Modicon X80

BMENOR2200H Advanced RTU Module User Manual

Original instructions

2/2020

PHA90072.00

www.schneider-electric.com

Schneider Electric

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.

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 guide describes the Modicon X80 BMENOR2200H advanced RTU module and its relationship to Modicon M580 controllers and X80 remote platforms.

The BMENOR2200H module acts as a communication module on an X80 platform and conforms to the general rules and guidelines for the use of those platforms.

The module provides telemetry protocol connection availability in complex M580 configurations through the Modbus TCP communication protocol.

This guide describes the following topics:

- installation *(see page 42)*
- configuration *(see page 93)*
- diagnostics *(see page 138)*
- embedded web pages *(see page 145)*

NOTE: The specific configuration settings contained in this guide are intended to be used for instructional purposes only. The settings required for your specific configuration may differ from the examples presented in this guide.

Validity Note

This document is valid for an M580 system when used with Control Expert 14.1 HF 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 described 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.

Information Related to Cyber Security

Information on cyber security is provided on the Schneider Electric website:
http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

Document available for download on cyber security support section:

Title of Documentation	Webpage Address
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cyber Security Recommendations	*http://www.schneider-electric.com/ww/en/download/document/STN v2*

Related Documents

Title of documentation	Reference number
Modicon M580 Standalone System Planning Guide for Frequently Used Architectures	HRB62666 (English), HRB65318 (French), HRB65319 (German), HRB65320 (Italian), HRB65321 (Spanish), HRB65322 (Chinese)
Modicon M580 System Planning Guide for Complex Topologies	NHA58892 (English), NHA58893 (French), NHA58894 (German), NHA58895 (Italian), NHA58896 (Spanish), NHA58897 (Chinese)
Modicon M580 Hot Standby System Planning Guide for Frequently Used Architectures	NHA58880 (English), NHA58881 (French), NHA58882 (German), NHA58883 (Italian), NHA58884 (Spanish), NHA58885 (Chinese)
Modicon M580, Hardware, Reference Manual	EIO0000001578 (English), EIO0000001579 (French), EIO0000001580 (German), EIO0000001582 (Italian), EIO0000001581 (Spanish), EIO0000001583 (Chinese)
Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	EIO0000002726 (English), EIO0000002727 (French), EIO0000002728 (German), EIO0000002730 (Italian), EIO0000002729 (Spanish), EIO0000002731 (Chinese)

Title of documentation	Reference number
Modicon M580, Change Configuration on the Fly, User Guide	EIO0000001590 (English), EIO0000001591 (French), EIO0000001592 (German), EIO0000001594 (Italian), EIO0000001593 (Spanish), EIO0000001595 (Chinese)
M580 BMENOS0300, Network Option Switch, Installation and Configuration Guide	NHA89117 (English), NHA89119 (French), NHA89120 (German), NHA89121 (Italian), NHA89122 (Spanish), NHA89123 (Chinese)
Modicon eX80, BMEAHI0812 HART Analog Input Module & BMEAHO0412 HART Analog Output Module, User Guide	EAV16400 (English), EAV28404 (French), EAV28384 (German), EAV28413 (Italian), EAV28360 (Spanish), EAV28417 (Chinese)
Modicon X80, Analog Input/Output Modules, User Manual	35011978 (English), 35011979 (German), 35011980 (French), 35011981 (Spanish), 35011982 (Italian), 35011983 (Chinese)
Modicon X80, Discrete Input/Output Modules, User Manual	35012474 (English), 35012475 (German), 35012476 (French), 35012477 (Spanish), 35012478 (Italian), 35012479 (Chinese)
Grounding and Electromagnetic Compatibility of PLC Systems, Basic Principles and Measures, User Manual	33002439 (English), 33002440 (French), 33002441 (German), 33003702 (Italian), 33002442 (Spanish), 33003703 (Chinese)
EcoStruxure™ Control Expert, Program Languages and Structure, Reference Manual	35006144 (English), 35006145 (French), 35006146 (German), 35013361 (Italian), 35006147 (Spanish), 35013362 (Chinese)
EcoStruxure™ Control Expert, Operating Modes	33003101 (English), 33003102 (French), 33003103 (German), 33003104 (Spanish), 33003696 (Italian), 33003697 (Chinese)
EcoStruxure™ Control Expert, Installation Manual	35014792 (English), 35014793 (French), 35014794 (German), 35014795 (Spanish), 35014796 (Italian), 35012191 (Chinese)
Modicon Controllers Platform Cyber Security, Reference Manual	EIO0000001999 (English), EIO0000002001 (French), EIO0000002000 (German), EIO0000002002 (Italian), EIO0000002003 (Spanish), EIO0000002004 (Chinese)
Modicon X80, BMXERT1604T Time Stamp Module, User Guide	EIO0000001121 (English), EIO0000001122 (French), EIO0000001123 (German), EIO0000001125 (Italian), EIO0000001124 (Spanish), EIO0000001126 (Chinese)

NOTE: Refer also to the online help for the Maintenance Expert tool *(see EcoStruxure Automation Device Maintenance, Firmware Upgrade Tool, Online Help)*.

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

Product Related Information

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

The application of this product requires expertise in the design and programming of control systems. Only persons with such expertise are allowed to program, install, alter, and apply this product.

Follow all local and national safety codes and standards.

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

Chapter 1
Introducing the Modicon X80 BMENOR2200H Advanced RTU Module

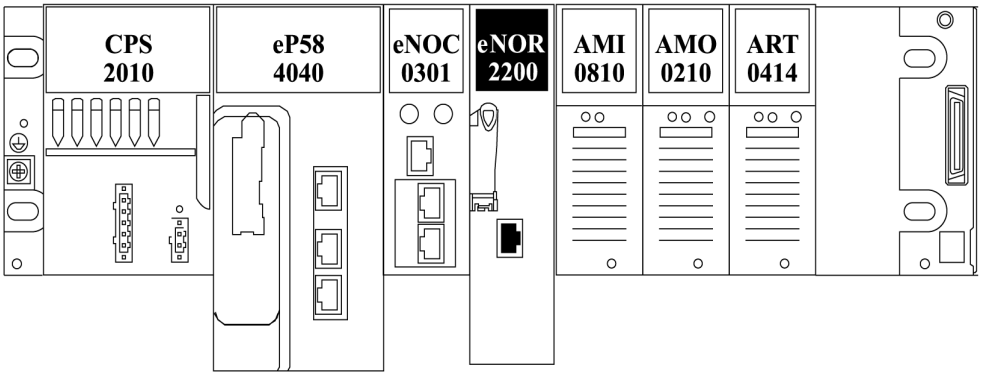
What Is in This Chapter?

This chapter contains the following topics:

Introduction

Overview

The BMENOR2200H advanced RTU module brings DNP3 communications to the Modicon M580 platform:



Compared to standard X80 communications and I/O modules, the BMENOR2200H module is a *long factor* module, the same height as the CPU. (Refer to the module dimensions *(see page 20)* topic.)

Install this module on a local Ethernet backplane in a Modicon M580 system. The module provides access to an Modicon M580 network (through the external ports of the CPU).

NOTICE
INOPERABLE RACK CONNECTION ● Do **not** mount the BMENOR2200H module on an BMX (X Bus-only) backplane. The module will not work. ● The module can operate properly **only** on a BME (X Bus and Ethernet) backplane. ● Refer to the rack descriptions and slot restrictions in the installation chapter in the *Modicon X80 Racks and Power Supplies, Hardware, Reference Manual*. **Failure to follow these instructions can result in equipment damage.**

Main Features and Functionality

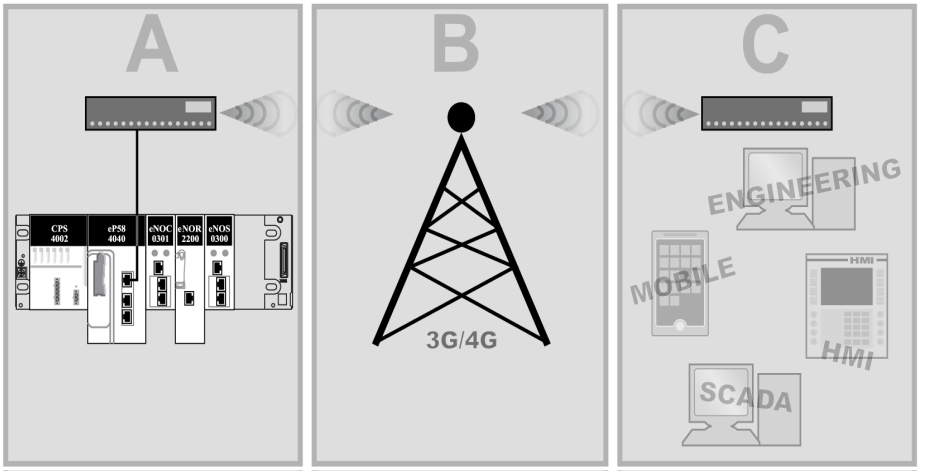
- **Improved Performance**
  The BMENOR2200H module offers these improvements over the BMXNOR0200H module:
  - easy connectivity with an Ethernet backplane
  - DNP3 secure authentication support

- enhanced cyber security features
- high performance data exchange method between the M580 controller and the BMENOR2200H module
- unique and easy-to-use DTM configuration within the Control Expert environment

- **Module Features**
  The BMENOR2200H module addresses a wide range of telemetry requirements in an M580 system:
  - ruggedized with conformal coating for operations in extended operating temperature ranges and harsh environments
  - upstream communications with SCADA master stations for polling interrogation of data, backfilling of time-stamped event data, and receiving master commands
  - downstream communications with other RTU substations, outstation field devices and IEDs (for data collection), sending commands, and synchronizing distributed control
  - remote programming and downloading of control program with Control Expert software through Ethernet or USB connections on an M580 CPU
  - remote cyber security settings and diagnostic monitoring with a built-in web server
- **Platform Features**
  The module shares these characteristics and applications that are available in an M580 environment:
  - specialized function blocks (AGA, flow calculations)
  - expandable rack-based modular I/O configurations and remote I/O capabilities
  - high-density, discrete, analog, and I/O counting modules
  - isolated input power supply (various voltage ranges available 24 Vdc, 24/48 Vdc, 125 Vdc, 100/240 Vac)
  - local or remote downloading of operating system firmware
- **Communication Protocols**
  Refer to the complete description of function and protocol support *(see page 63)*.

RTU Architecture

This sample architecture shows communications from an RTU substation that includes a BMENOR2200H module:



A A BMENOR2200H module communicates over the backplane with a CPU that is connected to a network router.

B The 3G/4G network forwards the communications.

C Communications are received by a router that connects to a control network and fieldbus devices.

BMENOR2200H and EcoStruxure™

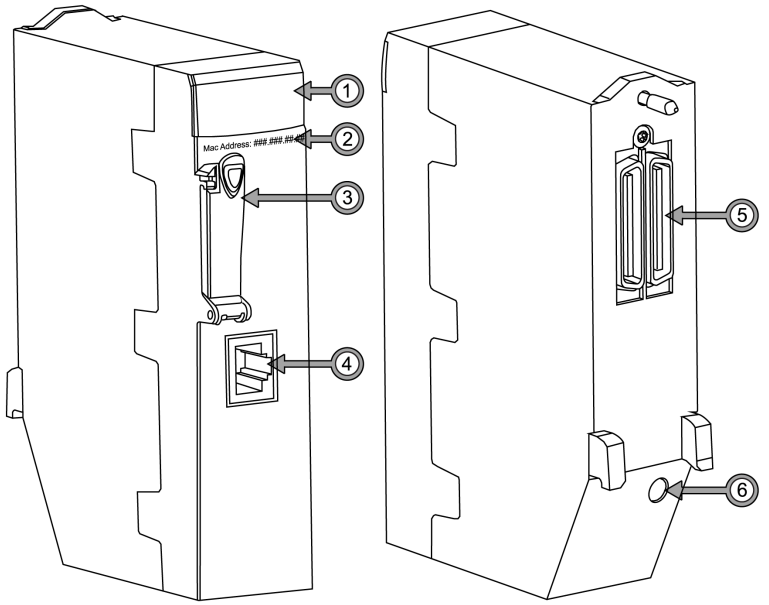
EcoStruxure™ is a Schneider Electric program designed to address the key challenges of many different types of users, including plant managers, operations managers, engineers, maintenance teams, and operators, by delivering a system that is scalable, flexible, integrated, and collaborative.

This document presents one of the EcoStruxure features, using Ethernet as the backbone around the Modicon M580 offer, in which an M580 local rack communicates with M580 RIO drops and distributed equipment in the same network.

Physical Description

External Features

The BMENOR2200H module has the same form factor as other M580 advanced communication modules. This figure shows the specific external features of this module:



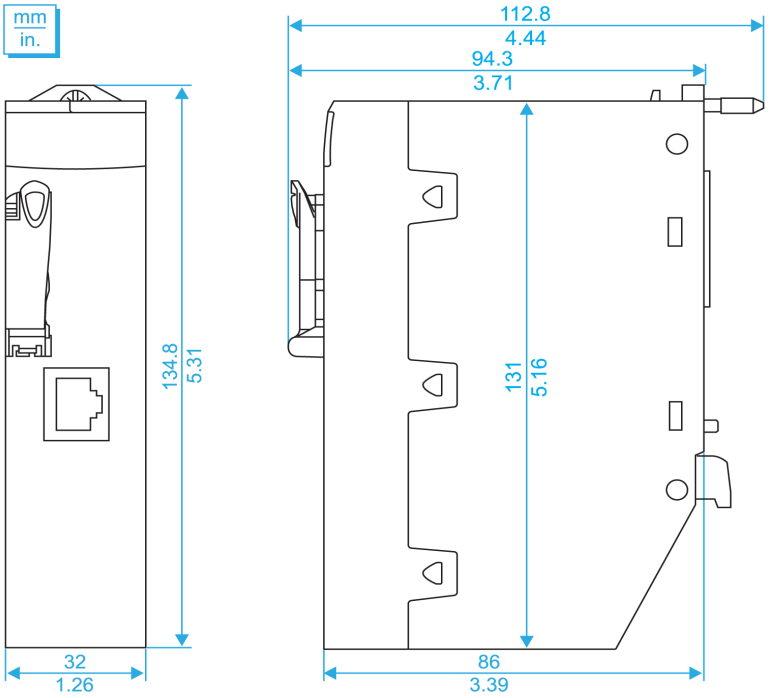
Legend:

Item	Description	Function
1	LED array *(see page 30)*	Observe the LED display to diagnose the module.
2	MAC address	This manufacturer-defined address is unique for each individual module.
3	memory card slot	Store datalogging files (.csv) to the SD card. **NOTE:** This feature is reserved for future use.
4	serial port	This port is an isolated RS232/RS485 serial connector. **NOTE:** This feature is reserved for future use.
5	dual-bus backplane connector *(see page 19)*	This connection to the Modicon M580 rack supports Ethernet and X Bus communications.
6	rotary switch *(see page 22)*	Use this switch to set the cyber security level for the module.

NOTE: A ferule placed on the end of the serial port reduces the pinching of the cable by the removable cover. This reduces the risk of degrading the quality of the link by decreasing the likelihood of achieving the maximum bending radius of the cable.

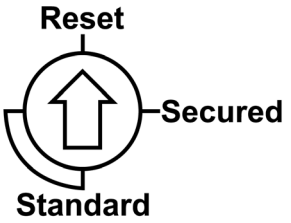
Dimensions

The BMENOR2200H module conforms to the height of an M580 CPU and the width of a standard single-slot M580 communications module that has an SD card slot:



Rotary Switch

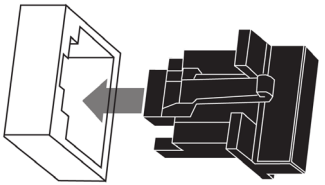
A three-position rotary switch is located on the back of the module. Set this switch to configure a cyber security operating mode for the module:



Refer to the detailed description of the rotary switch configuration *(see page 22)*.

Accessories

These additional hardware accessories are available:

Description	Comment
dust cover	Cover the module's unused RJ45 ports with this stopper:  The dust cover reduces the port's exposure to atmospheric dust.
screwdriver	Use only the small, plastic screwdriver that was delivered with the module to set the rotary switch *(see page 22)*.

Cyber Security Rotary Switch

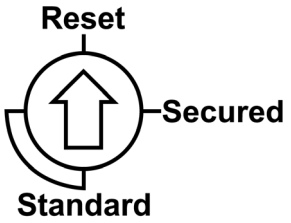
Introduction

A three-position rotary switch is on the back of the module. Set this switch to configure a cyber security operating mode for the module.

NOTICE
RISK OF UNINTENDED OPERATION To maintain the integrity of the hardware, use only the small, plastic screwdriver that ships with the module to change the switch position. Do not use a metal screwdriver. The use of a metal screwdriver can damage the switch and render it inoperable. **Failure to follow these instructions can result in equipment damage.**

Position Selection

This is an enlarged view of the three-position rotary switch on the back of the module:



Use the screwdriver to select a switch position that meets your cyber security requirements:

Icon	Setting	Description
Secured (default)	secure mode on	The module supports some level(s) of cyber security when a cyber security configuration is available.
Standard	standard mode on	The module does not support cyber security.
Reset	factory reset	The module implements its out-of-the-box cyber security configuration.

NOTICE
RISK OF UNINTENDED OPERATION Set the switch only to the *exact* "clock position" that corresponds to your security configuration: ● *12 o'clock:* **Reset** ● *3 o'clock:* **Secured** ● *6 o'clock/9 o'clock:* **Standard** (To implement the **Standard** level of cyber security, set the switch to *only* the 6 o'clock or 9 o'clock positions.) **Failure to follow these instructions can result in equipment damage.**

Set the Switch

Configure the cyber secrity mode for the module in the rack:

Step	Action
1	Remove the module from the rack by following the directions for module replacement *(see page 45)*.
2	Change the switch setting to **Reset**.
3	Re-insert the module in the rack to power it up in **Reset** mode.
4	Remove the module from the rack again.
5	Change the switch setting to **Secured** or **Standard**.
6	Re-insert the module in the rack to power it up in the selected (**Secured** or **Standard**) mode.

NOTE:

- Do not switch from the non-secure configuration (**Standard**) directly to the secure configuration (**Secured**) or vice-versa. Always power up the module with the rotary switch in the **Reset** position when you transition between the **Standard** and **Secured** modes to implement normal operations.
- The changes associated with the switch settings take effect after the module is re-inserted in the rack and powered up.

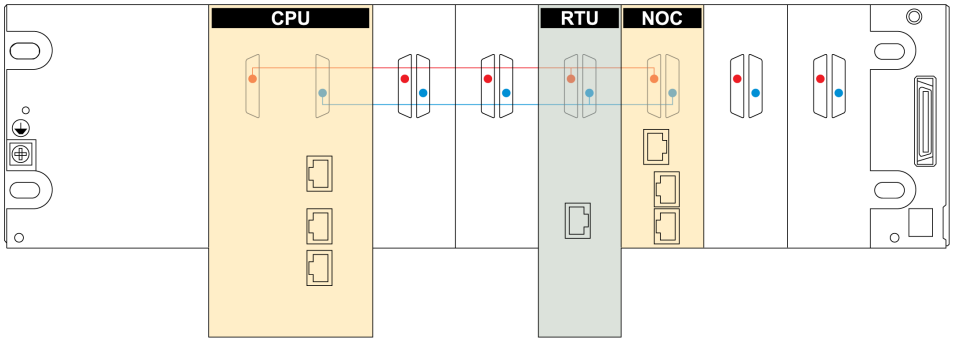
Backplane Connector

About Dual-Bus Backplanes

The dual-bus interface *(see page 19)* on the back of the BMENOR2200H module connects to the X Bus and Ethernet bus connectors across the backplane when you mount the module in the rack.

BMEXBP••0• backplanes are compatible with Modicon X80 modules in an M580 system.

Communications across the dual-bus backplane of this sample local rack (which includes an M580 CPU) implement both the Ethernet (red line) and X Bus (blue line) protocols:



NOTE:

- BMXXPB••00 X Bus backplanes do not have connections that support eX80 modules.
- Ethernet racks are described in detail in the *Modicon M580, Hardware, Reference Manual*.

Connection Protocols

The module supports communications over a BMEXBP••0• backplane using these protocols:

Bus	Description
X Bus	The module uses X Bus communications on the Ethernet backplane to obtain and exchange the following through the CPU: ● configuration data for the module ● application and diagnostic data
Ethernet	The module uses the Ethernet bus on the Ethernet backplane to manage connectivity to the module: ● The module provides Ethernet connectivity to the CPU. ● The module communicates with Ethernet communication modules on the local rack. ● The module communicates with network devices that are attached to the external ports of the CPU.

The data exchange uses implicit messaging to facilitate memory sharing between the module and the CPU. For each CPU scan cycle, the CPU publishes all data at the same time to share the most current information with the RTU.

I/O Data Exchange with the CPU

Observe these maximum input and output sizes when the module exchanges I/O data with the CPU:

Protocol	Characteristics	
DNP3 NET client	up to 64 slaves/servers (one session for each slave/server)	
	Memory consumption: ● *input data size:* 8 Kb of data includes user-configurable data and 4K words of overhead. The overhead includes module diagnostic data, data object headers, and the number of headers depending on the user configuration. As a result, the maximum user-configurable input data size is approximately 7.55Kb (1Kb = 1024 bytes). ● *output data size:* 8 Kb of data includes user-configurable data and 4K words of overhead. The overhead includes module control data, data object headers, and the number of headers depending on the user configuration. As a result, the maximum user-configurable output data size is approximately 7.56Kb (1Kb = 1024 bytes). **NOTE:** The module supports a maximum of four master/client channels (including three virtual channels that share the same database of points with the master channel).	
DNP3 NET server	Memory consumption: ● *input:* 8 Kb ● *output:* 8 Kb **NOTE:** Refer to the descriptions above.	
	up to 150,000-event queue for all data types	
	up to 40,000 event queue for DNP3 SAv5 security events	
	supports clock synchronization from a master	
	service over TCP	client IP address validation list (up to 10 IP addresses)
		four concurrent client connections with configurable TCP service port (default port is 20000)
		event backup up to 10000 events
	support for DNP3 secure authentication version 2 and version 5 *(see page 66)*.	

SAv2 and SAv5 *(see page 66)* work on both client and server sides.

Use this formula to achieve the recommended minimum MAST task cycle time per BMENOR2200H module:

```
Tcycle min= ((DataInB + 128)*2+(DataOutB + 32)) / 23500B/S)*30ms
```

The result is approximately a 30ms MAST task cycle with 8Kb in and 8Kb out.

Electrical Characteristics

Consumed Current

This is the current that the BMENOR2200H module consumes:

Power Source	Consumption
24 VDC rack	90 mA
power dissipation	2.2 W

Wiring Considerations

Modules are re-initialized when the power is switched back on. This can create a temporary disruption in the application or communications.

Standards and Certifications

Download

Click the link that corresponds to your preferred language to download standards and certifications (PDF format) that apply to the modules in this product line:

Title	Languages
Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	• English: *EIO0000002726* • French: *EIO0000002727* • German: *EIO0000002728* • Italian: *EIO0000002730* • Spanish: *EIO0000002729* • Chinese: *EIO0000002731*

Safety Standards and Certifications

References

Refer to these guidelines from the *Modicon M580 Safety Standards and Certifications* guide:

- Certificates and Declarations *(see Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications)*
- Operating and Storage Conditions *(see Modicon M580 Safety, Standards and Certifications)*
- Environment Test Compliance Levels *(see Modicon M580 Safety, Standards and Certifications)*

Module LED Indicators

Introduction

Refer to the LED indicators to monitor the status and performance of these items:

- BMENOR2200H module LEDs *(see page 30)*
- SD card LEDs

Module LED Descriptions

The module LED indicators are located on the front of the BMENOR2200H module. The LEDs provide information on:

- module status (run, error, downloading)
- serial communications
- Ethernet network communications
- SD memory card state
- cyber security status

This is the LED display on the front of the BMENOR2200H module:

The LEDs can be in these states:

- *on*: steady on
- *off*: steady off
- *flashing*: alternate (250 ms on, 250 ms off)

The module status is indicated by the color and state of the LEDs:

Label	Color	Pattern	Indication
RUN: operational state	green	on	The module is operating and configured.
		flashing	The module is blocked by a detected software error.
		off	The module is not configured. (The application is absent, invalid, or incompatible.)

Label	Color	Pattern	Indication
ERR: detected error	red	on	The processor, system, or configuration detected an error.
		flashing	• The module is not configured. (The application is absent, invalid, or incompatible.) • The module is blocked by a detected software error.
		off	Operations are normal (no detected errors).
DL: download firmware (upgrade)	red	on	A firmware download or factory reset is in progress.
		off	A firmware download or factory reset is not in progress.
ETH STS: Ethernet communication status	—	off	There is no link on the Ethernet backplane port.
	green	on	The module has an IP address, but there is no RTU connection.
		flashing	At least one RTU connection (client or server) is established in the module.
	red	on	The module has a duplicate IP address or factory reset mode.
CARD ERR: memory card detected error	red	on	• The memory card is missing. • The memory card is not usable (bad format, unrecognized type).
		off	The memory card is valid and recognized.
SER COM: serial data status	yellow	flashing	A data exchange (send/receive) is in progress on the serial connection.
		off	There is no data exchange on the serial connection.
SEC: secure communication status	green	on	Secure communications are enabled and running fine.
	red	on	Communications are *not* secure because a critical error in secure communications is detected. For example, there is no available security configuration, or the certificate expired when the communications stopped. No channel security is configured through the channel name for either master or slave.
		flashing	Secure communications are enabled and running, but an error is detected. For example, a certificate expires but the configuration authorizes communications to continue, or there are too many login attempts, etc.
	—	off	The module is not secure.

Chapter 2
The BMENOR2200H Module in Networks

What Is in This Chapter?

This chapter contains the following topics:

Standalone Architectures

Introduction

This topic describes the use of the BMENOR2200H module in a standalone M580 system.

Connection Media

Make connections to the BMENOR2200H module with a cable or a wireless medium:

- *upstream connection:* Connect the module to a SCADA system through the DNP3 protocol. (A Modbus TCP connection is another option.)
- *downstream connection:* Connect the module to remote outstation devices and stations through the DNP3 protocol.

Limitations

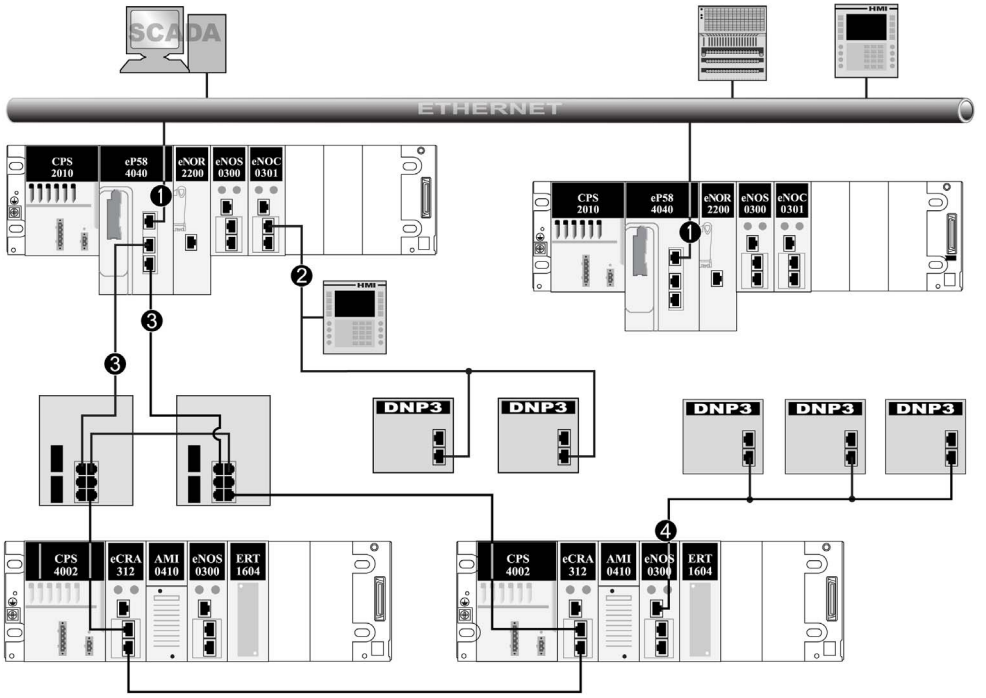
Observe these guidelines when you use the BMENOR2200H module:

- The module is compatible with Control Expert 14.1 Hot Fix and later.
- The module is compatible with CPUs that run firmware version 2.2 or later.
- The module does not support Hot Standby systems in Control Expert 14.1 or earlier versions.

Standalone Network with One Subnet

Sample Network

This sample standalone network includes BMENOR2200H modules on local racks in a single subnet:

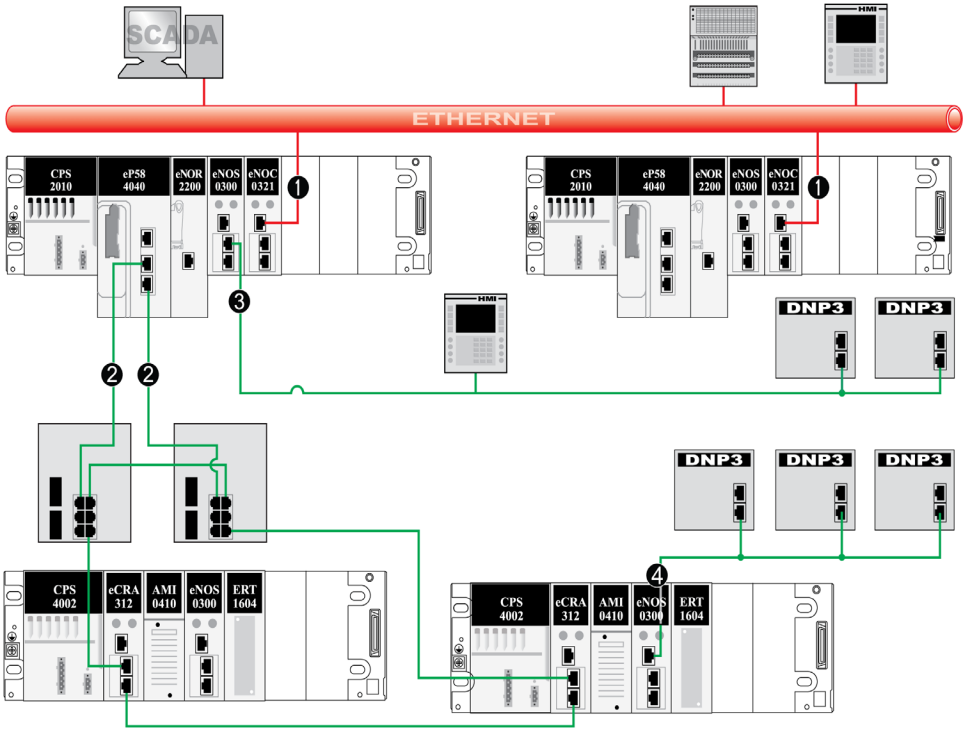


1. The service port on the CPU connects the RIO main ring and distributed equipment (DNP3 devices, HMI) to the Ethernet control network.
2. A BMENOC0301 module on the local rack connects distributed equipment (DNP3 devices, HMI) to the RIO main ring.
3. RIO main ring (Dual-ring switches connect the local rack to an RIO drop.)
4. A BMENOS0300 module on an RIO drop connects distributed equipment (DNP3 devices) to the RIO main ring.

