This Section?

This section contains the following topics:

Details of Implicit Exchange Objects of the IODDT of Type T_COM_ETY_1X0

Introduction

The IODDT of type `T_COM_ETY_1X0` has implicit exchange objects, which are described below. This type of IODDT applies to the modules TSX ETY 110 and TSX ETY 120.

Example of declaring a variable: `IODDT_VAR1` of type `T_COM_ETY_1X0`

Generally speaking, the meaning of bits is given for state 1 of this bit. In specific cases, the two states of the bit are explained.

List of Implicit Exchange Objects

⚠ WARNING

UNEXPECTED APPLICATION BEHAVIOR-VALIDITY OF COMMON WORDS

The update bit switches to 1 at the beginning of the PLC cycle if it receives common words from the corresponding station. At the end of the cycle the update bits automatically return to 0.

Consequently, common words can only be considered valid if the update bit of the corresponding station is set to 1.

After power up, common words are set to value 0.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The table below shows the implicit exchange objects of the IODDT of type `T_COM_ETY_1X0` which applies to the two modules TSX ETY110/120.

Standard symbol	Type	Access	Meaning	Address
CH_ERROR	EBOOL	R	Line error bit.	%Ir.m.c.ERR
NET_STS	BOOL	R	Reception bit of common words of at least one of the remote stations	%Ir.m.c.0.0
REFRESH_ID_0 to REFRESH_ID_15	BOOL	R	Indicates that the common words of the station 0 to 15 are refreshed	%Ir.m.c.1.0 to %Ir.m.c.1.15
REFRESH_ID_16 to REFRESH_ID_31	BOOL	R	Indicates that the common words of the station 16 to 31 are refreshed	%Ir.m.c.2.0 to %Ir.m.c.2.15
REFRESH_ID_32 to REFRESH_ID_47	BOOL	R	Indicates that the common words of the station 32 to 47 are refreshed	%Ir.m.c.3.0 to %Ir.m.c.3.15
REFRESH_ID_48 to REFRESH_ID_63	BOOL	R	Indicates that the common words of the station 48 to 63 are refreshed	%Ir.m.c.4.0 to %Ir.m.c.4.15

Details of Explicit Exchange Objects of the IODDT of Type T_COM_ETY_1X0

Introduction

This topic describes the explicit exchange objects of the IODDT of type `T_COM_ETY_1X0` which applies to the two modules TSX ETY 110 and TSX ETY 120. It includes word-type objects whose bits have a special meaning. These objects are described in detail below.

Example of declaring a variable: `IODDT_VAR1` of type `T_COM_ETY_1X0`

Remarks

- Generally speaking, the meaning of bits is given for state 1 of this bit. In specific case, each state of the bit is explained.
- Not all bits are used.

Explicit Exchange Indicators: EXCH_STS

The table below gives the meanings of the exchange control bits of the channel `EXCH_STS` (%MWr.m.c.0).

Standard symbol	Type	Access	Meaning	Address
STS_IN_PROGR	BOOL	R	Reading of status words of the channel in progress.	%MWr.m.c.0.0
CMD_IN_PROGR	BOOL	R	Exchange of parameters of command in progress	%MWr.m.c.0.1
ADJ_IN_PROGR	BOOL	R	Exchange of parameters of adjustment in progress	%MWr.m.c.0.2

Explicit exchange report: EXCH_RPT

The table below gives the meanings of the report bits `EXCH_RPT` (%MWr.m.c.1).

Standard symbol	Type	Access	Meaning	Address
STS_ERR	BOOL	R	Error in reading status words of the channel	%MWr.m.c.1.0
CMD_ERR	BOOL	R	Error when exchanging command parameters	%MWr.m.c.1.1
ADJ_ERR	BOOL	R	Error when exchanging adjustment parameters	%MWr.m.c.1.2

Standard Channel Faults, CH_FLT

The table below gives the meanings of the status word bits `CH_FLT` (%MWr.m.c.2). The reading is taken by a `READ_STS` (`IODDT_VAR1`).

Standard symbol	Type	Access	Meaning	Address
INTERNAL_FLT	BOOL	R	Internal or channel self-test fault	%MWr.m.c.2.4
APPLI_FLT	BOOL	R	Application fault (adjustment or configuration fault)	%MWr.m.c.2.7

Details of Implicit Exchange Objects of the IODDT of Type T_COM_ETYX103

Introduction

This topic describes the implicit exchange objects of the IODDT of type `T_COM_ETYX103` which applies to the modules TSX ETY 4103/PORT/5103 and TSX WMY 100. It includes word-type objects whose bits have a special meaning. These objects are described in detail below.

Example of declaring a variable: `IODDT_VAR1` of type `T_COM_ETYX103`

List of Implicit Exchange Objects

The table below shows the implicit exchange objects of the IODDT of type `T_COM_ETYX103` which applies to the modules TSX ETY4103/PORT/5103.

Standard symbol	Type	Access	Meaning	Number
CH_ERROR	EBOOL	R	Line error bit.	%Ir.m.c.ERR
REFRESH_IO_0 to REFRESH_IO_15	BOOL	R	Indicates that the Inputs/Outputs of I/O scanning from station 0 to 15 are refreshed	%IWr.m.c.1.0 to %IWr.m.c.1.15
REFRESH_IO_16 to REFRESH_IO_31	BOOL	R	Indicates that the Inputs/Outputs of I/O scanning from station 16 to 31 are refreshed	%IWr.m.c.2.0 to %IWr.m.c.2.15
REFRESH_IO_32 to REFRESH_IO_47	BOOL	R	Indicates that the Inputs/Outputs of I/O scanning from station 32 to 47 are refreshed	%IWr.m.c.3.0 to %IWr.m.c.3.15
REFRESH_IO_48 to REFRESH_IO_63	BOOL	R	Indicates that the Inputs/Outputs of I/O scanning from station 48 to 63 are refreshed	%IWr.m.c.4.0 to %IWr.m.c.4.15
VALID_GD_0 to VALID_GD_15	BOOL	R	Indicates that the Global Data from the station 0 to 15 are refreshed	%IWr.m.c.6.0 to %IWr.m.c.6.15
VALID_GD_16 to VALID_GD_31	BOOL	R	Indicates that the Global Data from the station 16 to 31 are refreshed	%IWr.m.c.7.0 to %IWr.m.c.7.15
VALID_GD_32 to VALID_GD_47	BOOL	R	Indicates that the Global Data from the station 32 to 47 are refreshed	%IWr.m.c.8.0 to %IWr.m.c.8.15
VALID_GD_48 to VALID_GD_63	BOOL	R	Indicates that the Global Data from the station 48 to 63 are refreshed	%IWr.m.c.9.0 to %IWr.m.c.9.15

Details of Explicit Exchange Objects of the IODDT of Type T_COM_ETYX103

Introduction

This topic describes the explicit exchange objects of the IODDT of type `T_COM_ETYX103` that applies to the modules TSX ETY 4103/PORT/5103 and TSX WMY 100. It includes word-type objects whose bits have a special meaning. These objects are described in detail below.

Example of declaring a variable: `IODDT_VAR1` of type `T_COM_ETYX103`

NOTE: Generally speaking, the meaning of bits is given for state 1 of this bit. In specific cases, each state of the bit is explained.
Also note that not all bits are used.

Explicit Exchange Indicators: EXCH_STS

The table below gives the meanings of the exchange control bits of the channel `EXCH_STS` (%MWr.m.c.0).

Standard Symbol	Type	Access	Meaning	Address
STS_IN_PROGR	BOOL	R	Reading of status words of the channel in progress.	%MWr.m.c.0.0
CMD_IN_PROGR	BOOL	R	Exchange of parameters of command in progress	%MWr.m.c.0.1
ADJ_IN_PROGR	BOOL	R	Exchange of parameters of adjustment in progress	%MWr.m.c.0.2

Explicit Exchange Report: EXCH_RPT

The table below gives the meanings of the report bits `EXCH_RPT` (%MWr.m.c.1).

Standard Symbol	Type	Access	Meaning	Address
STS_ERR	BOOL	R	Error in reading status words of the channel	%MWr.m.c.1.0
CMD_ERR	BOOL	R	Error when exchanging command parameters	%MWr.m.c.1.1
ADJ_ERR	BOOL	R	Error when exchanging adjustment parameters	%MWr.m.c.1.2

Standard Channel Faults: CH_FLT

The table below gives the meanings of the status word bits `CH_FLT` (%MWr.m.c.2). The reading is taken by a `READ_STS` (`IODDT_VAR1`).

Standard Symbol	Type	Access	Meaning	Address
INTERNAL_FLT	BOOL	R	Internal or channel self-test fault	%MWr.m.c.2.4
APPLI_FLT	BOOL	R	Application fault (adjustment or configuration fault)	%MWr.m.c.2.7

Network Diagnostics

The table below shows the status words (or double words) `CH_FLT` (%MWr.m.c.3 to 6, %MWr.m.c.11 to 15 and %MDr.m.c.7 and 9) used for diagnosing the network. The reading is taken by a `READ_STS` (`IODDT_VAR1`).

Standard Symbol	Type	Access	Meaning	Address
NB_P502_CNX	INT	R	Number of Port 502 connections and bridge configuration information	%MWr.m.c.3
NB_DENIED_CNX	INT	R	Number of denied Port 502 connections)	%MWr.m.c.4
NB_P502_REF	INT	R	Number of refused messages on Port 502	%MWr.m.c.5
XWAY_ADDR	INT	R	X-Way address (Network, station)	%MWr.m.c.6
NB_SENT_MSG	DINT	R	Number of sent messages on Port 502	%MDr.m.c.7
NB_RCV_MSG	DINT	R	Number of received messages on Port 502	%MDr.m.c.9
NB_IOS_MSG	INT	R	Number of I/O Scanner messages received	%MWr.m.c.11
NB_IOS_CNX	INT	R	Number of error-free modules scanned	%MWr.m.c.12
GLBD_ERROR	INT	R	Detected consistency error in Global Data	%MWr.m.c.13
BW_GLBD_IOS	INT	R	The Least Significant Byte of this word measures the percentage of load relating to IO Scanning. The Most Significant Byte of this word measures the percentage of load relating to Global Data.	%MWr.m.c.14
BW_OTHER_MSG	INT	R	Loading of messaging service and other services	%MWr.m.c.15

Details of Implicit Exchange Objects of the IODDT of Type T_COM_ETHCOPRO

Introduction

This topic describes the implicit exchange objects of the IODDT of type `T_COM_ETHCOPRO` that apply to the Ethernet channel of the TSX P57 6634/5634/4634 (channel 3). It concerns those word type objects whose bits have particular meanings. These objects are described in detail below.

