BMENOR2200H

Modicon X80 Advanced RTU Module

User Manual

Original instructions

PHA90072.06
07/2026

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric and its subsidiaries referred to in this document are the property of Schneider Electric or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

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.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Table of Contents 3
Safety Information 7
Before You Begin 8
Start-up and Test 9
Operation and Adjustments 9
About the Document 10
Introducing BMENOR2200H, the Modicon X80 Advanced RTU Module 14
Introduction 14
Physical Description 18
Module LED Indicators 23
SD Memory Card (BMXRMS004GPF) 26
Cyber Security Rotary Switch 28
Backplane Connector 30
Electrical Characteristics 32
Standards and Certifications 32
Safety Standards and Certifications 33
The BMENOR2200H Module in Networks 34
Standalone Networks 34
Standalone M580 Architectures 34
Standalone Network with One Subnet 35
Standalone Network with Two Subnets 36
Standalone Network with Link Redundancy 37
Standalone Network with Three Subnets 38
Isolated Network under Standalone Controller 39
Segmented Networks 40
Redundant M580 Networks 41
Introduction 41
Redundant Architecture with One Subnet 42
Redundant Architecture with Isolated Network 44
Hardware Installation 45
Mounting the Module on the Rack 45
Ethernet Communications 52
Ethernet Services 52
Available Ethernet Services 52
SNMP Service 53
SNMP Overview 53
SNMP Communication 54
SNMP Versions 55
SNMP Agent Details 56
SNMP Operations Example 57
MIB Support 58
Firmware Upgrade 59
EcoStruxure™ Automation Device Maintenance Tool 59
FDR Client Basic Service 60
FDR Client Basic Service 60
Modbus TCP Messaging 61

Data Access 61
Data Exchange 61
Ping Function 63
How to Work with RTU Protocols 64
Communication Protocols 64
IEC60870-5-101/104 Protocols 65
IEC60870-5-101/104 Supported Data Types 70
IEC60870-5-101/104 Features 72
DNP3 Protocol 74
DNP3 Supported Data Types 76
DNP3 Features 78
DNP3 Secure Authentication Concepts 80
Clock Synchronization 82
Clock Synchronization with the RTU Protocol 82
Clock Synchronization with SNTP 83
Clock Synchronization with the Controller 84
Events Management 85
Introduction to Event Management 85
Event Routing 87
Event Backup 90
RTU Protocol Data Flow 91
RTU Communications 91
Connection Status 93
Connection Status 93
Reset Communication 94
Hot Standby Capacity 95
Hot Standby Capacity 95
Managing Ethernet Services 99
Sequence Of Events 100
Time Stamp Sequence of Events 100
Configuring the Module 104
Configuration Overview 104
Configuration Components 104
Use the Module in a Control Expert Project 105
Add the DTM and Module to Control Expert 105
About the Control Expert DTM Browser 106
Add the Module to a Project 109
Configuration with Control Expert 110
IP Address Configuration 110
Debugging with Control Expert 111
Module Debugging Screen 111
Configuration in the DTM 112
Access the DTM 112
DNP3 Channel Configuration 114
DNP3 Device Configuration 119
DNP3 Data Object Mapping 123
DNP3 Events 136
IEC60870 Channel Configuration 137
IEC60870 Session/Device Configuration 141
IEC60870 Data Object Mapping 146

IEC60870 Events 154
SNMP Configuration 155
Network Time Service Configuration 157
Control Ports Configuration 161
Export and Import .xml Files with the DTM 163
Module Information in the DTM 165
Data Logging 166
About Data Logging 166
Before You Begin 167
Data Logging Control Expert Configuration 167
Web Page and Device DDT Diagnostics 176
Web Page Access 176
Web Page Diagnostics 178
Web Page Diagnostics 178
Module Diagnostics 179
Connected Device Diagnostics 183
Service Diagnostics 184
Device DDT Diagnostics 188
Device DDT Structure 188
Device DDT Diagnostics 190
File Explorer 194
Data Logging 194
Module Log 196
Cyber Security Configuration 197
Introduction to Cyber Security Web Pages 197
Setup Web Pages 198
User Account Policy Web Page 199
Event Logs Web Page 200
Network Services Web Page 201
Security Banner Web Page 202
HSBY Web Page 203
SNMP Web Page 204
Certificates Management 205
PKI Configuration Web Page 207
Trust List Management Web Page 211
Root CA Management Web Page 212
DNP3 Key Management Web Page 213
DNP3 Client Configuration Web Page 215
DNP3 Server Configuration Web Page 216
DNP3 Secure Authentication Setup 217
IEC60870 Client and Server Web Pages 219
IEEE 802.1x Authentication 220
ACL Configuration 222
Forwarding and NAT 224
User Management Web Page 226
Configuration Management Web Page 227
RBAC 229
Appendices 230
Interoperability 230
DNP3 Interoperability 231

IEC60870-5-104 Interoperability 248
IEC60870-5-101 Server and Client Device Profiles 266
Project Migration 276
XML File Migration 276
DNP3 Data Type Migration 277
IEC60870 Data Type Migration 280
Logged Events 285
Modbus Diagnostic Codes 286
Data Mapping for Modbus Function Code 3 with Unit ID 100 286
Detected Error Codes 318
Explicit Messaging: Communication and Operation Reports 318
Detected Error Codes for RTU Communication 320
Detected Error Codes for Open SSL/TLS 321
Detected Error Codes for Open SSL/TLS 321
Firmware Version Compatibility 329
Firmware Version Compatibility 329
Application Update from BMENOR2200.2 329
Glossary 331

Safety Information

Important Information

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 are 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:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- 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 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 Document

Document Scope

This guide describes the Modicon X80 BMENOR2200H advanced remote terminal unit (RTU) module and its relationship to Modicon M580 controllers and X80 remote platforms.

The BMENOR2200H module acts as a communication module on an M580 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.

This guide describes the following topics:

- installation, page 45
- configuration, page 104
- embedded web pages, page 176
- diagnostics, page 176

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 has been updated for the release of EcoStruxure Control Expert 16.4.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Product Related Information

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.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Follow all local and national safety codes and standards.

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

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the Cybersecurity Best Practices document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity posture.
  - Learn more about cybersecurity in the cybersecurity academy.
  - Explore the cybersecurity services from Schneider Electric.

Environmental Data

For product compliance and environmental information, refer to the Schneider Electric Environmental Data Program.

Available Languages of the Document

The document is available in these languages:

- English (PHA90072)
- French (EIO0000004870)
- German (EIO0000004871)
- Italian (EIO0000004872)
- Spanish (EIO0000004873)
- Chinese (EIO0000004874)

Related Documents

Title of documentation	Reference number
Cybersecurity Best Practices	Refer to General Cybersecurity Information, page 11 .
Modicon M580 Frequently Used Architectures System Guide	HRB62666 (ENG) HRB65318 (FRE) HRB65319 (GER) HRB65320 (ITA) HRB65321 (SPA) HRB65322 (CHS)
Modicon M580 System Planning Guide for Complex Topologies	NHA58892 (English), NHA58893 (French), NHA58894 (German), NHA58895 (Italian), NHA58896 (Spanish), NHA58897 (Chinese)

Title of documentation	Reference number
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)
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 Racks and Power Supplies, Hardware, Reference Manual	EIO0000002626 (English), EIO0000002627 (French), EIO0000002628 (German), EIO0000002630 (Italian), EIO0000002629 (Spanish), EIO0000002631 (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)
Electrical installation guide	EIGED306001EN (English)
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	35014793 (English), 35014792 (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)
Modicon X80 - BMXNOR0200H RTU Module, User Manual	EIO0000000505 (English), EIO0000000507 (French), EIO0000000506 (German), EIO0000000509 (Italian), EIO0000000508 (Spanish)

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Introducing BMENOR2200H, the Modicon X80 Advanced RTU Module

Introduction

Overview

RTU systems are designed to meet the needs of the water industry, the oil and gas sector, transportation, electrical utility and other infrastructures.