Standalone Network with Two Subnets

Sample Network

This sample standalone network builds upon the single-subnet example *(see page 35)* and includes BMENOR2200H modules on local racks that communicate with two different subnets:

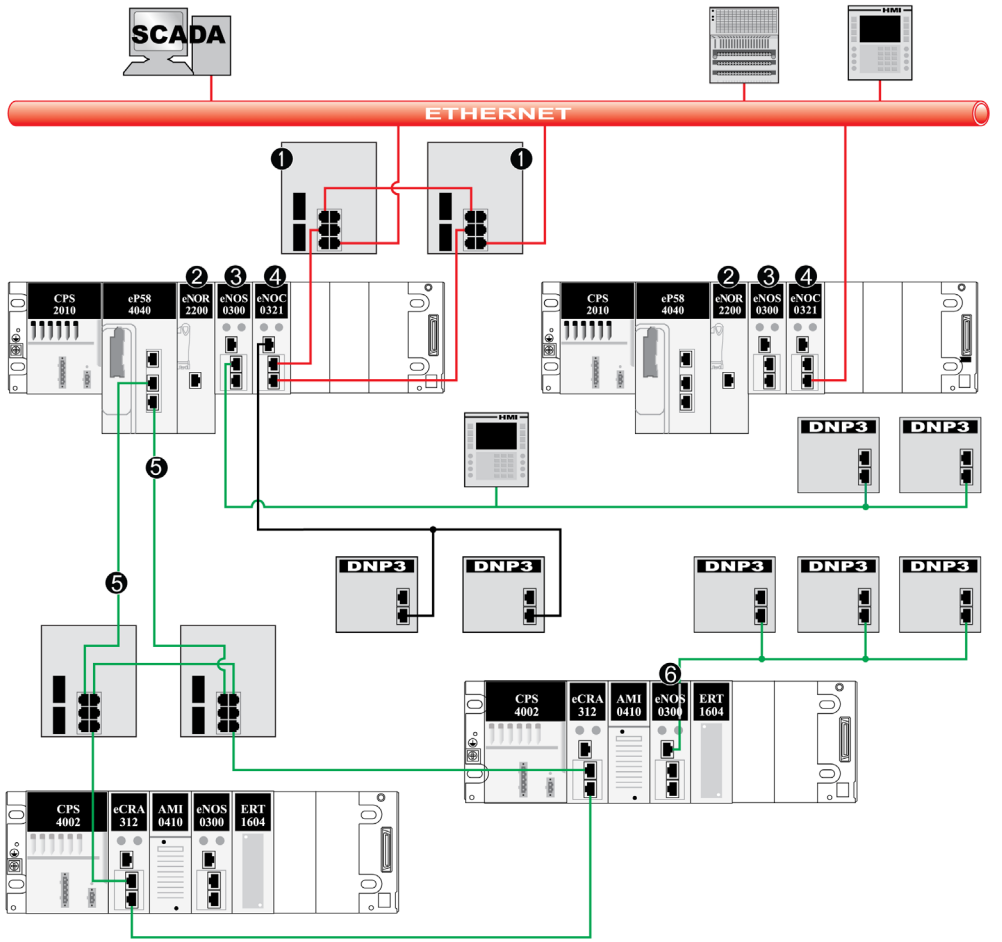


1 BMENOC0321 modules on the local racks connect the RIO main ring and distributed equipment (DNP3 devices, HMI) to the Ethernet control network (red).
2 RIO main ring (Dual-ring switches connect the local rack to two RIO drops and distributed equipment.)
3 A BMENOS0300 module connects the local rack to isolated distributed equipment (DNP3 devices, HMI).
4 A BMENOS0300 module on an RIO drop connects distributed equipment (DNP3 devices) to the RIO main ring.

Standalone Network with Link Redundancy

Sample Network

This sample standalone network builds upon the two-subnet example *(see page 36)*, which includes communications on different subnets (red and green). In this case, the connections between the local racks and dual-ring switches facilitate redundant connections between the subnets:



1 A dual-ring switch connected to the Ethernet port of a BMENOC0321 module on the local rack creates a redundant link to the control network (red).

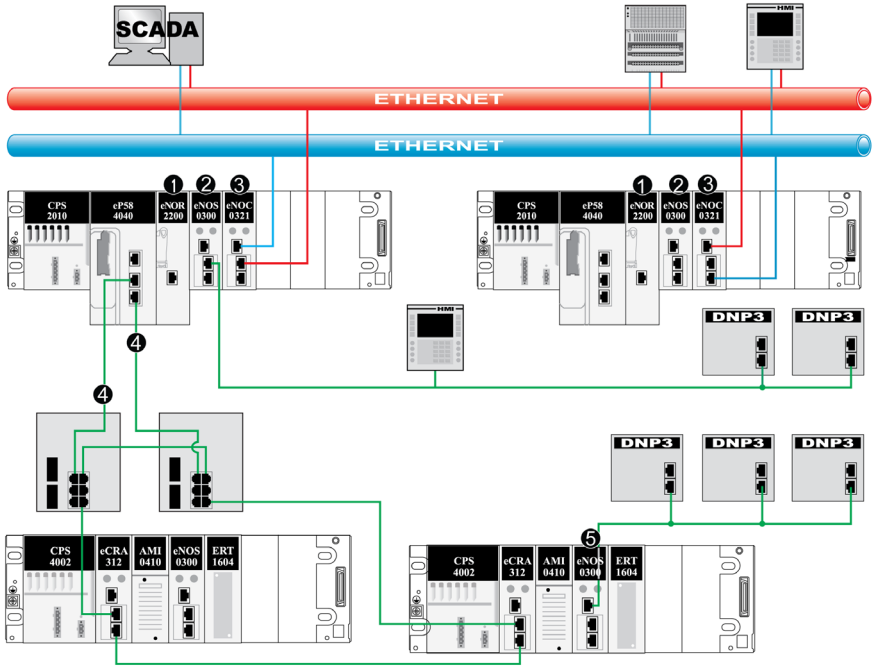
2 A BMENOR2200H module connects the local rack to distributed equipment (DNP3 devices, HMI) via the Ethernet backplane connection using redundant links.

3 A BMENOS0300 embedded switch module connects the local rack to distributed equipment (DNP3 devices) using redundant links.
4 The service port of a BMENOC0321 module allows distributed equipment (DNP3 devices, HMI) to communicate with the control network using redundant links.
5 RIO main ring
6 A BMENOS0300 embedded switch module on an RIO drop connects the RIO main ring to distributed equipment (DNP3 devices) using redundant links.

Standalone Network with Three Subnets

Sample Network

This sample standalone network builds upon the two-subnet example *(see page 36)* with different (red and green) subnets. In this case, BMENOC0321 modules with embedded IP forwarding in the local racks facilitate the connection to a third (blue) subnet:



1 A BMENOR2200H module
2 A BMENOS0300 module on the local rack connects distributed equipment (DNP3 devices, HMI) to the RIO main ring using redundant links
3 A BMENOC0321 module with IP forwarding enabled connects the RIO main ring and distributed equipment (DNP3 devices, HMI) to the blue network via the service port and the red network through the control network port using redundant links
4 RIO main ring
5 A BMENOS0300 module on an RIO drop connects distributed equipment (DNP3 devices) to the RIO main ring

Chapter 3
Hardware Installation

What Is in This Chapter?

This chapter contains the following topics:

Mounting the Module on the Modicon M580 Rack

Introduction

The BMENOR2200H module has a dual-bus connector *(see page 24)* that supports both Ethernet and X Bus communications.

Use these instructions to install the module in a single slot on a BMEXBP Ethernet backplane.

Before You Begin

⚠ WARNING

MODULE DESTRUCTION – LOSS OF APPLICATION

- Disconnect all power to the rack before installing the BMENOR2200H module.

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

Take these steps before you insert the module on the rack:

- Remove the protective cap from the module connector on the rack.
- Determine the cyber security operating mode for the module and configure the appropriate cyber security mode with the rotary switch *(see page 22)* before you install the module in the slot. The selected mode is implemented only after a power-up of the module.

Backplane Considerations

Install the module only on the local rack. You can install and configure a maximum of four communication modules (including BMENOR2200H modules) on a single local rack (depending on the selected CPU).

This table shows the maximum number of BMENOR2200H modules you can install in the local rack with respect to specific CPU references:

CPU	BMENOR2200H
BMEP582020	2
BMEP582040	3
BMEP584020	4
BMEP584040	4
BMEP586040	4

NOTE: Refer to the CPU selection table *(see Modicon M580 Standalone, System Planning Guide for, Frequently Used Architectures)* in the *Modicon M580 Standalone, System Planning Guide for Frequently Used Architectures*.

Install the module in a dual-bus slot on one of the following Ethernet backplanes:

Backplane	Description
BMEXBP0400(H)	4-slot Ethernet backplane
BMEXBP0800(H)	8-slot Ethernet backplane
BMEXBP1200(H)	12-slot Ethernet backplane
BMEXBP0602(H)	6-slot (hardened) dual-PWS Ethernet backplane
BMEXBP1002(H)	10-slot (hardened) dual-PWS Ethernet backplane

Rack and Slot Restrictions

The module occupies a single dual-bus slot. Observe these restrictions:

Rack	Slot	Instruction
all racks	0, 1	Do not insert the BMENOR2200H module in these slots. **NOTE:** These slots are reserved for the CPU module.
BMEXBP1200(H)	2, 8, 10, 11	These X Bus-only slots do not support the Ethernet functionality of the dual-bus BMENOR2200H module.
BMEXBP1002(H)	2, 8	
extended racks	—	You cannot install the dual-bus BMENOR2200H module in an extended rack. **NOTE:** Extended racks do not have Ethernet ports.
RIO drops	—	You cannot install the dual-bus BMENOR2200H module in an RIO drop.

Cyber Security Switch Considerations

NOTICE

UNINTENDED EQUIPMENT OPERATION

- Do not switch from the non-secure configuration (**Standard**) directly to the secure configuration (**Secured**) or vice-versa.
- Always power up the module with the rotary switch in the **Reset** position when you transition between the **Standard** and **Secured** modes.

Failure to follow these instructions can result in equipment damage.

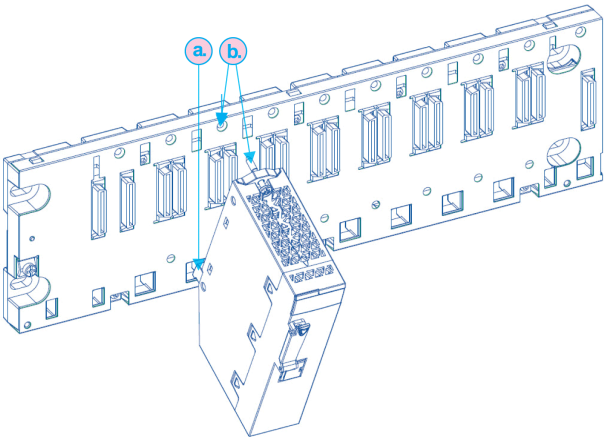
Follow these steps every time you insert a BMENOR2200H module on a powered rack:

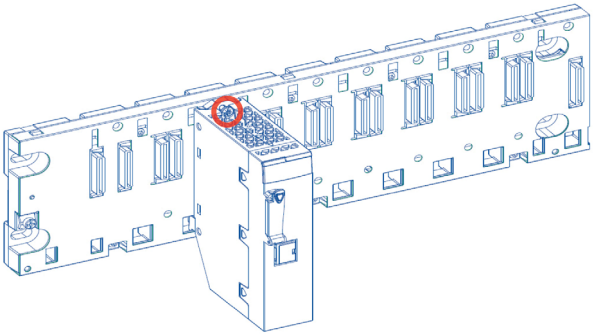
Step	Action
1	Set the rotary switch *(see page 22)* on the module to the **Reset** position.
2	Insert the module in the rack to power it up.
3	Remove the module from the rack to power it down.

Step	Action
4	Set the rotary switch on the module to the **Secured** or **Standard** position.
5	Reinsert the module in the rack to power it up.

Installing the Module on the Rack

Mount the module in a single slot on the backplane:

Step	Action
1	Turn off the power supply to the rack.
2	Remove the protective cover from the module interface on the rack.
3	Configure the cyber security level for the module with the rotary switch according to the cyber security considerations (above *(see page 43)*).
4	Notice sub-steps *a.* and *b.* in the graphic:  **a.** Insert the locating pins on the bottom of the module into the corresponding slots in the rack. **b.** Use the locating pins as a hinge and pivot the module until it is flush with the rack. (The twin connector on the back of the module inserts into the connectors on the rack.) **NOTE:** Do not insert the BMENOR2200H module in slot 0 or 1 in the local rack. Those slots are reserved for the CPU.

Step	Action
5	Tighten the retaining screw to hold the module in place on the rack:  **NOTE:** Tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).

Replacing a Module

NOTICE
UNINTENDED EQUIPMENT OPERATION • Do not switch from the non-secure configuration (**Standard**) directly to the secure configuration (**Secured**) or vice-versa. • Always power up the module with the rotary switch in the **Reset** position when you transition between the **Standard** and **Secured** modes. **Failure to follow these instructions can result in equipment damage.**

Any module on the rack can be hot-swapped at any time with another module with compatible firmware. The replacement module obtains its operating parameters over the backplane connection from the CPU. The transfer occurs immediately at the next cycle to the device.

When you switch from secure to non-secure operations or vice-versa, reset the module by setting the rotary switch to the **Reset** position to implement a clean configuration file and clear the security settings (including the user name and password).

We suggest that you export your cyber security configuration before you replace the module. When the rotary switch is set to the factory **Reset** mode, the entire cyber secure configuration is erased.

Replace the module:

Step	Action
1	Remove the module from the rack by reversing the above steps for installing the module. **NOTE:** Because this is a hot-swappable module, it is not necessary to power down the rack to remove the module.
2	Set the rotary switch *(see page 22)* on the replacement module to the **Reset** position.
3	Insert the replacement module in the rack to power it up.
4	Remove the replacement module from the rack to power it down.
5	Set the rotary switch on the replacement module to the **Secured** or **Standard** position.
6	Reinsert the replacement module in the rack to power it up.

NOTE: The replacement module does not automatically recover the security settings from the web-based configuration. The security configuration file is stored locally in the module. Export this file *(see page 155)* to create a backup configuration.

Grounding of Installed Modules

General

The grounding of modules is crucial to avoid electric shock.

Module Grounding

Follow all local and national safety codes and standards.

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK

If you cannot prove that the end of a shielded cable is connected to the local ground, the cable must be considered as dangerous and personal protective equipment (PPE) must be worn.

Failure to follow these instructions will result in death or serious injury.

⚠ ⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

Ensure ground connection contacts are present and not bent out of shape. If they are, do not use the module and contact your Schneider Electric representative.

Failure to follow these instructions will result in death or serious injury.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Securely tighten the mounting screw to attach the module firmly to the rack.

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

Chapter 4
Ethernet Communications

What Is in This Chapter?

This chapter contains the following sections:

Section 4.1
Ethernet Services

Available Ethernet Services

Introduction

This topic introduces the different services and functionalities that the BMENOR2200H module supports.

RTU Protocols

The module supports these RTU protocols:
- DNP3 NET server with SAv2 or SAv5
- DNP3 NET client with SAv2 or SAv5

Refer to the description of RTU protocols *(see page 62)*.

Ethernet Services

The module supports these Ethernet services:
- SNTPv1 client *(see page 113)*
- Modbus TCP server and client
- built-in HTTPS -based web pages *(see page 145)*
- FDR client *(see page 57)* (basic service)
- SNMPv1 Agent *(see page 55)*
- Firmware upgrade *(see page 56)*
- Cyber Security *(see page 141)* (RBAC, HTTPS, system hardening, cyber security event log, certificate management, etc.)

Other Services

The BMENOR2200H module supports these other services:
- clock synchronization *(see page 67)*
- SOE (sequence of events)
- event backup *(see page 79)*

Section 4.2
SNMP Service

Introduction

This section describes the Simple Network Management Protocol (SNMP).

NOTE: To configure the SNMP service, refer to the instructions to configure SNMP in the DTM *(see page 111)*.

What Is in This Section?

This section contains the following topics:

SNMP Overview

Introduction

An SNMP agent runs on:
- Ethernet communication modules
- CPUs with embedded Ethernet communications ports

Network management systems use SNMP to monitor and control Ethernet architecture components for the rapid network diagnosis.

Network management systems allows a network manager to:
- monitor and control network components
- isolate troubles and find their causes
- query devices, such as host computer(s), routers, switches, and bridges, to determine their status
- obtain statistics about the networks to which they are attached

NOTE: Network management systems are available from a variety of vendors.

Simple Network Management Protocol

Ethernet communication modules support SNMP, the standard protocol for managing local area networks (LANs). SNMP defines exactly how a manager communicates with an agent. SNMP defines the format of:
- requests that a manager sends to an agent
- replies that the agent returns to the manager

The MIB

The set of objects that SNMP can access is known as a Management Information Base (MIB). Ethernet monitoring and management tools use standard SNMP to access configuration and management objects included in the device's MIB, providing that:
- objects that SNMP can access are defined and given unique names
- manager and agent programs agree on the names and meanings of fetch and store operations

Transparent Ready products support the Standard MIB II SNMP network management level. This first level of network management can be accessed via this interface. It lets the manager identify the devices that create the architecture and retrieve general information on the configuration and operation of the Ethernet TCP/IP interface.

SNMP Communication

Overview

SNMP defines network management solutions in terms of network protocols and the exchange of supervised data.

The SNMP structure relies on the following elements:

- **Manager:** The manager allows entire or partial network supervision.
- **Agents:** Each supervised device has one or more software modules named Agent that are used by the SNMP protocol.
- **MIB:** The Management Information Base is a database or collection of objects.

The SNMP agent is implemented on the BMENOR2200H module. This allows a manager to access MIB-II standardized objects from the Modicon X80 agent through the SNMP protocol. The MIB-II allows management of TCP/IP communication layers.

SNMP Protocol

The SNMP protocol defines the types of messages between the agent and the manager. These messages are encapsulated in 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 resend the value of the requested variable.
- `Trap`: Allows asynchronous event signaling by the agent.

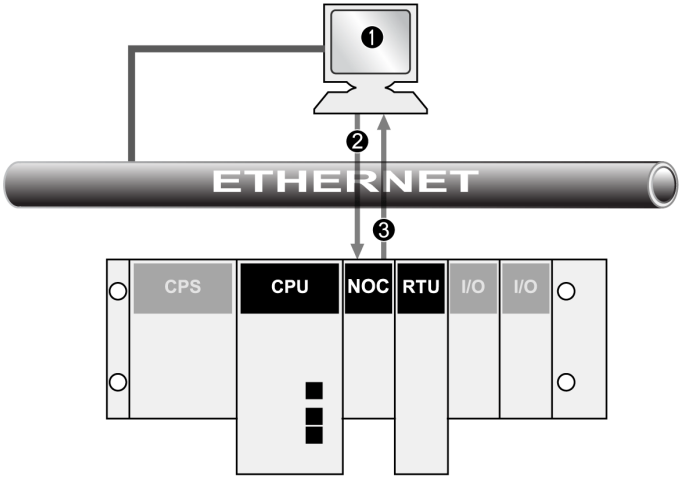
SNMP Operations Example

Introduction

The SNMP manager transmits read or write requests (**Set_Request**, **Get_Request**, **Get_Next_Request**), etc.) for objects defined in the MIB - II SNMP. The response is from the SNMP agent of the Modicon M580 module.

Modicon M580 Example

In this example, an SNMP manager on an Ethernet network sends a request to the SNMP agent in the BMENOR2200H RTU module (via a communications module in the same rack) and receives a response:



1 SNMP manager
2 request
3 response (trap)

The module's SNMP agent transmits events (traps) to the manager. The managed trap systems are as follows:

- `Coldstart Trap`: On the BMENOR2200H module, the event is transmitted following a module supply reset, a processor reset, or the downloading of an application to the PLC.
- `Authentication Failure Trap`: A transmitted event indicates that a network element cannot be authenticated. The **Community Name** field in the received message is different from the one that is configured on the module. Enable this trap during the configuration of the module.

SNMP Agent Details

Introduction

The widely available SNMP agent service allows easy access to the module's diagnostic information and event notification for certain services (for example, a change in network topology, an LED state, etc.).

Configure this service in the Control Expert DTM to manage IP addresses (MIB browser, ConneXview, etc.) or as an event trap.

MIB Support

The module uses the SNMP agent to support MIB II, which provides diagnostics information that is specified in the MIB files. The module supports these MIB levels:

- **MIB II:** The standard MIB II provides diagnostic information to manage the TCP/IP stack:
  - TCP/IP diagnostics
  - bridge MIB
- **MIB Lite:** This subset of the standard MIB II provides information to discover the identity of a device.

Management Services

This table describes the basic SNMP network management group functions:

Function	Description
system group management	Discover the device and identify it in a standard way by using an SNMP manager.
authentication checking	Configure the community name, and check the authentication of the requester.
system trap management	Configure the SNMP manager.
MIB II management	Manage the MIB.

The service runs on the module to allow SNMP manager applications to configure these SNMP objects:

- sysLocation
- sysContact

SNMP Version

The module runs SNMPv1 for this service. This version extends the capabilities of SNMP to address ministration and security issues. It is a Framework architecture that can be easily extended with new user security protocols. A new frame format has been defined for SNMPv1 adding among other things some security information. In particular, the PDU contents can be encrypted. SNMP uses UDP Transport layer protocol through port 161 and 162.

Section 4.3
Firmware Upgrade

EcoStruxure™ Maintenance Expert Tool

Tool Functions

Use the EcoStruxure™ Maintenance Expert too to upgrade the firmware of the BMENOR2200H module.

Perform these actions with this web-based tool:

- Automatically or manually discover one or more BMENOR2200H modules in your project, based on IP addresses.
- Upgrade the latest firmware version that is applicable to those modules over the web.

For details on how to install and use this firmware upgrade tool, refer to the online help *(see EcoStruxure Automation Device Maintenance, Firmware Upgrade Tool, Online Help)*.

NOTE: You cannot use Schneider Electric's Unity Loader™ software tool to upgrade the firmware for the BMENOR2200H module.

User Role

Use the **INSTALLER** user role to perform the firmware upgrade.

NOTE:

- When the module operates in **Standard** mode *(see page 22)*, the default user role is **INSTALLER**.
- When the module operates in **Secured** mode *(see page 22)*, the default user role is **SECADM**. In that case, log in to the security setting page to create a new user *(see page 156)* as an **INSTALLER** and upgrade the firmware in that role.

Section 4.4
FDR Client Basic Service

FDR Client Basic Service

Introduction

The basic FDR client service (FDR_CLIENT) is applied to the IP configuration that the BMENOR2200H module receives from the CPU via X Bus.

NOTE:

- This module does not support DHCP or BOOTP.
- Static IP parameters are not stored locally in this module.
- The cyber security configuration is not stored in the CPU.

Configuration Process

The service configures the IP parameters for the module:

Stage	Description
1	The BMENOR2200H module gets its IP configuration data from the user-specified configuration source.
2	The BMENOR2200H module gets its configuration file from the CPU.
3	The service validates the IP parameters (IP address, subnet mask, and gateway address).
4	The BMENOR2200H module configures the device with the validated IP parameters.

MAC-based default address information is used in these cases:

- There is no configuration file.
- The IP information is not valid.
- The configured IP address conflicts with the address of another module in the system.

When a default channel is used, the module does not get a valid IP address from the CPU. Instead, it uses the default IP address 10.10.mac5.mac.6. In this case, the module detects a duplicated IP status and does not run.

Behavior

When the initialization is complete, the FDR client service gets a MAC-based IP configuration (`10.10.mac5.mac6`) from the CPU. Then the service validates the parameters:

- OK: If the received IP parameters are valid and not duplicates, the FDR_CLIENT service uses those parameters.
- not OK: If any received IP parameter is invalid, missing, or a duplicate, the FDR_CLIENT service uses the default IP to execute DHCP until the device obtains a valid and non-duplicate IP.

NOTE: When a duplicate IP address is found in the system, the **ETH STS** LED is solid red. Refer to the description of LED indications. *(see page 30)*

If the default IP address is a duplicate, the FDR_CLIENT service configures the device with the loopback IP address 127.0.0.1.

After the IP configuration, the FDR_CLIENT service sends gratuitous ARPs.

Section 4.5
Modbus TCP Messaging

Data Exchange

Exchanges

Data exchanges take place in one of two modes:

- **server mode**: The RTU module supports all Modbus-over-TCP requests from the PLC.
- **client mode**: This type of exchange enables Modbus-over-TCP requests to be sent using the functions:
  - READ_VAR
  - WRITE_VAR
  - DATA_EXCH

For more details about functions, refer to *EcoStruxure™ Control Expert, Communication, Block Library*.

NOTE: The maximum Ethernet frame size depends on the type of transaction. The maximum frame size is 256 bytes for messaging.

The BMENOR2200H module manages these TCP connections through port 502 messaging:

- Modbus server: 32 connections
- Modbus client: 16 connections

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.

Port 502 messaging paths:

- server path:
  - Port 502 messaging can process up to 8 incoming requests from the network. Requests are received during the previous scan and sent to the Modbus server in the IN section.
  - Port 502 messaging can process up to 8 responses from the Modbus server in the IN section (including writing the data into the socket).
- client path:
  - Port 502 messaging can process up to 16 outgoing requests from the application in the OUT section (including writing the data into the socket).
  - Port 502 messaging can process up to 16 incoming responses from the network in the IN section. Responses are sent to the application.

Chapter 5
How to Work with RTU Protocols

Introduction

This chapter describes the built-in RTU protocols characteristics for use in Telemetry and Supervisory Control and Data Acquisition (SCADA) applications.

What Is in This Chapter?

This chapter contains the following sections:

Section 5.1
RTU Protocols

What Is in This Section?

This section contains the following topics:

Communication Protocols

Functions and Protocols

The BMENOR2200H module provides in-rack support for these functions and protocols in an M580 architecture:

RTU protocols	DNP3 NET (client or server) **NOTE:** When the module works as a DNP3 client, the number of connected servers affects the module performance (web page access, module start-up and data exchange through the backplane).
	Modbus TCP (client or server)
Main RTU protocol features	time synchronization through a protocol facility or SNTP *(see page 69)*
	data synchronization on demand of the SCADA
	balanced and unbalanced transmission mode
	event management with time stamping *(see page 72)* (Sequence of Events, SoE)
	event queue stored in RAM memory *(see page 75)* (up to 150,000 events)
	events data backfill to SCADA application via protocol facility *(see page 79)*
	event routing *(see page 76)*
	report by exception data exchanges
	unsolicited messaging data exchanges
	DNP3 secure authentication *(see page 66)* SAv2 and SAv5 with pre-shared key *(see page 66)*
	protocol setup via the DTM
Other built-in functionality	web server for security set-up and remote diagnostic
	advanced TCP/IP networking: SNTPv1 client, HTTPS server, and SNMP agent.

Limitations

NOTICE

UNINTENDED EQUIPMENT OPERATION

- Use different address values for each session in a channel or for each section in a session.
- Use successive DB mapping starting at 0 in the DNP3 protocol.
- Do not configure the DNP3 client to control a point that is not configured in the DNP3 server point mapping.

Failure to follow these instructions can result in equipment damage.

The BMENOR2200H module does not support multiple RTU protocols instances. Only one instance at a time of the DNP3 RTU can be launched to work with Modbus TCP.

DNP3 Protocols Overview

Introduction

The distributed network protocol (DNP3) was developed to achieve an open, standard interoperability for communications between master stations, substation devices, RTUs, and Intelligent Electronic Devices (IEDs). DNP3 has been used primarily by utilities such as the electric power industry in North America and has become widely used in other distributed infrastructures such as water/wastewater, transportation, and oil and gas industries.

DNP3 is based on the International Electrotechnical Commission Technical Committee 57 Working Group 03. The IEC TC57 WG03 has been working on the Enhanced Performance Architecture (EPA), a protocol standard for telecontrol applications. Each of the EPA's three layers corresponds to a layer on the OSI reference model.

DNP3 is specifically developed for inter-device communications that use SCADA RTUs. The protocol facilitates both RTU-to-IED (Intelligent Electronic Device) and master-to-RTU/IED.

The protocol was originally designed for slow serial communications, but the current DNP3 IP version also supports TCP/IP-based networking.

NOTE: For more details about the supported RTU protocols (including input and output sizes), refer to the description of the I/O data exchange with the CPU *(see page 25)*.

Supported Protocol Features

These are the main features that DNP3 supports:

- clock synchronization
- polled interrogations
- polled report-by-exception
- unsolicited report-by-exception
- DNP3 security authentication
- events transmission (time-stamped or not)
- counter-specific treatment
- master commands

Supported Data Types

The DNP3 protocol includes these data types:

- discrete inputs/outputs (single or double)
- measured values (with different formats)
- integrated totals
- string exchange
- commands

Interoperability Lists

This implementation of DNP3 is fully compliant with DNP3 Subset Definition Level 3, which suits larger RTU applications and offers practically the complete range of DNP3 functionality.

This standard defines interoperability *(see page 246)* between devices from different vendors. It includes a device profile that describes the basic protocol functionalities supported by the device and an Implementation table that defines information objects and their representation supported by the device.

DNP3 Security Authentication

Introduction

In some cases, an attacker can learn the protocol used by an RTU unit to gain dial-up access. When an RTU does not employ strong authentication or other security mechanisms, it accepts and responds to any caller.

To address such concerns, the BMENOR2200H module uses these security authorization services within DNP3 to facilitate communications between remote RTU units.

Secure Authentication Versions

The RTU supports these DNP3 secure authentication versions:

- **SAv2:** *Secure Authentication version 2* is a protocol family within DNP3 that facilitates the authentication of critical controls and commands and helps increase message confidentiality when the BMENOR2200H module is used in conjunction with a suitable SCADA host or other devices that support SAv2.
  SAv2 requires pre-shared keys to be pre-installed on all devices.
  SAv2 is defined by the IEEE 1815-2010 DNP3 standard.
- **SAv5:** *Secure Authentication version 5* is a newer protocol family within DNP3 that addresses evolving threats.
  SAv5 is defined by the IEEE 1815-2012 DNP3 standard.

NOTE:

- Schneider Electric recommends that you use the same secure authentication version (SAv2 or SAv5) on both the client and server sides.
- Manufacturers design a single device to be compatible with only one of these security authorization service versions.
- The implementation of SAv2 or SAv5 authentication requires the use of a security administrator application.

Pre-Shared Keys

The BMENOR2200H module implements secure DNP3 communications through pre-shared keys.

Many utilities that do not choose to manage security credentials in a more sophisticated manner may nonetheless require the level of protection afforded by pre-shared keys.

By definition, users on the SCADA side and module side use the same pre-shared key to effect mutual authentication. Communications are facilitated by a session key that is derived from the pre-shared key.

NOTE:

- Refer to the instructions for the management of pre-shared keys *(see page 152)*.
- For general information about pre-shared keys, refer to the *Modicon Controllers Platform Cyber Security, Reference Manual*.

Section 5.2
Clock Synchronization

Overview

The clock synchronization service establishes time accuracy among device clocks over a network. The BMENOR2200H module provides two ways to synchronize the clock with the SCADA (master) and the connected devices:

- via the RTU protocol facilities
- via the NTP protocol

NOTE:

- These clock synchronization methods are independent of one another. Configure your application to help avoid clock synchronization conflicts.
- If the NTP protocol is not configured, the module gets its time stamp from the controller during a module restart.

What Is in This Section?

This section contains the following topics:

Clock Synchronization with the RTU Protocol Facilities

Overview

One of the main features of the RTU is to manage events with time stamping. Time stamping requires effective time synchronization.

Behavior

The behavior of the clock synchronization command is determined by the role of the BMENOR2200H module:

Role(s)	Description
slave/server	When acting as a DNP3 slave or server, the BMENOR2200H module can synchronize its clock with a master or client station (SCADA). When your enable this feature, the module receives the clock synchronization command, it updates its internal clock, and posts the new value to the CPU. This maintains a consistent time on the local rack.
master/client	When acting as a DNP3 master or client, the BMENOR2200H module sends clock synchronization commands to connected slaves. As with the case above, the clock is initialized from the CPU when it starts up. It gets the new time from the CPU every time master/client sends the time synchronization command.

NOTE: When acting as both a master/client or slave/server, the BMENOR2200H module periodically synchronizes its local time with that of the CPU through the rack.

Configuration

The SNTP client runs only when you configure the service in the DTM. To configure the SNTP service, refer to the clock synchronization instructions *(see page 113)*.

Clock Synchronization with SNTP

Introduction

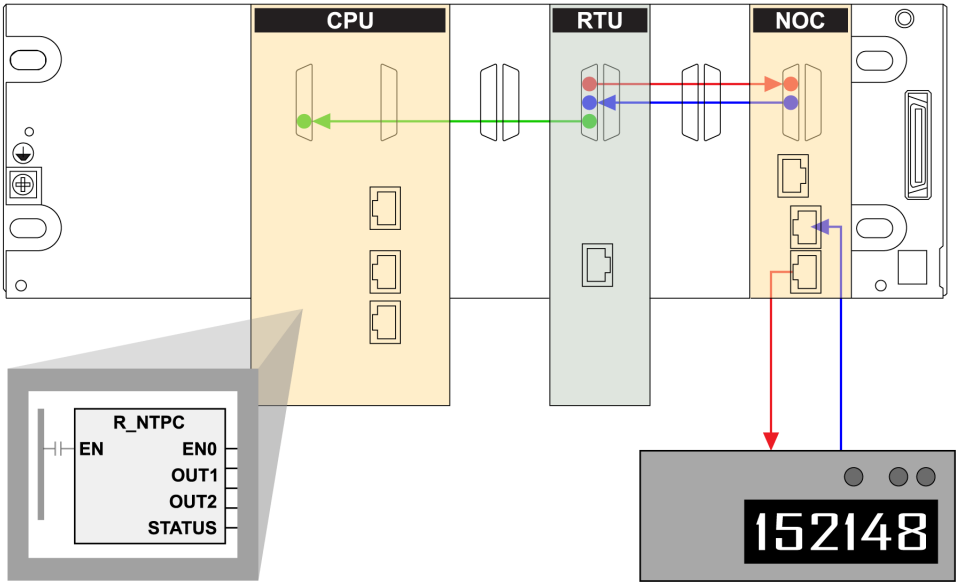
The BMENOR2200H module supports clock synchronization as an SNTP protocol client.

When the SNTP client is enabled, the module synchronizes the internal clock from the time server. This time is the basis for time stamping RTU events.

NOTE: Refer to the instructions for configuring the network time service in the DTM *(see page 113)*.

Clock Synchronization and Time Stamps

This sample network shows the flow of the synchronization signal from the perspective of the SNTP client in a BMENOR2200H module:



red line: The BMENOR2200H module sends an SNTP request over the Ethernet backplane to the NOC module, and the NOC module forwards the request to the SNTP server.

blue line: The SNTP server sends a reply to the NOC module, and the NOC module forwards the reply to the BMENOR2200H module.

green line: The BMENOR2200H module sends the source clock synchronization signal to the CPU over the Ethernet backplane.