Example of declaring a variable: `IODDT_VAR1` of type `T_COM_ETHCOPRO`

List of Implicit Exchange Objects

The table below shows the implicit exchange objects of the IODDT of type `T_COM_ETHCOPRO`, which applies to the Ethernet channel of the TSX P57 6634/5634/4634.

Standard symbol	Type	Access	Meaning	Address
CH_ERROR	EBOOL	R	Line error bit.	%Ir.m.3.ERR
REFRESH_IO_0 to REFRESH_IO_15	BOOL	R	Indicates that the inputs/outputs of I/O scanning from station 0 to 15 are refreshed.	%IWr.m.3.1.0 to %IWr.m.3.1.15
REFRESH_IO_16 to REFRESH_IO_31	BOOL	R	Indicates that the inputs/outputs of I/O scanning from station 16 to 31 are refreshed.	%IWr.m.3.2.0 to %IWr.m.3.2.15
REFRESH_IO_32 to REFRESH_IO_47	BOOL	R	Indicates that the inputs/outputs of I/O scanning from station 32 to 47 are refreshed.	%IWr.m.3.3.0 to %IWr.m.3.3.15
REFRESH_IO_48 to REFRESH_IO_63	BOOL	R	Indicates that the inputs/outputs of I/O scanning from station 48 to 63 are refreshed.	%IWr.m.3.4.0 to %IWr.m.3.4.15
REFRESH_IO_64 to REFRESH_IO_79	BOOL	R	Indicates that the inputs/outputs of I/O scanning from station 64 to 79 are refreshed.	%IWr.m.3.5.0 to %IWr.m.3.5.15
REFRESH_IO_80 to REFRESH_IO_95	BOOL	R	Indicates that the inputs/outputs of I/O scanning from station 80 to 95 are refreshed.	%IWr.m.3.6.0 to %IWr.m.3.6.15
REFRESH_IO_96 to REFRESH_IO_111	BOOL	R	Indicates that the inputs/outputs of I/O Scanning from station 96 to 111 are refreshed.	%IWr.m.3.7.0 to %IWr.m.3.7.15
REFRESH_IO_112 to REFRESH_IO_127	BOOL	R	Indicates that the inputs/outputs of I/O scanning from station 112 to 127 are refreshed.	%IWr.m.3.8.0 to %IWr.m.3.8.15
VALID_GD_0 to VALID_GD_15	BOOL	R	Indicates that the global data from the station 0 to 15 are refreshed.	%IWr.m.3.9.0 to %IWr.m.3.9.15

Standard symbol	Type	Access	Meaning	Address
VALID_GD_16 to VALID_GD_31	BOOL	R	Indicates that the global data from the station 16 to 31 are refreshed.	%IWr.m.3.10.0 to %IWr.m.3.10.15
VALID_GD_32 to VALID_GD_47	BOOL	R	Indicates that the global data from the station 32 to 47 are refreshed.	%IWr.m.3.11.0 to %IWr.m.3.11.15
VALID_GD_48 to VALID_GD_63	BOOL	R	Indicates that the global data from the station 48 to 63 are refreshed.	%IWr.m.3.12.0 to %IWr.m.3.12.15

Details of Explicit Exchange Objects of the IODDT of Type T_COM_ETHCOPRO

Overview

This part shows the explicit exchange objects of the IODDT of type `T_COM_ETHCOPRO` which applies to the Ethernet channel of the TSX P57 6634/5634/4634. It includes word-type objects whose bits have special meanings. These objects are described in detail below.

Example of declaring a variable: `IODDT_VAR1` of type `T_COM_ETHCOPRO`

About the Bits

- Generally speaking, the meaning of bits is given for state 1 of this bit. In specific cases, each state of the bit is explained.
- Not all bits are used.

Explicit Exchange Indicators: EXCH_STS

The table below gives the meanings of the exchange control bits of the channel `EXCH_STS` (%MWr.m.c.0).

Standard symbol	Type	Access	Meaning	Address
STS_IN_PROGR	BOOL	R	Status parameter read in progress	%MWr.m.c.0.0

Standard Channel Faults, CH_FLT

The table below gives the meanings of the status word bits `CH_FLT` (%MWr.m.c.2). The reading is taken by a `READ_STS` (`IODDT_VAR1`).

Standard symbol	Type	Access	Meaning	Address
INTERNAL_FLT	BOOL	R	Internal fault: Channel inoperative	%MWr.m.c.2.4
APPLI_FLT	BOOL	R	Application fault	%MWr.m.c.2.7

Network Diagnostics

The table below shows the status words (or double words) `CH_FLT` (%MWr.m.c.3 to 6, %MWr.m.c.11 to 15 and %MDr.m.c.7 and 9) used for diagnosing the network. The reading is taken by a `READ_STS` (`IODDT_VAR1`).

Standard symbol	Type	Access	Meaning	Address
NB_P502_CNX	INT	R	Number of connections on the Port 502 and bridge configuration information	%MWr.m.c.3
NB_DENIED_CNX	INT	R	Number of denied Port 502 connections)	%MWr.m.c.4
NB_P502_REF	INT	R	Number of refused messages on Port 502	%MWr.m.c.5
XWAY_ADDR	INT	R	X-Way address (Net, Sta)	%MWr.m.c.6
NB_SENT_MSG_L	INT	R	Number of sent messages on Port 502 (low)	%MDr.m.c.7
NB_SENT_MSG_H	INT	R	Number of sent messages on Port 502 (high)	%MDr.m.c.8
NB_RCV_MSG_L	INT	R	Number of received messages on Port 502 (low)	%MDr.m.c.9
NB_RCV_MSG_H	INT	R	Number of received messages on Port 502 (high)	%MDr.m.c10
NB_IOS_MSG	INT	R	Number of IO Scanner received messages	%MWr.m.c.11
NB_IOS_CNX	INT	R	Number of polled devices without errors	%MWr.m.c.12
GLBD_ERROR	INT	R	Detected consistency error in Global Data	%MWr.m.c.13
BW_GLBD_IOS	INT	R	The Least Significant Byte of this word measures the percentage of load relating to IO Scanning. The Most Significant Byte of this word measures the percentage of load relating to Global Data.	%MWr.m.c.14
BW_OTHER_MSG	INT	R	Load for other services and Messaging service	%MWr.m.c.15
IP_ADDR1	INT	R	IP Address	%MDr.m.c.16
IP_ADDR2	INT	R	IP Address	%MDr.m.c.17
IP_NETMASK1	INT	R	IP Subnet Mask	%MDr.m.c.18
IP_NETMASK2	INT	R	IP Subnet Mask	%MDr.m.c.19
IP_GATEWAY1	INT	R	IP Default gateway	%MDr.m.c.20
IP_GATEWAY2	INT	R	IP Default gateway	%MDr.m.c.21
MAC_ADDR1	INT	R	MAC Address	%MWr.m.c.22
MAC_ADDR2	INT	R	MAC Address	%MWr.m.c.23
MAC_ADDR3	INT	R	MAC Address	%MWr.m.c.24
FW_VERSION	INT	R	Firmware version	%MWr.m.c.25
BOARD_STS	INT	R	Board status	%MWr.m.c.26
NET_TIME1	INT	R	Network time	%MDr.m.c.27
NET_TIME2	INT	R	Network time	%MDr.m.c.28
NET_TIME3	INT	R	Network time	%MDr.m.c.29
NET_TIME4	INT	R	Network time	%MDr.m.c.30

Section 11.4
The IODDT Type T_GEN_MOD Applicable to All Modules

Details of the Language Objects of the T_GEN_MOD-Type IODDT

Introduction

Modules of Premium PLCs have an associated IODDT of type `T_GEN_MOD`.

Observations

- In general, the meaning of the bits is given for bit status 1. In specific cases, an explanation is given for each status of the bit.
- Not all bits are used.

List of Objects

The table below presents the objects of the IODDT:

Standard symbol	Type	Access	Meaning	Address
MOD_ERROR	BOOL	R	Module error bit	%Ir.m.MOD.ERR
EXCH_STS	INT	R	Module exchange control word	%MWr.m.MOD.0
STS_IN_PROGR	BOOL	R	Reading of status words of the module in progress	%MWr.m.MOD.0.0
EXCH_RPT	INT	R	Exchange report word	%MWr.m.MOD.1
STS_ERR	BOOL	R	Error detected while reading module status words	%MWr.m.MOD.1.0
MOD_FLT	INT	R	Internal error word of the module	%MWr.m.MOD.2
MOD_FAIL	BOOL	R	Internal error, inoperable module	%MWr.m.MOD.2.0
CH_FLT	BOOL	R	Channel error detected	%MWr.m.MOD.2.1
BLK	BOOL	R	Terminal block error	%MWr.m.MOD.2.2
CONF_FLT	BOOL	R	Hardware or software configuration mismatch	%MWr.m.MOD.2.5
NO_MOD	BOOL	R	Module missing or inoperative	%MWr.m.MOD.2.6
EXT_MOD_FLT	BOOL	R	Internal error word of the module (Fipio extension only)	%MWr.m.MOD.2.7
MOD_FAIL_EXT	BOOL	R	Module is unserviceable (Fipio extension only)	%MWr.m.MOD.2.8
CH_FLT_EXT	BOOL	R	Channel error detected (Fipio extension only)	%MWr.m.MOD.2.9
BLK_EXT	BOOL	R	Terminal block error detected (Fipio extension only)	%MWr.m.MOD.2.10

Standard symbol	Type	Access	Meaning	Address
CONF_FLT_EXT	BOOL	R	Hardware or software configuration mismatch (Fipio extension only)	%MWr.m.MOD.2.13
NO_MOD_EXT	BOOL	R	Module missing or inoperative (Fipio extension only)	%MWr.m.MOD.2.14

Section 11.5
Ethernet Configuration Language Objects

Purpose

This section describes the configuration language objects associated with the Ethernet communication modules on Premium and Atrium PLCs.

What Is in This Section?

This section contains the following topics:

Language Objects associated with the Configuration of a TSX ETY 110

At a Glance

This page describes the language objects for the configuration of a TSX ETY 110 module. These objects can be read by the application program.

Internal Constants

The following table describes the language objects for the configuration of a TSX ETY 110 module.