DNP3, IEC60870-5-101, and IEC60870-5-104 are global SCADA protocols, which are designed with various characteristics for RTU utilities (example: response event without request (unsolicited)).

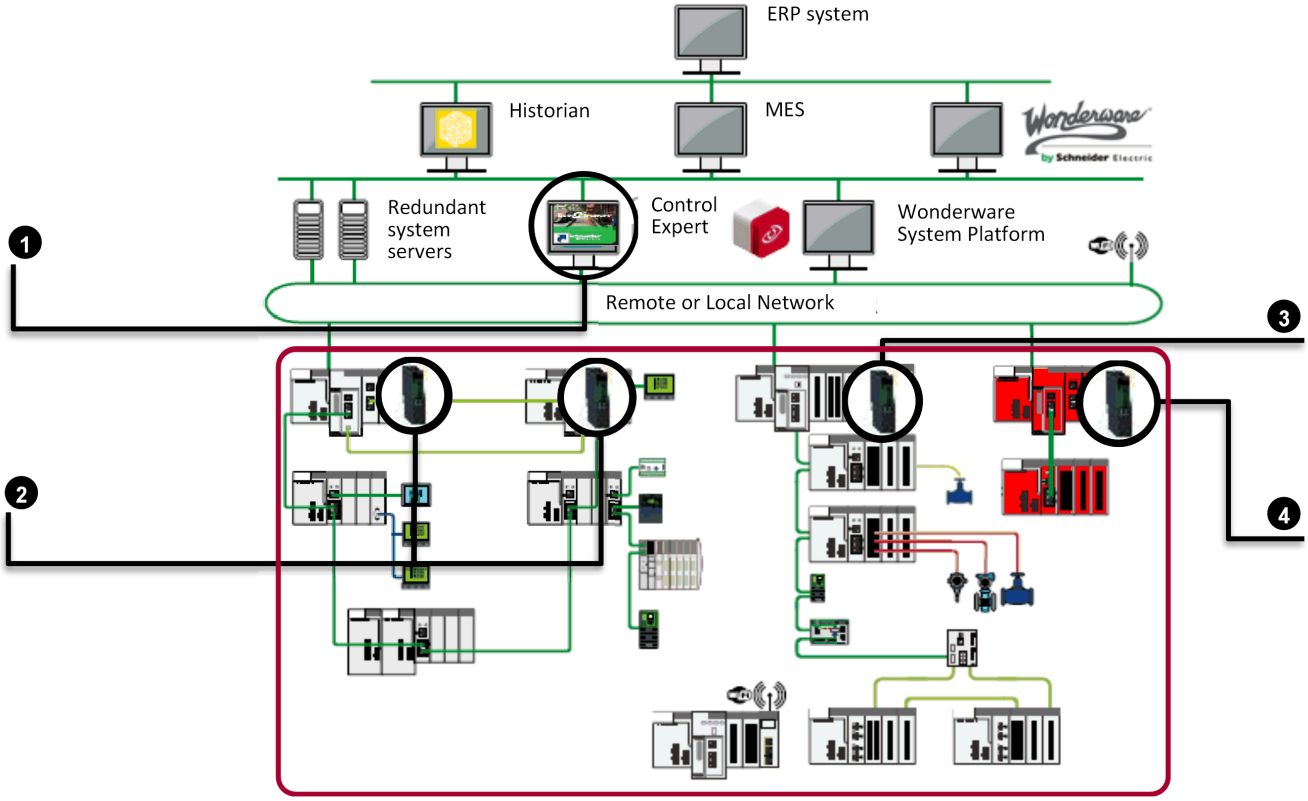
The Modicon X80 advanced RTU module (BMENOR2200H) is the new module on the Modicon M580 platform. You can configure this module for multiple Ethernet-based services, including RTU server and client implementation in a single module while supporting Ethernet and serial (ferrule) cable connections. Especially, the advanced RTU module supports M580 Hot standby systems and implements cybersecurity functions.

The module can operate properly only on a BME (X Bus and Ethernet) backplane.

NOTICE
INOPERABLE RACK CONNECTION Do not mount the BMENOR2200H module on an BMX (X Bus-only) backplane. **Failure to follow these instructions can result in equipment damage.**

For rack descriptions and slot restrictions, refer to the Modicon X80 Racks Installation chapter in *Modicon X80 Racks and Power Supplies, Hardware, Reference Manual* (Related Documents, page 11).

The BMENOR2200H advanced RTU module brings DNP3, IEC60870-5-101, and IEC60870-5-104 communications to the Modicon M580 platform:



Telemetry & Remote Architecture

1 Software: EcoStruxure Control Expert (Engineering tool), Automation Device Maintenance (firmware upgrade tool), Web Browser (diagnostic and cybersecurity settings)

2 BMENOR2200H module: M580 Hot Standby

3 BMENOR2200H module: M580 standalone

4 BMENOR2200H module: M580 Safety standalone, M580 Safety Hot Standby, non-interfering type 1

> **NOTE:** Before using the BMENOR2200H module, which is a non-interfering module, within a Modicon M580 Functional Safety project, you must verify the TÜV certification status: Go to https://www.certipedia.com/, search *M580*, and then select *SCHNEIDER ELECTRIC* certificate.

Red line Indicates the telemetry and remote architecture.

Compared with standard X80 communications and I/O modules, the BMENOR2200H module is a *long-factor* module, the same height as the controller. (Refer to the module dimensions topic, page 19.)

Install the 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 controller and communication modules that may be installed on the local rack.

Main Features and Functionality

Module Features

The BMENOR2200H module addresses telemetry requirements:

- Upstream communications with SCADA client stations for polling interrogation of data, backfilling of time-stamped event data, and receiving client commands.
- Downstream communications with other RTU substations, server field devices and IEDs (for data collection), sending commands, and synchronizing distributed control.
- Ruggedized with conformal coating for operations in extended operating temperature ranges and harsh environments.
- RTU protocol event routing as data concentrator.
- DNP3 (Serial and NET) level 3, IEC60870-5-101, IEC60870-5-104. Protocols are certified by third-party agencies.
- Remote programming and downloading of control program with Control Expert software through the BMENOR2200H module (The file transfer to the controller is via X Bus when the Modbus service is enabled.)
- Remote cybersecurity settings and diagnostic monitoring with a built-in web server.
- Compatibility with an M580 Hot Standby systems.
- Reset RTU communication by variable.
- Bulk configuration (Excel/CSV file) for RTU mapping table.
- Cybersecurity enhancements:
  - Secure boot
  - Firmware signing and integrity check
  - Help secure firmware upgrade
  - HTTPS-based Web pages
  - RBAC for Web page access
  - TLS for RTU protocols (DNP3 NET, IEC60870-5-104)
  - Password complexity
  - Cybersecurity mode selection with the rotary switch
  - DNP3 more secure authentication versions SAv2 and SAv5
  - Help secure Hot Standby communication between modules
  - Achilles Level 2
  - DNP3 Secure Authentification qualified by third-part agency
  - IEEE 802.1x supplicant
  - Access Control List (ACL)
- High data throughput capacity when the module acts as an RTU server (transmits 4,000 events/second to client devices throughEthernet).
- Maximum of 300,000 RTU events stored in module buffer.
- Up to 4GB storage size (in SD card) for data logging.
- SNMPv1 and SNMPv3.
- Time synchronization from SNTP, RTU protocol, or controller.
- Local Modbus TCP Server (module diagnostic purpose)/ Client.
- PING
- Module log
- IP Forwarding/NAPT