NOTE:

- The BMENOR2200H module sends the signal to update the CPU's internal clock only when you select **Update Clock to CPU** in the time synchronization parameters *(see page 114)*.
- The time received by the CPU is typically within 5 ms of the SNTP server time, with a worst-case difference of 10 ms and a free running drift time +/- 2.6 seconds per day.
- Between clock synchronization signals, the CPU updates its own clock every millisecond with its internal timer.
- Use the `R_NTPC` function block in either MAST, FAST, or Interrupt sections to read the clock from the PLC application.

Clock Synchronization with the CPU Clock

Introduction

You can configure the CPU as an NTP server. In this case, the CPU uses its internal clock and acts as an Ethernet NTP server for devices that are connected to the same Ethernet network.

Configure the CPU as an NTP Server

Access and set the NTP parameters in Control Expert:

Step	Action
1	Open a Control Expert project.
2	Expand these items in the **Project Browser**: **Project → Configuration**
3	Double-click **PLC bus** to see the modules and racks in your project.
4	Double-click **PLC bus** to see the modules and racks in your project.
5	Select the **NTP** tab.
6	From the **NTP** pull-down menu, select **NTP Server**.
7	Configure the parameters in the **NTP Server Configuration** area.

When the CPU is configured as an NTP server, the polling period is a parameter used by remote modules in the PAC. It represents the time elapsed before the remote modules resynchronize their internal clocks with the time from the CPU NTP server.

Section 5.3
Time Stamping

Event Time Stamping

Overview

The BMENOR2200H module provides two ways for time stamping of events:

- Time stamping done at source in the CPU (requires PLC programming).
- Time stamping done in the BMENOR2200H module (does **not** require PLC programming).

NOTE: Improved time stamping resolution can be obtained when performing in the CPU. Time stamping resolution depends on the CPU scan time and I/O module type.

Section 5.4
Events Management

What Is in This Section?

This section contains the following topics:

Event Management

Introduction

The BMENOR2200H module generates events on changes of state, handles event lists, and provides these services:

- The management of a buffer of events (time stamped or not), overall buffer (queue) size can be up to 150,000 events.
  NOTE: One dedicated event buffer is managed per slave/server application (up to four slave/server applications are supported).
- Automatic event backfill to the SCADA or the master station via RTU protocol facility (on DNP3).

For the RTU DNP3 slave configuration, each object type has an independent event queue setting. To generate an event, set an event queue for the corresponding object type.

Access the Configuration

Access the event configuration in Control Expert:

Step	Action
1	Follow the directions to configure a server channel *(see page 107)*.
2	Expand (+) **Channels → DNP3 NET server → <ServerName>**,
3	Select one of these items from the **Select Type Id** pull-down menu on the **DATA MAPPINGS** tab: ● **Generate Events** ● **Clear Events**
4	Select the **Add** button to view the parameters for the selected type: ● **Generate Events:** ❍ **Point Number** ❍ **Point Count** ❍ **Object Group** ❍ **Point Name** ❍ **Add CMD_STATUS** ● **Clear Events:** ❍ **Object Group** ❍ **Point Name** ❍ **Add CMD_STATUS** **NOTE:** When the Control Expert window is active, you can hover the cursor over any field to see a description of the functionality and the available range of values.
5	● Click the **Apply** button to implement your configuration changes. ● Click the **OK** button to implement your changes and close the dialog box.

Event Queue Setting Page

Configure the parameters on the **Events** tab to map the event queue status to the DDDT registers in the CPU. Each event queue status consumes one three-byte register.

NOTE: When the events number exceeds the configured buffer size, events are lost or overwritten.

Access the event queue configuration in Control Expert:

Step	Action
1	Expand (**+**) **Channels → DNP3 NET server → <ServerName>**,
2	Make a selection in the **Select Type Id** pull-down menu on the **EVENTS** tab
3	Select the **Add** button to view the parameters for the selected type: • **Event Store Mode** • **Max Event Count** • **Buffer Setting** • **Max Event Count-1** • **Max Event Count-2** • **Max Event Count-3** • **Event Backup** **NOTE:** When the Control Expert window is active, you can hover the cursor over any field to see a description of the functionality and the available range of values.
4	• Click the **Apply** button to implement your configuration changes. • Click the **OK** button to implement your changes and close the dialog box.

Maximum Event Buffer Size

You can increase the maximum event buffer size from 10,000 to 150,000 (in the case of a single client connection).

NOTE: All channels can support up to 150,000 events, but each point type only supports up to 65,535 events.

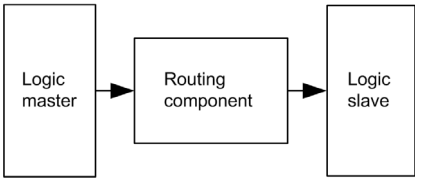
Event Routing

Introduction

The event routing component allows events from sub stations to be routed to SCADA within a single BMENOR2200H module.

To route events, one RTU master channel and at least one RTU outstation channel are needed inside the system. The solution is to create a logic RTU master and outstation in a single BMENOR2200H module. In the logic master, points are created to represent points in sub stations, and in the logic slave, points are created to simulate the behavior of points in sub stations. The event routing component is responsible for collecting events in the logic master. These events are sent from sub stations and trigger the same events in the logic slave.

BMENOR2200H module components:



NOTE: Event routing capabilities are possible only within a single module.
There are no automatic event routing capabilities between two BMENOR2200H modules (a slave/server and a master) that are configured in the same station.
In a hierarchical architecture, time stamped events are automatically transferred from low-end slave sub stations to the SCADA (or master) through the station. The automatic transfer uses path-through events functionality with a single BMENOR2200H module configured in both the master and outstation.

Configuration

Configure the BMENOR2200H module for event routing on the data mapping configuration page *(see page 116)*.

Considerations:

- The BMENOR2200H module does not detect events for event routing points in an outstation.
- There is no web page to configure event routing.
- In a valid configuration for event routing points, only one point is occupied in our database to reduce the data size stored in memory. Use the device DDT to see the point and its structure in the **Variables** list.

NOTE: With the loss of power management, you can specify in the configuration if you want to poll more events from the BMENOR2200H modules, fallback to SCADA, and help reduce the number of lost events.

Point configuration considerations:

Configuration	Description
channel (See the note below.)	For routing events, configure one master channel and at least one outstation channel. One master channel is required so that the system can connect with more sub slaves, and more slave channels allow for more SCADA in the system. **NOTE:** Refer to the channel configuration instructions *(see page 107)*.
master data mapping (See the note below.)	Add data points in the master channel. These points show the mapping of master points in the sub slave which communicate with the master channel **NOTE:** Refer to the DNP3 data object mapping instructions *(see page 116)*.
outstation point	After you configure the points in the master channel, the corresponding point is listed in the outstation channel. The points used to route are different from the normal points of the outstation. The parameters (CPU type, CPU address, variable name, and time stamp) of CPU mapping are no longer available, and the available parameters are read only. *Their lifetime is consistent with peer point configuration in the master*.
NOTE: When you configure these points in the master channel, select the events of the points to be routed, and route events to the corresponding outstation channel. For example, if the master channel receives events from the sub slave Binary Input point and routes them to the logic slave channel, they become events of the Binary Input point. Considerations: ● When you specify one point in the master for event routing, such as the binary input point, one corresponding point configuration is automatically generated in the logic outstation channel. The point configuration for the logic outstation channel is read only; it cannot be changed or removed in its DB mapping panel. ● If the channel number, session number, or point number mismatches in the outstation channel, an error page appears. ● If you choose the route to the channel as None, the point does not need to be routed to an outstation.	

Channel Combination for Event Routing

To route events inside the RTU module, use the configuration instructions *(see Modicon X80 , BMXNOR0200H RTU Module, User Manual)* to combine the master channel and outstation channel.

The supported combinations are:

Master Channel	Outstation Channel
DNP3 net client	DNP3 net server

Limitations

- Events are routed inside the module. This means that it is not possible to route events between two or more modules and also that the PLC application in the CPU cannot get and process the events. (The CPU can still get the point value in events just like the standalone master channel.)
- Only events are routed. Requests (commands) from SCADA are not routed to the sub slave. This means that inside the BMENOR2200H module, there is no other data exchange or communication between the master channel and the outstation channel except for events.
- In the system, SCADA cannot communicate with sub slaves. The solution uses the logic outstation in the BMENOR2200H module to simulate sub slaves, so SCADA can communicate only with the logic the outstation in the BMENOR2200H module, and the sub slave can communicate only with the logic master in the BMENOR2200H module.
- Some information related to events may be changed. Key information related to events like point value, flag, and time stamp is kept during event routing. Other information related to events like point number, events class, and variation is changed according to the outstation channel configuration.
- For broken connections, the downstream outstation does not generate events to an upstream supervision system.

Events Buffer Size

Confirm that the events buffer of the outstation are greater than the events buffer in the sub slave; otherwise, events are lost.

Event Backup

Introduction

The BMENOR2200H module's event backup buffer can store events when power to the module stops.

Event Backup Characteristics

You can configure the module for the events or data types that are saved upon a loss of power or a module hot-swap.

These are the capacities for event storage for the BMENOR2200H module and the RTU protocol:

- event buffer:
  - The module saves up to 150,000 event in the event buffer.
  - The module saves up to 10,000 events in the event buffer upon a loss of power.
  - The module saves up to 10,000 security events per server channel in the event buffer.
- flash memory:
  - The module saves up to 10,000 events into Flash memory upon a loss of power.
  - The module saves only the latest events when number of saved events exceeds 10,000.
  - The module reads events from Flash memory when power is restored.

NOTE: You can enable or disable the exchange of unsolicited messaging data.

Retain or Clear the Buffer

The event buffer in RAM is retained in these situations:

- The CPU experiences a warm start.
- There is a network swap in a dual-network application.

The event buffer in RAM is cleared in these situations:

- Use a SCADA command to clear the buffer in RAM.
- The CPU experiences a cold restart (such as during the download of a new configuration) or you press the reset button on the power supply. All communications are reset.
- The CPU experiences a cold restart (such as during the download of a new configuration), and communications are reset.
- Change the DNP3 cyber security configuration on the web page to clear the buffer.
- A SCADA command specifically clears the buffer.

Event Backup Behavior

The BMENOR2200H module has different backup behaviors in different cases. The type of case is defined from the user point view:

	Case	Description	Event
1	Loss of power	power lost	Saves events in non-volatile memory on loss of power.
2	Power start	power on/restore	Restores events when the RTU protocol starts.
3	Protocol restart	These actions clear the module event buffer: ● The RTU protocol configuration changes. ● The RTU receives a warm or cold start command from an RTU client.	Does not save events when the protocol exits.

Limitations

The BMENOR2200H module scans and stores events in each channel one by one when the number of events exceeds the Flash memory capacity, the module saves only the latest events.

Section 5.5
RTU Protocol Data Flow

RTU Communications

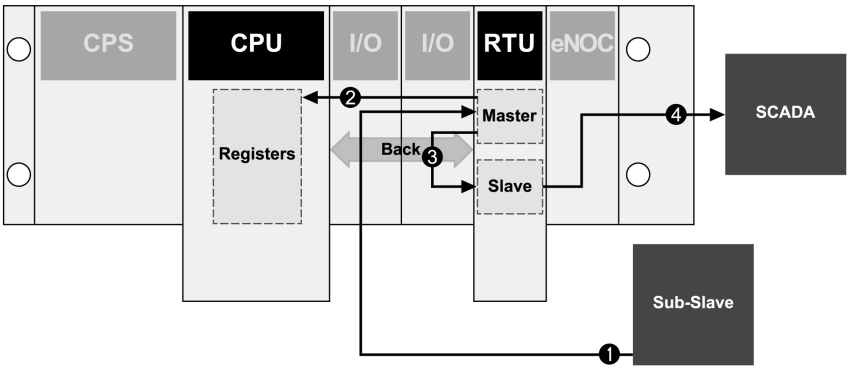
Communication Behavior

The BMENOR2200H module is equipped with a dual-bus connector *(see page 24)* that supports both Ethernet and X Bus communications.

This Ethernet backplane port is used mainly to communicate with the remote master or outstations with RTU protocols. The backplane interface is used to communicate with the CPU. The main activity of the backplane interface is the synchronization of data between CPU registers and the RTU point database inside the module. The synchronization cycle can be one or more PLC application scan cycles, depending on the data amount and backplane load.

When the Master Channel Receives Events from the Sub Slave

When something significant changes in the sub slave (like the value of a point), the sub slave sends an event. The system receives this event and the event is then routed to a SCADA system, as shown in this example:

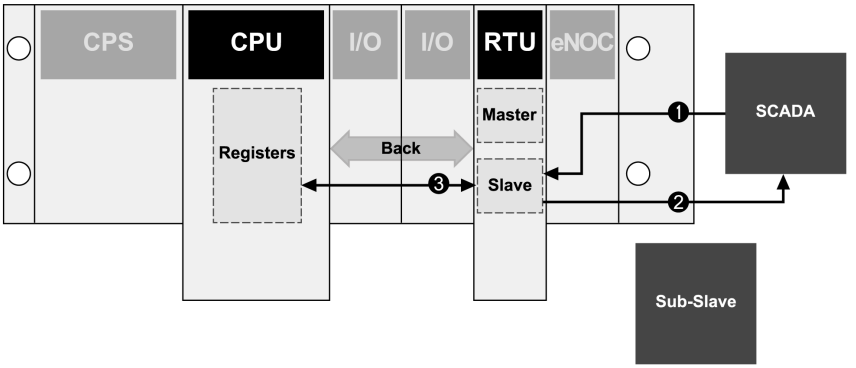


1 The sub slave sends events to the master channel of the BMENOR2200H module.
2 The master channel updates the point values in the module and the database of the logic outstation channel and synchronizes the value to CPU registers.
3 Events are routed to outstation channels according to point configuration.
4 The outstation channel buffers these events and sends events to SCADA when the communication link is established.

When the Outstation Channel Receives Request from SCADA

In the RTU system, a SCADA system sends requests (commands) like an Integrity Poll to the outstations connected to it. The outstation channel receives this request and sends a response to the SCADA system. With event routing, the behavior of the outstation channel is exactly the same as a standalone (no event routing) outstation channel. The master channel and sub slaves are not involved in this case.

This sample illustration shows a request from a SCADA system:

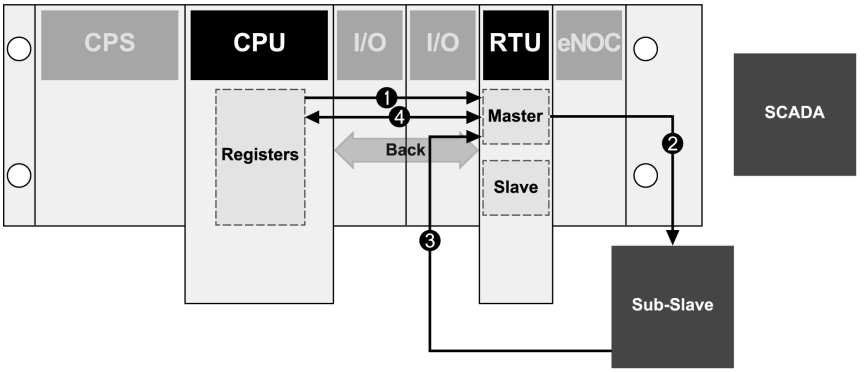


1 The SCADA system sends an Integrity Poll request to the outstation channel.
2 The point values are synchronized cyclically between the database of the outstation channel and CPU registers.
3 The outstation channel responds to the SCADA request with the point values in the database.

When the Master Channel Sends Request to the Sub Slave

The master channel can send requests to a sub slave connected to it, and a sub slave sends the response back to the master channel. The behavior of the master channel in this case is exactly the same as a standalone master channel. **The points in the logic outstation channel should be synchronized with the updated point in the master channel.**

Send request to a sub slave example:



1 The application in the M580 CPU sends an Integrity Poll command to the master channel.
2 The master channel sends Integrity Poll requests to the sub slave.
3 The sub slave responds to the request with the value of the latest points.
4 The logic slave data base is synchronized while the master channel updates the database.

NOTE: Point values are synchronized cyclically between the database of the master channel and CPU registers.

Section 5.6
Connection Status

Connection Status Overview

Introduction

The connection status of each channel of the BMENOR2200H module is put in a double-word descriptor in the DDDT mapping.

Detected Error Codes

The following tables describe the detected error codes for the connection status for both the slave/server and client/master roles.

Slave/Server:

Bit	Description
0	Channel security is not configured.
1	An initialization error for an unlocated variable is detected.
2	An internal error is detected (pipe create error IPT initialization error, etc.).
3...15	These bits are reserved.

Client/Master:

Bit	Description
0	Channel security is not configured.
1	An initialization error for an unlocated variable is detected.
2	An internal error is detected (pipe create error IPT initialization error, etc.).
3	The authentication failed.
4	There is an unexpected response.
5	There is no response.
6	Aggressive mode is not supported.
7	The MAC algorithm is not supported.
8	The key wrap algorithm is not supported.
9	The authorization failed.
10	The update key change method is not permitted.
11	The signature is not valid.

Bit	Description
12	The certification data are not valid.
13	An unknown user is detected.
14	The capacity of session key status requests is exceeded.
15	This bit is reserved.

Chapter 6
Sequence Of Events

Time Stamp Sequence of Events

Introduction

Sequence of events (SOE) software applications help you understand a chain of occurrences that can lead to potentially unsafe process conditions and possible shutdowns.

Many process events can be generated quickly when a system does not behave according to design or expectations. In this case, the X80 BMXERT1604 time stamping module records all events with a time stamp accuracy of 1ms. Data is stored in the module until it is transmitted by the application. The BMENOR2200H module can call this event data and transfer it to an external supervisor system (SCADA, DCS, etc.) through the RTU protocol.

This topic describes SOE in the transfer of the time stamping function from a BMXERT1604 module to the DNP3 protocol in a Control Expert project that includes a BMENOR2200H module.

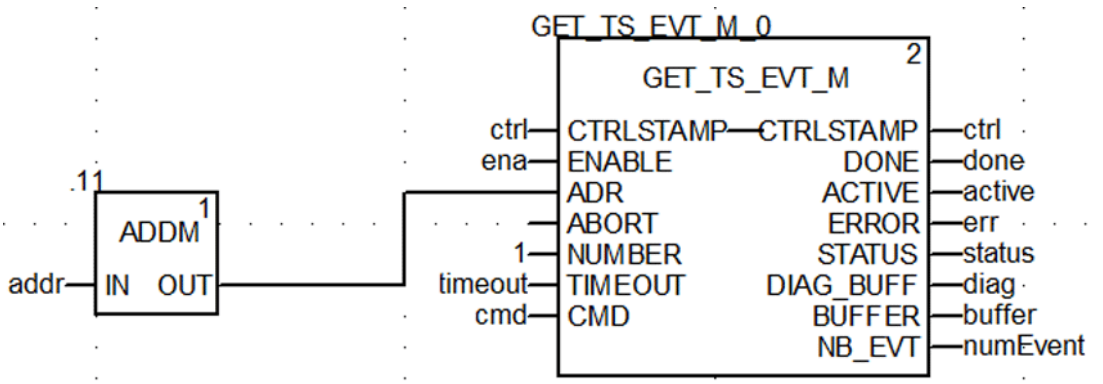
Process Overview

This is a broad overview of the time stamping SOE process.

Stage	Description
1	Use a DFB to read and send a time stamping event from a BMXERT1604 module to a BMENOR2200H module. In a single PLC cycle, a DFB instance processes a maximum of one time stamping event.
2	Based on the structure of the raw buffer read from the time stamping module, you can extract and convert the data.
3	Use a T850_TO_T870 EFB to convert the time stamping format into IEC60870 time format.

GET_TS_EVT_M Function Block

Use a `GET_TS_EVT_M` function block to read a time stamping event from a specific BMXERT1604 module:



NOTE: Read one event in a single PLC cycle for each time stamping module. When the `DONE` parameter turns to `TRUE`, the event has been read and stored in the buffer. You can move to the next step.
Refer to the EcoStruxure Control Expert System Block Library *(see EcoStruxure™ Control Expert, System, Block Library)* for detailed descriptions of the `GET_TS_EVT_M` function block parameters.

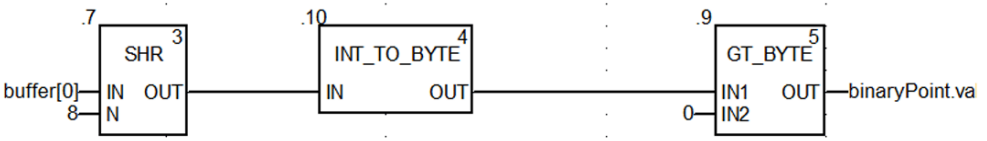
Event Format in Response Buffer

This table describes the format of the time stamping event in the response buffer:

Data Structure	Element	Type	Definition
Raw buffer format	Reserved	BYTE	Reserved
	Value	BYTE	Input value
	Event ID	WORD	Event ID defined by user or channel number
	SecondSinceEpoch	DWORD	The interval in seconds continuously counted from the epoch 1970-01-01 00:00:00 UTC
	FracOfSec_L	WORD	The fraction of the current second when the value of the TimeStamp has been determined. The fraction of the second is calculated as (SUM from i=0 to 23 of bi*2**—(i+1) s).
	FracOfSec_H	BYTE	
	TimeQuality	BYTE	Time Quality: • Bit 7: LeapSecondsKnown (not supported) • Bit 6: ClockFailure (not supported) • Bit 5: ClockNotSynchronized • Bit 0-4: Time accuracy

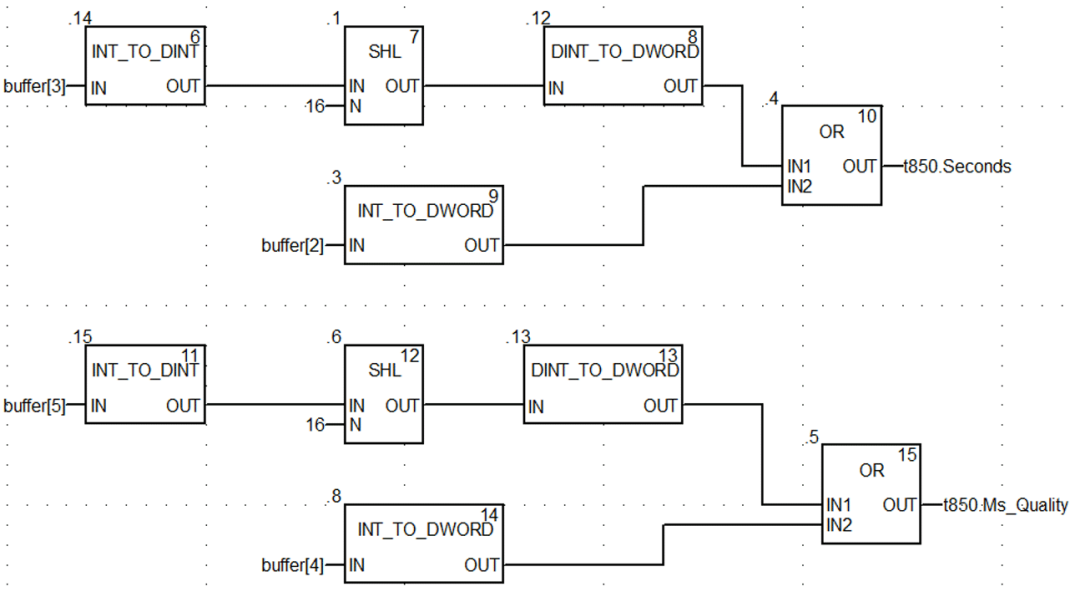
Extract the Time Stamp Event

Based on the raw buffer structure read from the time stamping module, you can extract and convert the data. First, extract the value of the binary point as shown in this example, which assumes that the first event starts from `Buffer[0]`:



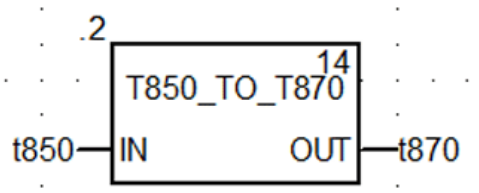
Extract the T850 Data

To extract the T850 data, as shown in this typical application example, put the binary point value in the right position of the DDT based on the BMXERT1604 module's address and channel in the raw buffer:



Convert the Time Stamp Format

To convert the time stamp format from IEC61850 to IEC60870, use the T850_TO_T870 EFB as follows, where the input parameter is the 850 time format and the output parameter is the 870 time format:



This table describes the structure of the 850 and 870 time format:

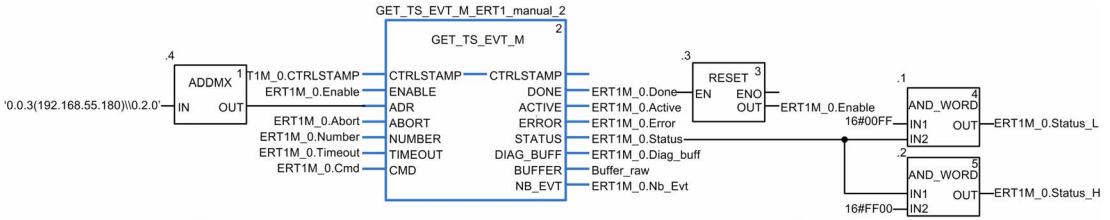
Data Structure	Element	Type	Definition
TIME_870_FORMAT	ms	WORD	Milliseconds: 0-59999 ms
	min	BYTE	Minutes: 0-59 min, the highest bit is invalid bit, 1: invalid time, 0: valid time
	hour	BYTE	Hour: 0-23 h, SU is not supported
	day	BYTE	Day: 1-31, day of week is not supported
	mon	BYTE	Month: 1-12 Year: 0-99
	year	BYTE	
	reserved	BYTE	Reserved
TIME_850_FORMAT	Seconds	DWORD	Seconds since 1970, confirm the time stamp is later than 2000.
	Ms_Quality	DWORD	• Bit 0-23: The fraction of the current second when the value of the TimeStamp has been determined. The fraction of second is calculated as (SUM from i = 0 to 23 of bi*2**—(i+1) s). • Bit 24-31: Time Quality • Bit 31: LeapSecondsKnown (not supported) • Bit 30: ClockFailure (not supported) • Bit 29: ClockNotSynchronized • Bit 24-28: Time accuracy

NOTE: The T870_TO_T850 function block does not consider time zone or summer when converting time. Set the T870 value to the DNP point's timestamp as follows:

```
binaryPoint.ms:=t870.ms;
binaryPoint.min:=t870.min;
binaryPoint.hour:=t870.hour;
binaryPoint.day:=t870.day;
binaryPoint.mon:=t870.mon;
binaryPoint.year:=t870.year;
```

Typical SOE Application Example

This screenshot shows the use of the `Send_V` command to transfer output of `GET_TS_EVT_M` (Buffer raw) to thge RTU points in a typical SOE application, in which read buffer and translation Time Stamp format in `Send_V` are equal to the function blocks in previous examples:



Send_V: [MAST]

```
(* read buffer*)
Time_850_1.value                := INT_TO_BYTE        ( SHRZ_INT(Buffer_raw[1], 8) ) ;
Time_850_1.EventID              := INT_TO_WORD                (Buffer_raw[2] );
Time_850_1.TImeStamp.Seconds    := DINT_TO_DWORD(INT_AS_DINT (Buffer_raw[3],
                                                              Buffer_raw[4] ) ) ;
Time_850_1.TImeStamp.Ms_Quallty:= DINT_TO_DWORD (INT_AS_DINT(Buffer_raw[5] ,
                                                              Buffer_raw[6] ) ) ;

(* translation TimeStamp format*)
Time_870_1.value        := Time_850_1.value;
Time_870_1.EventID      := Time_850_1.EventID;
Time_870_1.TImeStamp    := T850_TO_T870 (IN := Time_850_1.TimeStamp) ;

(* variable assignment*)

PLC0_d0_r0_s3_ENOR2200_CONN,SERVER,BI_P0[0],Value:=Time_870_1.Value;
PLC0_d0_r0_s3_ENOR2200_CONN,SERVER,BI_P0[0],TimeStamp.ms:=Time_870_1.TimeStamp.ms;
PLC0_d0_r0_s3_ENOR2200_CONN,SERVER,BI_P0[0],TimeStamp.minute:=Time_870_1.TimeStamp.min;
PLC0_d0_r0_s3_ENOR2200_CONN,SERVER,BI_P0[0],TimeStamp.hour:=Time_870_1.TimeStamp.hour;
PLC0_d0_r0_s3_ENOR2200_CONN,SERVER,BI_P0[0],TimeStamp.monthday:=Time_870_1.TimeStamp.day;
PLC0_d0_r0_s3_ENOR2200_CONN,SERVER,BI_P0[0],TimeStamp.month:=Time_870_1.TimeStamp.mon;
PLC0_d0_r0_s3_ENOR2200_CONN,SERVER,BI_P0[0],TimeStamp.year:=Time_870_1.TimeStamp.year;
```

Chapter 7
Configuring the Module

What Is in This Chapter?

This chapter contains the following sections:

Section 7.1
Configuration Overview

Configuration Components

Introduction

Observe these guidelines to configure the BMENOR2200H module after you add the module and its corresponding DTM to a Control Expert project *(see page 96)*.

Configuration Environment Components

Use this table to select the appropriate the component in the configuration environment with the intended configuration role:

Component	Functional Feature
Control Expert Configuration Overview	RTU module name definition *(see page 100)*
	IP address assignment *(see page 101)*
	Add the module to a Control Expert project. *(see page 100)*
	basic online diagnostics *(see page 138)*
Device DTM	channel configuration *(see page 107)*
	SNMP agent, SNMP client *(see page 111)*
	Network Timing Service (SNTP) *(see page 113)*
	DNP3 Net Client/Server *(see page 107)*
	Export / Import *(see page 135)*
	Module Information *(see page 137)*
	RTU protocol configuration *(see page 61)*
	RTU point configuration *(see page 116)*
	fast-access link to the diagnostic web page *(see page 139)*
HTTPS web pages	security configuration *(see page 141)*
	DNP3 Secure Authentication configuration *(see page 150)*
	RBAC configuration *(see page 156)*
Maintenance Expert	firmware upgrade *(see page 56)*
project migration	project migration considerations *(see page 203)*
	located variables with addresses (DNP3 AO/BO point “On Demand” mode *(see page 127)*)

Section 7.2
Use the Module in a Control Expert Project

Before You Begin

Use the instructions in this section to add a module and its corresponding DTM to a Control Expert project.

What Is in This Section?

This section contains the following topics:

Add the DTM and Module to Control Expert

About DTMs

Each module or device in the Control Expert **Hardware Catalog** is represented by a device type manager (DTM) that defines its parameters.

Any configuration done through the DTM is performed within the Control Expert environment.

DTM Installation

In general terms, the device DTM is automatically installed when you install Control Expert.

In any other case, you can install the DTM on a host PC (the PC that runs Control Expert) to make the device DTM available for use in Control Expert.

For third-party modules, the DTM installation process is defined by the manufacturer. Consult those instructions to install a DTM on your PC.

After a device DTM is successfully installed on your PC, update the Control Expert **Hardware Catalog** to see the new DTM in the catalog. The DTM is then added to your Control Expert configuration when the corresponding module is added to the project.

About the Control Expert DTM Browser

Introduction to FDT/DTM

Control Expert incorporates the Field Device Tool (FDT) / Device Type Manager (DTM) approach to integrate distributed devices with your process control application. Control Expert includes an FDT container that interfaces with the DTMs of EtherNet/IP and Modbus TCP devices and the BMENOR2200H module.

An EtherNet/IP device or Modbus TCP device is defined by a collection of properties in its DTM. For each device in your configuration, add the corresponding DTM to the Control Expert **DTM Browser**. From the **DTM Browser** you can open the device's properties and configure the parameters presented by the DTM.

Device manufacturers may provide a DTM for each of its EtherNet/IP devices, Modbus TCP devices, or the BMENOR2200H module. However, if you use a device that has no DTM, configure the device with one of these methods:

- Configure a generic DTM that is provided in Control Expert.
- Import the EDS file for the device. Control Expert populates the DTM parameters based on the content of the imported EDS file.

NOTE: The DTM for a BMENOR2200H module is automatically added to the **DTM Browser** when the module is added to the **PLC bus**.

Automatic DTM Creation

In a Control Expert application, DTMs for some Ethernet communication modules and other pre-configured devices (see the following list) are created automatically when added to an Ethernet rack on the main local or main remote drops. A default DTM name is assigned in the DTM topology, but you may modify the name:

- Right-click the desired DTM name in the **DTM Browser** and select **Properties**.
- select the **General** tab, and edit the DTM name in the **Alias name** field.
- Select **Apply** to save the changes.
  – or –
  Select **OK** to save the changes and close the dialog box.
  NOTE: The **OK** button is valid to press only when Control Expert has confirmed that the DTM is unique.