Object	Function	Meaning
%KWr.m.0.0	Type	Byte 0 = 11 for ETHWAY communication Byte 1: reserved
%KWr.m.0.1	Physical layer	Byte 0: reserved Byte 1: reserved
%KWr.m.0.2	Utilities supported	Byte 0: common data ● x0 = 1: activation of ETHWAY common words ● x1 = 0: reserved ● x2 = 1: common words read only ● x3 = 1: common words read/write ● x4 to x7 = 0: reserved Byte 1: reserved
%KWr.m.0.4	Common words	Byte 0: number of common words Byte 1: reserved
%KWr.m.0.5	X-Way network address	Byte 0: network number (0 by default) Byte 1: reserved
%KWr.m.0.6	Type of Ethernet driver for TCP/IP	Byte 0: ● = 16#00 : AUI (default value) ● = 16#01 : RJ45 Byte 1: ● = 16#00 : Ethernet II (default value) ● = 16#01 : 802.3
%KWr.m.0.7	TCP/IP configuration: address type	Byte 0: reserved Byte 1: inherited address ● = 16#00 : default address ● = 16#01 : from the application-specific function ● = 16#03 : from a server
%KWr.m.0.8 and %KWr.m.0.9	Local IP address	Example with the address 139.160.650.109 Byte 109 = 0 (least significant) Byte 1 = 65 Byte 2 = 160 Byte 3 = 139 (most significant)

Object	Function	Meaning
%KWr.m.0.10 and %KWr.m.0.11	IP address of gateway	Example with the address 139.160.65.1 Byte 0 = 1 Byte 1 = 65 Byte 2 = 160 Byte 3 = 139
%KWr.m.0.12 and %KWr.m.0.13	Subnetwork mask	Example with the address 255.255.255.0 Byte 0 = 0 Byte 1 = 255 Byte 2 = 255 Byte 3 = 255

Language Objects Associated with Configuration

Introduction

This topic describes the configuration language objects for Ethernet communication with the TSX ETY 4103/PORT/5103 module and the Ethernet channel of the TSX P57 6634/5634/4634, which can be displayed by the application program.

Internal Constants

The following table describes the internal constants:

Object	Function	Meaning
%KWr.m.c.0	Type	Byte 0 = 11 for Ethernet communication Byte 1: reserved
%KWr.m.c.1	Physical layer	Byte 0: fixed at 16#01 (corresponds to GPX2) Byte 1: reserved
%KWr.m.c.2	Reserved	-
%KWr.m.c.3	Reserved	-
%KWr.m.c.4	Reserved	-
%KWr.m.c.5	X-Way network address	Byte 0: network number (0 by default) Byte 1: reserved
%KWr.m.c.6	Type of Ethernet driver for TCP/IP	Byte 0: fixed at 16#01 (corresponds to RJ45) ● = 16#01: RJ45 Byte 1: ● = 16#00: Ethernet II (default value) ● = 16#01: 802.3
%KWr.m.c.7	TCP/IP configuration: address type	Byte 0: reserved Byte 1: inherited address ● = 16#01: from the application-specific function ● = 16#03: from a server
%KWr.m.c.8 and %KWr.m.c.9	Local IP address	Example with the address 139.160.650.109 Byte 0 = 109 Byte 1 = 65 Byte 2 = 160 Byte 3 = 139
%KWr.m.c.10 and %KWr.m.c.11	IP address of gateway	Example with the address 139.160.65.1 Byte 0 = 1 Byte 1 = 65 Byte 2 = 160 Byte 3 = 139

Object	Function	Meaning
%KWr.m.c.12 and %KWr.m.c.13	Subnetwork mask	Example with the address 255.255.255.0 Byte 0 = 0 (least significant) Byte 1 = 255 Byte 2 = 255 Byte 3 = 255 (most significant)
%KWr.m.c.14	Services used	Byte 0: • bit 0 =1: I/O Scanner is used • bit 1 =1: BOOTP server is used • bit 2 =1: Global Data is used • bit 3 =1: bandwidth adjustment is used Byte 1: reserved
%KWr.m.c.15	TCP services used	Byte 0: • bit 0 =1: Modbus communication on TCP/IP is used • bit 1 =1: access control is activated Byte 1: reserved

Chapter 12
Questions/Answers

Questions/Answers

General

Below you will find a list of the most frequently asked questions and answers regarding communication by Ethernet network.

Can a Momentum be searched by several ENT at a time?

Yes, in read only. Only one IO Scanner at a time should access the ENT in write mode,

Do I have to configure the IO Scanner connections in the connections table ("Messaging" tab)?

No.

What should I do if the TSX ETY 4103/PORT5103 module displays the LED status "Not configured" (Flashing ERR)?

- Check that it is configured in Control Expert.
- Check that there is no other module with the same X-Way network number in the PLC configuration.
- If the module is configured in "Servie address", make sure that a BOOTP server is operational and accessible.

What should I do if the module displays a correct LED status (STS=RUN=ON) but does not respond to requests?

Try a Ping command to this IP address, from a device on the same network:

- No response:
  - Check the network configuration: wiring, "hubs" status, IP addresses, masks and gateways if there are routers in the configuration.
- Correct response to the Ping:
  - Check the module's X_WAY address.
  - Check whether access control is activated or not.
  - Try to connect to the Rack Viewer page by http. If this connection works, check the X-Way address of the client application.

Can I change the MAC address of the module?

No. This is fixed for every Ethernet device to guarantee its unicity.

How can I find out the speed with which the module communicates?

Via an internet browser, by connecting to the Ethernet Module Statistics page.

What should I do if the messaging EFs do not get a response?

- Check that the X-Way destination address is part of the IP/X-Way connections table.
- Check that the configuration of the destination module does not prohibit this connection (access control).
- In debug mode, try the "Ping" command towards the IP address of the destination PLC, then try an "Identification" request towards the destination address, if it is part of the same X-Way network.

What should I do if I receive the 0xFF12 refusal code on the messaging EFs?

This code indicates that the module is full. Reduce the transition rate.

What should I do if the READ_ASYNC, WRITE_ASYN messaging EFs do not get a response (time out)?

Check that the "mast" tasks of the client and server PLCs are configured to "periodic", with a sufficient period to ensure that the PLCs are not overrun.

When should I configure my connections to "Mono-Connection"?

When this connection has to be established to a TSX ETY 110, Modbus protocol.

The destination PLC of my messages is a bridge. Which X-Way destination address should I configure in the connections table?

The X-Way address of the first communication module of the PLC bridge (if present, it is the processor PCMCIA card).

I have changed the IP addresses in Address Server and IO Scanner configuration, should I restart my client/server devices?

Yes. The devices only receive their IP address when starting up. This restart should be carried out once the TSX ETY 4103/5103 module has been reconfigured (fixed RUN and STS LEDs).

In the module configuration screens, the last entry inserted into one of the grids has not been taken into account at the validation. Why?

You need to remove the focus (the scale indicator) from the last cell of the grid in which new data has been entered in order to take this modification into account.

Why is the Bridge tab grayed out when I use a processor of type ???????????

These processors do not manage bridge data.

Why is the Bridge tab grayed out when I have already changed the position of the processor?

After this type of modification, you have to validate the new hardware configuration to access and modify the bridge data managed globally at the level of the processor.

The momentum 170 ENT modules do not manage to obtain their client/server address from the address server of the TSX ETY 4103, TSX ETY PORT or TSX ETY 5103 modules.

- Check in the TSX ETY 4103 or TSX ETY PORT module configuration that the subnetwork mask agrees with the IP address class.
- Check the software version of the 170 ENT module.

Global Data does not work. Why?

Make sure that the network switches are not configured in "multicast filtering".

Appendices

Introduction

These technical appendices supplement the information in this guide.

What Is in This Appendix?

The appendix contains the following chapters:

Appendix A
Schneider Private MIB

About this Chapter

This chapter provides the detailed tree structure of the Schneider private MIB and a description of its services.

What Is in This Chapter?

This chapter contains the following topics:

The Schneider Private MIB

Introduction

A MIB (Management Information Base) is an element used in network management. Network management services are based on the need to monitor and manage:

- performance
- fault occurrences
- security

NOTE: The Transparent Factory private MIB does not define specific management applications and policies.

Each MIB contains a finite number of objects. Use the SNMP manager's GET and SET to retrieve system information and to set system environment variables.

Schneider Private MIB

The Transparent Factory SNMP-embedded component controls the Schneider private MIB function. This private MIB, and its associated services, manages all system components. The private MIB provides the data to manage the main Transparent Factory communication services for all the communication components of the Transparent Factory architecture, including:

- Ethernet communication modules (NOE, ETY, M1E, etc.)
- CPUs with Ethernet communication ports

Elsewhere in this guide is the detailed tree structure of the transparentFactoryEthernet MIB *(see page 418)*.

Private MIB Identifier

Schneider Electric obtained a Private Enterprise Number (PEN) from the Internet Assigned Numbers Authority (IANA). That number represents a subtree in the SNMP MIB, a number that is a unique identifier used for Groupe Schneider.

The object identifier for the root of the Groupe Schneider subtree is `1.3.6.1.4.1.3833` and represents a path to the subtree as follows:

```
iso(1)
    org(3)
        dod(6)
            internet(1)
                private(4)
                    enterprises(1)
                        groupeschneider(3833)
                            transparentFactoryEthernet(1)
```

Under the Groupe Schneider private MIB is a TFE private MIB, transparentFactoryEthernet(1).

Schneider Private MIB Tree Structure

Introduction

This topic outlines the tree structure for the private Schneider MIB (Schneider TFE-V01-04.mib) for all Transparent Ready products.

The groupeschneider (3833) subtree is the root of Groupe Schneider's private MIB in the Structure of Management Information (SMI) used by SNMP and defined in RFC-1155, a specification that defines the structure and identification of management information for TCP/IP-based networks.