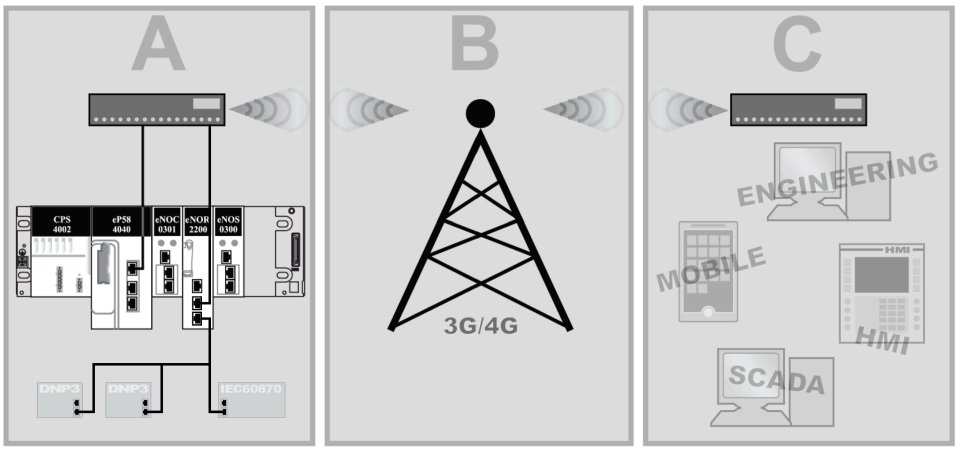
Platform Features

The module shares these characteristics and applications that are available in an M580 environment:

- Flexible Ethernet access through front ports and/or backplane
- Easy connectivity with an Ethernet backplane
- Specialized function blocks (AGA, flow calculations)
- Expandable rack-based modular I/O configurations and remote I/O capabilities
- High-density, analog/discrete I/O and counting modules
- Isolated input power supply (voltage ranges: 24 Vdc, 24/48 Vdc, 125 Vdc, 100/240 Vac)
- Local and remote downloading of operating system firmware
- Exclusive data exchange bandwidth for each module installed on the same rack

RTU Architecture

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



A A BMENOR2200H module communicates over the backplane Ethernet port and/or the front control ports with a controller 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™

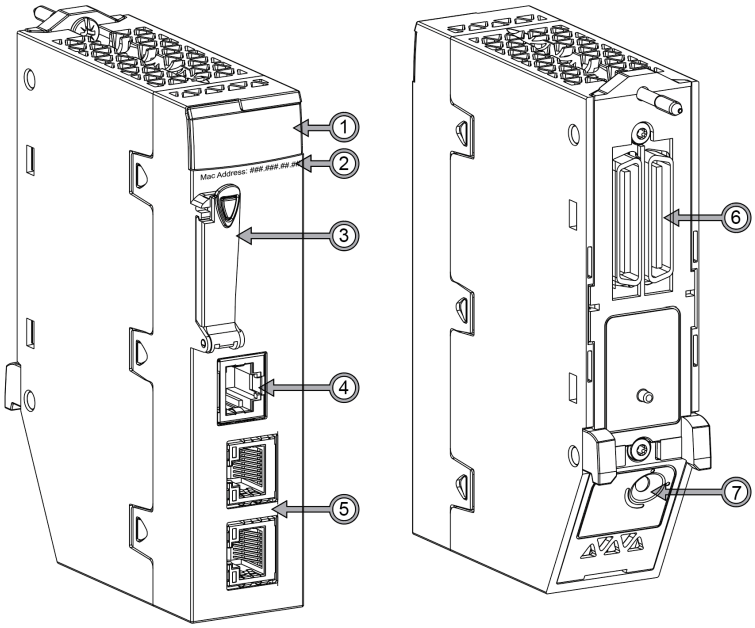
EcoStruxure™ is a Schneider Electric program designed to address the key challenges of many different types of users, including plant managers, operations managers, engineers, maintenance teams, and operators, by delivering a system that is scalable, flexible, integrated, and collaborative.

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:



NOTE: There is no front enterer ports on PV<04. In control expert, using BMENOR2200H.2 for old version and BMENOR2200H.3 for new version.

Legend:

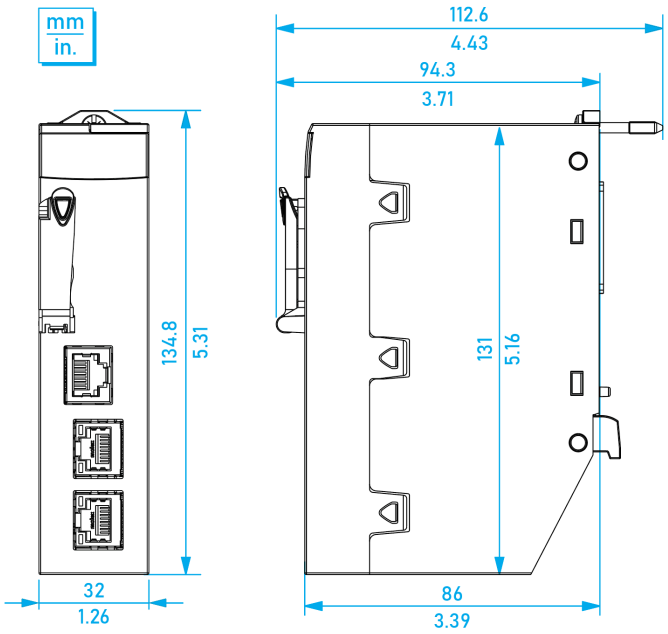
Item	Description	Function
1	LED array, page 23	Observe the LED display to diagnose the module.
2	MAC address	This manufacturer-defined address (front control ports) is unique for each individual module
3	memory card slot	Store data logging files (.csv) to the SD card.
4	serial port	This port is an isolated RS232/RS485 serial connector. Use a TCSXCN3M4F3S4 (ferrule) cable (serial link) to connect the module's serial (RS232) RJ45 port to a communication port on a modem. It supports all pins on the modem's nine-pin D-sub connector except for the ring indicator (RI) signal pin (sold separately).
5	control ports	Two RJ45 control ports with below characteristics: 1. Transmission rate: 1 Gbit/s,100 Mbit/s,10 Mbit/s (configurable) 2. Port(s) Enable/Disable is allowed 3. Share same IP address (like two ports on the switch) 4. Operating speed up to 1 Gb/s. When operating at the speed of: • 1 Gb/s, use only CAT6 copper shielded twisted four-pair cables. • 10/100 Mb/s, use CAT5e or CAT6 copper shielded twisted four-pair cables. **NOTE:** There is no link redundant protocols (RSTP, PRP, etc.) on these two ports. When enabling all control ports and getting connected to network, verify the network topology design to help avoid network loop issues and abnormal module behaviors.

Item	Description	Function
6	dual-bus backplane connector, page 30	This connection to the Modicon M580 rack supports Ethernet and X Bus communications.
7	rotary switch, page 28	Use this switch to set the cyber security level for the module.