Windows Compatibility

This table describes the minimum and recommended PC configuration to run M580 DTMs inside Control Expert:

Operating System	Requirements
Microsoft Windows 7 Professional 64-bit	*system:* Pentium Processor 2.4 GHz or higher, recommended 3.0 GHz
	RAM: 4GB minimum; 8GB recommended
	hard disk: 8GB minimum free space; 20GB recommended
	Microsoft Internet Explorer 5.5 or higher
	Windows Service Pack 1 (SP1) is required to use Control Expert V14.1 EcoStruxure™ Control Expert 15.0.
	NOTE: Microsoft Windows 7 Professional 32-bit is not supported.
Microsoft Windows 10 32(*)/64-bit	*system:* Pentium Processor 2.4 GHz or higher, recommended 3.0 GHz
	RAM: 4GB minimum; 8GB recommended
	hard disk: 8GB minimum free space; 20GB recommended
	The 64-bit OS is required to manage projects that implement a Modicon M580 controller or that install DTMs.
Microsoft Windows Server 2016	*recommended version*: standard
	recommended processor: 3.20 GHz
	recommended RAM: 16GB
Microsoft Windows XP	Control Expert does not support this OS.

DTM Types

The **DTM Browser** displays a hierarchical list of DTM nodes on a connectivity tree. The DTM nodes that appear in the list have been added to your Control Expert project. Each node represents an actual module or device in your Ethernet network.

There are two kinds of DTMs:

- *master (communication) DTMs*: This DTM is both a device DTM and a communication DTM. The master DTM is a pre-installed component of Control Expert.
- *generic DTMs*: The Control Expert FDT container is the integration interface for any device's communication DTM.

This list contains these node types:

DTM Type	Description
communication (master)	Communication DTMs appear under the root node (host PC). A communication DTM can support gateway DTMs or device DTMs as children if their protocols are compatible.
gateway	A gateway DTM supports other gateway DTMs or device DTMs as children if their protocols are compatible.

DTM Type	Description
device	A device DTM does not support any child DTMs.

Node Names

Each DTM node has a default name when it is inserted into the browser. The default name for gateway and device DTMs for the BMENOR2200H module are in this format:

```
<EtherNet IP address>PLC0_d0_rX_sY_ENOR2200
```

- *X* is the rack number (usually *0*).
- *Y* is the slot number based on the module's location in the rack.

Therefore, a real-world example of a default name looks like this:

```
<10.10.1.72>PLC0_d0_r0_s2_ENOR2200
```

This table describes the components of the default node name:

Element	Description
address	This is the bus address of the device that defines the connection point on its parent gateway network (for example, the device IP address).
device name	The default name is determined by the vendor in the device DTM, but the user can edit the name.

Add the Module to a Project

Add the Module to the PLC Bus

Add a BMENOR2200H advanced RTU module to a Control Expert project and assign a name to it:

Step	Action
1	Open a project in Control Expert.
2	Expand (**+**) the **Project Browser** to see the **PLC bus** (**Project → Configuration → PLC bus**).
3	Double-click **PLC bus** to view the assembled rack(s).
4	Right-click an empty rack slot and select scroll to **New Device**. **NOTE:** Select a rack position that conforms to the module's slot restrictions *(see page 43)*.
5	In the **Part Number** column in the **New Device** dialog box, expand **Communication** to see the available modules.
6	Double-click the BMENOR2200H module to open the **Properties of device** dialog box.
7	In the **Name** field, assign a name to the module (or accept the default name).
8	Confirm that the DTM for the module was automatically added to the project (**Tools → DTM Browser**). **NOTE:** When you add a module to the local rack configuration, the corresponding communication DTM is automatically added to the list (**All Devices → Device types → Communication Devices**).
9	Repeat these steps to add more RTU modules to the **PLC bus**. **NOTE:** The local rack in an M580 system can hold a maximum of four communications modules, including RTU modules.

Section 7.3
Configuration with Control Expert

IP Address Configuration

Introduction

Use these instructions to configure the IP address parameters for a BMENOR2200H module.

Access the Configuration

Access the **IP address configuration** in Control Expert:

Step	Action
1	Open a Control Expert project that includes a BMENOR2200H module.
2	Double-click the BMENOR2200H module to see the **Configuration** tab.
3	Configure these parameters: ● **IP Address:** Enter the IP address of the module. ● **Subnet Mask:** Enter a subnet mask that corresponds to the IP address. ● **Default Gateway:** This is the IP address of the gateway to which messages for other networks are transmitted.
4	● Click the **Apply** button to implement your configuration changes. ● Click the **OK** button to implement your changes and close the dialog box.

Limitations

The BMENOR2200H module uses the FDR client basic service to get IP parameters from the CPU.

NOTE:

- This module does not support DHCP or BOOTP.
- This module does not locally store static IP parameters.
- For details, refer to the description of the FDR client service configuration *(see page 57)*.

Section 7.4
Debugging with Control Expert

Overview

This section describes procedures for debugging the configuration of an RTU module with Control Expert.

What Is in This Section?

This section contains the following topics:

Module Debugging Screen

Introduction

Use the debugging screen to diagnose an Ethernet port on the BMENOR2200H module.

Parameters

Find these parameters on the **Debug** tab:

Field	Description
MAC address	BMENOR2200H module's MAC address
IP address	BMENOR2200H module's IP address
Subnetwork mask	BMENOR2200H module's subnetwork mask address
Gateway address	BMENOR2200H module's gateway address

LED Display

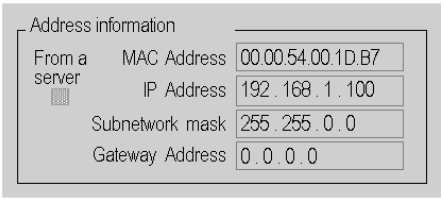
Observe these LEDs for conditions related to the module:

Location	LED	Description
upper-right window corner	**Run**	*on:* The module is operating normally.
		off: The PLC is not configured.
	Err.	*on:* A configuration or system error is detected.
		off: The module is operating normally.
Fault tab	**Fault**	Fault descriptions: • `%MW2.4`: detected internal fault • `%MW2.5`: detected configuration fault • `%MW2.6`: detected communication error • `%MW2.7`: detected application fault • `%MW2.8`: detected configuration error • `%MW2.9`: Ethernet disabled • `%MW2.10`: duplicate IP address • `%MW2.12`: link disconnection • `%MW2.13`: awaiting IP address • `%MW2.14`: storm detection

Debugging Parameters for TCP/IP Utilities

Address Information

The debugging parameters for TCP/IP utilities on the module debugging screen *(see page 103)* are grouped together in the Address information window:



This window displays this configuration information for the BMENOR2200H module:

- MAC address
- IP address
- subnetwork mask
- gateway address

Section 7.5
Configuration in the DTM

Introduction

Use the instructions in this section to configure services through the DTM after you access the services configuration link *(see page 106)*.

What Is in This Section?

This section contains the following topics:

Access the DTM

Introduction

Some features and services for your module are configured with the aid of a device type manager, or DTM. You can access the DTM in Control Expert.

Access the DTM Configuration

There are two ways to access the configuration screens for services provided by the DTM in Control Expert.

Step	Action
1	Open the Control Expert project that includes the appropriate module.
2	Open the **DTM Browser** (**Tools → DTM Browser**).
3	In the **DTM Browser**, double-click the name that you assigned to the module. *(see page 100)* to open the configuration window.

– or –:

Step	Action
1	Expand (**+**) the **Project Browser** to see the **PLC bus** (**Project → Configuration → PLC bus**).
2	Double-click **PLC bus** to view the assembled rack(s).
3	Double-click the module.
4	Click the **Services Configuration** link.

DNP3 Communications Configuration in the DTM

Introduction

Configure DNP3 communications for your module in the Control Expert DTM.

Configure Channels

Configure **MASTER** (client) or **OUTSTATION** (server) channels:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	In the open **CONFIGURATION** window, expand (**+**) **Communication** and select **Channel Configuration**. **NOTE:** The **Channels** menu item cannot be expanded because there are no configured channels.
3	Select the appropriate tab: ● Select the **MASTER** tab to add client channels. ● Select the **OUTSTATION** tab to add server channels.
4	Select the **Add New** button to view the **ADD NEW CHANNEL** configuration parameters.
5	Configure the parameters according to the new channel parameter descriptions below *(see page 108)*.
6	Select the **Add** button to see the newly configured channel in the table. **NOTE:** The **Channels** menu can now be expanded because there is at least one configured channel. All configured channels appear in this menu.
7	After you create a *server* channel on the **OUTSTATION** tab, repeat these steps to create the corresponding *client* channel on the **MASTER** tab. – or – After you create a *client* channel on **MASTER** tab, repeat these steps to create the corresponding *server* channel on the **OUTSTATION** tab. **NOTE:** ● Only one master and one outstation are supported. ● If the DNP3 Secure Authentication is configured in the web cyber security setting, confirm that the configured name of the RTU channel matches the channel name in the DTM. Otherwise, the secure setting does not map to corresponding channel in the DTM.
8	● Select the **Apply** button to implement the changes ● Select the **OK** button to implement the changes and close the dialog box. **NOTE:** When you create the first channel, the expandable **Channels** sub-menu appears on the **CONFIGURATION** screen.
9	Repeat these steps to create additional channels while observing these limitations: ● *client:* 64 connections ● *server:* 4 connections

NOTE: You can edit *(see page 110)* or delete *(see page 110)* a channel any time.

New Channel Parameter Descriptions

NOTE: When the Control Expert window is active, you can hover the cursor over any field to see a description of the functionality and the available range of values.

These parameters in the **ADD NEW CHANNEL** fields are available for the DNP3 client and server channel configurations:

Field	Master	Outstation	Description
Channel Name	✓	✓	Assign a name to the server. **NOTE:** The web pages use the **Channel Name** parameter to identify the configuration that is applied to this channel. Therefore, assign an identical **Channel Name** when you configure cyber security settings *(see page 150)*.
Protocol	✓	✓	**DNP3 NET Client:** Configure the new channel as a DNP3 client (outstation).
			DNP3 NET Server: Configure the new channel as a DNP3 server (master).
Dest Port	✓		Define the destination port to use.
Local Port		✓	Define the local port for network communications.
IP Address	✓		The IP address in this field is the IP address of the source of the communications packets.
IP Filter		✓	Enter the IP address of the remote device. **NOTE:** The default value is 255.255.255.255 (present disable IP filter)
Network Type	✓	✓	Select a network protocol: ● **TCP-IP** ● **UDP-IP** ● **TCP-UDP**

Advanced Parameter Configuration

After you create a channel with the instructions above, the new channel appears in the table on the **MASTER** tab or **OUTSTATION** tab. At this point, you can configure the **ADVANCED PARAMETERS** for the channel. These advanced parameters are global settings that are implemented on all server channels or client channels:

Step	Action
1	Select **Channel Configuration** from the **Communication** menu.
2	Select the appropriate tab: ● Select the **MASTER** tab to view the **MASTER CHANNEL** table. ● Select the **OUTSTATION** tab to view the **OUTSTATION CHANNELS** table.

Step	Action
3	Select a row in the table.
4	Click the **Advanced Settings** button to view the **ADVANCED PARAMETERS** table. **NOTE:** Depending on your Control Expert window size, you may have to scroll down in the **Client** or **Server** tab to see the **ADVANCED PARAMETERS** fields.
5	Configure the parameters according to the advanced parameter descriptions below *(see page 108)*.
6	• Select the **Apply** button to implement the changes. • Select the **OK** button to implement the changes and close the dialog box.

Advanced Parameter Descriptions

NOTE: When the Control Expert window is active, you can hover the cursor over any field to see a complete description of the functionality and the available range of values.

These are the available advanced parameters for the DNP3 client and server channel configurations:

Field	Master	Outstation	Description
Event Backup Enable		✓	*enabled (selected):* Events are backed up upon a power failure.
			disabled (empty): Events are not backed up upon a power failure.
Rx Frame Size	✓	✓	Configure the frame size in the receive link layer.
Rx Frame Timeout	✓	✓	Configure the timeout value for waiting for a complete frame after receiving the frame sync.
Confirm Timeout	✓	✓	Configure the maximum wait time for link level confirmation.
Offline Poll Period	✓		Configure an interval for reattempting to establish communications for an offline session.
Rx Buffer Size	✓	✓	Configure the receive buffer size for the physical port.
Tx Fragment Size	✓	✓	Configure the maximum transit application fragment sizes.
Channel Response Timeout	✓		Configure the wait time for the DNP3 master's response to a transmitted request.
Tx Frame Size	✓	✓	Configure the transmit link layer frame size.
Confirm Mode	✓	✓	**NEVER:** Never request link layer confirmations.
			SOMETIMES: Request link layer confirmations for multi-frame fragments.
			ALWAYS: Always request link layer confirmations.

Field	Master	Outstation	Description
Max Retries	✓	✓	Configure the number of reattempted link layer confirmation timeouts.
First Char Wait	✓	✓	Configure the minimum time (ms) after receiving a character before an attempt to transmit a character on this channel.
Rx fragment Size	✓	✓	Configure the maximum receive application fragment sizes.
Restore Mode		✓	**Main Channel:** Restore events for the main channel.
			All Channels: Restore all events.
Max Queue Size	✓		Configure the maximum number of requests that are queued on a DNP3 master.

After you edit any of these parameters, click the **Update** button to update the configuration.

Edit Channels

Edit the parameters for an existing channel:

Step	Action
1	Click the pencil icon in the **Edit** column for the channel you want to edit.
2	Reconfigure the parameters in the **EDIT CHANNEL** and **ADVANCED PARAMETERS** fields (described above).
3	Click the **Update** button to update the configuration.
4	Click the **OK** or **Apply** button to save the changes.

Delete a Channel

Delete an existing channel:

Step	Action
1	Select the check box that corresponds to the client or server channel.
2	Select the **Delete** button.
3	Select the **Update** button.
4	• Select the **Apply** button to save the changes. –or– • Select the **OK** button to save the changes and close the dialog box.

SNMP Configuration in the DTM

Access the SNMP Configuration

Access the SNMP parameters in the Control Expert DTM:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	In the **CONFIGURATION** menu, expand (**+**) the **Communication** sub-menu.
3	Select **SNMP**.
4	Configure the SNMP parameters. **NOTE:** The parameters are described in the next table.
5	• Select the **Apply** button to implement your configuration changes. • Click the **OK** button to implement your changes and close the dialog box.

Parameters

This table shows the SNMP parameters that are available for your module.

NOTE: When the Control Expert window is active, you can hover the cursor over any parameter field to see a description of the functionality and the available range of values.

SNMP parameters:

Field	Parameter	Description
IP ADDRESS MANAGERS	**IP Address Manager 1**	Configure an IP address of the primary SNMP manager in the range 0.0.0...255.255.255.255.
	IP Address Manager 2	Configure the IP address of the secondary SNMP manager.
AGENT	**Enable SNMP Manager**	*selected*: The SNMP manager is enabled.
		deselected: The SNMP manager is disabled.
	Location (SysLocation)	Specify the physical location of the module when the SNMP manager is enabled.
	Contact (SysContact)	Enter the name of a maintenance person to contact when the SNMP manager is enabled.
COMMUNITY NAMES	**Set**	Enter the community name for the **Set** utility.
	Get	Enter the community name for the **Get** utility.
	Trap	Enter the community name for the **Trap** utility. **NOTE:** • Traps are sent through UDP port 161. • Confirm whether you configure trap settings on the SNMP manager that are consistent with those on the processor.

Field	Parameter	Description
SECURITY	Enable Authentication Failure Trap	*selected*: The SNMP agent sends a trap message to the SNMP manager when an unauthorized manager sends a **Get** or **Set** command to the agent.
		deselected: This feature is disabled.

NOTE: The characteristics and details of the SNMP service are described in the Ethernet services chapter *(see page 51)*.

Network Time Service Configuration in the DTM

Introduction

The BMENOR2200H module supports clock synchronization as an SNTP client.

When the SNTP client is enabled, the module synchronizes the internal clock from the time server. This time is the basis for time stamping RTU events.

NOTE: For details, refer to the description of the BMENOR2200H module as an SNTP client *(see page 69)*.

Features of the Service

The clock synchronization via SNTP offers:

- periodic time corrections obtained from the reference standard, for example, the SNTP server
- automatic switchover to a backup time server if an abnormal event is detected with the normal server system
- local time zone configurable and customizable (including daylight saving time adjustments)

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 typical
- 10 ms worst case

Access the SNTP Configuration

Access the SNTP parameters in the Control Expert DTM:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	In the **CONFIGURATION** menu, expand (**+**) the **Communication** sub-menu.
3	Select **Network Timing Service**.
4	Configure the SNTP parameters. **NOTE:** The parameters are described in the next table.
5	• Click the **Apply** button to implement your configuration changes. • Click the **OK** button to implement your changes and close the dialog box.

Time Synchronization Parameters

This table shows the SNTP parameters that are available for your module:

Field	Parameter	Description
SNTP Server	**Primary IP Address**	Enter a valid IP address for the primary SNTP server.
	Secondary IP Address	Enter a valid IP address for the secondary SNTP server.
	Polling period	This value represents the number of seconds between updates from the SNTP server.
Time Zone	**Time Zone**	Select a time zone from the pull-down menu.
	Timezone Offset	This value represents the difference (in minutes between the configured time zone and UTC.
	Automatically adjust clock for daylight saving	*selected:* Adjust the clock for daylight saving time.
		deselected: Do not adjust the clock for daylight saving time.
	Start Daylight Saving	Configure the start and end times for daylight saving in the available fields.
	End Daylight Saving	
TIME TO CPU	**Update Clock to CPU**	*selected:* Update the clock with the time from the CPU.
		deselected: Do not update the clock with the time from the CPU.

NOTE: When the Control Expert window is active, you can hover the cursor over any parameter field to see a description of the functionality and the available range of values.

Clock Synchronization Terms

SNTP 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: `((T2 - T1) + (T4 - T3))/2` where: ● T1 = time when SNTP request is transmitted from the module ● T2 = time when SNTP server receives the request (provided by the module in response) ● T3 = time when the SNTP server transmits the response (provided to the module in the response) ● T4 = time when SNTP response is received by the module
time accuracy	The local time margin is < 10 ms compared to the referenced SNTP server time. ● typical: 5 ms ● worst case: <10 ms
settling time	Maximum accuracy is obtained after 2 updates from the SNTP server.

Term	Description of Service
polling period dependency	Accuracy depends on the polling period. Less than 10 ms of margin is achieved for polling periods of 120 ms or less. To obtain a high degree of accuracy (when your network bandwidth allows), reduce the polling period to a small value—for example, a polling time of 5 s provides better accuracy than a time of 30 s.
leap second	To compensate for the deceleration of the earth 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 SNTP server.

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
M580	January 1, 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.

NOTE: For details, refer to the descriptions of available time sources.

General Time Synchronization Terms

General terms:

Term	Description of Service
time zone	The default format is universal time, coordinated (UTC). Optionally you may configure the service to use a local time zone (for example, GMT+1 for Barcelona or Paris). *Refer to the note at the end of this table.*
daylight saving time	The module automatically adjusts the time change in the spring and fall. *Refer to the note at the end of this table.*
update clock to CPU	When no other time source is configured, the RTU receives a UTC time for synchronization from the CPU over the Ethernet backplane *(see page 69)*.
NOTE: This setting is implemented at the module level even if there is no SNTP configuration for the module. The implementation of this setting owes to the BMENOR2200H module's support for several time sources (for example, DNP3). It you, therefore, use DNP3 for time synchronization instead of SNTP, the time zone is applied to the module.	

DNP3 Data Object Mapping

Introduction

To facilitate communications with the BMENOR2200H module, create data points for the DNP3 communication protocol in the **DATA MAPPINGS** tab in the DTM.

Access the Configuration Tab

Access the configuration parameters on the **DATA MAPPINGS** tab in Control Expert:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	Confirm that you already created client or server channels *(see page 107)*.
3	In the **CONFIGURATION** menu, expand (**+**) the **Channels** sub-menu.
4	Make a selection in the **Channels** sub-menu: ● **DNP3 NET Server** ● **DNP3 NET Client**
5	Select a specific channel in the sub-menu.
6	Select the **DATA MAPPINGS** tab for the channel.
7	Configure the data mapping parameters.
8	● Select **Apply** to implement your configuration changes. ● Select **OK** to implement your changes and close the dialog box.

DNP3 Client Data Mappings

A newly applied data point configuration is added to the X80 master DTM. It appears in the Control Expert variable manager.

DNP3 Data Mappings

Using a **Binary Input** as an example, edit the data point configuration on the **DATA MAPPINGS** tab:

Step	Action
1	At **Select Type Id**, select a type ID. **NOTE:** For this example, select **Binary Input**.
2	Click **Add** to see the name of the binary input (**DNP3_SERVER_BINARY_INPUT**) in the **Type Identification** column.
3	Select the table row that corresponds to the new binary input to see the **BINARY INPUT** configuration options.
4	Modify the parameters. **NOTE:** When the Control Expert window is active, you can hover the cursor over any field to see a description of the functionality and the available range of values.

Step	Action
5	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

NOTE: A newly applied data point configuration is added to the X80 master DTM. It appears in the Control Expert variable manager.

Exchangeable CPU Data Object

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Do not create an instance of redundant data access.

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

Implement the data dictionary in Control Expert:

Step	Action
1	Open the **Project Settings** (**Tools → Project Settings**).
2	Expand (**+**) the menu: **Project Settings → General**
3	Select the **PLC Embedded Data** setting to see the **Property label** and **Property value** columns.
4	In the **Data label** column, find the **Data Dictionary** row and check the corresponding box in the **Property value** column. **NOTE:** Check this box when you program the PLC application. Otherwise, unlocated variables may not be mapped to RTU data points. However, a compiled application consumes more memory when the data dictionary is included, which can have an impact on unlocated variables that are implemented in RTU solutions.
5	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

Unlocated variables can be exchanged between the CPU and the BMENOR2200H RTU module after you define and manage the memory map of the CPU to exchange data with the module.

The CPU data objects are mapped and only linked for the BMENOR2200H module's purpose.

Data Exchange

To sustain a high rate of data exchange, we recommend that you define the BMENOR2200H module's RTU memory for data objects in a sequential ARRAY data type to group points with the same settings.

Use consecutive point numbers (0, 1, 2, 3...) in DNP3 request fragments.

Predefined Command List

The required input fields are requested to define a predefined command item for DNP3 master/DNP3 NET client *(see page 171)*.

Static Variation Name of DNP3

Data object type	Static variation
Binary Input	g1v1 Binary In
	g1v2 Binary In Flag
Double Input	g3v1 Double In
	g3v2 Double In Flag
Binary Output	g10v1 Binary Out
	g10v2 Binary Out Flag
Binary Counter	g20v1 32bit Counter
	g20v2 16bit Counter
	g20v5 32bit Ctr No Flag
	g20v6 16bit Ctr No Flag
Frozen Counter	g21v1 32bit Frozen Ctr Flag
	g21v2 16bit Frozen Ctr Flag
	g21v5 32bit Frozen Ctr Flag Time
	g21v6 16bit Frozen Ctr Flag Time
	g21v9 32bit Frozen Counter
	g21v10 32bit Frozen Counter
Analog Input	g30v1 32bit Analog In
	g30v2 16bit Analog In
	g30v3 32bit AI No Flag
	g30v4 16bit AI No Flag
	g30v5 Short Float AI
Analog Input Deadband	g34v1 16bit AI Deadband
	g34v2 32bit AI Deadband
	g34v3 Short Float AI Deadband
Analog Input Dband_Ctrl	g34v1 16bit AI Deadband
	g34v2 32bit AI Deadband
	g34v3 Short Float AI Deadband

Data object type	Static variation
Analog Output	g40v1 32bit Analog Output
	g40v2 16bit Analog Output
	g40v3 Short Float AO
Read_Group	—
Read_Class	—
Write_Octet_String	—
Freeze_Counter	—
Unsolicited_Class	—
Time_Sync	—
Restart	—
Octet String	g110 Octet Strings
Integrity_Poll	—
Gen_Events	—
Clear_Events	—

Mapping Tables

Depending on the data object type and the selected protocol profile, different configuration fields are required to define a data object mapping item. The tables below describe the available parameters for each selection in the **Select Type Id** pull-down menu on the client and server **DATA MAPPINGS** tabs.

NOTE: These tables include brief descriptions of each data mapping parameter. When the Control Expert window is active, hover the cursor over any parameter field to see a description of the functionality and the available range of values.

Binary Input

This table describes the DNP3 net client parameters that appear on the **DATA MAPPINGS** tab when you select a **Binary Input** in the **DATA MAPPINGS** tab:

Client Parameter	Description
Point Number	Indicates the start number of the point. **NOTE:** Confirm that the DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count	Indicates the number of points.

Client Parameter		Description
Store to CPU		Choose a source for the event time stamp and flag: ● **Value only:** module time ● **Value with time:** CPU register time ● **Value with flag:** point flag information from the CPU registers ● **Value with flag and time:** flag and time from the CPU registers
Point Name		Name of the unlocated register
Static Variation		Select the static variation for the data point.
Event Routing	**Route Channel**	● **Disable:** Disable routing for the channel. ● **Enable:** Enable routing for the channel.
	Route Point	Point number to route. (This point number appears in the server side but cannot be modified on the server side.)
	Event Class Mask	Defines the event class of points. `Unsolicited` is not allowed with class 0 only. In client, `Channel` is 0.
	Default Event Variation	Indicates the default event variation for data point.
	Routing Offline	Specify the flag when the routing channel is offline: ● **Valid Quality:** Use any available routing channel connection. ● **Invalid Quality:** Set the flag to offline when the routing channel is offline.

This table describes the DNP3 net server parameters that appear on the **DATA MAPPINGS** tab when you select a **Binary Input** in the **DATA MAPPINGS** tab:

Server Parameter	Description
Point Number	Indicates the start number of the point. **NOTE:** The DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not the case, the nonconsecutive points do not work normally.
Point Count	indicates the number of points.
CPU Reg Mapping	Choose a source for the event time stamp and flag: ● **Value only:** module time ● **Value with time:** CPU register time ● **Value with flag:** point flag information from the CPU registers ● **Value with flag and time:** flag and time from the CPU registers **NOTE:** Select one of these values to implement SOE for time stamping *(see page 87)*.
Point Name	Name of the unlocated register
Default Static Variation	Select the default static variation for the data point.
Default Event Variation	Select the default event variation for the data point.

Server Parameter	Description
Event Class Mask	Defines the event class of points. `Unsolicited` is not allowed with class 0 only. In client, `Channel` is 0.
PLC State	Specify the flag when the routing channel is offline: ● **No Impact Quality:** The quality is **valid** when the PLC runs. ● **Impact Quality:** If the PLC is stopped or removed from the rack, the quality is **invalid**.

Analog Input

This table describes the client data mapping parameters for analog input types:

Client Parameter		Description
Point Number		Indicates the start number of the point. **NOTE:** Confirm that the DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count		Indicates the number of points.
Store to CPU		Choose a source for the event time stamp and flag: ● **Value only:** module time ● **Value with time:** CPU register time ● **Value with flag:** point flag information from the CPU registers ● **Value with flag and time:** flag and time from the CPU registers
Static Variation		Select the static variation for the data point.,
Point Name		Name of the unlocated register
Display Deadband In Variable		Specify a deadband variable name.
Point Name		Name of the unlocated register when **Display Deadband In Variable** is selected (checked)
Event Routing	**Channel**	Enable or disable the routing of the channel number.
	Route Point	Define the point number to route.
	Event Class Mask	Defines the event class of points. `Unsolicited` is not allowed with class 0 only. In client, confirm that `Channel` is at 0.
	Default Event Variation	Indicates the default event variation for data point.
	Routing Offline	Specify the flag when the routing channel is offline: ● **Valid Quality:** Use any available routing channel connection. ● **Invalid Quality:** Set the flag to offline when the routing channel is offline.

This table describes the server data mapping parameters for analog input types:

Server Parameter	Description
Point Number	Indicates the start number of the point. **NOTE:** Confirm that the DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count	Indicates the number of points.
Event Class Mask	Defines the event class of points. `Unsolicited` is not allowed with class 0 only. In client, `Channel` is at 0 for normal operations.
Default Static Variation	Select the default static variation for the data point.
Default Event Variation	Select the default event variation for the data point.
CPU Reg Mapping	Choose a source for the event time stamp and flag: • **Value only:** module time • **Value with time:** CPU register time • **Value with flag:** point flag information from the CPU registers • **Value with flag and time:** flag and time from the CPU registers **NOTE:** Select one of these values to implement SOE for time stamping *(see page 87)*.
Deadband	Deadband value of the analog input
Use Percent Data	Use low and high range for the percentage of deadband calculation when the check box is selected.
Low Range	Lowest value in the range when the **Use Percent Data** check box is selected.
High Range	Highest value in the range when the **Use Percent Data** check box is selected.
Point Name	Name of the unlocated register
PLC State	Specify the flag when the routing channel is offline: • **No Impact Quality:** The quality is **valid** when the PLC runs. • **Impact Quality:** If the PLC is stopped or removed from the rack, the quality is **invalid**.
Display Deadband In Variable	Specify a deadband variable name.
Point Name	Name of the unlocated register when the **Display Deadband In Variable** check box is selected.

Binary Output

This table describes the client data mapping parameters for binary output types:

Client Parameter	Description
Point Number	Indicates the start number of the point. **NOTE:** Confirm that the DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count	Indicates the number of points.
Operation Mode	The selected operation mode
Control Code Type	Specify the control code used by the CROB: • **Latch_On_Off:** Trigger the CROB. • **Pulse_Trip_Close:** Trigger the CROB. • **Pulse_On:** Change the value. **NOTE:** Refer to the description of binary output behavior *(see page 126)*.
Default Static Variation	Select the default static variation for the data point.
Pulse Duration	Specify the width of the pulse (ms).
Point Name	Name of the unlocated register
Add CMD_STATUS	Specify the CMD_STATUS variable name.

Server data mapping parameters for binary output types:

Server Parameter	Description
Point Number	Indicates the start number of the point. **NOTE:** Confirm that the DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count	Indicates the number of points.
TCC	When **Trip_Close** is enabled, the odd point in this configuration is a closed output, and the following point is a trip out when an outstation receives a close or trip command. Use an even number for the point count value when enabled.
Default Static Variation	Select the default static variation for the data point.
Default Event Variation	Select the default event variation for the data point.
Add Flag Variable	Specify the flag variable name.
Point Name	Name of the unlocated register when the **Add Flag Variable** check box is selected.

Server Parameter	Description
PLC State	Specify the flag when the routing channel is offline: ● **No Impact Quality:** The quality is **valid** when the PLC runs. ● **Impact Quality:** If the PLC is stopped or removed from the rack, the quality is **invalid**.
Prefix	This prefix for the variable name is followed with an underscore (_). Configure the prefix in the server advanced parameters. Example: `RTU001_Point1`.
CPU Register Type	The only available option for the binary output is %MW.
CPU Register Address	This is the start %MW address in the CPU. This field applies only to located variables. To create a variable without a %MW address, use the value -1. Considerations: ● The binary output value (0 or 1) is bit 0 the %MW (INT) in the global variable list. The binary output flag data remains in the Device DDT. ● The %MW range depends on the CPU %MW register range (default 2048).

NOTE:
- The **Binary_Output_Status** is applied in the master, which saves the latest value, state (flag), and time stamp.
- Floating point values (scientific notation) can be entered for the **deadband**.

Analog Output

This table describes the client data mapping parameters for analog output types:

Client Parameter	Description
Point Number	Indicates the start number of the point. **NOTE:** Confirm that the DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count	Indicates the number of points.
Operation Mode	Selected operation mode
Default Static Variation	Select the default static variation for the data point.
Point Name	Name of the unlocated register
Add CMD_STATUS	Specify the CMD_STATUS variable name.

This table describes the server data mapping parameters for analog output types:

Server Parameter	Description
Point Number	Indicates the start number of the point. **NOTE:** Confirm that the DNP3 point number starts at 0 and is contiguous in slave/server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count	Indicates the number of points.
Event Class Mask	Defines the event class of points. `Unsolicited` is not allowed with class 0 only. In client, confirm that `Channel` is at 0.
Default Static Variation	Select the default static variation for the data point.
Default Event Variation	Select the default event variation for the data point.
Deadband	Deadband value of the analog point
Point Name	Name of the unlocated register
Add Flag Variable	Specify the flag variable name.
Point Name	Name of the unlocated register when the **Add Flag Variable** check box is selected.
PLC State	Specify the flag when the routing channel is offline: ● **No Impact Quality:** The quality is **valid** when the PLC runs. ● **Impact Quality:** If the PLC is stopped or removed from the rack, the quality is **invalid**.
Prefix	This prefix for the variable name is followed with an underscore (_). Configure the prefix in the server advanced parameters. The final variable name follows this format: `Prefix_VariableName.Pointx.value` Example: `RTU001_AO01.Point[10].value`
CPU Register Type	The only available option for the analog output is %MW.
CPU Register Address	This is the start %MW address in the CPU. This field applies only to located variables. To create a variable without a %MW address, use a start address of the type float/32 bit. A valid analog output type value is an even number. Use address `-1`. Considerations: ● The analog output value is in the global variable list. The binary output flag data remains in the Device DDT. ● The %MW range depends on the CPU %MW register range (default 2048).

NOTE:

- The **Analog_Output_Status** is applied in the master, which saves the latest value, state (flag), and time stamp.
- Floating point values (scientific notation) can be entered for the **deadband**.

Behavior of a Binary Output

This configuration depends on the selection you made in the **Control Code Type** field in the binary output client parameters *(see page 123)*.