Tree Structure

```
groupeschneider (3833)
(1) transparentFactoryEthernet
|---(1) switch
|------(14) saConfiguration
|----------(1) saChassis
|----------(2) saAgent
|----------(3) saUserGroup
|----------(5) saRingRedundancy
|----------(7) saLLDP
|------(15) saPlatform4
|----------(1) saPlatform4BasicL2
|---(2) Port502Messaging
|------(1) port502Status
|------(2) port502SupportedProtocol
|------(3) port502IpSecurity
|------(4) port502MaxConn
|------(5) port502LocalConn
|------(6) port502RemConn
|------(7) port502IpSecurityTable
|----------(1) port502IpSecurityEntry
|--------------(1) attemptFails
|--------------(2) ipSourceAddress
|------(8) port502ConnTable
|----------(1) port502ConnEntry
|----------(1) port502ConnLocalPort
```

```
|----------(2) port502ConnRemAddress
|----------(3) port502ConnRemPort
|----------(4) port502ConnType
|----------(5) port502ConnMsgIn
|----------(6) port502ConnMsgOut
|----------(7) port502ConnMsgErr
|----------(8) port502XwayNet
|----------(9) port502XwayStation
|------(9) port502MsgIn
|------(10) port502MsgOut
|------(11) port502MsgOutErr
|------(12) port502AddStackStat
|------(13) port502AddStackStatTable
|------------(1) port502AddStackStatEntry
|----------------(1) port502AddStackStatIndex
|----------------(2) port502PeaKTcpRetransSegs
|---(3) ioScanning
|------(1) ioScanStatus
|------(2) ioScanMaxDevice
|------(3) ioScanPolledDevice
|------(4) ioScanTransSend
|------(5) ioScanGlbHealth
|------(6) ioScanningDeviceTable
|----------(1) ioScanDeviceEntry
|--------------(1) IoScanDeviceRemAddress
|--------------(2) IoScanDeviceHealth
|--------------(3) IoScanDeviceRate
|--------------(4) ioScanInputLocalAddress
|--------------(5) ioScanOutputLocalAddress
|---(4) globalData
|------(1) glbDataStatus
|------(2) glbDataMaxPub
|------(3) glbDataMaxSub
```

```
|------(4) glbDataPub
|------(5) glbDataSub
|------(6) glbDataPubErr
|------(7) glbDataSubErr
|------(8) glbDataGlbSubHealth
|------(9) glbDataPubTable
|----------(1) glbDataPubEntry
|--------------(1) glbDataPubSourceAddress
|--------------(2) glbDataPubHostId
|--------------(3) glbDataPubNetId
|--------------(4) glbDataPubGroupId
|--------------(5) glbDataPubCnt
|--------------(6) glbDataPubErrCnt
|--------------(7) glbDataPubDistribRate
|--------------(8) glbDataPubDuplicateErr
|------(10) glbDataSubTable
|--------------(1) glbDataSubEntry
|------------------(1) glbDataSubSourceAddress
|------------------(2) glbDataSubHostId
|------------------(3) glbDataSubNetId
|------------------(4) glbDataSubGroupId
|------------------(5) glbDataSubCnt
|------------------(6) glbDataSubErrCnt
|------------------(7) glbDataMinimumSeparation
|------------------(8) glbDataHealth
|------------------(9) glbDataHealthTimeOut
|------------------(10) glbDataLastRecErr
|---(5) Web
|------(1) webStatus
|------(2) webPassword
|------(3) webSuccessfullAccess
|------(4) webFailedAttempts
|---(6) addressServer
```

```
|------(1) addressServerStatus
|---(7) equipmentProfile
|------(1) profileProductName
|------(2) profileVersion
|------(3) profileCommunicationServices
|------(4) profileGlobalStatus
|------(5) profileConfigMode
|------(6) profileRoleName
|------(7) profileBandwidthMgt
|------(8) profileBandwidthDistTable
|---------(1) profileBandwidthDistEntry
|------------(1) bandwidthDistributionIndex
|------------(2) port502Bandwidth
|------------(3) ioScanningBandwidth
|------------(4) globalDataBandwidth
|------------(5) otherBandwidth
|------(9) profileLedDisplayTable
|---------(1) profileLedDisplayEntry
|------------(1) ledIndex
|------------(2) ledName
|------------(3) ledDescr
|------------(4) ledState
|------(10) profileSlot
|------(11) profileCPUType
|------(12) profileTrapTableEntriesMax
|------(13) profileTrapTable
|---------(1) profileTrapEntry
|------------(1) trapCommunityName
|------------(2) remoteIpAddress
|------------(3) authenticationTrap
|------------(4) port502Trap
|------------(5) ioScanningTrap
|------------(6) globalDataTrap
```

```
|------------(7) webTrap
|------------(8) addressServerTrap
|------------(9) profileTrap
|------------(10) timeManagementTrap
|------------(11) emailTrap
|------(14) profileSpecificId
|------(15) profileIpAddress
|------(16) profileIpNetMask
|------(17) profileIpGateway
|------(18) profileMacAddress
|------(19) profileImplementationClass
|------(100) premiumProfile
|------(101) quantumProfile
|------------(100) qnoe
|---------------(1) qNoeCommand
|------(102) microProfile
|------------(100) mEtz
|---------------(1) etzIpMgtStatus
|---------------(2) etzIpMgtDhcpTries
|---------------(3) etzIpMgtDhcpMode
|---------------(4) etzRepUserBkups
|---------------(5) etzRepAutoBkups
|---------------(6) etzRepStatus
|---------------(7) etzRepTFPcnxErrors
|---------------(8) etzRepTFPxferErrors
|------(103) momentumIoProfile
|------------(1) momentumIoBaseType
|------------(2) momentumIoBaseName
|------------(3) momentumIoMasterIPTable
|---------------(1) momentumIoMasterIPEntry
|------------------(1) momentumIoMasterIPValue
|------------(4) momentumIoModuleTimeOut
|------------(5) momentumIoASCIIModuleHeader
```

```
|------------(6) momentumIoReservationTime
|------------(7) momentumIoInputDataTable
|---------------(1) momentumIoInputDataEntry
|------------------(1) momentumIoInputDataIndex
|------------------(2) momentumIoInputDataValues
|------------------(3) momentumIoInputDataWords
|------------------(4) momentumIoInputDataPoints
|------------(8) momentumIoOutputDataTable
|---------------(1) momentumIoOutputDataEntry
|------------------(1) momentumIoOutputDataIndex
|------------------(2) momentumIoOutputDataValues
|------------------(3) momentumIoOutputDataWords
|------------------(4) momentumIoOutputDataPoints
|------(104) momentumM1eProfile
|------(105) advantysProfile
|------(106) gatewayProfile
|------(107) modiconM340Profile
|------(255) tfProducts
|------------(1) ety
|------------(2) noe
|------------(3) etz
|------------(4) momentumIo
|------------(5) momentumM1e
|------------(6) altivar
|------------(7) stbNip
|------------(8) tsxntp
|------------(9) nwm
|------------(10) wmy
|------------(11) quantumPLC
|------------(12) premiumPLC
|------------(13) etg
|------------(14) egx
|------------(15) ecc
```

```
|------------(16) cev
|------------(17) inducteIXGKS
|------------(18) ositrackTAP
|------------(19) twidoPLC
|------------(20) modiconM340PLC
|------------(21) modiconM340DPLC
|------------(22) modiconM340CPLC
|------------(23) modiconM340NOE
|---(8) timeManagement
|------(1) ntp
|--------(1) ntpStatus
|--------(2) ntpSrvAddr
|--------(3) ntpLnkSrvStatus
|--------(4) ntpReqCnt
|--------(5) ntpRespCnt
|--------(6) ntpErrCnt
|--------(7) ntpDate
|--------(8) ntpTime
|--------(9) ntpTimeZone
|--------(10) ntpDSTStatus
|--------(11) ntpLastErr
|---(9) email
|------(1) smtp
|---------(1) emailTable
|------------(1) emailEntry
|--------------(1) emailIndex
|--------------(2) smtpStatus
|--------------(3) smtpSrvAddr
|--------------(4) smtpMailSentCnt
|--------------(5) smtpErrCnt
|--------------(6) smtpLastErr
|--------------(7) smtpLastMailElapsedTime
|--------------(8) smtpLnkSrvStatus
```

```
|--------------(9) smtpSrvChkFailCnt
|---(255) tfeMibVersion
|------(1) tfeMibVersionNumber
|------(2) tfeMibVersionDate
```

MIB Subtree Description

Transparent Factory Ethernet Subtree

This topic details some of the objects in the Schneider private MIB tree. The **transparentFactoryEthernet(1)** subtree defines groups that support the TFE services and devices:

Service	Subtree Definition
switch(1) *(see page 427)*	the brand of switches labeled
port502Messaging(2) *(see page 428)*	objects for managing explicit client/server communications to support applications (for example, HMI, SCADA, or programming tools)
ioScanning(3) *(see page 429)*	objects for managing I/O device communications that use the I/O Scanner with the Modbus/TCP protocol
globalData(4) *(see page 430)*	objects for managing the application coordination service using a publish/subscribe protocol
web(5)	objects for managing the activity of the embedded Web servers
addressServer(6) *(see page 432)*	objects for managing the activity of the BOOTP or DHCP servers
equipmentProfile(7) *(see page 433)*	objects for each device type in Transparent Factory Ethernet product portfolio
timeManagement(8) (NTP) *(see page 435)*	objects for managing the UTC time stamp service
email(9) (SMTP) *(see page 436)*	objects for managing the email service
tfeMibVersion(255) *(see page 437)*	the version of the Schneider TFE MIB supported by the product

NOTE: All listed services are not available on all communications modules. Refer to the available services for your module.

When devices are added to the Schneider catalog, the private MIB is extended in the following manner:

- If needed, a Transparent Factory communication-service object is added for the new device in the subtree that corresponds to **equipmentProfile(7)** *(see page 433)*. This subtree can hold as many objects as are required.
- If needed, a new branch is added at the same level as **transparentFactoryEthernet(1)**. This subtree is created for product-specific objects.

When a new device is added to the catalog a corresponding object description is created in the ASN.1 format. The ASN.1 file(s) are then given to producers of SNMP manager software for inclusion in their products.

Switch Subtree Description

Switch Subtree

The switch (1) subtree, or group, indicates the brand of switches labeled. The following list describes the function of each object.

Service	Indicates . . .
saChassis(1)	configuration of the chassis
saAgent(2)	configuration of Agent
saRingRedundancy(3)	management of Ring Redundancy
saUserGroup(5)	management of user groups
saLLDP(7)	management of proprietary extensions of 802.1AB (station and Media access control Connectivity Discovery)

Port 502 Messaging Subtree Description

Port 502 Messaging Subtree

The port502Messaging (2) subtree, or group, provides connection management and data flow services. The following list describes the function of each object.

Service	Indicates . . .
port502Status(1)	status of the service (idle or operational)
port502SupportedProtocol(2)	supported protocols (MODBUS, X-way, etc.)
port502IpSecurity(3)	status of the Port 502 IP Security service (enabled or disabled)
port502MaxConn(4)	maximum number of TCP connections supported by the Port 502 entity
port502LocalConn(5)	number of TCP connections currently opened by the local Port 502 entity
port502RemConn(6)	number of TCP connections currently opened by the remote entity to the local Port 502 entity
port502IpSecurityTable(7)	a table containing the number of unsuccessful attempts to open a TCP connection from a remote TCP entity
port502ConnTable(8)	a table containing Port 502 TCP specific information (MsgIn, MsgOut)
port502MsgIn(9)	total number of Port 502 messages received from the network
port502MsgOut(10)	total number of Port 502 messages sent from the network
port502MsgOutErr(11)	total number of diagnostic messages built by the Port 502 messaging entity and sent to the network
port502AddStackStat(12)	the support of additional Port 502 stack statistics
port502AddStackStatTable(13)	additional stack statistics for Port 502 (optional)

I/O Scanning Subtree Description

I/O Scanning Subtree

The ioScanning (3) subtree, or group, contains the objects related to I/O scanning device management and associated Modbus communications on port 502.