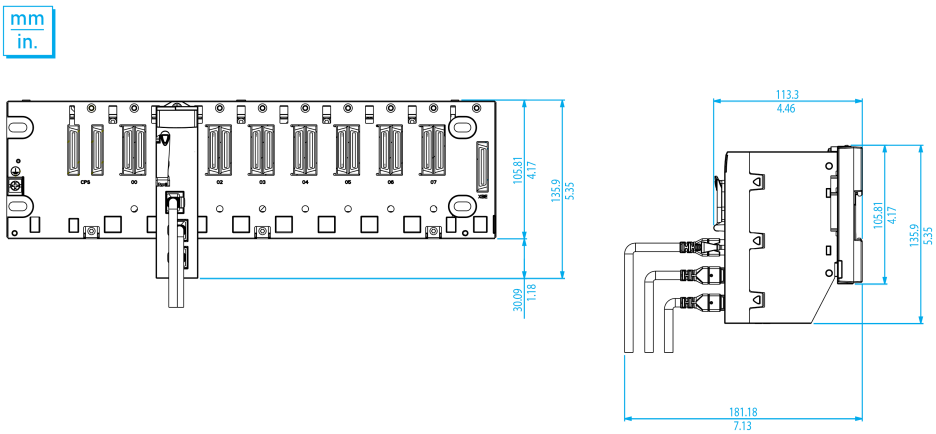
NOTE: A ferule placed on the end of the serial port reduces the pinching of the cable by the removable cover. This reduces the risk of degrading the quality of the link by decreasing the likelihood of achieving the maximum bending radius of the cable.

Dimensions

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



Module mounted on rack:



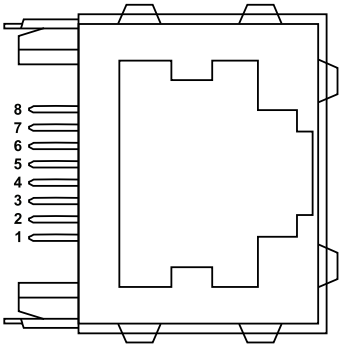
Serial Port

The BMENOR2200H module has a built-in serial port that supports either serial communications through a serial link.

This table describes the serial communication channels:

Characteristic	Description
supported protocols	RTU protocols: • IEC60870-5-101 • DNP3 serial
connection	RJ45 socket
physical link	• RS485 isolated serial link • RS232 isolated serial link

Serial port pins:



Pinout (functionality):

Pin	Signal	Pin	Signal
1	RXD	5	D0/DSR
2	TXD	6	CTS
3	RTS	7	DCD
4	D1/DTR	8	common
shielding			

The RJ45 connector has eight pins. The pins used differ according to the physical link used.

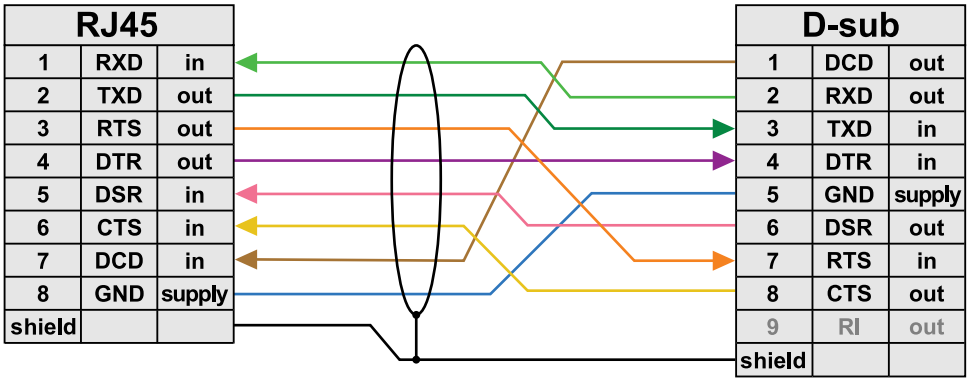
The RS 232 serial link uses these pins:

- *pin 1:* RXD signal
- *pin 2:* TXD signal
- *pin 3:* RTS signal
- *pin 4:* DTR signal
- *pin 5:* DSR signal
- *pin 6:* CTS signal

The TCS MCN 3M4F3C2 serial crossover (ferrule) cable has two connectors:

- RJ45 male
- Nine-pin SUB-D female

These are the pin assignments between an RJ45 plug and a 9–pin SUB-D socket for a TCSMCN3M4F3C2 serial crossover (ferrule) cable:



The RS 485 serial link uses these pins:

- *pin 4:* D1 signal
- *pin 5:* D0 signal

The serial link uses these pins as described here:

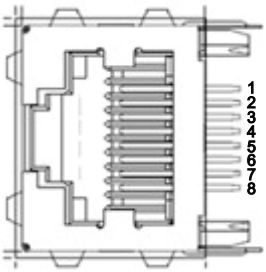
- *pin 7:* not connected

  pin 8: common of the network power supply (0 V)

  NOTE: The RS232 four-wire, RS485 two-wire, and RS 485 two-wire and power-supply (ferrule) cables use the same RJ45 male connector.

Control Ports

The BMENOR2200H module has two Ethernet RJ45 ports on front face.



This table describes ETH Port Pins definition:

Pin	Definition	ETH Port
1	TX_D1+	Tranceive Data+
2	TX_D1-	Tranceive Data-
3	RX_D2+	Receive Data+
4	BI_D3+	Bi-directional Data+
5	BI_D3-	Bi-directional Data-
6	RX_D2-	Receive Data-
7	BI_D4+	Bi-directional Data+
8	BI_D4-	Bi-directional Data-

ETH port isolation voltage level is 2000 VDC.

This list below shows the line speeds that are available for the BMENOR2200H module:

- 1000 Mb in full duplex
- 100 Mb in half duplex

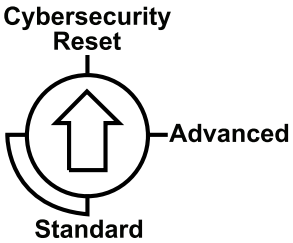
- 100 Mb in full duplex
- 10 Mb in half duplex
- 10 Mb in full duplex

Characteristics of speed adaptation include:

- Auto-negotiation allows the BMENOR2200H module to quickly adapt itself to the local Ethernet switch's speed and duplex mode.
- The negotiated speed between two Ethernet devices is limited to the speed of the slower device.
- The module supports Auto MDIX, prefers MDI here.

Rotary Switch

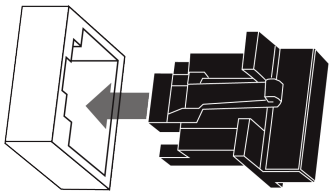
A three-position rotary switch is located on the back of the module. Set this switch to configure a cyber security operating mode for the module:



Refer to the detailed description of the cyber security rotary switch, page 28.

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, page 28.

Module LED Indicators

Introduction

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

- BMENOR2200H module LEDs (below)
- SD card LEDs, page 26

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)
- Ethernet network communications
- RTU communications
- SD memory card state
- serial communications
- cyber security mode

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)

NOTE: There is no NS/BS/RTUCNX LED on the module PV<04.

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.)
ERR: detected error	red	on	• The processor, system, or configuration detected an error. • If you move the rotary switch from **Standard > Advanced** (or vice versa) directly instead of moving to **Cybersecurity Reset** in between, an error is detected: Missing Cybersecurity Reset, page 25
		flashing	• The module is not configured. (The application is absent, invalid, or incompatible.) • The module is blocked by a detected software error. • A Hot Standby problem is detected.
		off	Operations are normal (no detected errors).
DL: download firmware (upgrade)	red	on	A firmware upgrade or factory reset is in progress.
		off	A firmware upgrade or factory reset is not in progress.
NS: control port status	green	on	One of the two control ports is enabled and linked successfully.
	red	on	There is duplicated IP on the backplane Ethernet port or the factory reset mode.
	—	off	There is no link on the two control ports.
RTUCNX: RTU connection status	green	on	At least one RTU connection (Client or Server) established in the module.
		flashing	There is no RTU connection.
BS: backplane Ethernet port status	green	on	Link is successfully connected on the backplane Ethernet port.
	red	on	There is duplicated IP on the backplane Ethernet port or the factory reset mode.
CARD ERR: memory card detected error	red	on	• The data logging service is enabled, but the memory card is missing. • The data logging service is enabled, but the memory card is not usable (for example, bad format, unrecognized type, etc.).
		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: communication security status	green	on	The selected communication security level is enabled and running fine.
	red	on	• Communications are *not* secure because a critical error in communication security 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 client or server.
		flashing	The selected communication security level is enabled and running, but a critical error is detected. For example, there is no available security configuration, or the certificate expired when the communications stopped.
	—	off	The cybersecurity function is not enabled.