The configuration applies **latch on/off**, **pulse on**, and **close/trip pulse on**:

TCC (Trip-Close Code)	Operation type field	Control code	Point model in outstation
None	pulse on	01 hex	activation
	latch on	03 hex	latch complement
	latch off	04 hex	
Close	pulse on	41 hex	two's complement
Trip		81 hex	

NOTE:

- The DNP3 master provides only on-time configuration data but does not provide configured off-time and count. The DNP3 outstation also only applies pulse on which the count is 1 and the off-time value is 0.
- Two's complement **trip** and **close** are provided for a single index in the DNP3 master, but two separately physical outputs in the DNP3 outstation. For example, a **close/pulse on** request for a specific DNP3 index is mapped to a specific relay output, whereas a **trip/pulse on** request for the same DNP3 index is mapped to another different relay output which follows the specific relay output (close) in the BMENOR2200H RTU module.

CROB sent in DNP3 master	Point number in DNP3 master	Point number in DNP3 outstation
Pulse on	0	0
Trip/Pulse on	0	1
Close/Pulse on	2	2
Trip/Pulse on	2	3
Close/Pulse on	n+2	n+2
Trip/Pulse on	n+2	n+2+1

In the DNP3 outstation, it is decided by configuration whether the point index applies **trip/close** request. As the **trip/close** need to bind a couple of points, the point count is even in the configuration.

This configuration depends on the selection you made in the **TCC** field in the binary output server parameters *(see page 123)*.

The selection of the `Trip_Close` mode depends on the **Trip-Close Mode** parameter setting (**Channel → Session → Advanced Parameter**).

When `Trip-Close Mode` is in Even Mode, the behavior is as follows: the close command controls the even point and the trip command controls the odd point.

When `Trip-Close Mode` is in Consecutive Mode, the behavior is as follows: the binary output occupies two registers in the CPU memory. The low register is for the close command and the high register is for the trip command.

- CROB usage in master

Op type field	Trigger mechanism	Description
Close/Pulse_on	any value change (0...65535)	pulse on if value change
Latch_on	0 to 1	latch on
Latch off	1 to 0	latch off
Close/Pulse_on	0 to 1	pulse on for close output
Trip/Pulse_on	1 to 0	pulse on for trip output

- The binary output in the DNP3 outstation is updated in the CPU register only after receiving a command from the DNP3 master, but not synchronized cyclically. Keep the corresponding CPU register not written any more.

Long and Short Pulses of Binary Outputs

This configuration depends on the selection you made for these parameters in the binary output client parameters *(see page 123)*:

- **Pulse Duration**
- **Short Pulse Duration**

NOTE: The outstation uses the entered **Pulse Duration**. The value 0 indicates that the device uses a pre-configured value.

DNP3 Net Server Parameters

The tables below describe the DNP3 net server parameters that appear on the **SERVER MAPPINGS** tab.

NOTE: When the Control Expert window is active, you can hover the cursor over any field to see a description of the functionality and the available range of values.

PARAMETERS:

Parameter	Description
Local Address	This field contains the source address for this session.
Master Address	This field contains the remote master (destination) address for this session.

ADVANCED PARAMETERS:

Parameter	Description
Link Status Periodic	Configure the frequency (ms) for the transmission of status requests when no DNP3 frames are received during this session.

Parameter	Description
Validate Source Address	Check this box to validate the source address in received frames.
Enable Self Address	Check this box to have the slave respond to address 0xfffc as if it received a request at its configured address. The slave responds with its own address so that the master can automatically discover the slave address.
Multi Frag Resp Allowed	Check this box to allow the application to send multi-fragment responses.
Multi Frag Confirm	Check this box to request application layer confirmations for non-final fragments of a multi-fragment response. (Application layer confirmations are always requested for responses that contain events.)
Respond Need Time	Check this box to tell the device to set the Need Time IIN bit in response to this session at start-up after the clock valid period elapses.
Clock Valid Period	Configure the length of time (ms) that the local clock remains valid after it receives a time synchronization.
Application Confirm Timeout	Configure the length of time (ms) that the slave DNP3 device waits for an application layer confirmation from the master for a solicited response.
Select Before Operation (SBO) Timeout	Configure the maximum amount of time (ms) that a selection remains valid before the corresponding operate is received.
Warm Restart Delay	Configure the length of time that the master waits after it receives a response to a warm restart request. This value is encoded in a time delay fine object in the response of a warm restart request.
Cold Restart Delay	Configure the length of time (ms) that the master waits after it receives a response to a cold restart request. This value is encoded in a time delay fine object in the response of a cold restart request.
Allow Multi CROB Requests	Check this box to allow multiple control relay block objects (CROBs) in a single request.
Max Control Requests	Configure the maximum number of binary (CROB) or analog control outputs that are allowed in a single request.
Unsol Allowed	Check this box to allow unsolicited responses.
Send Unsol When Online	Check this box to send unsolicited null responses when the session comes online.
Unsol Class 1 Max Events	When unsolicited responses are enabled, configure this value to specify the maximum number of events in the corresponding class (1, 2, or 3) that are allowed before an unsolicited response is generated.
Unsol Class 2 Max Events	
Unsol Class 3 Max Events	
Unsol Class 1 Max Delay	Configure the maximum amount of time (ms) after an event in the corresponding class (1, 2, or 3) is received before an unsolicited response is generated.
Unsol Class 2 Max Delay	
Unsol Class 3 Max Delay	
Unsol Max Retries	Configure the maximum number of unsolicited retries before changing to the offline retries value.
Unsol Retry Delay	Configure the length of the delay (ms) after an unsolicited response.

Parameter	Description
Unsol Offline Retry Delay	Configure the length of the delay (ms) after an unsolicited timeout before retrying the unsolicited response after the configured number of **Unsol Max Retries**.
Delete Oldest Event	Configure the behavior for an event queue that is full: ● *checked:* Delete the oldest event. ● *unchecked:* Delete the newest event.
Counts to Class0 Poll	Configure the type of value that is returned in a poll of class 0 data: ● **Count Value:** Return a static binary counter value. ● **Frozen Value:** Return a static frozen counter value.
SBO Mode	Select a mode for a before-and-after operation: ● **Interference Mode:** The outstation cancels the selection if the next received request is not an operate request. (Only read requests are processed.) ● **Noninterference Mode:** The outstation does not cancel the selection even if the next received request is not an operate request by following the selection. The DNP3 group recommends this selection.
Unsol Confirm Timeout	Configure the value for an unsolicited confirm timeout.
Data Synch Mode	Select a data synchronization mode: ● **Cyclic Synch:** Use the default (cyclic) synchronization. ● **Synch On Demand:** Allow the PLC application to implement local changes on the binary or analog output. **NOTE:** Enabling a **Synch On Demand** point changes the variable structure (out of the Device DDT).
Prefix	This string is part of the variable name for analog or binary output points when you select **Synch On Demand** as the **Data Synch Mode** (range: 1 ... 6). Considerations: ● Use **Prefix** names that are unique for each BMENOR2200H module. Duplicate names cause the overwriting of variables. ● In the **Synch On Demand** mode, client-side routing points for the analog or binary output status do not support server-side mapping. ● Do not use an underscore (_) as the last character in the **Prefix**. ● In the **Synch On Demand** mode, the **Prefix** consumes 7 characters. The remaining available length of the variable name is therefore reduced to 23 characters.

Set Measured Value

Apply analog input deadband (**obj34**) to set deadband of measured value. The parameters of the measured points are activated immediately after the DNP3 outstation receives the request from the DNP3 master.

For DNP3 **obj34**, there is no qualifier to set as it only applies the parameter **deadband**. Set the static variation and point number at the same setting of the analog input. Analog input **deadband** is applied both on the DNP3 master and the DNP3 outstation. The DNP3 server uses it to store the current value which is reported in the response of read requests, the DNP3 client uses it to display the current **deadband** value which can be controlled by the server through the analog input **deadband** control block.

This configuration depends on the deadband settings you made in these fields:

- **Point Number** (analog input client parameters)
- **Point Number** (analog input server parameters)
- **Default Static Variation** (analog input server parameters)

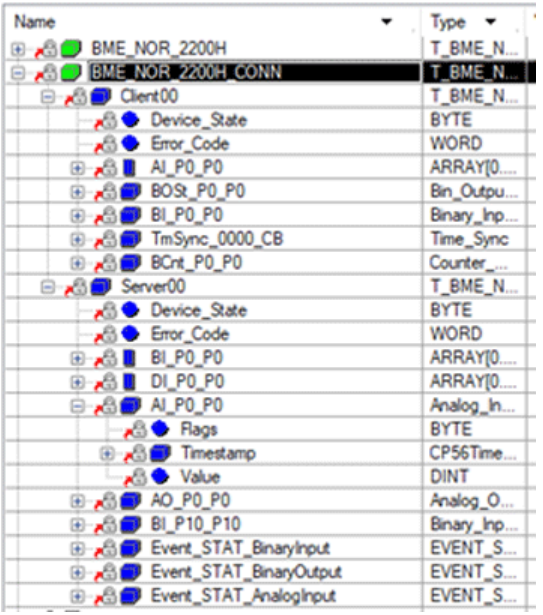
NOTE: Refer to the description of the analog input client and server parameters *(see page 121)*.

Generating Events in Outstation

A DNP3 outstation can determine if the user it is communicating with is authorized to access the services of outstation. This standard addresses the following security threats as defined in IEC/TC 62351-2:

- spoofing
- modification
- replay
- eavesdropping (on exchange of cryptographic keys only, not on other data)

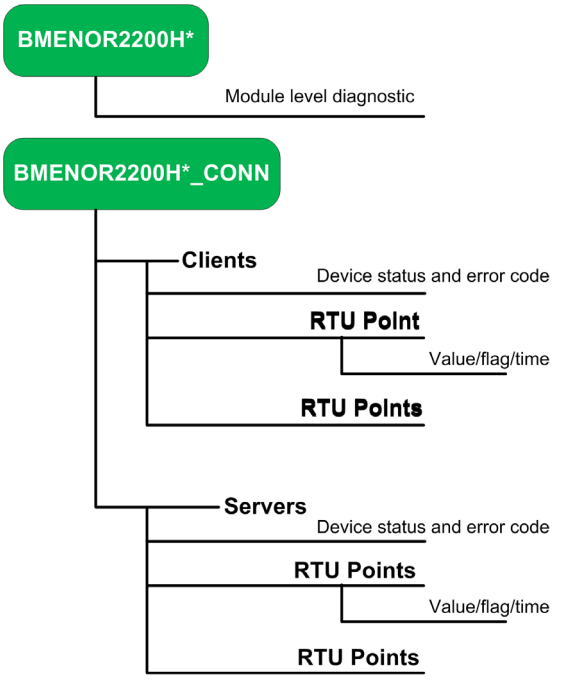
In the Outstation DTM configuration tab, the device DDT structure (unlocated variable) looks like this:



where (as shown in the following illustration:

- The customer-defined variable name corresponds to the T_BME_NOR type.
- The client corresponds to these RTU points:
  - Device_State: BYTE type
  - Error_Code: WORD type
  - AI_Px: Analog_input_xxx Type
    NOTE: When the point count is less than 1, the point type uses the `ARRAY` format.
  - BOSt_P0_P0: Bin_Output_xxx type
  - BI_P0_P0: Binary_Input_xxx type
  - TmSync_0000_CB: Time_Sync type
  - BCnt_P0_P0: Counter_... type
- The server corresponds to the following RTU points:
  - Device_State: BYTE type
  - Error_Code: WORD type
  - BI_P0_P0: Binary_Input_xxx type
  - DI_P0_P0: Double_Input_xxx type
  - AI_P0_P0: Analog_Input type (Flags, Timestamp, Value)
  - AO_P0_P0: Analog_Output type
  - BI_P10_P10: Binary_Input_xxx type

- Event_STAT_BinaryInput: WORD type (counter); BYTE type (overflow)
- Event_STAT_BinaryOutput: WORD type (counter); BYTE type (overflow)
- Event_STAT_AnalogInput: WORD type (counter); BYTE type (overflow)



** customer-defined name*

Clearing Events in Outstation

`Clear_Events` supports a new point type which clears the event buffer in the DNP3 Server/Slave. It enables the user to clear the events buffer in a local or remote SCADA through mapping memory.

`Clear_Events` can be created only for DNP3 Slave/Server; select Data Mapping.

When the value of the `Clear_Events` register changes, the BMENOR2200H module clears the events of the object group in the configuration.

Parameter	Value Scope	Definition
Object Group	All Objects Binary Input Double Input Binary Counter Analog Input Binary Output Analog Output	Specifies the object group whose event is cleared o. demand
Variable Name	—	Indicates the name of the located register.

Octet String Mapping for DNP3

In DNP3, Octet String applies to group 110. It supports read, write, and response function codes.

For the BMENOR2200H module, the octet string splits into two types of points, input points and output points.

The master uses a Read_Group command to read the Octet String.

This is the interpretation of the Octet String from the perspective of the master:

- **Octet String** points are input points.
- **Write Octet String** points are output points.

This is the interpretation of the Octet String from the perspective of the outstation:

- **Octet String** points with **protocol** variable access are input points for the DNP3 master.
- **Octet String** points with **CPU** variable access are output points from the controller.

Octet String lengths:

maximum	255 characters
default	16 characters

DNP3 Events Tab

Introduction

You can configure the **Events** tab for DNP3 NET server channels.

Access the Configuration Tab

Access the configuration parameters on the **EVENTS** tab in Control Expert:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	Confirm that you already created client or server channels.
3	In the **CONFIGURATION** menu, expand (**+**) the **Channels** sub-menu.
4	Select **DNP3 NET Server** from the **Channels** sub-menu. **NOTE:** The **EVENTS** tab is not available for **DNP3 NET Client** channels.
5	Select the tab **EVENTS** tab.
6	Configure the event parameters. **NOTE:** The parameters on the **Events** tab are similar to the DNP3 data mapping parameters *(see page 116)*.
7	Click the **OK** or **Apply** button to implement your configuration changes.

NOTE: Configure the DNP3 SAv5 security events (object 121/122) on the web pages *(see page 156)*

Export and Import .xml Files with the DTM

Introduction

A BMENOR2200H module stores its configuration in an .xml file. You can use the import and export functions in the Control Expert DTM to share that file among different modules to implement the same configuration.

Use the Control Expert **EXPORT/IMPORT** functionality:

- *export:* Save the module and protocol configurations to an .xml file.
- *import:* Import .xml files that include configuration parameters and data mapping to one or more modules.

Use Cases

These practical examples represent some common implementations of the import and export functions:

Use Case	Action	
Redundant Configuration	1	Export the .xml configuration file from a BMENOR2200H module.
	2	Import the .xml configuration file to one *or more* BMENOR2200H modules.
	3	Reuse the BMENOR2200H module's configuration file in other BMENOR2200H modules
Project Migration	Migrate the configuration file from a BMXNOR0200H module to a BMENOR2200H module. **NOTE:** All located addresses are lost after the import of .xml files from the BMXNOR0200H module. The type and length of the name are changed according to the new format. Account for the data type substitutions that are required when you migrate the XML file *(see page 204)*.	

Import

Import an .xml file to use its configuration settings:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	In the **CONFIGURATION** menu, expand (**+**) the **General** sub-menu.
3	Click the **Browse** button to find an .xml file to import.
4	Select a file.
5	Click the **Open** button to see the navigation path for the file in the **Import File Name** field.
6	Configure the **Use system defined data mapping point names** check box: - *selected:* Generate mapping point names that are based on the point type and point number. Otherwise variable names are imported from the .xml configuration file. - *deselected:* You can import user-defined mapping point names.

Step	Action
7	Click the **Import** button to import the file in the **Import File Name** field.

Export

Export an .xml configuration file:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	In the **CONFIGURATION** menu, expand (**+**) the **General** sub-menu.
3	Click the **Export** button.
4	Select a destination location for the exported .xml file.
5	Click the **Save** button to save the file with standard Windows commands.

Module Information in the DTM

Access the Information

View the **Module Information** function in the Control Expert DTM:

Step	Action
1	Access the DTM configuration for your module *(see page 106)*.
2	In the **CONFIGURATION** menu, expand (**+**) the **General** sub-menu.
3	Select **Module Information**.

Description

The **Module Information** page shows read-only information:

- **IP ADDRESS INFORMATION:** These fields contain the IP parameters for the module.
- **MEMORY STATUS:** These bar graphs indicate the space that is consumed and available for the exchange of implicit messages. The **Input** and **Output** graphs are presented from the perspective of the CPU:
  - **Input:** The green arrow indicates the number of bytes that are used for implicit messages from the module to the CPU.
  - **Output:** The green arrow indicates the number of bytes that are used for implicit messages from the CPU to the module.

  NOTE: Use the memory status information as a guide for future configuration changes. (The memory status is a byproduct of the point configuration.)

Limitations

Monitor the consumed implicit resources while respecting the total size of input and output types as follows:

Type	Consumption
Input	8 K bytes
Output	8 K bytes
total:	16 K bytes

NOTE: For details, refer to the description of the I/O data exchange with the CPU *(see page 25)*.

Section 7.6
Diagnostics

What Is in This Section?

This section contains the following topics:

Introduction to Module Diagnostics

Introduction

This section describes the methods and mechanisms you can use to diagnose the performance of your BMENOR2200H module.

Refer to the description of input DDT mapping and output DDT mapping.

Accessing Web Diagnostics from the DTM

Introduction

The Control Expert DTM provides a hyperlink to facilitate access to diagnostic web pages from the DTM.

Access the Diagnostics Information

Make the connection between the DTM and the target BMENOR2200H module to access the diagnostics information:

Step	Action
1	Open a Control Expert project that includes a BMENOR2200H module.
2	Open the Control Expert **DTM Browser** (**Tools → DTM Browser**).
3	In the **DTM Browser**, find the name that you assigned to the BMENOR2200H module *(see page 96)*.
4	Double-click the module.
5	Click the **Launch** button to link to the diagnostics web pages:
6	Scroll to **Device Menu → Diagnosis**.
7	Expand (**+**) the **Diagnosis** menu to view the available diagnostics pages.

Chapter 8
Cyber Security Configuration

What Is in This Chapter?

This chapter contains the following sections:

Section 8.1
About Cyber Security Web Pages

What Is in This Section?

This section contains the following topics:

Introduction to Cyber Security Web Pages

Introduction

The BMENOR2200H module has a built-in Hyper Text Transfer Protocol Secure (HTTPS) web server that provides access to various secure web pages. Use these pages to monitor the status of the module without installing Control Expert or the module's corresponding DTM.

Use these web pages to import, export, or delete encrypted cyber security management files.

You can monitor the security of communications through the **SEC** LED *(see page 30)*.

NOTE: Web page access is available only when the module is in secure mode. Refer to the directions for configuring the appropriate level of cyber setting with the rotary switch *(see page 22)*.

Before You Begin

Use the web pages described in this chapter to apply cyber security features to configured channels on the BMENOR2200H module

You can apply cyber security to the module after you satisfy these requirements:

- You have configured at least one communications channel for the module in the Control Expert DTM.
- You have configured the appropriate setting (**Secured**) on the rotary switch *(see page 22)*.

The first time you log in to secure mode, the cyber security file is not valid. Therefore, follow these steps to configure the file:

Stage	Description
1	Log in to the web pages as an administrator. *(see page 154)*
2	Access the cyber security setting page. *(see page 145)*
3	Configure the event log with a valid IP address (or disable event log). *(see page 148)*
4	Apply the configuration to the module.

Main Features

This list represents the major cyber security features for the module in terms of communications management:

- individual security:
  - HTTPS *(see page 145)*
  - DNP3 *(see page 64)*
- confidential transmission:
  - HTTPS *(see page 145)*
  - DNP3 *(see page 64)*
- enabled/disabled unused services:

- SNMP v1 *(see page 51)*
- Modbus TCP server
- DNP3 server

Browser Requirements

The BMENOR2200H module's HTTPS web server facilitates secure remote and local access to the embedded web pages through these standard browsers:

- Google Chrome 50+ (recommended)
- Mozilla Firefox 40+
- Microsoft Edge 14+
- Internet Explorer 11

Web Page Access

Access the Web Pages

Step	Action
1	Enter the module's IP address or URL (`https://...`) in a web browser to open the module's **Home** page. **NOTE:** ● You may see an on-screen message that says the web pages are not secured. Ignore this message and open the web page. ● When the module processes a heavy communications load, the web page may not open immediately. In this case, execute your browser's refresh function.
2	In the pull-down menu, select the appropriate language.
3	Enter the default user name and password that conforms to the selected cyber security mode *(see page 21)* the first time you access the web: ● **Secured** cyber security mode: ❍ *user name:* **admin** ❍ *password:* **password** ● **Standard** cyber security mode: ❍ *user name:* **installer** ❍ *password:* **Inst@ller1**
4	Click the **Login** button.
5	Change your user name and password when prompted.

You can now access these tabs from the **Home** page:
- **Setup** *(see page 147)*
- **Diagnostics** *(see page 159)*

Section 8.2
Cyber Security Setup

What Is in This Section?

This section contains the following topics:

Setup Web Page

Access the Parameters

Access the setup parameters for the BMENOR2200H module:

Step	Action
1	Access the cyber security web pages for the module *(see page 145)*.
2	Select the **SETUP** tab in the page banner.

3	Expand one of these sub-menus:
	• **DEVICE SECURITY SETTINGS** *(see page 148)*:
	  ❍ **User Account Policy**
	  ❍ **Event Logs**
	  ❍ **Network Services**
	  ❍ **Security Banner**
	• **DNP3 SECURE AUTHENTICATION** *(see page 150)*:
	  ❍ **Master Configuration**
	  ❍ **Outstation Configuration**
	  ❍ **Key Management**
	• **MANAGEMENT** *(see page 154)*:
	  ❍ **Certificates Management**
	  ❍ **User Management**
	  ❍ **Configuration Management**

Firmware Modifications

Most web pages have **Apply** or **OK** buttons to allow you to apply or save your modifications.

The firmware, however, is updated (or not) with the buttons in the banner across the top of each web page:

- **Apply:** Click to apply modifications to the firmware.
- **Discard:** Click to discard modifications.

Device Security Settings

Access the Settings

Access the **DEVICE SECURITY SETTINGS** from the **SETUP** web page:

Step	Action
1	Access the cyber security web pages for the module *(see page 145)*.
2	Select the **SETUP** tab in the page banner.
3	Expand the **MENU** navigation tree.
4	Expand the **DEVICE SECURITY SETTINGS** in the navigation tree banner to see these settings: • **User Account Policy** • **Event Logs** • **Network Services** • **Security Banner**

NOTE: These security settings are described individually below. When the Control Expert window is active, you can hover the cursor over any field or click the information (*i*) icon to see a description of the functionality and the available range of values.

User Account Policy

Apply time and attempt limits to user interactions:

Parameter	Description
Session maximum inactivity (minutes)	The idle session timeout period for HTTPS connections.
Maximum login attempts	The number of times a user may attempt, and fail, to login. **NOTE:** When this maximum is reached, no additional logins may be attempted for the configured period.
Login attempt timer (minutes)	The maximum time to enter a user password.
Account locking duration (minutes)	Time period during which no additional logins may be attempted after the maximum login attempts is reached.
Apply	Click this button to apply your changes.

Event Logs

Configure the syslog client in the module. The logs are stored locally in the module and exchanged with a remote syslog server:

Parameter	Description
Service activation	Turn the Syslog client service on or off.

Parameter	Description
Syslog server IP address	This is the IPv4 address of the syslog server. **NOTE:** If you configure the Syslog server, all events are forwarded to this IP address.
Syslog server port	The Syslog client service uses this port number.
Apply	Click this button to apply your changes.

Refer to the topic Event Log Descriptions *(see page 210)* for a description of event log entries.

Network Services

The SNMP, Syslog, and Modbus network services are not inherently secure protocols. They are rendered secure when they are installed in external VPN devices.

The synergy of these network services constitutes a firewall that permits or denies the passage of communications through the RTU module

Configuration:

Service	Enforce Security	Unlock Security
SNMP Agent	disabled	enabled
Modbus TCP Server	disabled	enabled
DNP3 Outstation	enabled	disabled

Security Banner

Parameter	Description
Banner text	View this editable text when you access the web pages.

DNP3 Secure Authentication

About DNP3 Secure Authentication

The implementation of DNP3 secure authentication (SA) facilitates mutual authentication for communications between a DNP3 master and a DNP3 outstation:

- A DNP3 outstation uses DNP3 SA to unambiguously determine that it is communicating with a user who is authorized to access the services of outstation.
  NOTE: Secure authentication option is enabled by default. The server works properly only when a valid server channel is configured in the cyber security settings. Disable this function when your application does not require secure authentication. This global setting applies to all server channels. You cannot enable or disable a single specific channel independently of other channels. If the DNP3 service is disabled, no channels work, regardless of the configured security level.
- A DNP3 master uses DNP3 SA to unambiguously determine that it is communicating with the appropriate outstation.
  NOTE: On the client side, you can configure individual client channels for secure authentication. For such cases, confirm that those channels are included in the table with an assigned security level (None, SAv2, SAv5).

Access the Settings

Access the **DNP3 SECURE AUTHENTICATION** page from the **SETUP** web page:

Step	Action
1	Access the cyber security web pages for the module *(see page 145)*.
2	Select the **SETUP** tab in the page banner.
3	Expand the **MENU** navigation tree.
4	Expand the **DNP3 SECURE AUTHENTICATION** in the navigation tree banner to see these settings: • **Master Configuration** • **Outstation Configuration** • **Key Management** **NOTE:** These security settings are described individually below.

Master Configuration

Define master (local PLC) access:

Step	Action
1	Select the **Secure Authentication Enabled** check box to enable the mechanism.
2	Select the **Add Channel** button.

Step	Action
3	Populate the fields in the **Add Channel** dialog box. • **Channel Name:** Use a name that matches the configured DNP3 channel name *(see page 108)*. • **Secure Authentication:** Select a DNP3 authentication version (**SAV5**, **SAV2**, **Disabled**). • **Enable Aggressive Mode:** ❍ *check box selected*: Enable aggressive mode. ❍ *check box deselected*: Disable aggressive mode. • **Key/Account Table:** • **Advanced Settings:** **NOTE:** When the Control Expert window is active you can hover over the blue circle (*i*) next to the feature to see an explanation for each field.
4	Select **Apply**.
5	Repeat these steps to add additional channels.

Outstation Configuration

Define outstation access:

Step	Action
1	Select the **Secure Authentication Enabled** check box to enable the mechanism.
2	Select the **Add Channel** button.
3	Populate the fields in the **Add Channel** dialog box. • **Channel Name:** Use a name that matches the configured DNP3 channel name *(see page 108)*. • **Secure Authentication:** Select a DNP3 authentication version (**SAV5**, **SAV2**, **Disabled**). • **MAC Algorithm (HMAC):** Select the appropriate algorithm. • **Enable Aggressive Mode:** ❍ *check box selected*: Enable aggressive mode. ❍ *check box deselected*: Disable aggressive mode. • **Key/Account Table:** • **Advanced Settings:** **NOTE:** When the Control Expert window is active you can hover over the blue circle (*i*) next to the feature to see an explanation for each field.
4	Select **Apply**.
5	Repeat these steps to add additional channels.

Key Management

Create a list of users that can access your module:

Step	Description
1	In the **Key Management** web page, press the **Create Table** button and follow the directions to assign a name to the table. **NOTE:** The tables you create appear in a pull-down menu next to the **Create Table** button.
2	Press the **Add User** button to add a list of authorized users at the supervision (SCADA) environment. **NOTE:** You can configure a maximum of 64 users for DNP3 Secure Authentication.
3	Populate the fields in the **Add User** dialog box. **NOTE:** When the Control Expert window is active you can hover over the blue circle (*i*) next to the feature to see an explanation for each field.
4	*optional step*: For the pre-shared key field (**Update Key**), you have the option to click the **Generate** button to use a randomly generated key.
5	*optional step*: You can copy the **Update Key** information by clicking the copy icon next to the **Generate** button. **NOTE:** You can copy the key to share the key more easily with the SCADA system.
6	Press the **Apply** button to add the user to the table of authorized users.
7	Repeat these steps to add additional users. **NOTE:** The DNP3 standard limits the number of users to 64.

The user(s) in your table will be able to access your module from the SCADA environment.

This table describes the **Key Management** parameters:

Parameter	Description
MASTER (tab)	**User Number:** This number corresponds to the current DNP3 user. **NOTE:** Use the value *1* when this user is assigned SAv5.
	User Name: This field shows the current user. **NOTE:** Because the BMENOR2200H RTU module acts as a data concentrator, the current user role on the **MASTER** side is SINGLE USER.
	Key Wrap: Select the appropriate wrap algorithm (**AES-128**, **AES-256**). Encryption Standard. **NOTE:** AES-256 does not work with SAv2. In this case, the **Update Key** value is 32 Hex.
	Key: This column shows the content of the **Update Key** value.

Parameter	Description
OUTSTATION (tab)	**User Number:** This number corresponds to the current DNP3 user.
	User Name: This field shows the current user.
	User Role: This field shows the role performed by the user (**OPERATOR**, **ENGINEER**, **INSTALLER**, **SECURITY ADMINISTRATOR**, **VIEWER**, **SINGLE USER**).
	Key Wrap: Select the appropriate wrap algorithm (**AES-128**, **AES-256**). Encryption Standard. **NOTE:** AES-256 does not work with SAv2. In this case, the **Update Key** value is 32 Hex.
	Key: This column shows the content of the **Update Key** value.

Cyber Security Management

Access the Settings

Access the **MANAGEMENT** page from the **SETUP** web page:

Step	Action
1	Access the cyber security web pages for the module *(see page 145)*.
2	Select the **SETUP** tab in the page banner.
3	Expand the **MENU** navigation tree.
4	Expand **MANAGEMENT** in the navigation tree banner to see these settings: • **Certificates Management** • **User Management** • **Configuration Management** **NOTE:** These security settings are described individually below.

Certificates Management

These **Certificates Management** parameters assist in the import and export functions relative to a secure (HTTPS) browser:

Parameter	Description
Name (CN)	This field shows the name of the certificate.
Distinguished Name (DN)	This field corresponds to the name of the certificate.
Expiration Date	This field shows the expiration date of the certificate.
Trusted Certificate	This field shows the name of a trusted certificate that is purchased from a Certification Authority.
Browse	Click this button to locate a different certificate.
Submit	Click this button to implement the selected **Trusted Certificate** file.

User Management

This table describes the **User Management** parameters:

Parameter	Description
User Name	This field shows the current user.
Roles	This field shows the role performed by the user (**OPERATOR**, **ENGINEER**, **INSTALLER**, **SECURITY ADMINISTRATOR**). **NOTE:** A single user can perform multiple roles.
Add User	Click this button to add a maximum of 15 new users with defined roles in the process. **NOTE:** To add a user, use your web page login credentials *(see page 145)*.

Click the pencil icon to edit these parameters, and click the **Apply** button.

NOTE: Hover over the blue circle next to the feature (*i* icon) to see an explanation for each field.

Configuration Management

Import, export, or reset the cyber security management:

Parameter	Description
IMPORT CONFIGURATION	Use the **IMPORT CONFIGURATION** fields to import a cyber security configuration file and apply it to the module. The cyber security settings that are applied with this command overwrite the existing settings and are immediately applied to the module. To import a cyber security configuration file and apply it to the module: **1** In the **IMPORT** page, click the file icon to open a window where you can select a **Configuration** archive. **2** Navigate to and select the configuration file you want to import, and click **OK**. **NOTE:** This is not the web login password. It is a password for exporting the cyber security settings. **3** In the **IMPORT** page, enter your security administrator **Password**. **4** Click **Upload** to apply the selected configuration file to the local module. (See the note below.)
	Configuration Archive: Make a selection.
	Import: Click this button to import the configuration.
EXPORT CONFIGURATION	Export the cyber security configuration file for the module: **1** In the **EXPORT** page, enter your **Password**, which is an **encryption key** to archive the exported configuration file. This password is also used to archive an imported configuration file. **2** Re-enter your password in the **Confirm password** field. **3** Click **Export** to export the configuration. (See the note below.)
RESET CONFIGURATION	Click the **Reset** button to restore the factory default cyber security settings for the module. Restart the module to implement the reset.
NOTE: Use the same password to encrypt the **EXPORT CONFIGURATION** value and decrypt the **IMPORT CONFIGURATION** value. Only a user with permission to update the configuration file can execute these commands.	

RBAC

Introduction

Role-based access control (RBAC) is a method for reducing the risk of cyber security attacks by assigning different levels of access that are based on the access privileges associated with a user's defined role.

The BMENOR2200H module uses RBAC to provide defined levels of access for users. RBAC is predefined according to IEC 62351-2, but it is also configurable according to user requirements.

These threats are defined by IEC 62351-2:

- spoofing
- modification
- replay
- eavesdropping (on the exchange of cryptographic keys)

Limitations

- The maximum number of active web server user connections is 5.
- Observe theses maximums for the number of DNP3 users that can participate in key management configuration:
  - DNP3 SAv2: 10
  - DNP3 SAv5: 64

RBAC Workflow

This is the global RBAC workflow:

Stage	Description
1	Access the RBAC management page.
2	Create a new **USER** and assign a role from list.
3	Enter and confirm a password.
4	Submit the RBAC configuration.
5	Access the slave key management page for DNP3 secure authentication.
6	Pick a **USER** from the slave user table for RBAC management.
7	Enter the other security settings for the DNP3 secure authentication version.