Service	Indicates . . .
ioScanStatus(1)	global status of the I/O scanning service
ioScanMaxDevice(2)	maximum number of devices supported by the I/O scanning entity
ioScanPolledDevice(3)	number of devices currently polled by the I/O scanning entity
ioScanTransSend(4)	total number of transactions sent by the I/O scanning entity
ioScanGlbHealth(5)	global health status for the I/O scanning service
ioScanningDeviceTable(6)	a table containing information on each remote device polled by the I/O scanning entity

Global Data Subtree Description

Global Data Subtree

The globalData (4) subtree, or group, contains the objects related to Global Data.

Service	Indicates . . .
glbDataStatus(1)	global status of the Global Data service
glbDataMaxPub(2)	maximum number of published variables configured by the Global Data entity
glbDataMaxSub(3)	maximum number of subscribed variables configured by the Global Data entity
glbDataPub(4)	total number of publications sent to the network
glbDataSub(5)	total number of subscriptions received from the network
glbDataPubErr(6)	total number of publication errors detected by the local entity
glbDataSubErr(7)	total number of subscription errors detected by the local entity
glbDataGlbSubHealth(8)	global health status of the Global Data service
glbDataPubTable(9)	a table containing information on each published variable (the number of publications, the source IP address, the number of errors, etc.)
glbDataSubTable(10)	a table containing information on each subscribed variable (the number of subscriptions, the source IP address, the number of errors, health, etc.)

Web Subtree Description

Web Subtree

The web (5) subtree, or group, contains the objects related to the Web server service.

Service	Indicates . . .
webStatus(1)	global status of the Web service
webPassword(2)	enable or disable Web passwords
webSuccessfullAccess(3)	total number of successful attempts to access Web site
webFailedAttempts(4)	total number of failed attempts to access Web site

Address Server Subtree Description

Address Server Subtree

The addressServer (6) subtree, or group, contains the objects related to the Address Server. The address server can be either a BOOTP server or a DHCP server.

Service	Indicates . . .
addressServerStatus(1)	global status of the address server service

Equipment Profile Subtree Description

Equipment Profile Subtree

The equipmentProfile (7) subtree contains a set of common objects.

Service	Indicates . . .
profileProductName(1)	the commercial name of the communication product in string form (for example: 140 NOE 771 11, BMX NOE 0100, etc.)
profileVersion(2)	the software version of the communication product in string form (for example, Vx.y or V1.1)
profileCommunicationServices(3)	the communication services supported by the profile (Port502Messaging, I/O scanning Messaging, Global Data, Web, and Address Server)
profileGlobalStatus(4)	the global status of the communication module
profileConfigMode(5)	the IP configuration mode of the communication module
profileRoleName(6)	the role name for the IP address management if it exists (empty string if there is none)
profileBandwidthMgt(7)	the status of Bandwidth Management
profileBandwidthDistTable(8)	the CPU time distribution between Global Data, Port 502 Messaging, I/O scanning
profileLedDisplayTable(9)	a table giving the name and the state of each module's LEDs
profileSlot(10)	the position of the communication module inside the rack if there is one (if there is no rack, the profileSlot value is 0)
profileCPUType(11)	the host for which that communication module is a part when a CPU type exists (if there is no host, the string is empty)
profileTrapTableEntriesMax(12)	the maximum numbers of entries in the Trap Table (equal to the number of possible remote managers)
profileTrapTable(13)	a table allowing you to enable or disable the private traps for each of the communication services
profileSpecificId(14)	a unique Profile Specific Identification inside the equipmentProfile object of the Schneider Transparent Factory MIB (for example, the PLC Premium family is 100)
profileIpAddress(15)	the IP address of the SNMP agent

Service	Indicates . . .
profileIpNetMask(16)	the subnetwork mask associated with the IP address of the SNMP agent (the value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0)
profileIpGateway(17)	the default Gateway IP address of the SNMP agent
profileMacAddress(18)	the Ethernet media-dependent address of the SNMP agent
profileImplementationClass(19)	a textual description of the implementation class supported by the product
premiumProfile(100)	managed products (ETY, ETY port)
quantumProfile(101)	managed products (NOE)
microProfile(102)	managed products (ETZ)
momentumIoProfile(103)	managed products (ENT)
momentumM1eProfile(104)	managed products (M1E)
advantysProfile(105)	managed products (STB NIP)
gatewayProfile(106)	managed products (ETG)
modiconM340profile(107)	managed products (Modicon M340 PLC)
tfProducts(225)	Transparent Factory products

Time Management Subtree Description

Time Management Subtree

The timeManagement (8) subtree contains a set of common NTP objects.

Service	Indicates . . .
ntpStatus(1)	the status of the NTP service (not server)
ntpSrvAddr(2)	the IP address of the NTP server in dot notation format
ntpLnkSrvStatus(3)	the status of the link between the module and the NTP server
ntpReqCnt(4)	the number of requests sent to the NTP server
ntpRespCnt(5)	the number of responses received from the NTP server
ntpErrCnt(6)	the total number of communication errors
ntpDate(7)	date of the day
ntpTime(8)	time of the day
ntpTimeZone(9)	current time zone
ntpDSTStatus(10)	daylight saving time status
ntpLastErr(11)	last error code generated by system

Email Subtree Description

Email Subtree

The email(9) subtree contains a set of common SMTP objects.

Service	Indicates . . .
emailIndex(1)	the index value in the email service table
smtpStatus(2)	the status of SMTP service (not server)
smtpSrvAddr(3)	the IP address of SMTP server in dot notation format
smtpMailSentCnt(4)	the total number of emails sent to the network and successfully acknowledged by the server
smtpErrCnt(5)	the total number of email messages that could not be sent to the network or that have been sent but not acknowledged by the server
smtpLastErr(6)	the error code of the last error that occurred while trying to send an email message to the network
smtpLastMailElapsedTime(7)	the number of elapsed seconds since last successful email was sent to the server
smtpLnkSrvStatus(8)	the status of link with SMTP server
smtpSrvChkFailCnt(9)	the number of times the link to SMTP server is detected as ‘down.’

Transparent Factory MIB Version

tfeMibVersion Subtree

This group contains information about the version of the Schneider TFE MIB *(see page 416)* supported by the product.

Service	Indicates . . .
tfeMibVersionNumber(1)	the version of the SchneiderTFE Mib in Vxx.yy form (example V01.04)
tfeMibVersionDate(2)	the date of last update of the SchneiderTFE MIB in ‘ddMmmyy’ form (example: 09Jan06)

Private Traps and MIB Files

Private Traps and MIB Files

Traps are used to signal status changes to the manager while avoiding additional traffic:

- **LEDs** (`profileLED`): This trap is sent if the LED state changes.
- **communications ports** (`port502StatusChange`): This trap is sent if `port502Status` changes.
- **I/O scanning health value** (`ioScanStatusChange`): This trap is sent if `ioScanStatus` changes.
- **global data health value** (`glbDataStatusChange`): This trap is sent if `glbDataStatus` changes.
- **Web service** (`webStatusChange`): This trap is sent if `webStatus` changes.
- **address server** (`addressServerStatusChange`): This trap is sent if `addressServer-Status` changes.
- **NTP service** (see below)
- **SMTP service** (see below)

Private traps can:

- send messages to the two managers whose IP addresses are configured in the SNMP configuration
- use the community name given to this configuration
- enable or disable each of the Transparent Factory Ethernet Private MIB groups listed in the Transparent Factory Ethernet Subtree *(see page 426)*.

Private traps are described in the MIB ASN.1 description, which is contained in a `.mib` text file.

NTP Traps

- **NTP status** (`ntpStatusChange`): This trap is sent if `ntpStatus` changes.
- **server change** (`ntpServerChange`): This trap is sent if the NTP component switches from the Primary NTP server to the standby NTP server or vice versa.
- **link server status change** (`ntpLnkSrvStatusChange`): This trap is sent if the NTP link server status changes.
- **leap second** (`ntpLeapSecond`): This trap is sent when leap seconds are inserted.
- **DST change** (`ntpDSTChange`): This trap notifies the manager that the NTP server time has changed from either:
  - standard time to daylight savings time, or
  - daylight savings time to standard time

SMTP Traps

- **SMTP status change** (`smtpStatusChange`): This trap is sent if `smtpStatus` of the email service referenced by emailIndex changes.
- **SMTP link to server status** (`smtpLnkSrvChange`): This trap is sent when the `smtpLnkS-rvStatus` of the email service referenced by `emailIndex` changes. The trap is sent when the service tries to send an email. Every 30 minutes a periodic test checks the connection to the SMTP server.

Appendix B
Installation & Configuration of a Modicon Premium Ethernet Network

Overview

This quick start guide describes how to install and configure a Modicon Premium Ethernet module. It also sets up the I/O scanning service to allow data transfer to occur between the PLC and a remote slave device. Instructions for accessing the module's diagnostic capabilities are included at the end of the guide.

What Is in This Chapter?

This chapter contains the following topics:

Overview

Introduction

This quick start guide explains how to install and configure Modicon Premium Ethernet modules, set up and configure an I/O scanning communication service, and access the modules diagnostic capabilities. The following modules are applicable to this guide:

- TSX ETY 4103
- TSX ETY 5103
- TSX P57 1634M
- TSX P57 2634M
- TSX P57 3634M
- TSX P57 4634M
- TSX P57 5634M

NOTE: When starting up a TSX P57 6634/5634/4634 processor, the CPU may send an address resolution protocol (ARP) request to verify the existence of a device using the IP address 192.168.2.1. The source IP address of this packet is the broadcast address of the CPU (the last IP address used in the PLC application, ending in 255).

Hardware/Software Requirements

For the example discussed in this guide, the following Modicon Premium Ethernet modules are required:

- TSX PSY 2600M power supply
- TSX P56 5634M CPU
- TSX ETY 4103 communications module

Also, a PC running Windows 2000 or XP with Schneider's Control Expert configuration software installed on it is required.

Finally, a USB cable is required to connect the PC to the network PLC.

Intended Audience

This user guide is intended for anyone who is involved in installing and configuring Modicon Premium Ethernet modules in a network arrangement that performs basic communication services.