Typical Status and Related LED Behavior

Label	Pattern	Indication
ERR	Red on	Missing Cybersecurity Reset: The rotary switch was moved directly between **Standard** mode and **Advanced** mode. A factory reset is required before switch to alternative mode.
DL		
BS		
NS		
SEC		

Module status	LED	Description
Factory mode	RUN: green on	–
	DL: red on DL: red off	Factory reset is ongoing. Factory reset is complete.
	BS: red on	–
	NS: red on	–
Initial cybersecurity mode (first-time start up without valid cybersecurity setting)	ERR: red flashing	Module is not running; a validated cybersecure setting is required.
	BS: green flashing	
	SEC: red on	

LEDs on Control Ports

There are two LEDs on each RJ45 port. One is ACT (Active) and another is LNK (Link). The two LEDs can be used to diagnose the state of Ethernet communications over the control ports:

- The ACT LED indicates the presence of Ethernet activity on the port.
- The LNK LED indicates the existence of an Ethernet link and the link speed.

LED	State	Description
ACT	green	Link established, no activity.
	green flashing	Link established, activity detected.
	off	No link established.
LNK	green	Link established at speed equal to module maximum capability (1000Mbps).
	yellow	Link established at speed less than module maximum capability (10/100Mbps).
	off	No link established.

SD Memory Card (BMXRMS004GPF)

Introduction

You can use a BMXRMS004GPF memory card with this module to facilitate some services. (for example, the data logging feature.)

NOTE: The BMENOR2200H module is only compatible with the BMXRMS004GPF memory card which is specifically formatted with Schneider Electric. The BMXRMS004GPF memory card is an optional purchase. It is not shipped with the module.

Location

The slot for the secure digital (SD) memory card (BMXRMS004GPF) is on the front of the module.

The insertion of the SD card during module operations is not recommended. In this case, the module may not recognize the card.

⚠WARNING

RISK OF LOST APPLICATION

- Do not remove the memory card from the module while the PLC is running.
- Do not insert a SD card during module operation.
- Remove the memory card only when the power is off.

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

Card Functionality

This table describes the functionality of the BMXRMS004GPF memory card when inserted into the module:

SD Memory Card	Data Storage	Functionality
BMXRMS004GPF	4 GB	Storage of data logging files (.csv)

LED Indicators

An LED is associated with the memory card slot. It displays the status of data exchange with the card:

- *on:* The SD card is available and recognized.
- *off:* The SD card is not available or the data logging feature is not enabled.

Card Services

NOTICE

INOPERABLE MEMORY CARD

- Do not format the memory card with a non-Schneider tool.
- Do not use a write-protected memory card with the module.

Failure to follow these instructions can result in equipment damage.

The memory card needs a structure to contain program and data. Formatting with another tool destroys this structure.

Some services do not operate properly when the memory card is write-protected.

Precautions

NOTICE

MEMORY CARD DESTRUCTION

- Do not touch the memory card connections.
- Keep the memory card away from electrostatic and electromagnetic sources as well as heat, sunlight, water, and moisture.
- Avoid impacts to the memory card.
- Verify the postal service security policy before sending a memory card by postal service.

Failure to follow these instructions can result in equipment damage.

In some countries, the postal service exposes mail to high levels of radiation as a security measure. These high levels of radiation may erase the contents of the memory card and render it unusable.

Without SD Memory Card

If the memory card slot is empty during the power-up, the module can operate normally without the data logging service.

Cyber Security Rotary Switch

Introduction

NOTICE

RISK OF UNINTENDED OPERATION

Do not use a metal screwdriver.

Failure to follow these instructions can result in equipment damage.

To maintain the integrity of the hardware, use only the small, plastic screwdriver that ships with the module to change the switch position.

The use of a metal screwdriver can damage the switch and render it inoperable.

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.

Position Selection

NOTICE

RISK OF UNINTENDED OPERATION

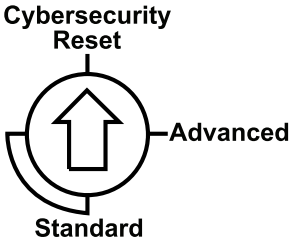
Set the switch only to the exact “clock position” that corresponds to your security configuration.

Failure to follow these instructions can result in equipment damage.

The following “clock positions” are enabled to set the switch:

- *12 o’clock:* **Cybersecurity Reset**
- *3 o’clock:* **Advanced**
- *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.)

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
Advanced	Advanced mode on	The module supports some level(s) of cyber security when a cyber security configuration is available.
Standard	standard mode on	The module supports a basic level of cyber security.
Cybersecurity Reset	factory reset	The module implements its out-of-the-box cyber security configuration.

Set the Switch

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

Step	Action
1	Remove the module from the rack: *a.* Verify that the module power is OFF. *b.* Loosen the locating pins at the rear of the module (on the bottom part) in the corresponding slots in the rack. *c.* Swivel the module toward the bottom of the rack to lift the module off the rack.
2	Change the switch setting to **Cybersecurity Reset**.
3	Re-insert the module in the rack to power it up in **Cybersecurity Reset** mode. **Result**: The module performs a factory reset and is properly powered when the RUN LED is steady green.
4	Remove the module from the rack again.
5	Change the switch setting to **Advanced** or **Standard**.
6	Re-insert the module in the rack to power it up in the selected (**Advanced** or **Standard**) mode. **Result**: The module is properly powered when the LED is steady green for both advanced and standard modes.

NOTE:

- If you move the rotary switch from the standard configuration (**Standard**) directly to the secure configuration (**Advanced**) or vice-versa, an error is detected.
  - Always power up the module with the rotary switch in the **Cybersecurity Reset** position when you transition between the **Standard** and **Advanced** modes to implement normal operations.
  - You can also use the **Management** dialog on the **Setup** web page to move the rotary switch to clean all cybersecurity configuration. Click the **Cybersecurity Reset** button to restore the factory default cyber security settings for the module. A module restart is required.
- The changes associated with the switch settings take effect after the module is re-inserted in the rack and powered up.

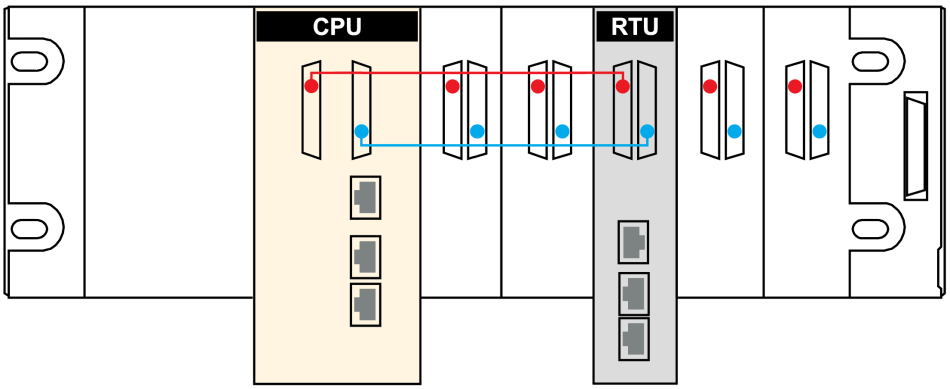
Backplane Connector

About Dual-Bus Backplanes

The dual-bus interface 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 controller) implement both the Ethernet (red line) and X-Bus (blue line) protocols:



Red The red dot/line indicates Ethernet.