NOTE: A single user is now active (master only).

Available Functionality

This table shows the available functionalities for each value and its corresponding name:

Value	Name	DNP3 Protocol		Firmware	Web Page Settings		FTP	HTTPS
		Monitor Data	Operator Control	Upgrade	Security	Diagnostic	Data Logging Server	Web Login Server
1	OPERATOR	✓	✓			✓	✓	✓
2	ENGINEER	✓				✓	✓	✓
3	INSTALLER	✓		✓		✓		✓
4	SECADM				✓	✓		✓
32768	SINGLEUSER (COMMON)	✓	✓					X

Section 8.3
Cyber Security Diagnostics

What Is in This Section?

This section contains the following topics:

Diagnostics Web Page

Access the Parameters

Monitor diagnostics information for the module:

Step	Action
1	Access the web pages *(see page 145)*.
2	Select the **DIAGNOSTICS** tab.
3	Expand the **MENU**.
4	Expand the appropriate sub-menu: • **MODULE** *(see page 160)*: ❍ **Status Summary** ❍ **Event Buffer Status** ❍ **Port Statistics** • **CONNECTED DEVICES** *(see page 164)*: ❍ **DNP3** ❍ **Messaging** • **SERVICES** *(see page 166)*: ❍ **STNP** ❍ **Clock**

Module Diagnostics

Introduction

View this information when you access the **DIAGNOSTICS** web page *(see page 159)* for the BMENOR2200H module.

Status Summary

Monitor the status of the module:

Field	Description
RUN, **ERR**	• *green* • *red* **NOTE:** The diagnostics information is explained in the description of LED activity and indications *(see page 30)*.
SERVICE STATUS	Monitor the performance of each listed service on the communications link: • *green:* The service is operating normally. • *red:* An error is detected for a service. • *black:* The service is not present or not configured.
NETWORK INFORMATION	**Host Name:** This field shows provides the host name for the module (**BME NOR 2200H**).
	IP Address: This field shows the IP address of the module.
	Subnet Address: This field shows the subnet address of the module.
	Gateway Address: This field shows the gateway address of the module.
	MAC Address: This field shows the MAC address of the module.
VERSION INFORMATION	View the software versions that currently run on the module: • **SV** • **Web Server Version** • **Web Page Version**
MISCELLANEOUS	**Communication Security:** The status of the security service (enabled or disables) is reported.
	Rack ID: This field identifies the local rack (1).
	Slot ID: This field shows the slot number in which the BMENOR2200H module is installed.
MANUFACTURING INFORMATION	View the serial number for the device.

Event Buffer Status

View the module's event buffer status for the commissioning of communications:

Parameter	Description
EVENT BUFFER USAGE	This indicates the percentage of the event buffer that is consumed.
EVENT OVERFLOW	This field indicates that the capacity of the event buffer is exceeded or not.
EVENT RESOURCE USAGE	This indicates the percentage of event resources that are consumed.
EVENT BACKUP	**Enabled:** Events are backed up.
	Disabled: Events are **not** backed up.
CHANNEL/POINT EVENT STATUS	**No.:** This number is represents the sequence of device connections.
	Channel Name: This is the configured DNP3 channel name *(see page 108)*.
	Current Event Buffer Usage%: This indicates the percentage of the event buffer that is consumed.
	Current Event Quantity: This is the number of events in the buffer.
	Configured Event Quantity: This is the configured size of the event buffer.
	Current Overflow Event Quantity: This is the number of events that are not in the buffer owing to an overflow.
	Total Current Overflow: This is the total number of current overflow events for the module.
	NOTE: Click the plus (+) or minus (-) sign to expand or collapse any channel in the **Event Buffer Status** page to view status details from the perspective of the module.

Port Statistics

The **Port Statistics** page reports the statistics for the module's Ethernet backplane connection:

Parameter	Description
backplane port	• *green:* The port is active. • *gray:* The port is not active. • *yellow:* An error is detected on the port. • *red:* An error is detected on the port.
Speed	This field shows the configured port speed (0, 100, 1000 Mbps).
Duplex, **Half**	The current duplex mode is composed of some combination of these elements: • **TP**/**Fiber** • **-Full**/**-Half**/**-None** • **Link**/(no word) • **None** **NOTE:** When the thirteenth bit of the word in the Modbus response is 1, "**Link**" is added to the duplex mode string (**TP-Full Link**, **TP-Half Link**, etc.).

Parameter	Description
Success Rate	This field shows the percentage of successful requests out of the total number of requests.
Total Errors	This field shows the number of detected errors.
Toggle Detail View	Click this button to expand or compress the list of port statistics.

This table describes the port statistic parameters:

Parameter	Description
Frames Transmitted	This field shows the number of frames that are successfully transmitted from the port.
Frames Received	This field shows the number of frames that are successfully received from the port.
Excessive Collisions	This field shows the number of times that the transmission of an Ethernet frame on this port was not successful owing to excessive collisions (more than 16 attempts per packet).
Late Collisions	This field shows the number of times a collision is detected after the slot time of the channel elapses. **NOTE:** A value appears in this field only wen the hardware provides the information.
CRC Errors	This field shows the number of received frames for which the Cyclic Redundancy Check (CRC) is not valid. A detected CRC error is an RMON statistic that combines the values for **FCS Errors** and **Alignment Errors**.
Bytes Received	This field shows the number of octets that are received on the port.
Inbound Packet Errors	This field shows the number of packets that are received on the port for which errors are detected. **NOTE:** Does not include Out Discards.
Inbound Packets Discarded	The field shows the number of inbound packets that are received on the port but discarded.
Bytes Transmitted	This field shows the number of octets that are sent on the port.
Outbound Packet Errors	This field shows the number of packets that are sent on the port for which errors are detected. **NOTE:** Does not include Out Discards.
Outbound Packets Discarded	The field shows the number of outbound packets that are sent on the port but discarded.
Carrier Sense Errors	This field shows the number of times that the carrier sense condition was lost or was never asserted in an attempt to transmit a frame on this port.
FCS Errors	This field shows the number of frames that are received on this port that are an integral number of octets but do not pass the FCS check.
Alignment Errors	This field shows the number of frames that are received on this port that are not an integral number of octets long and do not pass the FCS check.

Parameter	Description
Internal MAC Trans. Errors	This field reports the number of frames that the port does not successfully transmit owing to a detected internal MAC sub-layer receive error.
Internal MAC Rec. Errors	This field reports the number of frames that the port does not successfully receive owing to a detected internal MAC sub-layer receive error.
SQE Test Errors	This field shows the number of times a SQE TEST ERROR is received on the port. **NOTE:** This counter does not increment on ports that operate at speeds greater than 10 Mb/s or on ports that operate in full-duplex mode

Connected Device Diagnostics

Introduction

View this information when you access the **DIAGNOSTICS** web page *(see page 159)*.

DNP3

This table shows the DNP3 connection status for client devices and server RTUs:

Parameter	Description
Number of Connected / Connecting Devices	This value represents the number of connected devices.
Number of Disconnected Devices	This value represents the number of disconnected devices.
RTU CONNECTIONS - SERVERS / CLIENTS	**No.:** This number is represents the sequence of device connections.
	Channel Name: This is the configured DNP3 channel name *(see page 108)*.
	Protocol: This field shows the implemented connection protocol.
	State: This is the status of the connection (**Connected**, **Connecting**, **Disconnected**).
	Remote Address: This is the remote IP address.
	Remote Port: This is the remote TCP port.
	Local Port: This is the local TCP port.
	Secure Statistics: Click the link in this column to access detailed statistics *(see page 213)* for the specific secure authentication version *(see page 66)*.
	Error Code: Click the error code *(see page 243)* in this column to get information about a detected error.

Messaging

This table contains information about the exchange of data in terms of Modbus statistics:

Parameter	Description
MESSAGING STATISTICS	View the total number of sent and received messages on port 502: • **Msgs. Sent:** This field shows the number of messages sent from port 502. • **Msgs. Received:** This field shows the number of messages received by port 502. • **Success Rate:** This field shows the percentage of successful requests out of the total number of requests. **NOTE:** These values are not reset when the port 502 connection closes. The values, therefore, account for the number of messages since the last module restart.

Parameter	Description
ACTIVE CONNECTIONS	View the connections that are active when the **Messaging** page is refreshed: • **Remote Address:** This column shows the remote IP address. • **Local Port:** This column shows the local TCP port. • **Type:** This column shows the connection type. • **Sent:** This column shows the number of messages sent from this connection. • **Received:** This column shows the number of messages received by this connection. • **Errors:** This column shows the number of errors that are detected in association with this connection.

Service Diagnostics

Introduction

View this information when you access the **DIAGNOSTICS** web page *(see page 159)*.

SNTP

This table describes the SNTP parameters:

Parameter	Description
SERVICE STATUS	**Running:** The correctly configured service is running.
	Disabled: The service is disabled.
	Unknown: The status of the service is not known.
SERVER TYPE	**Primary:** A primary server polls a master time server for the current time.
	Secondary: A secondary server polls a master time server for the current time.
CURRENT DATE	**This field shows the current date in the selected time zone.**
SERVER STATUS	• *green:* The server is connected and running. • *red:* An error is detected. • *gray:* The server status is not known.
DST STATUS	**On:** DST (daylight saving time) is configured and running.
	Off: DST is disabled.
	Unknown: The DST status is not known.
CURRENT TIME	This field shows the time of day.
TIME ZONE	This field shows the time zone.

Clock

This table describes the clock parameters:

Parameter	Description
CURRENT DATE AND TIME	**Date** (module date)
	Time (module time)
TIME ZONE	(module time zone)

Parameter	Description
LATEST TIME SYNCHRONIZATION	**Date** (synchronization timestamp)
	Time (synchronization timestamp)
	Time Source (synchronization timestamp): • — (none): If the RTU protocol is not configured, the RTU clock runs free and gets its time from 1970/1/1. • **CPU Module:** If the RTU protocol is configured, the RTU can get its initial time from the CPU when the RTU protocol starts or restarts. • **Controlling Station:** field shows the time source when a SCADA system or a master synchronizes its time with the RTU. • **NTP Server:** If the SNTP client is enabled and connected to the SNTP server, its time source is from an SNTP server that synchronizes to the BMENOR2200H module's internal clock.

Appendices

What Is in This Appendix?

The appendix contains the following chapters:

Appendix A
Interoperability

DNP3 Interoperability for the BMENOR2200H Module

Introduction

The purpose of this information is to describe the specific implementation of the Distributed Network Protocol (DNP3) within the BMENOR2200H module as master and slave.

This information, in conjunction with the DNP3 Basic 4 Document Set and the DNP3 Subset Definitions Document, provides detailed information on how to communicate with the BMENOR2200H module as master via the DNP3 protocol.

This implementation of DNP3 is fully compliant with DNP3 Subset Definition Level 3.

DNP3 Device Profile - Master

This table provides a *Device Profile Document* in the standard format defined in the DNP3 Subset Definitions Document. While it is referred to in the DNP3 Subset Definitions as a *Document*, it is only a component of a total interoperability guide. This table uses a BMENOR2200H module as a master as an example. (Your module may be different.)

Parameter	Capabilities	Value
Device Identification		
Device Function	Master	Master
Vendor Name	–	Schneider Electric Industries SAS
Device Name	Device Name	BMENOR2200H
Device Manufacturer hardware version	Device Manufacturer hardware version	N/A
Device Manufacturer software version	Device Manufacturer software version	1,0 IR14
Device Profile Document Version Number	Device Profile Document Version Number	1
DNP3 Levels Supported	For both requests and responses: None, Levels 1...5	For requests: Level 3
		For responses: Level 3
Supported Function Blocks	Self Address Support	Secure Authentication
	Secure Authentication	
Notable Additions	Refer to Implementation Table	

Parameter	Capabilities	Value
Methods to set Configurable Parameters	Software	Software (EcoStruxure Control Expert)
	Proprietary file loaded via other transport mechanism	
DNP3 XML files available On-line	dnpDP.xml	–
	dnpDPC.xml	
	dnpDPCfg.xml	
External DNP3 XML files available Off-line	dnpDP.xml (read)	dnpDP.xml (read)
Connections Supported	IP Networking	IP Networking
Conformance Testing	N/A	–
Serial Connections		
Not Supported	–	–
IP Networking		
Port Name	–	Ethernet
Type of End Point	TCP Initiating	TCP Initiating
	TCP Datagram	
IP Address of this device	–	0.0.0.0
Subnet Mask	–	255.255.255.255
Gateway IP Address	–	0.0.0.0
Accepts TCP Connections or UDP Datagrams from	Limits based on IP address	IP address
IP Addresses from which TCP Connections or UDP Datagrams are accepted	–	192.168.0.1
TCP Listen Port Number	N/A	N/A
TCP Listen Port Number of remote device	Configurable range 1...65536	20000
TCP Keep-alive timer	Fixed at 75000 ms	75000 ms
Local UDP Port	Configurable range 1...65536	20000
Destination UDP Port for DNP3 Requests	Configurable range 1...65536	20000
Destination UDP Port for initial unsolicited null responses	None	None
Destination UDP Port for DNP3 Responses	Configurable range 1...65536	20000
Multiple outstation connections	Supports multiple outstations	TRUE
Multiple master connections	Not supported	Not supported

Parameter	Capabilities	Value
Time synchronization support	DNP3 LAN procedure (function code 24)	LAN procedure
	DNP3 Write Time	
	Other	
Link Layer		
Data Link Address	Configurable range 0...65519	4
DNP3 Source Address Validation	Always, single address	Always, single address
DNP3 Source Addresses expected when Validation is Enabled	Configurable range 0...65519	3
Self Address Support using address 0xFFFC	Yes	No
	No	
Sends Confirmed User Data Frames	Never	Never
	Always	
	Sometimes	
Data Link Layer Confirmation Timeout	Configurable range 0...2147483647 ms	2000 ms
Maximum Data Link Retries	Configurable range 0...255	3
Maximum number of octets Transmitted in a Data Link Frame	Configurable range 24...292	292
Maximum number of octets that can be Received in a Data Link Frame	Configurable range 24...292	292
Application Layer		
Maximum number of octets Transmitted in an Application Layer Fragment other than File Transfer	Configurable range 0...2048	2048
Maximum number of octets Transmitted in an Application Layer Fragment containing File Transfer	Fixed at 0	0
Maximum number of octets that can be received in an Application Layer Fragment	Configurable range 0...2048	2048
Timeout waiting for Complete Application Layer Fragment	None	None
Maximum number of objects allowed in a single control request for CROB (Group 12)	Fixed at 10	10
Maximum number of objects allowed in a single control request for Analog Outputs (Group 31)	Configurable range 1...512	10

Parameter	Capabilities	Value
Maximum number of objects allowed in a single control request for Data Sets (Groups 85, 86, 87)	Configurable range 1...128	8
Supports mixed object groups (AOBs, CROBs and Data Sets) in the same control request	Yes	Yes
	No	
Control Status Codes Supported	4 NOT_SUPPORTED	–
	8 TOO_MANY_OBJS	–
Master-Only Properties		
Timeout waiting for Complete Application Layer Responses (ms)	–	–
Maximum Application Layer Retries for Request Messages	–	–
Timeout waiting for First or Next Fragment of an Application Layer Response	–	–
Issuing controls to Off-line devices	–	–
Issuing controls to off-scan devices	–	–
Maximum Application Layer Retries for Control Select Messages (same sequence number)	–	–
Maximum Application Layer Retries for Control Select Messages (new sequence number)	–	–
Security Parameters		
DNP3 device support for secure authentication	Version 2 (IEEE 1815-2010)	–
	Version 5 (IEEE 1815-2012)	
Maximum number of users	Configurable range 1...300	Maximum number of user supported: 0
Security message response timeout	Configurable range 1...640 ms	2 ms
Aggressive mode of operation (receive)	Yes	Yes
	No	
Aggressive mode of operation (issuing)	Yes	No
	No	
Session key change interval	Configurable range 60...604800 seconds (when enabled	Enabled at 900 seconds
Session key change message count	Configurable range 0...65535	1000

Parameter	Capabilities	Value
Maximum error count (SAv2 only)	Configurable range 0...255	2
MAC algorithm requested in a challenge exchange	SHA-1 (truncated to the leftmost 4 octets)	SHA-256 (16)
	SHA-1 (truncated to the leftmost 8 octets)	
	SHA-1 (truncated to the leftmost 10 octets)	
	SHA-256 (truncated to the leftmost 8 octets)	
	SHA-256 (truncated to the leftmost 16 octets)	
Key-wrap algorithm to encrypt session keys	AES-128	AES-128
	AES-256	
Cipher Suites used with DNP implementations using TLS	Not relevant TLS is not used	Not relevant
Change cipher request timeout	Not relevant TLS is not used	Not relevant
Number of Certificate Authorities supported	–	–
Certificate Revocation check time	Not relevant TLS is not used	Not relevant
Additional critical function codes	None	None
Other critical fragments	None	None
Support for remote update key changes	None	None
Default user credentials are permitted to expire	Yes	No
	No	
Secure Authentication enabled	Configurable: On or Off	Off
Length of the challenge data	Configurable range 4...60 octets	4 octets
Maximum statistic counts (SAv5):		
Max Authentication Failures	Configurable range 4...60	4
Max Reply Timeouts	Configurable range 1...65535	3
Max Authentication Rekeys	Configurable range 1...65535	3
Max Error Messages Sent	Configurable range 1...65535	3
Broadcast Functionality		
Disabled Not configurable	–	–

DNP3 Device Profile - Outstation

This table provides a *Device Profile Document* in the standard format defined in the DNP3 Subset Definitions Document. While it is referred to in the DNP3 Subset Definitions as a *Document*, it is only a component of a total interoperability guide. This table uses a BMENOR2200H module as a master as an example. (Your module may be different.)

Parameter	Capabilities	Value
Device Identification		
Device Function	Outstation	Outstation
Vendor Name	–	Schneider Electric Industries SAS
Device Name	Device Name	BMENOR2200H
Device Manufacturer hardware version	Device Manufacturer hardware version	N/A
Device Manufacturer software version	Device Manufacturer software version	1,0 IR14
Device Profile Document Version Number	Device Profile Document Version Number	1
DNP3 Levels Supported	For both requests and responses: None, Levels 1...5	For requests: Level 3
		For responses: Level 3
Supported Function Blocks	Self Address Support	Secure Authentication
	Secure Authentication	
Notable Additions	Refer to Implementation Table	
Methods to set Configurable Parameters	Software	Software (EcoStruxure Control Expert)
	Proprietary file loaded via other transport mechanism	
DNP3 XML files available On-line	dnpDP.xml	–
	dnpDPC.xml	
	dnpDPCfg.xml	
External DNP3 XML files available Off-line	dnpDP.xml (read)	dnpDP.xml (read)
Connections Supported	IP Networking	IP Networking
Conformance Testing	Independently tested	Independently tested
Serial Connections		
Not Supported	–	–
IP Networking		
Port Name	–	Ethernet
Type of End Point	TCP Listening	TCP Listening
	TCP Datagram	

Parameter	Capabilities	Value
IP Address of this device	–	0.0.0.0
Subnet Mask	–	255.255.255.255
Gateway IP Address	–	0.0.0.0
Accepts TCP Connections or UDP Datagrams from	Allows All (*.*.*.*)	Allows All
	Limits based on IP address	
	Limits based on list of IP addresses	
IP Addresses from which TCP Connections or UDP Datagrams are accepted	–	*.*.*.*
TCP Listen Port Number	Configurable range 1...65536	20000
TCP Listen Port Number of remote device	N/A	N/A
TCP Keep-alive timer	Fixed at 75000 ms	75000 ms
Local UDP Port	Configurable range 1...65536	20000
Destination UDP Port for DNP3 Requests	Configurable range 1...65536	20000
Destination UDP Port for initial unsolicited null responses	None	None
Destination UDP Port for DNP3 Responses	Configurable range 1...65536	20000
Multiple outstation connections	N/A	N/A
Multiple master connections	Supports multiple masters	IP Address
	Method 1 (based on IP address)	
Time synchronization support	DNP3 LAN procedure (function code 24)	LAN procedure
	DNP3 Write Time	
	Other	
Link Layer		
Data Link Address	Configurable range 0...65519	4
DNP3 Source Address Validation	Never	Never
	Always, single address	
DNP3 Source Addresses expected when Validation is Enabled	Configurable range 0...65519	3
Self Address Support using address 0xFFFC	Yes	No
	No	

Parameter	Capabilities	Value
Sends Confirmed User Data Frames	Never	Never
	Always	
	Sometimes	
Data Link Layer Confirmation Timeout	Configurable range 0...4294977295 ms	2000 ms
Maximum Data Link Retries	Configurable range 0...255	3
Maximum number of octets Transmitted in a Data Link Frame	Configurable range 24...292	292
Maximum number of octets that can be Received in a Data Link Frame	Configurable range 24...292	292
Application Layer		
Maximum number of octets Transmitted in an Application Layer Fragment other than File Transfer	Configurable range 0...2048	2048
Maximum number of octets Transmitted in an Application Layer Fragment containing File Transfer	–	–
Maximum number of octets that can be received in an Application Layer Fragment	Configurable range 0...2048	2048
Timeout waiting for Complete Application Layer Fragment	Configurable range 0...2147483647	15000 ms
Maximum number of objects allowed in a single control request for CROB (Group 12)	Configurable range1...10	10
Maximum number of objects allowed in a single control request for Analog Outputs (Group 31)	Configurable range1...10	10
Maximum number of objects allowed in a single control request for Data Sets (Groups 85, 86, 87)	–	–
Supports mixed object groups (AOBs, CROBs and Data Sets) in the same control request	Yes	Yes
	No	

Parameter	Capabilities	Value
Control Status Codes Supported	1 TIMEOUT	–
	2 NO_SELECT	
	3 FORMAT_ERROR	
	4 NOT_SUPPORTED	
	5 ALREADY_ACTIVE	
	6 HARDWARE_ERROR	
	7 LOCAL	
	8 TOO_MANY_OBJS	
	9 NOT_AUTHORIZED	
	10 AUTOMATION_INHIBIT	
	11 PROCESSING_LIMITED	
	12 OUT_OF_RANGE	
	13 DOWNSTREAM_LOCAL	
	14 ALREADY_COMPLETE	
	15 BLOCKED	
	16 CANCELLED	
	17 BLOCKED_OTHER_MASTER	
	18 DOWNSTREAM_FAIL	
	19 UNDEFINED	
Outstation Only Properties		
Timeout waiting for Application Confirm of solicited response message	Configurable, range 0...2147483647ms	10000 ms
How often is time synchronization required from the master	Never needs time	Periodically, fixed at 1800seconds
	Periodically, fixed at 1800seconds	
Device Trouble Bit IIN1.6	Never used	Never used
File Handle Timeout	Not applicable	Not applicable
Event Buffer Overflow Behavior	Discard the oldest event	Discard the newest event
	Discard the newest event	
Event Buffer Organization	Per object group	Per object group
Semds Multi-Fragment Responses	Yes	Yes
	No	
Last Fragment Confirmation	Sometimes	Sometimes
DNP Command Settings preserved through a device restart	–	–
Supports configuration signature	Not supported	Not supported

Parameter	Capabilities	Value
Requests application confirmation	For event responses: Yes	Yes
	For non-final fragments: Configurable (Yes/No)	Yes
Supports DNP3 Clock Management	–	–
Outstation Unsolicited Response Support Properties		
Supports unsolicited reporting	Comfigurable (On/Off)	On
Master Data Link Address	Comfigurable range 0...65519	3
Unsolicited Response Confirmation Timeout	Comfigurable range 0...2147483647	5000 ms
Number of Unsolicited Retries	Comfigurable range 0...65535	3
Outstation Unsolicited Response Trigger Conditions		
Number of class 1 events	Comfigurable range 1...512	5
Number of class 2 events	Comfigurable range 1...512	5
Number of class 3 events	Comfigurable range 1...512	5
Total nuber of events from any class	Total Number of Events not used to trigger Unsolicited Responses	–
Hold time after class 1 event	Configurable range 0...2147483647ms	5000 ms
Hold time after class 2 event	Configurable range 0...2147483647ms	5000 ms
Hold time after class 3 event	Configurable range 0...2147483647ms	5000 ms
Hold time after event assigned to any class	Fixed at 0 ms	0 ms
Retrigger Hold Time	Hold-time timer will not be retriggered for each new event detected (guaranteed update time)	Not retriggered
Other Unsolicited Response Trigger Conditions	–	–
Outstation Performance Properties		
Maximum Time Base Drift	–	–
When does outstation set IIN1.4	Never	Never
	Asserted at startup until first Time Synchronization request received	
	Range 1 to 2147483 seconds after last time sync	
Maximum Internal Time Reference Error when set via DNP	–	–

Parameter	Capabilities	Value
Maximum Delay Measurement Error	–	–
Maximum Response Time	–	–
Maximum time from start-up to IIN 1.4 assertion	–	–
Maximum Event Time-tag error for local Binary and Double Bit I/O	–	–
Maximum Event Time-tag error for local I/O other than Binary and Double Bit data types	–	–
Individual Field Outstation Parameters		
User-assigned location name or code string (same as g0v245)	–	–
User-assigned ID code/number string (same as g0v246)	–	–
User-assigned name string for the outstation (same as g0v247)	–	–
Device serial number string (same as g0v248)	–	–
Secondary operator name (same as g0v206)	–	–
Primary operator name (same as g0v207)	–	–
System name (same as g0v208)	–	–
Owner name (same as g0v244)	–	–
Security Parameters		
DNP3 device support for secure authentication	Version 2 (IEEE 1815-2010)	–
	Version 5 (IEEE 1815-2012)	
Maximum number of users	Configurable range 1...300	Maximum number of user supported: 0
Security message response timeout	Configurable range 1...640 ms	2 ms
Aggressive mode of operation (receive)	Yes	Yes
	No	
Aggressive mode of operation (issuing)	Yes	No
	No	
Session key change interval	Configurable range 60...604800 seconds (when enabled	Enabled at 900 seconds
Session key change message count	Configurable range 0...65535	1000
Maximum error count (SAv2 only)	Configurable range 0...255	2

Parameter	Capabilities	Value
MAC algorithm requested in a challenge exchange	SHA-1 (truncated to the leftmost 4 octets)	SHA-256 (16)
	SHA-1 (truncated to the leftmost 8 octets)	
	SHA-1 (truncated to the leftmost 10 octets)	
	SHA-256 (truncated to the leftmost 8 octets)	
	SHA-256 (truncated to the leftmost 16 octets)	
Key-wrap algorithm to encrypt session keys	AES-128	AES-128
	AES-256	
Cipher Suites used with DNP implementations using TLS	Not relevant TLS is not used	Not relevant
Change cipher request timeout	Not relevant TLS is not used	Not relevant
Number of Certificate Authorities supported	–	–
Certificate Revocation check time	Not relevant TLS is not used	Not relevant
Additional critical function codes	None	None
Other critical fragments	None	None
Support for remote update key changes	None	None
Default user credentials are permitted to expire	Yes	No
	No	
Secure Authentication enabled	Configurable: On or Off	Off
Length of the challenge data	Configurable range 4...60 octets	4 octets
Maximum statistic counts (SAv5):		
Max Authentication Failures	Configurable range 4...60	4
Max Reply Timeouts	Configurable range 1...65535	3
Max Authentication Rekeys	Configurable range 1...65535	3
Max Error Messages Sent	Configurable range 1...65535	3
Broadcast Functionality		
Disabled Not configurable	–	–

DNP3 Implementation Table

The following table identifies the object groups, variations, function codes, and qualifiers that the BMENOR2200H module supports in both requests and responses. The *Request* columns identify all requests that may be sent by a master or all requests that are parsed by an outstation. The *Response* columns identify all responses that are parsed by a master or all responses that may be sent by an outstation

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifier Codes (hex)**	**Function Codes (dec)**	**Qualifier Codes (hex)**
1	0	Binary Input - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
1	0	Binary Input - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
1	1	Binary Input - Single-bit packed	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
1	2	Binary Input - Single-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
2	0	Binary Input Change Event - any variation	1(read)	06 (no range, or all), 07, 08 (limited qty)		
2	1	Binary Input Change Event - without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
2	1	Binary Input Change Event - without time			(Unsol. Resp.)	17, 28 (index)
2	2	Binary Input Change Event - with absolute time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
2	2	Binary Input Change Event - with absolute time			(Unsol. Resp.)	17, 28 (index)
2	3	Binary Input Change Event - with relative time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
2	3	Binary Input Change Event - with relative time			(Unsol. Resp.)	17, 28 (index)
3	0	Double-bit Input - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
3	0	Double-bit Input - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
3	1	Double-bit Input - Double-bit packed	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
3	2	Double-bit Input - with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
4	0	Double-bit Input Change Event - any variation	1(read)	06 (no range, or all), 07, 08 (limited qty)		
4	1	Double-bit Input Change Event - without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
4	1	Double-bit Input Change Event - without time			(Unsol. Resp.)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
4	2	Double-bit Input Change Event - with absolute time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
4	2	Double-bit Input Change Event - with absolute time			(Unsol. Resp.)	17, 28 (index)
4	3	Double-bit Input Change Event - with relative time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
4	3	Double-bit Input Change Event - with relative time			(Unsol. Resp.)	17, 28 (index)
10	0	Binary Output - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 28 (index)		
10	0	Binary Output - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
10	1	Binary Output - packed format	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
10	1	Binary Output - packed format	2(write)	00, 01 (start-stop)		
10	2	Continuous Control - output status with flags	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
11	0	Binary Output Change Event - any variation	1(read)	06 (no range, or all), 07, 08 (limited qty)		
11	1	Binary Output Change Event - status without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
11	1	Binary Output Change Event - status without time			(Unsol. Resp.)	17, 28 (index)
11	2	Binary Output Change Event - status with time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
11	2	Binary Output Change Event - status with time			(Unsol. Resp.)	17, 28 (index)
12	0	Binary Output Command (CROB) - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
12	1	Binary Output Command (CROB) - control relay output block	3(select)	17, 27, 28 (index)	(Response)	echo of request
12	1	Binary Output Command (CROB) - control relay output block	4(operate)	17, 27, 28 (index)	(Response)	echo of request
12	1	Binary Output Command (CROB) - control relay output block	5(direct op.)	17, 27, 28 (index)	(Response)	echo of request
12	1	Binary Output Command (CROB) - control relay output block	6(direct op, no ack)	17, 27, 28 (index)	(Response)	echo of request
12	2	Binary Output Command - pattern control block	3(select)	07 (limited qty = 1)	(Response)	echo of request
12	2	Binary Output Command - pattern control block	4(operate)	07 (limited qty = 1)	(Response)	echo of request

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
12	2	Binary Output Command - pattern control block	5(direct op.)	07 (limited qty = 1)	(Response)	echo of request
12	2	Binary Output Command - pattern control block	6(direct op, no ack)	07 (limited qty = 1)	(Response)	echo of request
12	3	Binary Output Command - pattern mask	3(select)	00, 01 (start-stop)	(Response)	echo of request
12	3	Binary Output Command - pattern mask	4(operate)	00, 01 (start-stop)	(Response)	echo of request
12	3	Binary Output Command - pattern mask	5(direct op.)	00, 01 (start-stop)	(Response)	echo of request
12	3	Binary Output Command - pattern mask	6(direct op, no ack)	00, 01 (start-stop)	(Response)	echo of request
20	0	Counter - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
20	0	Counter - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
20	0	Counter - any variation	7(freeze)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty)		
20	0	Counter - any variation	8(freeze, no ack)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty)		
20	0	Counter - any variation	9(freeze & clear)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty)		