Anyone reading this guide should:

- be familiar with Ethernet networks and the TCP/IP protocol
- understand the operation of PLCs

Installation

Introduction

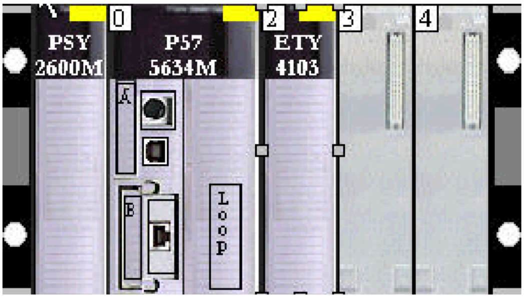
The Modicon Premium Ethernet modules used for the example in this guide may vary from the ones available at your site. You can substitute the appropriate power supply, CPU, and Ethernet communication module(s) and other Premium modules to make up a rack similar to the one described below.

Assembling the Rack

Assemble the modules into the rack as follows:

Step	Action
1	Insert the power supply into the leftmost slot on the rack.
2	Add the CPU to the next two slots (0 and 1) on the right of the power supply.
3	Place the remaining Premium communication modules, beginning with slot 2, to complete your installation.

In our example (see below), we use a TSX PSY 2600M power supply, a TSX P56 5634M processor, and a TSX ETY 4103 communications module to make up our rack.



Configuring the Rack with Control Expert

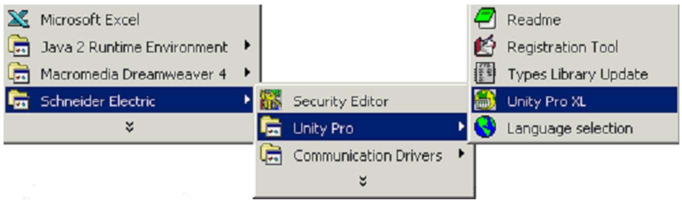
Introduction

Once the modules have been physically installed in the rack, we can configure it using Schneider Electric’s Control Expert configuration program.

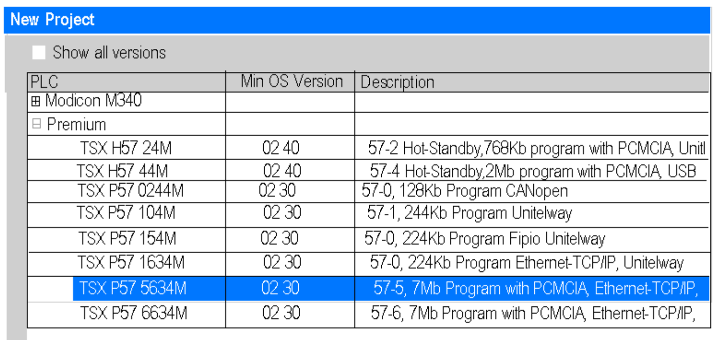
Configuring the Rack

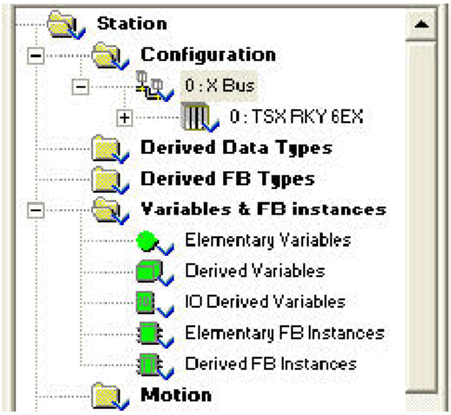
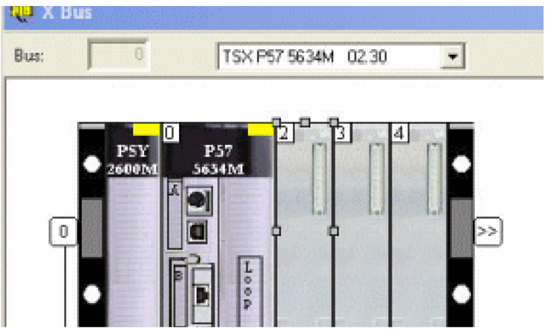
Use a PC that is loaded with the Control Exper software to configure the rack:

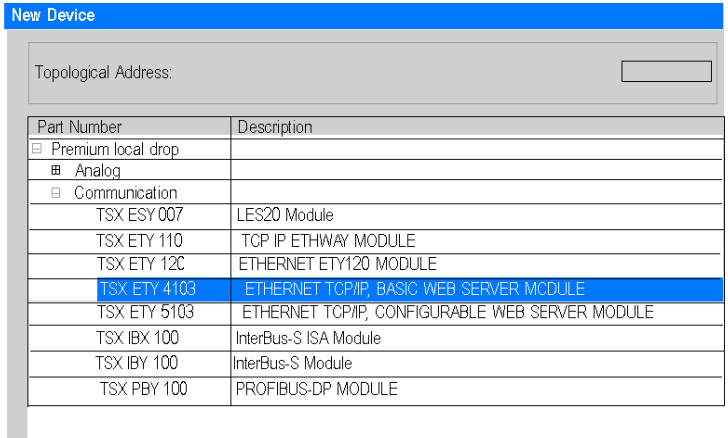
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Click Start.</td></tr>
<tr><td>2</td><td>Select Programs.</td></tr>
<tr><td>3</td><td>Then select Schneider Electric → Unity Pro → Unity Pro XL.



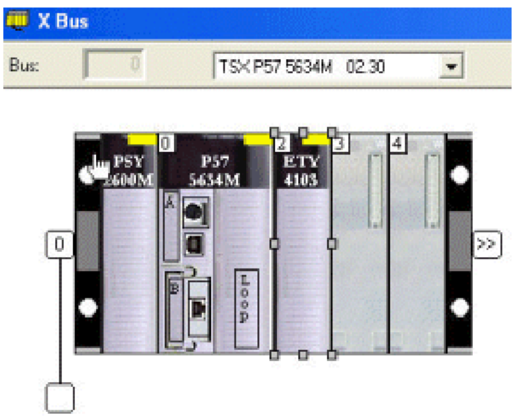
Note: The name of your Unity Pro package may be different. It may be Unity Pro M, Unity Pro L, Unity Pro XL, etc.</td></tr>
<tr><td>4</td><td>Select New in the File menu to create a New Project dialog box.</td></tr>
<tr><td>5</td><td>In the New Project dialog box, expand the Premium family to select the installed processor.


</td></tr>
</table>

Step	Action
6	In the project browser, double-click **Station/Configuration/XBus** to access the configuration of the local rack. 
7	Double-click slot 2 to bring up the New Device dialog box (see step 8). 

Step	Action
8	Double-click the module that goes in slot 2 (**TSX ETY 4103** in our example).  **Note**: Alternately, you can click the module and drag it to the selected slot on the rack.
9	Repeat step 8 for each module included in your configuration.

The figure below shows the completed rack assembly for our example with the TSX ETY 4103 module in slot 2.



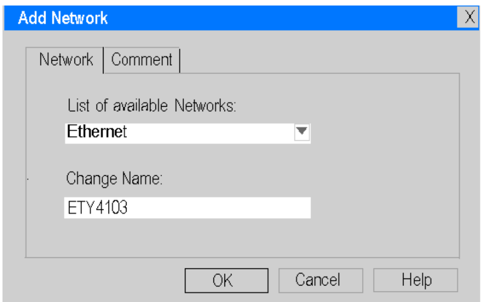
Configuring the Ethernet Network with Control Expert

Introduction

The following procedure describes how to add a new Ethernet network and link it to the Premium Quantum modules we configured in the previous section.

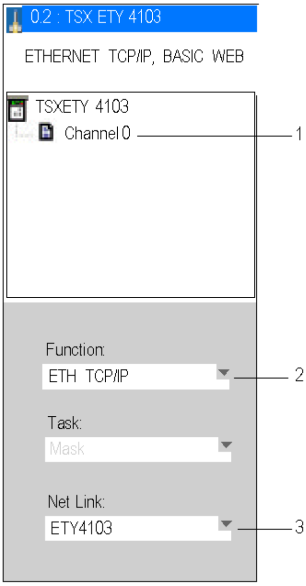
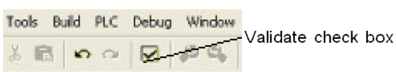
Setting Up the Netwok

Perform the following steps to add the Ethernet network.

Step	Action
1	Locate the **Communications** directory in the Project browser.
2	Right click the **Network** subdirectory located under the **Communications** directory.
3	Select the **New Network** option to bring up the **Add Network**dialog box.
4	Scroll to **Ethernet** in the **List of available Networks** field.
5	Enter a meaningful name for your network in the **Change Name** field (ETY 4103 was used in our example). 
6	Click **OK**.

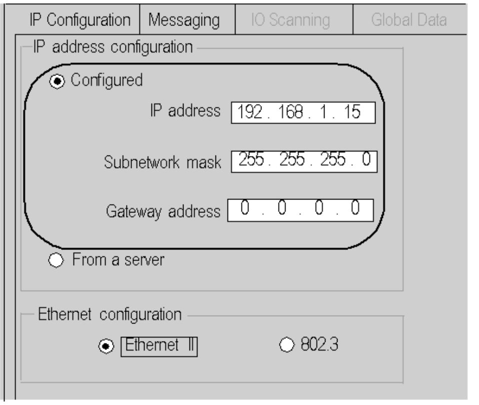
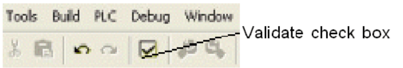
Linking the Network to the TSX ETY 4103 Module

Perform the following steps to link the new logical Ethernet network with the TSX ETY 4103.

Step	Action
1	Double click **XBus** in the Project browser to bring up the rack configuration.
2	Double click **TSX ETY 4103** module located at slot 2 to bring up the network link screen. 
3	Under TSX ETY 4103, click **Channel 0** (item 1, above) to display the **Function** box.
4	In the **Function** box (item 2, above), scroll to **ETH TCP IP** to bring up the **Net Link**.
5	In the **Net Link** box (item 3, above), scroll to the name of your logical network (**ETY 4103** in the example).
6	Click the validate check box in the upper toolbar to confirm the network link configuration. 

Assigning an IP Address to the TSX ETY 4103 Module

Perform the following steps to assign an IP address to the TSX ETY 4103 communication module.

Step	Action
1	Locate the **Communications\Networks** directory in the Project browser.
2	Double-click your new logical network (ETY 4103 in our example) to open the ETY 4103 configuration screen. 
3	Click **Configured** in the IP Address Configuration group (circled area shown above). **Note:** Be sure to contact you network administrator and request the IP, Subnetwork mask, and Gateway addresses prior to performing the next step.
4	Enter the appropriate values in the **IP address**, **Subnetwork mask**, and **Gateway address** fields. In our example, we assigned 192.168.1.15, 255.255.255.0, and 0.0.0.0 respectively.
5	Click the validate check box in the upper tool bar to confirm the IP configuration settings. 