Blue The blue dot/line indicates X Bus.

NOTE:

- BMXXBP••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* (Related Documents, page 11).

Connection Protocols

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

Bus	Description
X Bus	The module uses X Bus communications to obtain and exchange the following through the controller: • configuration data for the module • application and Device DDT diagnostic data • download the PLC application to the controller via the BMENOR2200H module when the Modbus service is enabled. • variable data exchange between the module and the controller • time synchronization messages to the controller and other modules on the backplane The data exchange uses implicit messaging to facilitate memory sharing between the module and the controller. For each controller scan cycle, the controller publishes all data at the same time to share the most current information with the RTU.
Backplane Ethernet	**NOTE:** The Ethernet backplane port is always enabled for the BMENOR2200H module. Confirm your network topology design to help avoid network loop issues. The module uses Ethernet communications to provide an access path to the BMENOR2200H module for the following: • External devices can talk with the BMENOR2200H module when accessing one of the following: ◦ BMEP58••/BMEH58•• controller ◦ BMENOC03•• communication module ◦ BMENOS0300 network option switch module ◦ BM•CRA312•• adapter ◦ Other Ethernet modules with similar capabilities • The module communicates with Ethernet communication modules on the local rack. • When module is configured as **Ethernet Performance** mode. The following data will be exchanged via the E-bus:: ◦ Application and Device diagnostic data (DDT) ◦ Variable data exchange between module and the controller ◦ Download of the PLC application to the controller through the BMENOR2200H module when the Modbus service is enabled

I/O Data Exchange with the Controller

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

Protocol	Characteristics
• IEC 60870-5-101 • IEC 60870-5-104 • DNP3	Memory consumption: • *input data size:* 8 KB (16 KB in high performance mode) 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. • *output data size:* 8 KB (16 KB in high performance mode) 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. **NOTE:** 1. You can view the memory usage in the Control Expert DTM (**Generation > Module Information > Memory Status**). Refer to the description of the module information in the DTM, page 165. 2. Concerning the maximum input and output sizes, the exact memory consumption depends on the type of data mapping to the controller; different data types consume different amounts of memory. Refer to the project migration appendix, page 276.

NOTE: The **Ethernet High Performance** is only available starting with version BMENOR2200.3 and later.

Minimum MAST Cycle Time

When the data between the Modicon M580 controller and BMENOR2200H module are performed through the Xbus (Ethernet Mode). Use this formula to achieve the recommended minimum MAST task cycle time for a single BMENOR2200H module:

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

The result is approximately a 30ms MAST task cycle with 8 KB in and 8 KB out (16 KB in high performance mode).

When the data between the Modicon M580 controller and the BMENOR2200H module are performed through the Ethernet backplane. Calculate the minimum cycle time required by the MAST cycle duration to correctly perform these exchanges with this formula:

```
Mast Cycle Min (ms) = the greater value between (implicit_data_IN
+ implicit_data_OUT) / 2 and 8ms
```

The formula uses these variables:

- *implicit_data_IN:* This variable represents the size (KB) of implicit data inputs between the controller and all BMENOR2200H scanners (Modbus or EtherNet/IP requests) configured in the application.
- *implicit_data_OUT:* This variable represents the size (KB) of implicit data outputs between the controller and all BMENOR2200H scanners (Modbus or EtherNet/IP requests) configured in the application.

  NOTE: When more than one BMENOR2200H RTU module (or other modules enabling Ethernet High performance mode) is installed, the minimum cycle time is the sum of the cycle times for all modules.

Electrical Characteristics

Consumed Current

This is the current that the BMENOR2200H module consumes:

Power Source	Consumption
24 VDC rack	137 mA
power dissipation	3.3 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

View related documents 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

You can download these technical publications, the present document and other technical information from domestic SE website.

Safety Standards and Certifications

References

Refer to these guidelines from the *Modicon M580 Safety Standards and Certifications* guide (Related Documents, page 11).

- Certificates and Declarations
- Operating and Storage Conditions
- Environment Test Compliance Levels

The BMENOR2200H Module in Networks

Standalone Networks

Standalone M580 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 (ferrule) cable:

- *upstream connection:* Connect the module to a SCADA system through the DNP3, IEC60870-5-101, or IEC60870-5-104 protocols. (A Modbus TCP connection is another option.)
- *downstream connection:* Connect the module to remote server devices and stations through the DNP3, IEC60870-5-101, or IEC60870-5-104 protocols.

Ethernet Connections

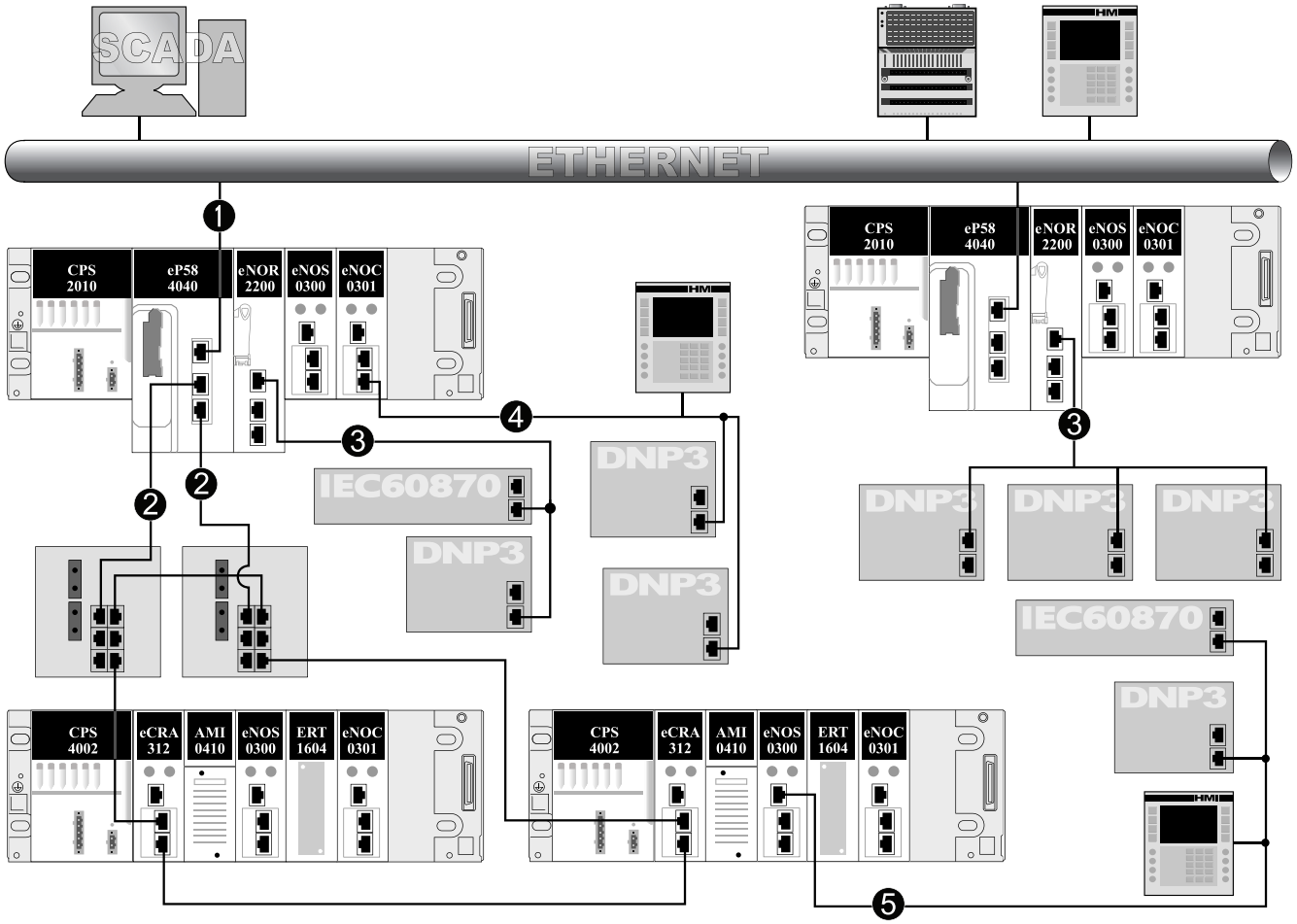
The Ethernet connection can be made either through the control ports on the front of the BMENOR2200H or through an enabled backplane port