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
20	0	Counter - any variation	10(frz & clr, no ack)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty)		
20	1	Counter - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
20	2	Counter - 16-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
20	5	Counter - 32-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
20	6	Counter - 16-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
21	0	Frozen Counter - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
21	0	Frozen Counter - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
21	1	Frozen Counter - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
21	2	Frozen Counter - 16-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
21	5	Frozen Counter - 32-bit with flag and time	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
21	6	Frozen Counter - 16-bit with flag and time	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
21	9	Frozen Counter - 32-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
21	10	Frozen Counter - 16-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
22	0	Counter Change Event - any variation	1(read)	06 (no range, or all), 07, 08 (limited qty)		
22	1	Counter Change Event - 32-bit with flag	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
22	1	Counter Change Event - 32-bit with flag			(Unsol. Resp.)	17, 28 (index)
22	2	Counter Change Event - 16-bit with flag	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
22	2	Counter Change Event - 16-bit with flag			(Unsol. Resp.)	17, 28 (index)
22	5	Counter Change Event - 32-bit with flag and time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
22	5	Counter Change Event - 32-bit with flag and time			(Unsol. Resp.)	17, 28 (index)
22	6	Counter Change Event - 16-bit with flag and time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
22	6	Counter Change Event - 16-bit with flag and time			(Unsol. Resp.)	17, 28 (index)
23	0	Frozen Counter Change Event - any variation	1(read)	06 (no range, or all), 07, 08 (limited qty)		
23	1	Frozen Counter Change Event - 32-bit with flag	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
23	1	Frozen Counter Change Event - 32-bit with flag			(Unsol. Resp.)	17, 28 (index)
23	2	Frozen Counter Change Event - 16-bit with flag	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
23	2	Frozen Counter Change Event - 16-bit with flag			(Unsol. Resp.)	17, 28 (index)
23	5	Frozen Counter Change Event - 32-bit with flag and time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
23	5	Frozen Counter Change Event - 32-bit with flag and time			(Unsol. Resp.)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
23	6	Frozen Counter Change Event - 16-bit with flag and time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
23	6	Frozen Counter Change Event - 16-bit with flag and time			(Unsol. Resp.)	17, 28 (index)
30	0	Analog Input - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all)		
30	0	Analog Input - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
30	1	Analog Input - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
30	2	Analog Input - 16-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
30	3	Analog Input - 32-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
30	4	Analog Input - 16-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
30	5	Analog Input - single-precision, floating-point with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
32	0	Analog Input Change Event - any variation	1(read)	06 (no range, or all), 07, 08 (limited qty)		
32	1	Analog Input Change Event - 32-bit without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
32	1	Analog Input Event 32-bit without time			(Unsol. Resp.)	17, 28 (index)
32	2	Analog Input Change Event - 16-bit without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
32	2	Analog Input Change Event - 16-bit without time			(Unsol. Resp.)	17, 28 (index)
32	3	Analog Input Change Event - 32-bit with time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
32	3	Analog Input Change Event - 32-bit with time			(Unsol. Resp.)	17, 28 (index)
32	4	Analog Input Change Event - 16-bit with time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
32	4	Analog Input Change Event - 16-bit with time			(Unsol. Resp.)	17, 28 (index)
32	5	Analog Input Change Event - single-precision, floating-point without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
32	5	Analog Input Change Event - single-precision, floating-point without time			(Unsol. Resp.)	17, 28 (index)
32	7	Analog Input Change Event - single-precision, floating-point with time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
32	7	Analog Input Change Event - single-precision, floating-point with time			(Unsol. Resp.)	17, 28 (index)
34	0	Analog Input Deadband - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
34	1	Analog Input Deadband - 16-bit	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
34	1	Analog Input Deadband - 16-bit	2(write)	00, 01 (start-stop), 07, 08 (limited qty), 17, 27, 28 (index)		
34	2	Analog Input Deadband - 32-bit	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
34	2	Analog Input Deadband - 32-bit	2(write)	00, 01 (start-stop), 07, 08 (limited qty), 17, 27, 28 (index)		

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
34	3	Analog Input Deadband - single-precision, floating-point	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
34	3	Analog Input Deadband - single-precision, floating-point	2(write)	00, 01 (start-stop), 07, 08 (limited qty), 17, 27, 28 (index)		
40	0	Analog Output Status - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
40	0	Analog Output Status - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		
40	1	Analog Output Status - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
40	2	Analog Output Status - 16-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
40	3	Analog Output Status - single-precision, floating-point with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
41	0	Analog Output Block - any variation	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 27, 28 (index)		

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
41	1	Analog Output Block - 32-bit	3(select)	17, 27, 28 (index)	(Response)	echo of request
41	1	Analog Output Block - 32-bit	4(operate)	17, 27, 28 (index)	(Response)	echo of request
41	1	Analog Output Block - 32-bit	5(direct op.)	17, 27, 28 (index)	(Response)	echo of request
41	1	Analog Output Block - 32-bit	6(direct op, no ack)	17, 27, 28 (index)	(Response)	echo of request
41	2	Analog Output Block - 16-bit	3(select)	17, 27, 28 (index)	(Response)	echo of request
41	2	Analog Output Block - 16-bit	4(operate)	17, 27, 28 (index)	(Response)	echo of request
41	2	Analog Output Block - 16-bit	5(direct op.)	17, 27, 28 (index)	(Response)	echo of request
41	2	Analog Output Block - 16-bit	6(direct op, no ack)	17, 27, 28 (index)	(Response)	echo of request
41	3	Analog Output Block - single-precision, floating-point	3(select)	17, 27, 28 (index)	(Response)	echo of request
41	3	Analog Output Block - single-precision, floating-point	4(operate)	17, 27, 28 (index)	(Response)	echo of request
41	3	Analog Output Block - single-precision, floating-point	5(direct op.)	17, 27, 28 (index)	(Response)	echo of request
41	3	Analog Output Block - single-precision, floating-point	6(direct op, no ack)	17, 27, 28 (index)	(Response)	echo of request
42	0	Analog Output Change Event - any variation	1(read)	06 (no range, or all), 07, 08 (limited qty)		

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
42	1	Analog Output Change Event - 32-bit without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
42	1	Analog Output Change Event - 32-bit without time			(Unsol. Resp.)	17, 28 (index)
42	2	Analog Output Change Event - 16-bit without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
42	2	Analog Output Change Event - 16-bit without time			(Unsol. Resp.)	17, 28 (index)
42	3	Analog Output Change Event - 32-bit with time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
42	3	Analog Output Change Event - 32-bit with time			(Unsol. Resp.)	17, 28 (index)
42	4	Analog Output Change Event - 16-bit with time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
42	4	Analog Output Change Event - 16-bit with time			(Unsol. Resp.)	17, 28 (index)
42	5	Analog Output Change Event - single-precision, floating-point without time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
42	5	Analog Output Change Event - single-precision, floating-point without time			(Unsol. Resp.)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
42	7	Analog Output Change Event - single-precision, floating-point with time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
42	7	Analog Output Change Event - single-precision, floating-point with time			(Unsol. Resp.)	17, 28 (index)
50	1	Time and Date - absolute time	1(read)	07 (limited qty = 1)	(Response)	07 (limited qty = 1)
50	1	Time and Date - absolute time	2(write)	07 (limited qty = 1)		
50	3	Time and Date - absolute time at last recorded time	2(write)	07 (limited qty = 1)		
51	1	Time and Date CTO - absolute time, synchronized			(Response)	07 (limited qty = 1)
51	1	Time and Date CTO - absolute time, synchronized			(Unsol. Resp.)	07 (limited qty = 1)
51	2	Time and Date CTO - absolute time, un-synchronized			(Response)	07 (limited qty = 1)
51	2	Time and Date CTO - absolute time, un-synchronized			(Unsol. Resp.)	07 (limited qty = 1)
52	1	Time Delay - coarse			(Response)	07 (limited qty = 1)
52	2	Time Delay - fine			(Response)	07 (limited qty = 1)
60	1	Class Objects - class 0 data	1(read)	06 (no range, or all)		

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
60	1	Class Objects - class 0 data	22(assign class)	06 (no range, or all)		
60	2	Class Objects - class 1 data	1(read)	06 (no range, or all), 07, 08 (limited qty)		
60	2	Class Objects - class 1 data	20(enable unsol.)	06 (no range, or all)		
60	2	Class Objects - class 1 data	21(disable unsol.)	06 (no range, or all)		
60	2	Class Objects - class 1 data	22(assign class)	06 (no range, or all)		
60	3	Class Objects - class 2 data	1(read)	06 (no range, or all), 07, 08 (limited qty)		
60	3	Class Objects - class 2 data	20(enable unsol.)	06 (no range, or all)		
60	3	Class Objects - class 2 data	21(disable unsol.)	06 (no range, or all)		
60	3	Class Objects - class 2 data	22(assign class)	06 (no range, or all)		
60	4	Class Objects - class 3 data	1(read)	06 (no range, or all), 07, 08 (limited qty)		
60	4	Class Objects - class 3 data	20(enable unsol.)	06 (no range, or all)		
60	4	Class Objects - class 3 data	21(disable unsol.)	06 (no range, or all)		
60	4	Class Objects - class 3 data	22(assign class)	06 (no range, or all)		
80	1	Internal Indications - packed format	1(read)	00, 01 (start-stop)	(Response)	00, 01 (start-stop)
80	1	Internal Indications - packed format	2(write)			
91	1	Status of Requested Operation			(Response)	07 (limited qty = 1)
91	1	Status of Requested Operation			(Response)	5B

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
110	string length	Octet String	1(read)	00, 01 (start-stop), 06 (no range, or all), 07, 08 (limited qty), 17, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
110	string length	Octet String	2(write)	00, 01 (start-stop), 07, 08 (limited qty), 17, 28 (index)		
110	string length	Octet String	31(activate config)	5B		
120	0	Authentication - Assign Class	22(assign class)	06 (no range, or all)		
120	1	Authentication - Challenge	32(auth req)	5B	(Auth. Resp.)	5B
120	2	Authentication - Reply	32(auth req)	5B	(Auth. Resp.)	5B
120	3	Authentication - Aggressive Mode	any of 1 to 31	07 (limited qty = 1)	(Response)	07 (limited qty = 1)
120	3	Authentication - Aggressive Mode			(Unsol. Resp.)	07 (limited qty = 1)
120	4	Authentication - Session Key Status Request	32(auth req)	07 (limited qty = 1)		
120	5	Authentication - Session Key Status			(Auth. Resp.)	5B
120	6	Authentication - Session Key Change	32(auth req)	5B		
120	7	Authentication - Error	33(auth req, no ack)	5B	(Auth. Resp.)	5B
120	8	Authentication - User Certificate	32(auth req)	5B		
120	9	Authentication - MAC	any of 1 to 31	5B	(Response)	5B
120	9	Authentication - MAC			(Unsol. Resp.)	5B

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
120	10	Authentication - User Status Change	32(auth req)	5B		
120	11	Authentication - Update Key Change Request	32(auth req)	5B		
120	12	Authentication - Update Key Change Reply			(Auth. Resp.)	5B
120	13	Authentication - Update Key Change	32(auth req)	5B		
120	14	Authentication - Update Key Change Signature	32(auth req)	5B		
120	15	Authentication - Update Key Change Confirmation	32(auth req)	5B	(Auth. Resp.)	5B
121	0	Security Statistic	1(read)	00, 01 (start-stop), 06 (no range, or all), 17, 28 (index)		
121	0	Security Statistic - Assign Class	22(assign class)	00, 01 (start-stop), 06 (no range, or all), 17, 28 (index)		
121	1	Security Statistic	1(read)	00, 01 (start-stop), 06 (no range, or all), 17, 28 (index)	(Response)	00, 01 (start-stop), 17, 28 (index)
122	0	Security Statistic Event - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all), 17, 28 (index)		
122	1	Security Statistic Event - 32-bit with flag	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
122	1	Security Statistic Event - 32-bit with flag and time			(Unsol. Resp.)	17, 28 (index)

DNP OBJECT GROUP & VARIATION			REQUEST Master may issue Outstation parses		RESPONSE Master parses Outstation may issue	
Object Group Number	Variation Number	Description	Function Codes (dec)	Qualifier Codes (hex)	Function Codes (dec)	Qualifier Codes (hex)
122	2	Security Statistic Event - 32-bit with flag and time	1(read)	06 (no range, or all), 07, 08 (limited qty)	(Response)	17, 28 (index)
122	2	Security Statistic Event - 32-bit with flag and time			(Unsol. Resp.)	17, 28 (index)

Appendix B
Project Migration

Introduction

Observe the considerations in this chapter when you migrate a configuration file from a BMXNOR0200H module in an M340 network to a BMENOR2200H module in an M580 network.

What Is in This Chapter?

This chapter contains the following topics:

XML File Migration

Introduction

You can migrate the configuration file from a BMXNOR0200H module to a BMENOR2200H module.

NOTE: Refer to the general instructions to export and import .xml files with the Control Expert DTM *(see page 135)*.

Project Migration Use Case

Migrate the configuration file from a BMXNOR0200H module to a BMENOR2200H module:

Stage	Description
1	Export the .xml configuration file from a BMXNOR0200H module in an M340 PAC controller application.
2	Import the .xml configuration file to a BMENOR2200H module in an M580 PAC controller application.

NOTE: All located addresses are lost after you import .xml files from the BMENOR2200H module. The type and length of the name are changed according to the new format *(see page 205)*.

Data Type Migration

Introduction

When you migrate an RTU application from a BMXNOR0200H RTU module to a BMENOR2200H RTU module, be aware of the conversion of some specific data types and variable names.

These tables follow:

- DNP3 Server RTU Point Data Type Migration *(see page 205)*
- DNP3 Client RTU Point Data Type Migration *(see page 206)*

Apply this information when you configure DNP3 communications in the BMENOR2200H DTM *(see page 107)*.

DNP3 Server RTU Point Data Type Migration

The data types that change in the migration are shown in red:

Object Type (Default Variable Name)	Object Element	BMXNOR0200H		BMENOR2200H	
		Parameter	Data Type	Parameter	Data Type
Binary Input (BI_Px)	Value	.value	WORD	.value	BYTE
	Flag	.flags	WORD	.flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Double_Input (DI_Px)	Value	.value	WORD	.value	BYTE
	Flag	.flags	WORD	.flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Binary_Output (BO_Px)	Value	.value	WORD	.value	BYTE
					INT (**Sync On Demand** mode *(see page 127)* only)
Binary_Counter (BCnt_Px)	Value - 16 bit	.value	DWORD	.value	INT
	Value - 32 bit	.value	DWORD	.value	DINT
	Flag	.flags	DWORD	.flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Analog_Input (AI_Px)	Value - 16 bit	.value	INT	.Value	INT
	Value - 32 bit	.value	DINT	.Value	DINT
	Value - Short	.value	REAL	.Value	REAL
	Flag - 16 bit	.flags	WORD	.Flags	BYTE
	Flag - 32 bit/Short	.flags	DWORD	.Flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56

Object Type (Default Variable Name)	Object Element	BMXNOR0200H		BMENOR2200H	
		Parameter	Data Type	Parameter	Data Type
Analog_Output (AO_Px)	Value - 16 bit	.value	INT	.Value	INT
	Value - 32 bit	.value	DINT	.Value	DINT
	Value - Short	.value	REAL	.Value	REAL
Analog_Input_Deadband (AI_Px_Dband)	Value	.Value	DWORD	.Value	DWORD
Binary_Output_Flags (BO_Px_Flag)	—	— None Structure	WORD	.Flag	BYTE
Analog_Output_Flags (AO_Px_Flag)	—	— None Structure	WORD	.Flag	BYTE
Gen_Event (GE_xxxx)	—	.Command	WORD	.Command	BYTE
	—	.Status	WORD	.Status	WORD
Clear_Event (CE_xxxx_CB)	—	.Command	WORD	.Command	BYTE
	—	.Status	WORD	.Status	WORD
Octet String (Str_Px)		—	—	.Value	STRING [0-255]

DNP3 Client RTU Point Data Type Migration

The data types that change in the migration are shown in red:

Object Type (Default Variable Name)	Object Element	BMXNOR0200H		BMENOR2200H	
		Parameter	Data Type	Parameter	Data Type
Binary_Input (BI_Px)	Value	.value	WORD	.value	BYTE
	Flag	.flags	WORD	.flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Double_Input (DI_Px)	Value	.value	WORD	.value	BYTE
	Flag	.flags	WORD	.flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Binary_Output (BO_Px)	—	.value	WORD	.value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Binary_Output_Status (BO_Px_Sts)	Value	.value	WORD	.value	BYTE
	Flag	.flags	WORD	.flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Octet String (Str_Px)		—	—	.Value	STRING [0-255]

Object Type (Default Variable Name)	Object Element	BMXNOR0200H		BMENOR2200H	
		Parameter	Data Type	Parameter	Data Type
Write Octet String (WOctStr_I_Px) (Str_Px_Wrt)		—	—	.Value	STRING [0-255]
		—	—	.Status	WORD
Binary_Counter (BCnt_Px)	Value - 16 bit	.value	DWORD	.counter	WORD
	Value - 32 bit	.value	DWORD	.counter	DWORD
	Flag - 16 bit/32 bit	.flags	DWORD	.flag	BYTE
	Time	.timestamp	CP56	.timestamp	CP56
Frozen_Counter (FrozCnt_xxxx)	Value - 16 bit	.value	DWORD	.counter	WORD
	Value - 32 bit	.value	DWORD	.counter	DWORD
	Flag - 16 bit/32 bit	.flags	DWORD	.flag	BYTE
	Time	.timestamp	CP56	.timestamp	CP56
Analog_Input (AI_Px)	Value - 16 bit	.value	INT	.Value	INT
	Value - 32 bit	.value	DINT	.Value	DINT
	Value - Short	.value	REAL	.Value	REAL
	Flag - 16 bit	.flags	WORD	.Flags	BYTE
	Flag - 32 bit/Short	.flags	DWORD	.Flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Analog_Input_Deadband (AI_Px_Dband)	Value - 16 bit	.value	WORD	.Value	WORD
	Value - 32 bit	.value	DWORD	.Value	DWORD
Analog_Input_Deadband _Control (AIDBCtrl_Px)	Value - 16 bit	.Value	WORD	.Value	WORD
	Value - 32 bit	.Value	DWORD	.Value	DWORD
	Value - Short	.Value	REAL	.Value	REAL
	Command Status	.Status	WORD	.Status	WORD
	Command Status	.Status	DWORD	.Status	WORD
Analog_Output (AO_Px)	Value - 16 bit	.Value	INT	.Value	INT
	Value - 32 bit	.Value	DINT	.Value	DINT
	Value - short	.Value	REAL	.Value	REAL
	Command Status	.Status	WORD	.Status	WORD
	Command Status	.Status	DWORD	.Status	WORD

Object Type (Default Variable Name)	Object Element	BMXNOR0200H		BMENOR2200H	
		Parameter	Data Type	Parameter	Data Type
Analog_Output_Status (AO_Px_Sts)	Value - 16 bit	.value	INT	.Value	INT
	Value - 32 bit	.value	DINT	.Value	DINT
	Value - short	.value	REAL	.Value	REAL
	Flag - 16 bit	.flags	WORD	.Flags	BYTE
	Flag - 32 bit	.flags	DWORD	.Flags	BYTE
	Time	.timestamp	CP56	.Timestamp	CP56
Read_Class (RC_xxxx)	—	.Value	WORD	.Value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Freeze_Counter (FrezCnt_xxxx)	—	.Value	WORD	.Value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Unsolicited_Class (UnsC_xxxx)	—	.Value	WORD	.Value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Time_Sync (TS_xxxx)	—	.Value	WORD	.Value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Restart (Rst_xxxx)	—	.Value	WORD	.Value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Integrity_Poll (IP_xxxx)	—	.Value	WORD	.Value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Read_Group (RG_xxxx)	—	.Value	WORD	.Value	BYTE
	Command Status	.Status	WORD	.Status	WORD
Connect Status		.Status	DWORD	Device_ State	BYTE

Appendix C
Logged Events and Secure Statistics

Introduction

This chapter describes the logged events and secured statistics for the BMENOR2200H module.

What Is in This Chapter?

This chapter contains the following topics:

Event Log Descriptions

Event Log Items

The following collection of messages can be included in the BMENOR2200H event log:

Severity	Service	Message Type	Message
Info	HTTPS	Li1: Successful connection (MNT_ENG_MSG_TYP_CNCTN_SUCCESS)	“”Successful login””
	HTTPS		“”Successful login””
Warning	HTTPS	Li2: Failed connection (wrong credential) (MNT_ENG_MSG_TYP_CNCTN_FAILURE)	“”Failed login””
	HTTPS		“”Failed login””
Info	HTTPS	Li5: disconnection triggered by the peer/user (MNT_ENG_MSG_TYP_DISCONNECTION)	“”Disconnection””
	HTTPS		“”Disconnection””
Info	HTTPS	Li6: Disconnection triggered by a timeout (MNT_ENG_MSG_TYP_DSCNCT_TIMEOUT)	“”Auto logout””
Info	Device_Manager	Li9: Upload of a configuration file (CID) into the device (MNT_ENG_MSG_TYP_CONF_UL)	XXX upload”” where XXX=Application or Configuration
Info	HTTPs	Li10: Upload of a new firmware in the device MNT_ENG_MSG_TYP_FIRMWARE_UPDATE	“”Firmware upload””
Warning	Device_Manager	Li18: Any port, either physical (Serial, USB) or logical (telnet, FTP) activation/deactivation? (MNT_ENG_MSG_TYP_PORT_MANAGEMENT)	“”Major Communication parameter update: XXXX YYYY”“ (with XXXX = communication parameter ID, YYYY= value) Example:””Major Communication parameter update: SNMP enable””
Warning	Device_Manager	LI19: Any network physical port status change. Can be the simple status of a Ethernet port, or information gathered from RSTP / HSR / PRP algorithm for redundant systems (MNT_ENG_MSG_TYP_NETWK_PORT_CHG)	“”Major network physical port status change: XXXX link YYYY”” (with XXXX= port ID, YYYY= status value) Example: “”Major network physical port status change: port 1 link Up/Down)
Warning	Device_Manager	LI20: PORT CONTROL Change (MNT_ENG_MSG_TYP_NTWK_TPLGY_CHG)	“”Topology change detected”“
Error	Device_Manager	LI84: Data Integrity Error MNT_ENG_MSG_DATA_INTEGRITY_ERROR	“”Firmware Integrity error”error””
Error	Device_Manager	LI84: Data Integrity Error MNT_ENG_MSG_DATA_INTEGRITY_ERROR	“”Data Integrity error””

Severity	Service	Message Type	Message
Info	Device_Manager	LI26: Hardware change MNT_ENG_MSG_HARDWARE_CHANGE	“”XXXX hardware update: YYYY”” (with XXXX that identifies the hardware object which changes and YYYY that describes the update) EXAMPLE: hardware update: Secure Mode
Warning	HTTPS	Li11: MNT_ENG_MSG_TYP_RBAC_UPDATE	Update RBAC
Warning	HTTPS	Li12: MNT_ENG_MSG_TYP_SECURITY_UPDATE_UPDATE	“”Major Cyber Security parameter update: network services”“ ””Major Cyber Security parameter update: event log”“ “”Major Cyber Security parameter update: security policy”“
Warning	Device_Manager	Li86??: Failed authorization (MNT_ENG_MSG_TYP_AUTHORIZATION_FAILURE) OR Li21: MNT_ENG_MSG_TYP_AUTH_REQ?	“”Failed authorization””
Warning	Device_Manager	Li89: Certificate Management (MNT_ENG_MSG_TYP_CERT_MGT)	“”Add Client Certificate”” “”Remove Client Certificate””
Warning	HTTPS	Li13: MNT_ENG_MSG_TYP_DSS_UPDATE	“”Major Cyber Security parameter update: ipsec”“ ””Major Cyber Security parameter update: OPC UA”“
Warning	DNP3_Master / DNP3_Outstation	Li90:MNT_ENG_MSG_TYPE_AUTHENTICATION_FAILUE	“”channel[“”+channel name+””] authentication failed”“
Warning	DNP3_Master / DNP3_Outstation	Li91:MNT_ENG_MSG_TYPE_UNEXPECTED_RESPONSE	“”channel[“”+channel name+””] unexpected response””
Warning	DNP3_Master / DNP3_Outstation	Li92:MNT_ENG_MSG_TYPE_NO_RESPONSE	“”channel[“”+channel name+””] no response””
Warning	DNP3_Master / DNP3_Outstation	Li93:MNT_ENG_MSG_TYPE_AGGRESSIVE_MODE_NOT_SUPPORTED	“”channel[“”+channel name+””] aggressive mode not supported””
Warning	DNP3_Master / DNP3_Outstation	Li94:MNT_ENG_MSG_TYPE_MAC_ALGORITHM_NOT_SUPPORTED	“”channel[“”+channel name+””] MAC algorithm not supported””

Severity	Service	Message Type	Message
Warning	DNP3_Master / DNP3_Outstation	Li95:MNT_ENG_MSG_TYPE_KEYWRAP_ALGORITHM_NOT_SUPPORTED	“”channel[“”+channel name+””] key wrap algorithm not supported””
Warning	DNP3_Master / DNP3_Outstation	Li86:MNT_ENG_MSG_TYP_AUTHORIZATION_FAILURE)	“”channel[“”+channel name+””] authorization failed””
Warning	DNP3_Master / DNP3_Outstation	Li96:MNT_ENG_MSG_TYPE_UPDATE_KEY_CHANGE_METHOD_NOT_PERMITTED	“”channel[“”+channel name+] update key change method not permitted””
Warning	DNP3_Master / DNP3_Outstation	Li97:MNT_ENG_MSG_TYPE_INVALID_SIGNATURE	“”channel[“”+channel name+””] invalid signature
Warning	DNP3_Master / DNP3_Outstation	Li98:MNT_ENG_MSG_TYPE_INVALID_CERTIFICATION_DATA	“”channel[“”+channel name+””] invalid certification data””
Warning	DNP3_Master / DNP3_Outstation	Li99:MNT_ENG_MSG_TYPE_UNKNOWN_USER	“”channel[“”+channel name+””] unknown user””
Warning	DNP3_Master / DNP3_Outstation	Li100:MNT_ENG_MSG_TYPE_MAX_SESSION_KEY_STATUS_REQ_EXCEED	“”channel[“”+channel name+””] max session key status request exceed””
Info	DNP3_Master / DNP3_Outstation	Li101:MNT_ENG_MSG_TYPE_SESSION_KEY_CHANGE_SUCCESS	“”channel[“”+channel name+””] session key change success””

Secure Statistics

Secure Statistics

The following statistics are recorded for DNP3 secure connections to the BMENOR2200H RTU:

This Statistic ...	Describes the number of:
unexpectedMessages	Unexpected messages
authorizationFailures	Detected authorization failures
authenticationFailures	Detected authentication failures
replyTimeout	Reply timeouts
rekeyDueToAuthenticationFailure	Re-keys due to detected authentication failure
totalMessageSent	Total messages sent
totalMessageReceived	Total messages received
criticalMessageSent	Critical messages sent
criticalMessageReceived	Critical messages received
disCardedMessages	Discarded messages
errorMessageSent	Detected error message sent
errorMessageRxed	Detected error message received
successfulAuthentications	Successful authentications
sessionKeyChanges	Session key changes
sessionKeyChangesFailed	Detected failed session key changes
updatekeyChanges	Update key changes
updateKeyChangesFailed	Detected failed update key changes
rekeysDueToRestart	Re-keys due to restart

Appendix D
Modbus Diagnostic Codes

What Is in This Chapter?

This chapter contains the following topics:

Data Mapping for Modbus Function Code 3 with Unit ID 100

Function Code 3

Some module diagnostics (I/O connection, extended health, redundancy status, FDR server, etc.) are available to Modbus clients that read the local Modbus server area. Use Modbus function code 3 with the unit ID set to 100 for register mapping:

Type	Offset Modbus Address	Size (Words)
Basic Networks Diagnostic Data	0	39
Ethernet Port Diagnostic Data	39	103
Modbus TCP/Port 502 Diagnostic Data	554	114
Modbus TCP/Port 502 Connection Table Data	668	515
SMTP Diagnostic Data	1183	130
SNTP Diagnostic Data	1313	43
DNP/IEC Connection Information	1356	6
DNP/IEC Server/Slave Connection Diagnostic	1362	1141
DNP/IEC Client/Master Connection Diagnostic	2503	1281
DNP Server/Slave Security Diagnostic	3784	157
DNP Client/Master Security Diagnostic	4097	2497
Clock Diagnostic	6750	13

Basic Networks Diagnostic Data

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	Basic network diagnostic validity
Offset + 1	MS Byte	LS Byte	
Offset + 2	MS Byte	LS Byte	Communication global status
Offset + 3	MS Byte	LS Byte	Supported communication services
Offset + 4	MS Byte	LS Byte	Status of communication services
Offset + 5	IP 1	IP 2	IP address
Offset + 6	IP 3	IP 4	
Offset + 7	SN mask 1	SN mask 2	Subnet mask
Offset + 8	SN mask 3	SN mask 4	
Offset + 9	GW IP 1	GW IP 2	Default gateway
Offset + 10	GW IP 3	GW IP 4	

Address	MS Byte	LS Byte	Comments
Offset + 11	MAC 00	MAC 01	MAC address
Offset + 12	MAC 02	MAC 03	
Offset + 13	MAC 04	MAC 05	
Offset + 14	MS Byte 00	01	Ether frame format capability / configuration / operational
Offset + 15	02	03	
Offset + 16	04	LS Byte 05	
Offset + 17	C00	C01	Ethernet receive frames OK
Offset + 18	C02	C03	
Offset + 19	C00	C01	Ethernet transmit frames OK
Offset + 20	C02	C03	
Offset + 21	MS Byte	LS Byte	Number open client connections
Offset + 22	MS Byte	LS Byte	Number open server connections
Offset + 23	C00	C01	Number of Modbus error messages sent
Offset + 24	C02	C03	
Offset + 25	C00	C01	Number of Modbus messages sent
Offset + 26	C02	C03	
Offset + 27	C00	C01	Number of Modbus messages received
Offset + 28	C02	C03	
Offset + 29	Char 1	Char 2	Device name
Offset + 30	Char 3	Char 4	
Offset + 31	Char 5	Char 6	
Offset + 32	Char 7	Char 8	
Offset + 33	Char 9	Char 10	
Offset + 34	Char 11	Char 12	
Offset + 35	Char 13	Char 14	
Offset + 36	Char 15	Char 16	
Offset + 37	MS Byte 00	01	IP assignment mode capability / operational
Offset + 38	02	LS Byte 03	

Ethernet Port Diagnostic Data

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	Port diagnostics data validity
Offset + 1	MS Byte	LS Byte	Logical/physical port number
Offset + 2	MS Byte	LS Byte	Ether control capability

Address	MS Byte	LS Byte	Comments
Offset + 3	MS Byte	LS Byte	Link speed capability
Offset + 4	MS Byte	LS Byte	Ether control configuration
Offset + 5	MS Byte	LS Byte	Link speed configuration
Offset + 6	MS Byte	LS Byte	Ether control operational
Offset + 7	MS Byte	LS Byte	Link speed operational
Offset + 8	MAC 00	MAC 01	Port MAC address
Offset + 9	MAC 02	MAC 03	
Offset + 10	MAC 04	MAC 05	
Offset + 11	MSB - C00	C01	Media counters data validity
Offset + 12	C02	LSB - C03	
Offset + 13	MSB - C00	C01	Number frames transmitted OK
Offset + 14	C02	LSB - C03	
Offset + 15	MSB - C00	C01	Number frames received OK
Offset + 16	C02	LSB - C03	
Offset + 17	MSB - C00	C01	Number Ether collisions
Offset + 18	C02	LSB - C03	
Offset + 19	MSB - C00	C01	Carrier sense errors
Offset + 20	C02	LSB - C03	
Offset + 21	MSB - C00	C01	Number Ether excessive collisions
Offset + 22	C02	LSB - C03	
Offset + 23	MSB - C00	C01	CRC errors
Offset + 24	C02	LSB - C03	
Offset + 25	MSB - C00	C01	FSC errors
Offset + 26	C02	LSB - C03	
Offset + 27	MSB - C00	C01	Alignment errors
Offset + 28	C02	LSB - C03	
Offset + 29	MSB - C00	C01	Number internal MAC transmit errors
Offset + 30	C02	LSB - C03	
Offset + 31	MSB - C00	C01	Late collisions
Offset + 32	C02	LSB - C03	
Offset + 33	MSB - C00	C01	Number internal MAC transmit errors
Offset + 34	C02	LSB - C03	
Offset + 35	MSB - C00	C01	Multiple collisions
Offset + 36	C02	LSB - C03	

Address	MS Byte	LS Byte	Comments
Offset + 37	MSB - C00	C01	Single collisions
Offset + 38	C02	LSB - C03	
Offset + 39	MSB - C00	C01	Deferred transmissions
Offset + 40	C02	LSB - C03	
Offset + 41	MSB - C00	C01	Frames too long
Offset + 42	C02	LSB - C03	
Offset + 43	MSB - C00	C01	Frames too short
Offset + 44	C02	LSB - C03	
Offset + 45	MSB - C00	C01	SQE test error
Offset + 46	C02	LSB - C03	
Offset + 47	MS Byte	LS Byte	Interface label length
Offset + 48	IL_char64	IL_char63	Interface label characters
Offset + ...	...	...	
Offset + 79	IL_char2	IL_char1	
Offset + 80	MS Byte	LS Byte	Interface counters diagnostic validity
Offset + 81	MSB - C00	C01	Number octets received
Offset + 82	C02	LSB - C03	
Offset + 83	MSB - C00	C01	Number unicast packets received
Offset + 84	C02	LSB - C03	
Offset + 85	MSB - C00	C01	Number non-unicast packets received
Offset + 86	C02	LSB - C03	
Offset + 87	MSB - C00	C01	Number inbound packets discard
Offset + 88	C02	LSB - C03	
Offset + 89	MSB - C00	C01	Number inbound packets error
Offset + 90	C02	LSB - C03	
Offset + 91	MSB - C00	C01	Number inbound packets unknown
Offset + 92	C02	LSB - C03	
Offset + 93	MSB - C00	C01	Number octets sent
Offset + 94	C02	LSB - C03	
Offset + 95	MSB - C00	C01	Number unicast packets sent
Offset + 96	C02	LSB - C03	
Offset + 97	MSB - C00	C01	Number non-unicast packets sent
Offset + 98	C02	LSB - C03	

Address	MS Byte	LS Byte	Comments
Offset + 99	MSB - C00	C01	Number outbound packets discard
Offset + 100	C02	LSB - C03	
Offset + 101	MSB - C00	C01	Number outbound packets error
Offset + 102	C02	LSB - C03	
Offset + 103			Port 2
			103 words per port
Offset + 206			Port 3
			103 words per port
Offset + 309			Port 4
			103 words per port