Configuring the I/O Scanning Service

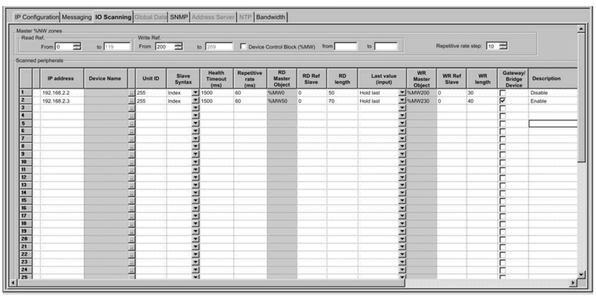
Introduction

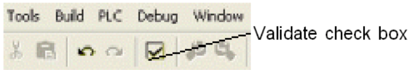
The Premium TSX ETY 4103 module supports Ethernet communication services such as I/O scanning, Global Data, Modbus messaging, SNMP, etc.

The following example shows you how to configure the I/O scanning service, which is used to:
- transfer data between network devices
- allow a CPU to regularly read data from and write data to the scanned devices

Selecting the I/O Scanning Parameters

Perform the following steps to setup the I/O scanning parameters:

Step	Action
1	Open your application using the TSX ETY 4103 module in Control Expert.
2	In the **Project Browser**, locate the **Communication** → **Networks** directory.
3	Click the Ethernet module (TSX ETY 4103 in our example) to open the configuration screen.
4	In **Module Utilities**, select **Yes** in the **I/O Scanning** menu. 
5	Click the **I/O Scanning** tab to display the I/O scanning configuration screen. 
6	Enter the parameter settings under each of the column headings for one line of the I/O Scanner Configuration. Refer to the following I/O Scanning Parameters topic to see the settings used for this example.

Step	Action
7	Click the validate check box in the upper tool bar to confirm the I/O scanning parameter settings. 

I/O Scanner Parameters above I/O Scanner Table

A description of the parameters above the I/O scanning table used in the example are listed in the following table:

Parameter	Field	Description
Read Ref.	**From** and **to** check boxes	The values in these boxes define the range of destination address values in the CPU for the data read from each device. The addresses you enter here are displayed in the **RD Master Object** column of the dialog. In the example above, the **Read Ref.** values range from 0 to 599; notice that these values are displayed as %MW0, %MW599, etc. in the **Master Object** column.
Write Ref.	**From** and **to** check boxes	The values in these boxes define the range of source address values in the CPU. The address you enter here is displayed in the **WR Master Object** column. In the example above, values starting at %MW2000 are shown in the **WR Master Object** column.
Device Control Block	check box	If this check box is selected, the device control block is enabled and the master can send requests to a slave. If the check box is not selected, the device control block functionality is disabled and all I/O scanner table entries are active at all times.
	From and **to** check boxes	If a **Device Control Block** bit is disabled, the I/O scanner closes the connection and sets the health bit to an unhealthy state (bit value = 1).
Repetitive Rate Step	data box	The **Repetitive Rate Step** is set in multiples of 5 ms (the minimum) through 200 ms (the maximum). The **Repetitive Rate** column is where you enter a rate of time for how often you want the I/O scanner to send a query to the device after the rate has timed out. **NOTE:** The **Repetitive Rate** of the I/O scanner table is a multiple of the rate displayed in the **Repetitive Rate Step**. The real repetitive rate being executed by the I/O scanner service is shown in the **Repetitive Rate** column. **NOTE:** An entry in the **Repetitive Rate** column is rounded up to the next multiple that was entered in the **Repetitive Rate Step** box if the entry is not a multiple of the **Repetitive Rate Step**. For example, if the entry in the **Repetitive Rate Step** is 5 and you enter a 7 in the **Repetitive Rate** column, the 7 is rounded up to 10; if you change the **Repetitive Rate Step** to 6 and enter a 7 in the **Repetitive Rate** column, the 7 is rounded up to 12.

I/O Scanner Table Parameters

A description of the parameters in the I/O scanning table used in the example are listed in the following table:

Parameter	Description	Example
Entry #	This is the first column; it has no name. Valid range: 1 ... 128 Each entry represents an I/O Scanning exchange on the network.	
IP address	This is the IP address of the scanned Ethernet slave device.	192.168.1.100
Device Name	To configure a device (Advantys island or DTM), click the **...** button to open the **Property** box *(see page 183)* to start the device configuration software. For an introduction to this procedure for Advantys, go here *(see page 173)*. For an introduction to this procedure for DTMs, go to FDT Container *(see EcoStruxure™ Control Expert, Operating Modes)*. **NOTE:** While the **Property** box is open, I/O scanning cannot be edited.	MySTB1 or Master_PRM_DTM_10
Unit ID	This field associates the slave address of the device connected to an Ethernet/Modbus gateway with the IP address of that gateway: ● Value range: 1 to 255 ● Default value: 255 When using a bridge, enter the bridge index (1 to 255) in this field.	255
Slave Syntax	Use this drop-down menu to pick the way **RD Ref Slave** and **WR Ref Slave** values are displayed. The 4 choices are (with an example): ● Index: 100 ● Modbus: 400101 ● IEC 0: %MW100 ● IEC 1: %MW101	Index (default value)
Health Timeout (ms)	This field sets the maximum interval between the responses from a remote device. After this time period expires, the received data is invalid. The **Health Timeout** must be longer than the **Repetitive Rate** time (ms). For a Premium ETY Ethernet module, it must be longer than the CPU scan time. For the **Health Timeout**: ● Range: 0ms to 50 seconds ● Interval: 1ms	1500 ms

Parameter	Description	Example
Repetitive rate (ms)	The rate at which data is scanned, from 0...50000 in multiples of the **Repetitive Rate Step**: ● If you are running Unity Pro V3.1 or earlier with the following firmware versions: ❍ ETY 4103/5103/Port (V4.0 or earlier): 10 ms ❍ TSX P57 4634/5634/6634 (V2.5 or earlier): 10 ms ● If you are running Unity Pro V4.0 or later with the following firmware versions: ❍ ETY 4103/5103/Port (V4.1 or later): 5 - 200 ms ❍ TSX P57 4634/5634/6634 (V2.6 or later): 5 - 200 ms	60 ms
RD Master Object*	Destination address in the master PLC where, from each device, newly read information is stored	%mw10
RD Slave Ref.**	Source address index in the slave/remote device	The format of this value depends on the **Slave Syntax**: ● Index: 5 ● Modbus: 400006 ● IEC 0: %MW5 ● IEC 1: %MW6
RD length	Number of words to read	10
Last value (Input)	This field configures the behavior of inputs in the event of an access error in relation to the remote device (for example: inoperative network or device power supply, etc.): ● Set to 0: fall back to 0 ● Hold last: maintain last value	Hold last
WR Master Object*	Source address of the master PLC whose data is being written into the slave/remote device. Write operations are always performed at the word level.	%mw20
WR Slave Ref.**	The address of the first word written into the slave/remote device.	The format of this value depends on the **Slave Syntax**: ● Index: 1 ● Modbus: 400002 ● IEC 0: %MW1 ● IEC 1: %MW2
WR length	Number of words to be written	10

Parameter	Description	Example
Gateway/Bridge Device	To allow slower TCP/IP network devices (i.e., gateways and bridges) to be compatible with the I/O Scanner: • Select the check box to enable this feature. Defines a new bit, and sets it to high (1).Deselect the check box to disable this feature (default). Defines a new bit, and sets it to zero (0).	• **Disable**: deselected check box • **Enable**: selected check box
Description	Additional information	
*Master refers to the client PLC that makes the request. **Slave refers to the server from which data is read or to which data is written.		

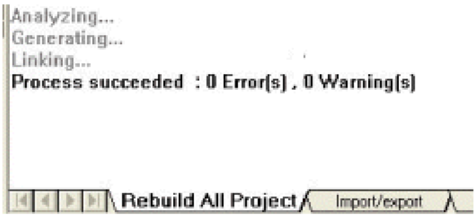
NOTE: For more information, refer to the Contextual Menu for Copy/Cut/Paste topic *(see page 169)*.

NOTE: For more information, refer to the I/O Scanning with Multiple Lines topic *(see page 171)*.

Building and Downloading the Configuration Program

Building the Program

Next, you need to build the whole program before downloading it to the PLC. To do this, select **Build\Rebuild All Project** in the toolbar at the bottom of the screen (shown below). If it is successful, a **Process succeeded** message will appear at the program's completion.



Connection Options

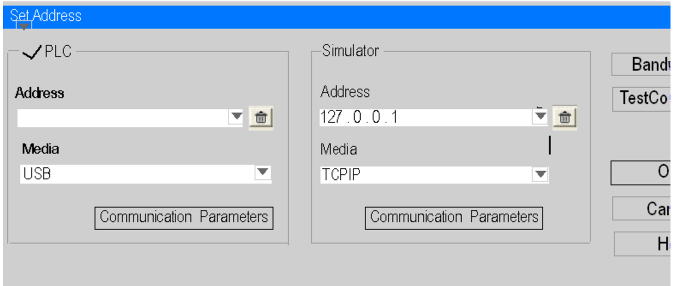
In order to run the configuration program it must first be downloaded to the PLC. Prior to downloading the program the PLC must be connected to the PC containing the Control Expert software. The connection can be accomplished using a a communication network such as Ethernet, USB, or Unitelway. We describe both the USB and Unitelway setups in the following examples.

Connecting the PC to the PLC with a USB Cable

Proceed as follows to connect the PC to the PLC with USB.

Step	Action
1	Ensure that the Premium system is powered up.
2	Select the standard mode on the upper toolbar. 
3	Connect the PLC to the PC with a USB cable.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>4</td><td>On the PC, click the Control Expert PLC\Set Address tab to bring up the Set Address dialog box.