- *flat networks:* For these networks, the Ethernet network connections to the BMENOR2200H are achieved through the service port or a BMENOC0301/ BMENOC0311 or a BMENOS0300 module.
- *isolated networks:* For these networks, the Ethernet network connections are achieved through control ports directly. Control ports are physically isolated with backplane port (by 2 MAC address). If the control ports are not enabled, logic isolated network could also be achieved through a BMENOC0321 module with the IP forwarding. The installation of multiple controllers withBMENOR2200H and BMENOC0321 modules required the use of a static routing table for the upstream system.
- *segmented networks (service exposure with **NAT On**):* For these networks, keep inter subnet routing disabled and expose only specific services from internal devices through the control port. For more details, refer to Forwarding and NAT, page 224.

Standalone Network with One Subnet

Sample Network

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



Legend:

1 The service port on the controller connects the RIO main ring and distributed equipment (RTU devices, IEC 60870 devices, HMI) to the Ethernet control network.

2 RIO main ring (Dual-ring switches connect the local rack to an RIO drop.)

3 A BMENOR2200H module has a RS232/RS485 connection to RTU Serial devices.

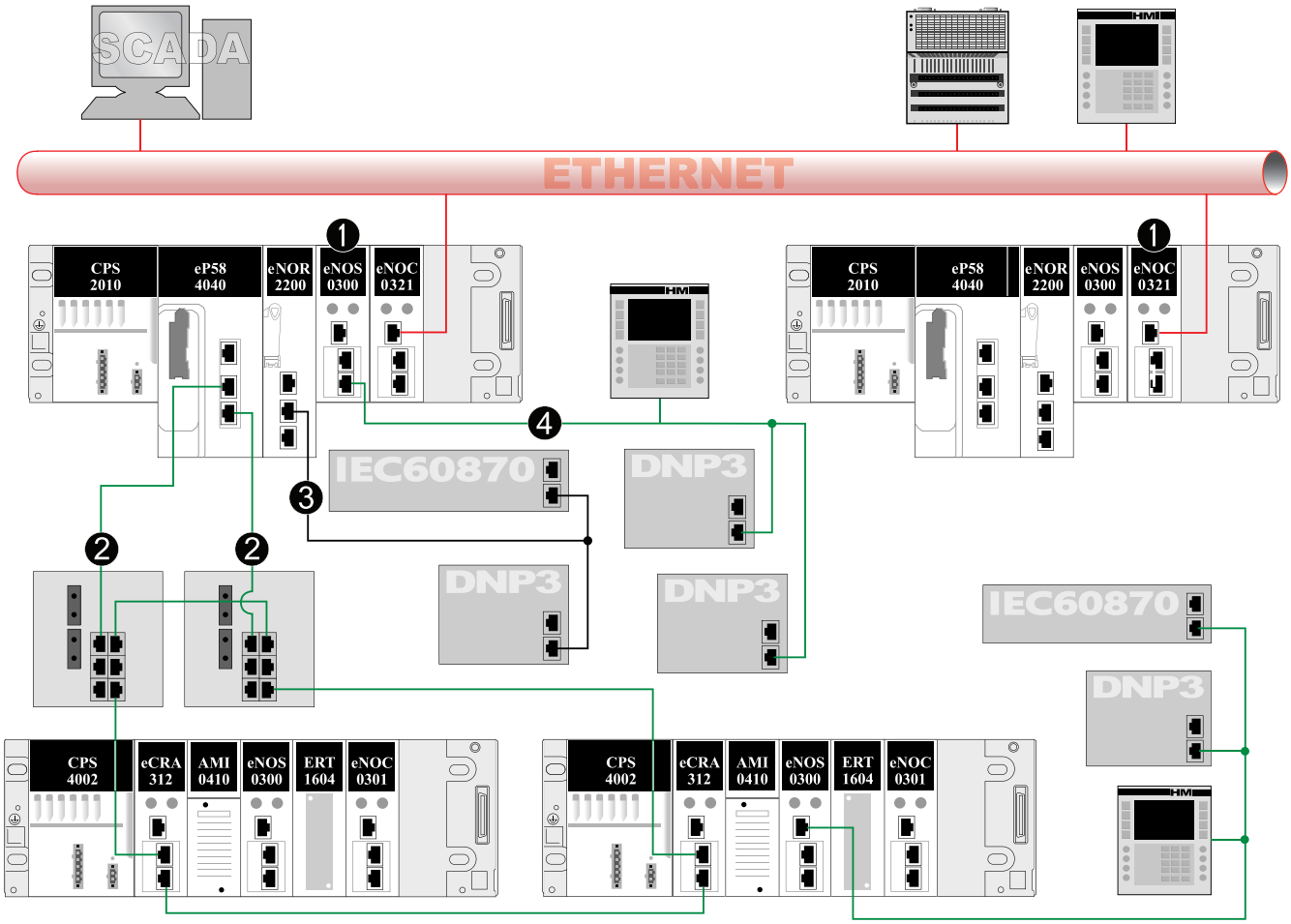
4 A BMENOC0301 module on the local rack connects distributed equipment (RTU devices, IEC 60870 devices, HMI) to the RIO main ring.

5 A BMENOS0300 module on an RIO drop connects distributed equipment (RTU devices, IEC 60870 devices, HMI) to the RIO main ring.

Standalone Network with Two Subnets

Sample Network

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



Legend:

1 BMENOC0321 modules on the local racks connect the RIO main ring and distributed equipment (RTU 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.)