Modbus TCP/Port 502 Diagnostic Data

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	Modbus TCP/Port 502 diagnostic data validity
Offset + 1	MS Byte	LS Byte	
Offset + 2	MS Byte	LS Byte	Port 502 status
Offset + 3	MS Byte	LS Byte	Number open connections
Offset + 4	MSB - C00	C01	Number Modbus messages sent
Offset + 5	C02	LSB - C03	
Offset + 6	MSB - C00	C01	Number Modbus messages received
Offset + 7	C02	LSB - C03	
Offset + 8	MS Byte	LS Byte	Number Modbus open client connections
Offset + 9	MS Byte	LS Byte	Number Modbus open server connections
Offset + 10	MS Byte	LS Byte	Maximum number connections
Offset + 11	MS Byte	LS Byte	Maximum number client connections
Offset + 12	MS Byte	LS Byte	Maximum number server connections
Offset + 13	MSB - C00	C01	Number Modbus error messages sent
Offset + 14	C02	LSB - C03	
Offset + 15	MS Byte	LS Byte	Number open priority connections
Offset + 16	MS Byte	LS Byte	Maximum number priority connections
Offset + 17	MS Byte	LS Byte	Number entries in unauthorized table
Offset + 18	MSB - IP1	IP2	Remote IP address 1
Offset + 19	IP3	LSB - IP4	

Address	MS Byte	LS Byte	Comments
Offset + 20	MS Byte	LS Byte	Number attempts to open unauthorized connection 1
...			
Offset + 111	MSB - IP1	IP2	Remote IP address 32
Offset + 112	IP3	LSB - IP4	
Offset + 113	MS Byte	LS Byte	Number attempts to open unauthorized connection 32

Modbus TCP/Port 502 Connection Table Data

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	Connection table validity
Offset + 1	MS Byte	LS Byte	Number of entries
Offset + 2	MS Byte	LS Byte	Starting entry index
Offset + 3	MS Byte	LS Byte	Connection index
Offset + 4	IP 1	IP 2	Remote IP address
Offset + 5	IP 3	IP 4	
Offset + 6	MS Byte	LS Byte	Remote port number
Offset + 7	MS Byte	LS Byte	Local port number
Offset + 8	MS Byte	LS Byte	Number Modbus messages sent on Connex
Offset + 9	MS Byte	LS Byte	Number Modbus messages received on Connex
Offset + 10	MS Byte	LS Byte	Number Modbus error messages sent on Connex

SMTP Diagnostic Data

Address	MS Byte	LS Byte	CIP Type	Comments
Offset	MS Byte	LS Byte	UDINT	SMTP server IP address
Offset + 1	MS Byte	LS Byte		
Offset + 2	MS Byte	LS Byte	UDINT	Email service status
Offset + 3	MS Byte	LS Byte		
Offset + 4	MS Byte	LS Byte	UDINT	Link to SMTP server status
Offset + 5	MS Byte	LS Byte		
Offset + 6	MS Byte	LS Byte	UDINT	Number of emails sent
Offset + 7	MS Byte	LS Byte		
Offset + 8	MS Byte	LS Byte	UDINT	Number of responses from the server
Offset + 9	MS Byte	LS Byte		

Address	MS Byte	LS Byte	CIP Type	Comments
Offset + 10	MS Byte	LS Byte	UDINT	Number of errors
Offset + 11	MS Byte	LS Byte		
Offset + 12	MS Byte	LS Byte	UDINT	Last error
Offset + 13	MS Byte	LS Byte		
Offset + 14	SenderAddress[0]	SenderAddress[1]	ARRAY of octets	Last email header used
Offset + 15	SenderAddress[2]	SenderAddress[3]		
...				
Offset + 45	SenderAddress[62]	SenderAddress[63]		
Offset + 46	SenderAddress[0]	SenderAddress[1]		
Offset + 47	SenderAddress[2]	SenderAddress[3]		
...				
Offset + 109	SenderAddress[126]	SenderAddress[127]		
Offset + 110	MailSubject[0]	MailSubject[1]		
Offset + 111	MailSubject[2]	MailSubject[3]		
...				
Offset + 125	MailSubject[30]	MailSubject[31]		
Offset + 126	MSW - MSB	MSW - LSB	DINT	Time elapsed from the last email
Offset + 127	LSW - MSB	LSW - LSB		
Offset + 128	MSW - MSB	MSW - LSB	UDINT	Number of time server was not reachable
Offset + 129	LSW - MSB	LSW - LSB		

SNTP Diagnostic Data

Address	MS Byte	LS Byte	CIP Type	Comments
Offset	MSW - MSB	MSW - LSB	UDINT	Enabled/disabled
Offset + 1	LSW - MSB	LSW - LSB		
Offset + 2	MSW - MSB	MSW - LSB	UDINT	Primary NTP server IP address
Offset + 3	LSW - MSB	LSW - LSB		
Offset + 4	MSW - MSB	MSW - LSB	UDINT	Secondary NTP server IP address
Offset + 5	LSW - MSB	LSW - LSB		
Offset + 6	Unused	LS Byte	USINT	Polling period
Offset + 7	Unused	LS Byte	USINT	Daylight saving auto adjustment
Offset + 8	Unused	LS Byte	USINT	Update CPU with module time

Address	MS Byte	LS Byte	CIP Type	Comments
Offset + 9	Unused	LS Byte	USINT	Reserved
Offset + 10	MSW - MSB	MSW - LSB	UDINT	Time zone
Offset + 11	LSW - MSB	LSW - LSB		
Offset + 12	MS Byte	LS Byte	INT	Time zone offset
Offset + 13	Unused	Unused	USINT	Reserved
Offset + 14	Unused	Unused	USINT	Reserved
Offset + 15	Unused	LS Byte	USINT	Daylight saving start date - month
Offset + 16	Unused	LS Byte	USINT	Daylight saving start date - week #, day of week
Offset + 17	Unused	LS Byte	USINT	Daylight saving end date - month
Offset + 18	Unused	LS Byte	USINT	Daylight saving end date - week #, day of week
Offset + 19	MSW - MSB	MSW - LSB	UDINT	Network time service status
Offset + 20	LSW - MSB	LSW - LSB		
Offset + 21	MSW - MSB	MSW - LSB	UDINT	Link to NTP server status
Offset + 22	LSW - MSB	LSW - LSB		
Offset + 23	MSW - MSB	MSW - LSB	UDINT	Current NTP server IP address
Offset + 24	LSW - MSB	LSW - LSB		
Offset + 25	MSW - MSB	MSW - LSB	UDINT	NTP server IP address
Offset + 26	LSW - MSB	LSW - LSB		
Offset + 27	MSW - MSB	MSW - LSB	UDINT	NTP server time quality
Offset + 28	LSW - MSB	LSW - LSB		
Offset + 29	MSW - MSB	MSW - LSB	UDINT	Number of NTP requests sent
Offset + 30	LSW - MSB	LSW - LSB		
Offset + 31	MSW - MSB	MSW - LSB	UDINT	Number of communication errors
Offset + 32	LSW - MSB	LSW - LSB		
Offset + 33	MSW - MSB	MSW - LSB	UDINT	Number of NTP responses received
Offset + 34	LSW - MSB	LSW - LSB		
Offset + 35	MS Byte	LS Byte	UINT	Last error
Offset + 36	MSW - MSB	MSW - LSB	UDINT	Current time
Offset + 37	LSW - MSB	LSW - LSB		
Offset + 38	MS Byte	LS Byte		Current date
Offset + 39	MSW - MSB	MSW - LSB	UDINT	Daylight savings status
Offset + 40	LSW - MSB	LSW - LSB		

Address	MS Byte	LS Byte	CIP Type	Comments
Offset + 41	MSW - MSB	MSW - LSB	UINT	Time since last update
Offset + 42	LSW - MSB	LSW - LSB		

DNP/IEC Connection Information

Address	MS Byte	LS Byte	Comments
Offset	Client Connected Count	Client Configured Count	DNP3/IEC Client Count
Offset + 1	Server Connected Count	Server Configured Count	DNP3/IEC Server Count
Offset + 2			Reserved
Offset + 3			Reserved
Offset + 4			Reserved
Offset + 5			Reserved

DNP/IEC Server/Slave Connection Diagnostic

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	Number of entries
Offset + 1	MS Byte	LS Byte	MS byte: Event USED/CONFIGURED 0-100% LS byte: CONFIGURED/TOTAL 0-100%
Offset + 2	MSB - C03	C02	Module total Configured event buffer size
Offset + 3	C01	LSB - C00	
Offset + 4	MSB - C03	C02	Module total Current event buffer used
Offset + 5	C01	LSB - C00	
Offset + 6	MSB - C03	C02	Module total current overflow
Offset + 7	C01	LSB - C00	
Offset + 8	MS Byte	LS Byte	MS Byte: Event buffer overflow LS Byte: Event backup status
Offset + 9	MS Byte	LS Byte	Channel index
Offset + 10	MS Byte Reserved	LS Byte 1: DNP3 serial 3: DNP3 NET 5: IEC 101 7: IEC 104	Protocol: DNP3 serial slave DNP3 NET server IEC 101 slave IEC 104 server

Address	MS Byte	LS Byte	Comments
Offset + 11	MS Byte	LS Byte	LS Byte connection state 0: disconnected 1: connected 2: connecting MS Byte authentication type 0: none 1: SAv2 2: SAv5 3: TLS_ONLY 4: TLS_SAv2 5: T:LS_SAv5
Offset + 12	Char 1	Char 2	Channel name
Offset + 13	Char 3	Char 4	
Offset + 14	Char 5	Char 6	
Offset + 15	Char 7	Char 8	
Offset + 16	Char 9	Char 10	
Offset + 17	Char 11	Char 12	
Offset + 18	Char 13	Char 14	
Offset + 19	Char 15	Char 16	
Offset + 20	IP 1	IP 2	Remote IP address
Offset + 21	IP 3	IP 4	
Offset + 22	MS Byte	LS Byte	Remote port number
Offset + 23	MS Byte	LS Byte	Local port number
Offset + 24	MS Byte	LS Byte	Error code
Offset + 25	C03	C02	Channel total Configured event buffer size
Offset + 26	C01	C00	
Offset + 27	C03	C02	Channel total Current event buffer used
Offset + 28	C01	C00	
Offset + 29	C03	C02	Channel total Current overflow
Offset + 30	C01	C00	
Offset + 31	MS Byte	LS Byte	MS Byte: reserved LS Byte: event buffer overflow
Offset + 32	MS Byte	LS Byte	Reserved 1
Offset + 33	MS Byte	LS Byte	Reserved 2
Offset + 34	MS Byte	LS Byte	Reserved 3
Offset + 35	MS Byte	LS Byte	Number of data type Event status Always 16

Address	MS Byte	LS Byte	Comments
Offset + 36	MS Byte	LS Byte	MS Byte Bit 0: validity Bit 1: event buffer overflow LS Byte: index
Offset + 37	MS Byte	LS Byte	DNP data type: 1. Binary input 2. Double input 3. Binary output 4. Binary counter 5. Frozen counter 6: Analog input 7. Analog output 8-16. For extended IEC data type: 1. M_SP 2. M_DP 3. M_ST 4. M_BO 5. M_ME_A 6. M_ME_B 7. M_ME_C 8. M_IT 9. Custom_M_IT_D 10-16. For extended
Offset + 38	Char 1	Char 2	Data type name
Offset + 39	Char 3	Char 4	
Offset + 40	Char 5	Char 6	
Offset + 41	Char 7	Char 8	
Offset + 42	Char 9	Char 10	
Offset + 43	Char 11	Char 12	
Offset + 44	Char 13	Char 14	
Offset + 45	Char 15	Char 16	
Offset + 46	C03	C02	Configured event buffer size
Offset + 47	C01	C00	
Offset + 48	C03	C02	Current event buffer used
Offset + 49	C01	C00	
Offset + 50	C03	C02	Current event buffer used
Offset + 51	C01	C00	Current overflow

DNP/IEC Client/Master Connection Diagnostic

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	Number of entries
Offset + 1	MS Byte	LS Byte	Channel index
Offset + 2	MS Byte Reserved	LS Byte 2: DNP3 serial 4: DNP3 NET 6: IEC 101 8: IEC 104	Protocol: DNP3 serial master DNP3 NET client IEC 101 master IEC 104 client
Offset + 3	MS Byte	LS Byte	LS Byte connection state: 0: disconnected 1: connected 2: connecting MS Byte
Offset + 4	Char 1	Char 2	Channel name
Offset + 5	Char 3	Char 4	
Offset + 6	Char 5	Char 6	
Offset + 7	Char 7	Char 8	
Offset + 8	Char 9	Char 10	
Offset + 9	Char 11	Char 12	
Offset + 10	Char 13	Char 14	
Offset + 11	Char 15	Char 16	
Offset + 12	IP 1	IP 2	Remote IP address
Offset + 13	IP 3	IP 4	
Offset + 14	MS Byte	LS Byte	Remote port number
Offset + 15	MS Byte	LS Byte	Local port number
Offset + 16	Bit 15-8	Bit 7-0	Error code Bit 0: authentication failed Bit 1: unexpected response Bit 2: no response Bit 3: aggressive mode not supported Bit 4: MAC algorithm not supported Bit 5: key wrap algorithm not supported Bit 6: authorization failed Bit 7: update key change method not permitted Bit 8: invalid signature Bit 9: invalid certification data Bit 10: unknown user Bit 11:max session key status requests exceed Bit 12-15: reserved
Offset + 17	MS Byte	LS Byte	Reserved 0

Address	MS Byte	LS Byte	Comments
Offset + 18	MS Byte	LS Byte	Reserved 1
Offset + 19	MS Byte	LS Byte	Reserved 2
Offset + 20	MS Byte	LS Byte	Reserved 3

DNP Server/Slave Security Diagnostic

Address	MS Byte	LS Byte	Comments
Offset			Number of entries
Offset + 1	MS Byte reserved	LS Byte channel index	Channel index
Offset + 2	C03	C02	Unexpected messages
Offset + 3	C01	C00	
Offset + 4	C03	C02	Authorization failures
Offset + 5	C01	C00	
Offset + 6	C03	C02	Authentication failures
Offset + 7	C01	C00	
Offset + 8	C03	C02	Reply timeout
Offset + 9	C01	C00	
Offset + 10	C03	C02	Re-keys due to authentication failure
Offset + 11	C01	C00	
Offset + 12	C03	C02	Total message sent
Offset + 13	C01	C00	
Offset + 14	C03	C02	Total messages received
Offset + 15	C01	C00	
Offset + 16	C03	C02	Critical message sent
Offset + 17	C01	C00	
Offset + 18	C03	C02	Critical message received
Offset + 19	C01	C00	
Offset + 20	C03	C02	Discarded messages
Offset + 21	C01	C00	
Offset + 22	C03	C02	Error message sent
Offset + 23	C01	C00	
Offset + 24	C03	C02	Error message transmitted
Offset + 25	C01	C00	
Offset + 26	C03	C02	Successful authentications
Offset + 27	C01	C00	

Address	MS Byte	LS Byte	Comments
Offset + 28	C03	C02	Session key changes
Offset + 29	C01	C00	
Offset + 30	C03	C02	Failed session key changes
Offset + 31	C01	C00	
Offset + 32	C03	C02	Update key changes
Offset + 33	C01	C00	
Offset + 34	C03	C02	Failed update key changes
Offset + 35	C01	C00	
Offset + 36	C03	C02	Re-keys due to restart
Offset + 37	C01	C00	
Offset + 38	C01	C00	Current user number
Offset + 39	C01	C00	Reserved

DNP Client/Master Security Diagnostic

Address	MS Byte	LS Byte	Comments
Offset			Number of entries
Offset + 1	Reserved	Channel index	
Offset + 2	C03	C02	Unexpected messages
Offset + 3	C01	C00	
Offset + 4	C03	C02	Authorization failures
Offset + 5	C01	C00	
Offset + 6	C03	C02	Authentication failures
Offset + 7	C01	C00	
Offset + 8	C03	C02	Reply timeout
Offset + 9	C01	C00	
Offset + 10	C03	C02	Re-keys due to authentication failure
Offset + 11	C01	C00	
Offset + 12	C03	C02	Total message sent
Offset + 13	C01	C00	
Offset + 14	C03	C02	Total messages received
Offset + 15	C01	C00	
Offset + 16	C03	C02	Critical message sent
Offset + 17	C01	C00	

Address	MS Byte	LS Byte	Comments
Offset + 18	C03	C02	Critical messages received
Offset + 19	C01	C00	
Offset + 20	C03	C02	Discarded messages
Offset + 21	C01	C00	
Offset + 22	C03	C02	Error message sent
Offset + 23	C01	C00	
Offset + 24	C03	C02	Error message transmited
Offset + 25	C01	C00	
Offset + 26	C03	C02	Successful authentications
Offset + 27	C01	C00	
Offset + 28	C03	C02	Session key changes
Offset + 29	C01	C00	
Offset + 30	C03	C02	Failed session key changes
Offset + 31	C01	C00	
Offset + 32	C03	C02	Update key changes
Offset + 33	C01	C00	
Offset + 34	C03	C02	Failed update key changes
Offset + 35	C01	C00	
Offset + 36	C03	C02	Rekeys due to restart
Offset + 37	C01	C00	
Offset + 38	C01	C00	Current user number (1-65535)
Offset + 39	C01	C00	Reserved

Clock Diagnostic

Address	MS Byte	LS Byte	Comments
Offset			Number of entries
Offset + 1	MS Byte reserved	LS Byte clock status 1: Synchronized 0: Unsynchronized	Clock status
Offset + 2	C03	C02	Current time
Offset + 3	C01	C00	
Offset + 4	C01	C00	Current date
Offset + 5			Reserved
Offset + 6	C03	C02	Time zone

Address	MS Byte	LS Byte	Comments
Offset + 7	C01	C00	
Offset + 8	C03	C02	Time of last time synchronization
Offset + 9	C01	C00	
Offset + 10	C01	C00	Date of last time synchronization
Offset + 11			Reserved
Offset + 12	MS Byte reserved	LS Byte time source 1: SNTP 2: DNP3	Time source of last time synchronization

Modbus Function Code 8, Sub-Function Code 21

Get Status Summary (Op Code 0x76)

This function returns information about the LEDs and various services running on the BMENOR2200H module.

Request

Field	Length (bytes)	Value (hex)
Function code	1	08
Sub-function code hi	1	00
Sub-function code low	1	15
Operation code hi	1	00
Operation code low	1	76

Response

Field	Length (bytes)	Value (hex)
Function code	**1**	**08**
Sub-function code hi	**1**	**00**
Sub-function code low	**1**	**15**
Operation code hi	**1**	**00**
Operation code low	**1**	**76**
Byte count	**1**	**206**
Number of LEDs	**2**	**7**
LED 1 color	2	Off (default): byte0=0, byte1=0 On (green): byte0=1, byte1=0 Flashing (green): byte0=1, byte1=1
LED 1 status	2	0
LED 1 name string	4	RUN
LED 2 color	2	Off (default): byte0=0 On (red): byte0=2, byte 1=0 Flashing (red): byte0=2, byte1=1
LED 2 status	2	0
LED 2 name string	4	ERR
LED 3 color	2	Off (default): byte0=0, byte1=0 On (red): byte0=2, byte1=0
LED 3 status	2	0

Field	Length (bytes)	Value (hex)
Function code	**1**	**08**
Sub-function code hi	**1**	**00**
Sub-function code low	**1**	**15**
Operation code hi	**1**	**00**
Operation code low	**1**	**76**
Byte count	**1**	**206**
LED 3 name string	3	DL
LED 4 color	2	Off (default): byte0=0, byte1=0 On (green): byte0=1, byte1=0 Flashing (green): byte0=1, byte1=1 On (red): byte0=2, byte1=0
LED 4 status	2	0
LED 4 name string	8	ETH STS
LED 5 color	2	Off (default): byte0=0, byte1=0 On (red): byte0=2, byte1=0
LED 5 status	2	0
LED 5 name string	9	CARD ERR
LED 6 color	2	Off (default): byte0=0, byte1=0 On (green): byte0=1, byte1=0 On (red): byte0=2, byte1=0
LED 6 status	2	0
LED 6 name string	7	SECURE
LED 7 color	2	Off (default): byte0=0, byte1=0 Flashing (yellow): byte0=3, byte1=1
LED 7 status	2	0
LED 7 name string	8	SER COM
Number of services	**2**	**9**
Service 1 color	2	0 = off or n/a 1 = green 2 = red
Service 1 status	2	4 (corresponds to LED color 0) (default) 2 (corresponds to LED color 1) 5 (corresponds to LED color 2)
Service 1 name string	12	DNP3 Client / DNP3 Master
Service 2 color	2	0 = off or n/a 1 = green 2 = red

Field	Length (bytes)	Value (hex)
Function code	**1**	**08**
Sub-function code hi	**1**	**00**
Sub-function code low	**1**	**15**
Operation code hi	**1**	**00**
Operation code low	**1**	**76**
Byte count	**1**	**206**
Service 2 status	2	4 (corresponds to LED color 0) (default) 2 (corresponds to LED color 1) 5 (corresponds to LED color 2)
Service 2 name string	11	IEC Client / IEC Master
Service 3 color	2	0 = off (default) 1 = green
Service 3 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) (default)
Service 3 name string	12	DNP3 Server /DNP3 Slave
Service 4 color	2	0 = off (default) 1 = green
Service 4 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) (default)
Service 4 name string	11	IEC Server / IEC Slave
Service 5 color	2	0 = off (default) 1 = green
Service 5 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) (default)
Service 5 name string	15	Access Control
Service 6 color	2	0 = off (default) 1 = on green 2 = on red
Service 6 status	2	4 (corresponds to LED color 0) (default) 2 (corresponds to LED color 1) 5 (corresponds to LED color 2 - link to server is down))
Service 6 name string	12	SNTP Status
Service 7 color	2	0 = off (default) 1 = on green 2 = on red

Field	Length (bytes)	Value (hex)
Function code	**1**	**08**
Sub-function code hi	**1**	**00**
Sub-function code low	**1**	**15**
Operation code hi	**1**	**00**
Operation code low	**1**	**76**
Byte count	**1**	**206**
Service 7 status	2	4 (corresponds to LED color 0) (default) 2 (corresponds to LED color 1) 5 (corresponds to LED color 2 - link to server is down))
Service 7 name string	14	E-mail Status
Service 8 color	2	0 = off (default) 1 = green
Service 8 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) (default)
Service 8 name string	14	Modbus Server
Service 9 color	2	0 = off (default) 1 = green
Service 9 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) (default)
Service 9 name string	12	FTP Server

LED Status

Refer to the Module LED Indicators topic *(see page 30)* for LED descriptions.

LED Status Number (hex)	Description
1	Ready for operation.
2	Not ready for operation.
3	Fault detected.
4	No fault detected.
5	In operation.
6	Duplicate IP address.
7	Waiting for address server response.
8	Default IP address in use.
9	IP address configuration conflict detected.
A	Not configured.
B	Recoverable fault detected.

LED Status Number (hex)	Description
C	Connectors established.
D	No EtherNet/IP or RTU connections.
E	Connections error.
F	Running.
10	Error present.
11	Ethernet link established.
12	No Ethernet link established.
13	Connected to 100 Mbps link.
14	Not connected to 100 Mbps link.
15	Connected to full duplex link.
16	Not connected to full duplex line.
17	Configuration error.
18	Memory card is missing.
19	Memory card is not usable (bad format, unrecognized type).
20	Data exchange (send/receive) on the serial connection is in progress.
21	No data exchange on the serial connection.
22	Firmware download in progress.
23	Firmware download not in progress.
24	Module and communication are secure.
25	Module is secure, and communication is not secure.
26	Module is not secure.

Services Status

Service Status Number	Description
1	Enabled.
2	Working properly.
3	Disabled.
4	Not configured.
5	One connection or more are bad.
6	Enabled on.
7	Enabled off.

Get Firmware Version (Op Code 0x70)

This function returns the firmware version of the BMENOR2200H module.

Request

Field	Length (bytes)	Value (hex)
Function code	1	08
Sub-function code hi	1	00
Sub-function code low	1	15
Operation code hi	1	00
Operation code low	1	70

Response

Field	Length (bytes)	Value (hex)
Function code	1	08
Sub-function code hi	1	00
Sub-function code low	1	15
Operation code hi	1	00
Operation code low	1	70
Byte count	1	
PV version	1	xx
RL version	1	xx
SV major version	1	xx
SV minor version	1	xx
Web server version	1	xx
Rack	1	xx
Slot	1	xx
MAC	6	xx.xx.xx.xx.xx.xx
SN	n	xxxxxxxxxx

Appendix E
Detected Error Codes

Explicit Messaging: Communication and Operation Reports

Overview

Communication and operation reports are part of the management parameters.

NOTE: It is recommended that communication function reports be tested at the end of their execution and before the next activation. On cold start-up, confirm that all communication function management parameters are checked and reset to 0.
It may be helpful to use the%S21 *(see EcoStruxure™ Control Expert, System Bits and Words, Reference Manual)* to examine the first cycle after a cold or warm start.

Communication Report

This report is common to every explicit messaging function. It is significant when the value of the activity bit switches from 1 to 0. The reports with a value between 16#01 and 16#FE concern errors detected by the processor that executed the function.

The different values of this report are indicated in the following table:

Value	Communication report (least significant byte)
16#00	Correct exchange
16#01	Exchange stop on timeout
16#02	Exchange stop on user request (CANCEL)
16#03	Incorrect address format
16#04	Incorrect destination address
16#05	Incorrect management parameter format
16#06	Incorrect specific parameters
16#07	Error detected in sending to the destination
16#08	Reserved
16#09	Insufficient receive buffer size
16#0A	Insufficient send buffer size
16#0B	No system resources: the number of simultaneous communication EFs exceeds the maximum that can be managed by the processor
16#0C	Incorrect exchange number
16#0D	No telegram received
16#0E	Incorrect length

Value	Communication report (least significant byte)
16#0F	Telegram service not configured
16#10	Network module missing
16#11	Request missing
16#12	Application server already active
16#13	UNI-TE V2 transaction number incorrect
16#FF	Message refused

NOTE: The function can detect a parameter error before activating the exchange. In this case the activity bit remains at 0, and the report is initialized with values corresponding to the detected error.

Operation Report

This report byte is specific to each function, and specifies the result of the operation on the remote application:

Value	Operation report (most significant byte)
16#05	Length mismatch (CIP)
16#07	Bad IP address
16#08	Application error
16#09	Network is down
16#0A	Connection reset by peer
16#0C	Communication function not active
16#0D	• Modbus TCP: transaction timed out • EtherNet/IP: request timeout
16#0F	No route to remote host
16#13	Connection refused
16#15	• Modbus TCP: no resources • EtherNet/IP: no resources to handle the message; or an internal detected error; or no buffer available; or no link available; or cannot send message
16#16	Remote address not allowed
16#18	• Modbus TCP: concurrent connections or transactions limit reached • EtherNet/IP: TCP connection or encapsulation session in progress
16#19	Connection timed out
16#22	Modbus TCP: invalid response
16#23	Modbus TCP: invalid device ID response
16#30	• Modbus TCP: remote host is down • EtherNet/IP: connection open timed out
16#80...16#87: Forward_Open response detected errors:	

Value	Operation report (most significant byte)
16#80	Internal detected error
16#81	Configuration detected error: the length of the explicit message, or the RPI rate, needs to be adjusted
16#82	Device detected error: target device does not support this service
16#83	Device resource detected error: no resource is available to open the connection
16#84	System resource event: unable to reach the device
16#85	Data sheet detected error: incorrect EDS file
16#86	Invalid connection size
16#90...16#9F: Register session response detected errors:	
16#90	Target device does not have sufficient resources
16#98	Target device does not recognize message encapsulation header
16#9F	Unknown detected error from target

Appendix F
DNP3 Communication Detected Error Codes

DNP3 Communication Detected Error Codes

DNP3 Detected Error Codes

Detected Error Code	Description
0x0000	No detected error
0x0001	Security not configured
0x0002	Unlocated variable initialize detected error
0x0004	Internal detected error
0X0008	Detected authentication failure
0x0010	Unexpected response
0x0020	No response
0x0040	Aggressive mode not supported
0x0080	MAC algorithm not supported
0x0100	Key Wrap algorithm not supported
0x0200	Detected authorization failure
0x0400	Update key change method not permitted
0x0800	Invalid signature
0x1000	Invalid certification data
0x2000	Unknown user
0x4000	Max session key status requests exceed
0x8000	Reserved

Glossary

B

bridge

A bridge device connects two or more physical networks that use the same protocol. Bridges read frames and decide whether to transmit or block them based on their destination address.

D

DFB

(*derived function block*) DFB types are function blocks that can be defined by the user in ST, IL, LD or FBD language.

Using these DFB types in an application makes it possible to:

- simplify the design and entry of the program
- make the program easier to read
- make it easier to debug
- reduce the amount of code generated

DTM

(*device type manager*) A DTM is a device driver running on the host PC. It provides a unified structure for accessing device parameters, configuring and operating the devices, and troubleshooting devices. DTMs can range from a simple graphical user interface (GUI) for setting device parameters to a highly sophisticated application capable of performing complex real-time calculations for diagnosis and maintenance purposes. In the context of a DTM, a device can be a communications module or a remote device on the network.

See FDT.

E

EFB

(*elementary function block*) This is a block used in a program which performs a predefined logical function.

EFBs have states and internal parameters. Even if the inputs are identical, the output values may differ. For example, a counter has an output indicating that the preselection value has been reached. This output is set to 1 when the current value is equal to the preselection value.

Ethernet

A LAN cabling and signaling specification used to connect devices within a defined area, e.g., a building. Ethernet uses a bus or a star topology to connect different nodes on a network.

EtherNet/IP™

A network communication protocol for industrial automation applications that combines the standard internet transmission protocols of TCP/IP and UDP with the application layer common industrial protocol (CIP) to support both high speed data exchange and industrial control. EtherNet/IP employs electronic data sheets (EDS) to classify each network device and its functionality.

F

FDR

(*fast device replacement*) A service that uses configuration software to replace an inoperable product.

G

gateway

A device that connects networks with dissimilar network architectures and which operates at the Application Layer of the OSI model. This term may refer to a router.

H

Hot Standby

A Hot Standby system uses a primary PAC (PLC) and a standby PAC. The two PAC racks have identical hardware and software configurations. The standby PAC monitors the current system status of the primary PAC. If the primary PAC becomes inoperable, high-availability control is maintained when the standby PAC takes control of the system.

HTTP server

The installed HTTP server transmits Web pages between a server and a browser, providing Ethernet communications modules with easy access to devices anywhere in the world from standard browsers such as Internet Explorer or Netscape Navigator.

I

IP address

Internet protocol address. This 32-bit address is assigned to hosts that use TCP/IP.

L

local rack

An M580 rack containing the CPU and a power supply. A local rack consists of one or two racks: the main rack and the extended rack, which belongs to the same family as the main rack. The extended rack is optional.

M

MAC address

media access control address. A 48-bit number, unique on a network, that is programmed into each network card or device when it is manufactured.

MB/TCP

(*Modbus over TCP protocol*) This is a Modbus variant used for communications over TCP/IP networks.

P

PLC

programmable logic controller. The PLC is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. PLCs are computers suited to survive the harsh conditions of the industrial environment.

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.

R

RIO network

An Ethernet-based network that contains 3 types of RIO devices: a local rack, an RIO drop, and a ConneXium extended dual-ring switch (DRS). Distributed equipment may also participate in an RIO network via connection to DRSs or BMENOS0300 network option switch modules.

router

A router device connects two or more sections of a network and allows information to flow between them. A router examines every packet it receives and decides whether to block the packet from the rest of the network or transmit it. The router attempts to send the packet through the network on an efficient path.

S

SNMP

(*simple network management protocol*) Protocol used in network management systems to monitor network-attached devices. The protocol is part of the internet protocol suite (IP) as defined by the internet engineering task force (IETF), which consists of network management guidelines, including an application layer protocol, a database schema, and a set of data objects.

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.

SNTP
(*simple network time protocol*) See NTP.

SOE
(*sequence of events*) SOE software helps users understand a chain of occurrences that can lead to unsafe process conditions and possible shutdowns. SOEs can be critical to resolving or preventing such conditions.

subnet
The subnet is that portion of the network that shares a network address with the other parts of the network. A subnet may be physically or logically independent from the rest of the network. A part of an Internet address called a subnet number, which is ignored in IP routing, distinguishes the subnet.

subnet mask
The subnet mask is a bit mask that identifies or determines which bits in an IP address correspond to the network address and which correspond to the subnet portions of the address. The subnet mask comprises the network address plus the bits reserved for identifying the subnetwork.

switch
A network switch connects two or more separate network segments and allows traffic to be passed between them. A switch determines whether a frame should be blocked or transmitted based on its destination address.

T

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

UDP
user datagram protocol. UDP is an Internet communications protocol defined by IETF RFC 768. This protocol facilitates the direct transmission of datagrams on IP networks. UDP/IP messages do not expect a response, and are therefore ideal for applications in which dropped packets do not require retransmission (such as streaming video and networks that demand real-time performance).

Index

E

F

G

I

L

M

N

O

P

R

S

T

W