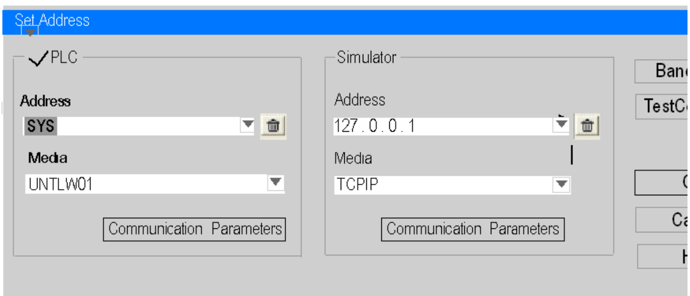


</td></tr>
<tr><td>5</td><td>Select USB in the PLC Media box.</td></tr>
<tr><td>6</td><td>Leave the PLC Address box blank.</td></tr>
<tr><td>7</td><td>Click OK.</td></tr>
<tr><td>8</td><td>Proceed to Downloading and Running the Configuration Program (see page 457).</td></tr>
</table>

Using a Unitelway Link

Proceed as follows to setup the PC with Unitelway.

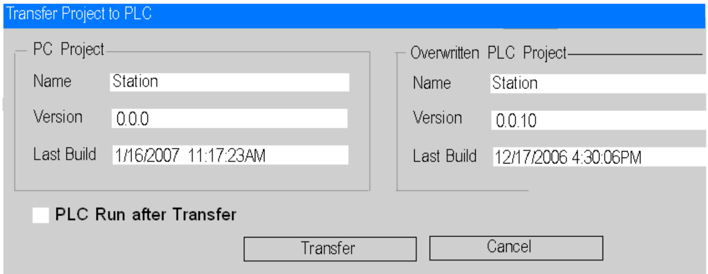
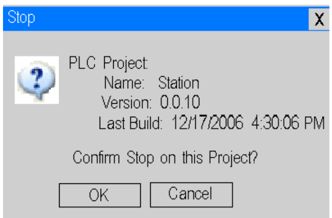
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Ensure that the Premium system is powered up.</td></tr>
<tr><td>2</td><td>Connect the PLC to the PC with a Unitelway (serial) cable.</td></tr>
<tr><td>3</td><td>On the PC, click the Control Expert PLC\Set Address tab to bring up the Set Address dialog box.



</td></tr>
<tr><td>4</td><td>Select UNTLW01 in the PLC Media box.</td></tr>
<tr><td>5</td><td>Select SYS in the PLC Address box.</td></tr>
<tr><td>6</td><td>Click OK .</td></tr>
<tr><td>7</td><td>Proceed to Downloading and Running the Configuration Program (below).</td></tr>
</table>

Downloading and Running the Configuration Program

Once the PC and the PLC are connected as describe above, the configuration program can be downloaded to the PLC.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>On the PC, select PLC\Connect on the Control Expert screen.</td></tr>
<tr><td>2</td><td>Click the PLC\Transfer Project to PLC tab to bring up the Transfer Project to PLC dialog box.

</td></tr>
<tr><td>3</td><td>Click the Transfer button to download the program to the PLC.</td></tr>
<tr><td>4</td><td>When the confirm screen appears, click OK.

</td></tr>
<tr><td>5</td><td>Click Run on the Control Expert upper toolbar to start the program.</td></tr>
</table>

Accessing the Ethernet Module’s Diagnostic Capabilities

Introduction

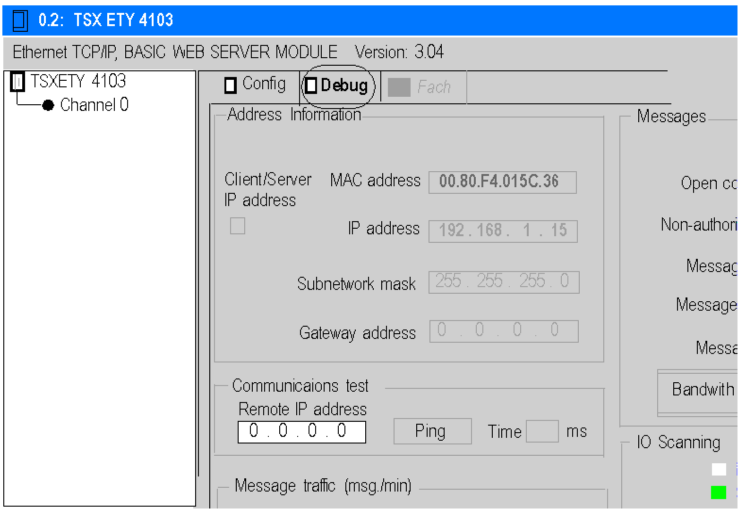
There are 3 ways to diagnose problems that may occur to Premium Ethernet modules:

- view the module’s LED display
- use the debug screen provided by the Control Expert software
- use the module’s embedded web server

In this section, we describe how to access the TSX ETY 4103 module’s debug screen and web pages.

Setting Up the TSX ETY 4103 Debug Screen

To access the TSX ETY 4103 module’s debug page proceed as follows:

Step	Action
1	Perform the steps using a Unitelway Link *(see page 456)*.
2	Select **PLC → Connect** on the Control Expert screen.
3	In the **Project Browser**, double-click **TSX ETY 4103** under **Station → Configuration → XBus**.
4	Select the **Debug** tab to display the debug screen. 

Accessing the Ethernet Module's Web Page

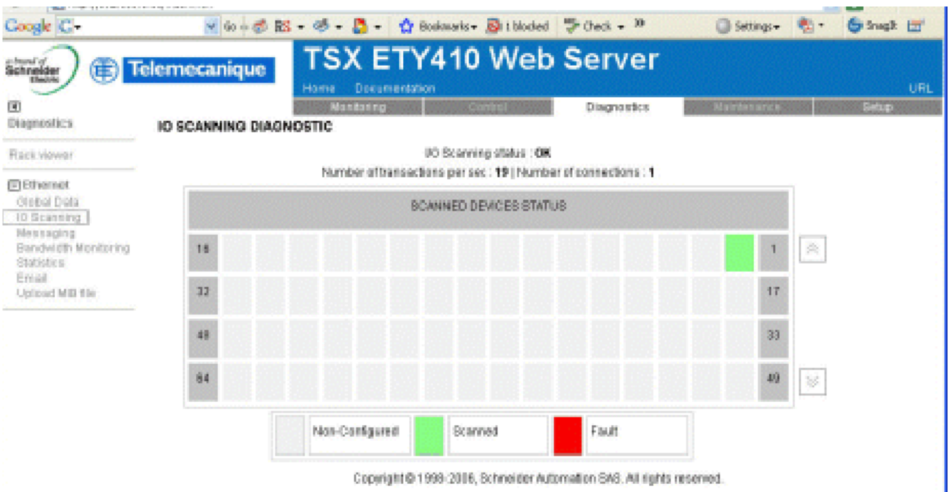
Premium Ethernet modules have an embedded web server that provides web pages to diagnose the Ethernet module services, such as statistics, I/O scanning, messages, global data, etc. You can access an Ethernet module's web pages by entering the IP address of the module in the Web browser. No password is required to display the home page.

To access the TSX ETY 4103 module's web page, proceed as follows:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>At the PC, start a Web browser such as Internet Explorer.</td></tr>
<tr><td>2</td><td>Enter the TSX ETY 4103's currently assigned IP address in the Address field of the browser to bring up the module's home page.

</td></tr>
<tr><td>3</td><td>Click the Diagnostics tab.</td></tr>
<tr><td>4</td><td>Enter a user name and password. (The default is USER for both.)
NOTE: Check with your system administrator to see if the user name and password have been changed.</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>5</td><td>Click OK to bring up the ETY’s diagnostic web page.

</td></tr>
<tr><td>6</td><td>Click the I/O Scanning link on the left-hand side of the screen to access the I/O scanning diagnostics web page.

</td></tr>
</table>

Glossary

!

802.3 frame

A frame format, specified in the IEEE 802.3 (Ethernet) standard, in which the header specifies the data packet length.

B

BOOTP

bootstrap protocol. A UDP/IP protocol that allows an Internet node to obtain its IP parameters based on its MAC address.

D

DHCP

dynamic host configuration protocol. DHCP is a TCP/IP protocol that allows network devices (DHCP clients) to obtain their IP addresses from a DHCP server through a request to the server.

E

Ethernet II

A frame format in which the header specifies the packet type, Ethernet II is the default frame format for STB NIP 2212 communications.

F

FDR

The *fast device replacement* service offers a method of handling device replacement without disrupting the system nor interrupting service.

FTP

File Transfer Protocol. FTP is the World Wide Web’s file transfer protocol.

G

Global Data

Global Data provides the automatic exchange of data variables for the coordination of PLC applications.

H

HTTP

HyperText Transfer Protocol. HTTP is the protocol for the formatting and transmission of files on the world wide web. HTTP runs on top of TCP/IP (Internet) protocols.

I

I/O scanning

An I/O scan continuously polls I/O modules to collect data bits and status and diagnostics information. This process monitors inputs and control outputs.

IODDT

input/output derived data type. IODDT is a structured data type representing a module or a channel of a PLC module. Each application expert module possesses its own IODDTs.

M

MIB

management information base. The MIB is an object database that is monitored by a network management system like SNMP. SNMP monitors devices that are defined by their MIBs. Schneider has obtained a private MIB, groupeschneider (3833).

Modbus

Modbus is an application layer messaging protocol. Modbus provides client and server communications between devices connected on different types of buses or networks. Modbus offers many services specified by function codes. There are two types of Modbus transmission, based on information in the physical layer:

- MB/serial: the Modbus type that transmits data over serial RS-232 and RS-422/485
- MB/TCP: the Modbus type that transmits data over Ethernet

N

NTP

network time protocol. NTP synchronizes the time of one client or server to the time of another server or referenced source (such as a satellite receiver).

P

port 502

TCP/IP reserves specific server ports for specific applications through IANA (Internet Assigned Numbers Authority). Modbus requests are sent to registered software port 502.

S

SMTP

Simple Mail Transfer Protocol. SMTP is a transmission protocol for sending and receiving e-mail. SMTP messages are usually retrieved from a server with an e-mail client (such as POP or IMAP).

SNMP

simple network management protocol. The UDP/IP standard protocol used to monitor and manage devices on an IP network.

SNMP agent

The SNMP application that runs on a network device.

T

TCP/IP

Transmission Control Protocol/Internet Protocol. TCP/IP is the communication protocol of the Internet.

TFTP

Trivial File Transfer Protocol. TFTP is a scaled-down version of FTP that uses UDP, often to initialize diskless workstations.

Transparent Ready

Schneider Electric’s Transparent Ready products (based on universal Ethernet TCP/IP and Web technologies) can be integrated into real-time, data sharing systems, with no need for interfaces.

U

Unity Pro

Unity Pro is the programming software for all Unity PLCs. It includes 5 IEC languages that comply with IEC 61131-3. Depending on requirements, the application may use a mixture of different languages.

NOTE: Unity Pro is the former name of Control Expert for version 13.1 or earlier.

Index

L

M

N

P

R

S

T

U