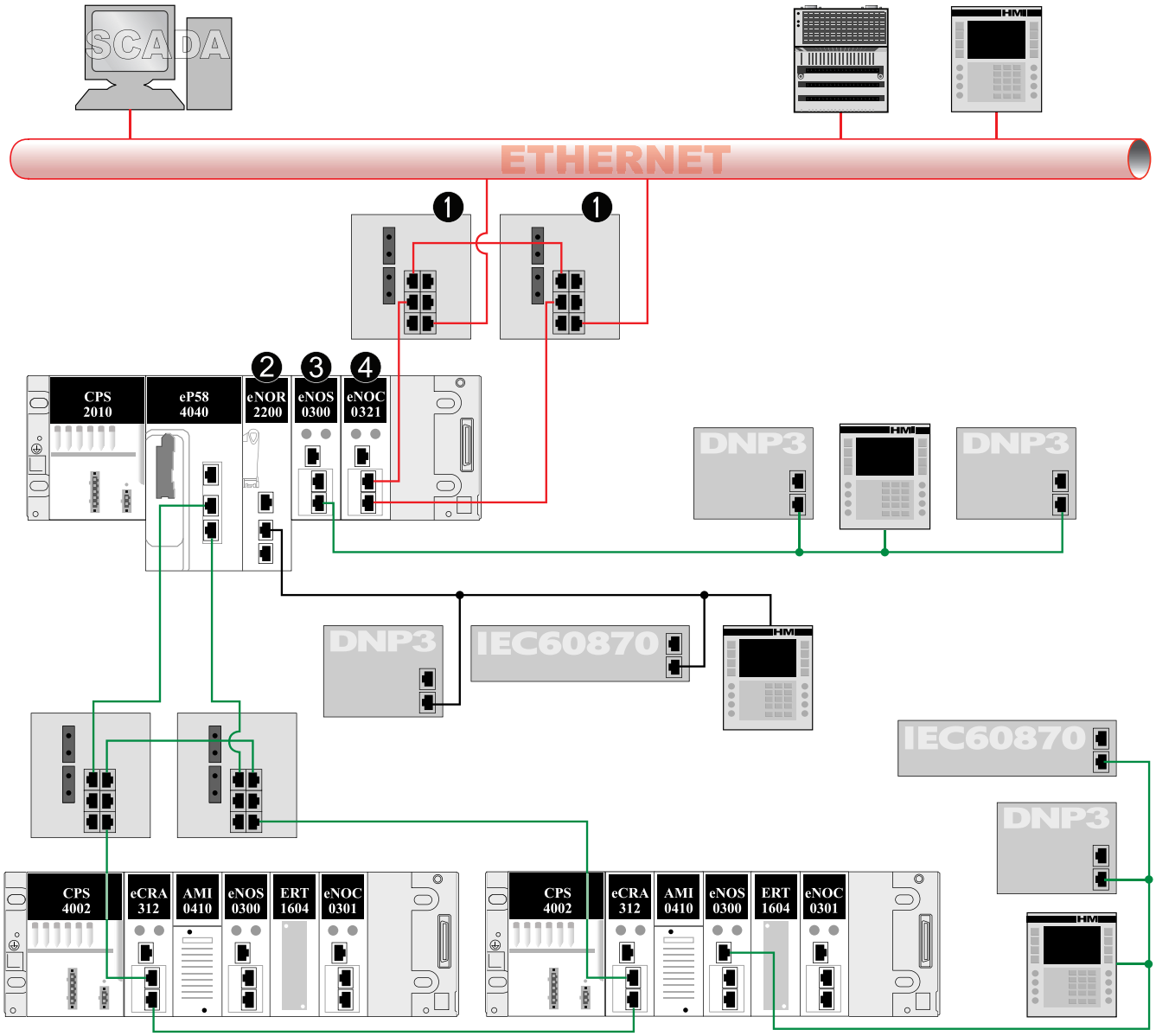
3 A BMENOR2200H module has a direct RS232 connection to a RTU serial device.

4 A BMENOS0300 module on an RIO drop connects distributed equipment (RTU devices) to the RIO main ring.

Standalone Network with Link Redundancy

Sample Network

This sample standalone network builds upon the two-subnet example, 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:



Legend:

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 (RTU devices, HMI) via the control port or serial port.

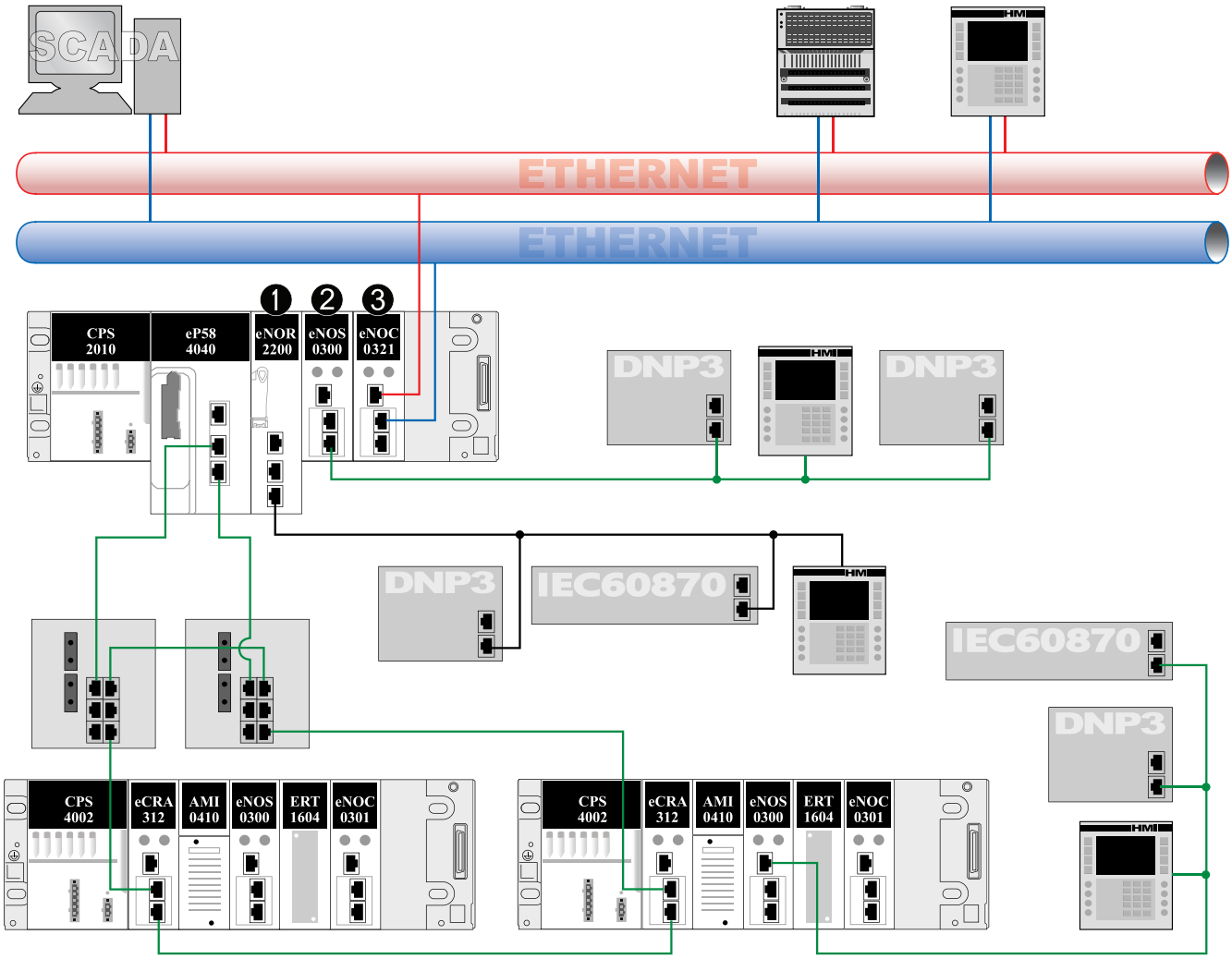
3 A BMENOS0300 embedded switch module connects the local rack to distributed equipment (RTU devices) using redundant links.

4 The service port of a BMENOC0321 module allows distributed equipment (RTU devices, HMI) to communicate with the control network using redundant links.

Standalone Network with Three Subnets

Sample Network

This sample standalone network builds upon the two-subnet example, 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:



Legend:

1 A BMENOR2200H module connects the local rack to distributed equipment (RTU devices, HMI) via the control ports or serial port.

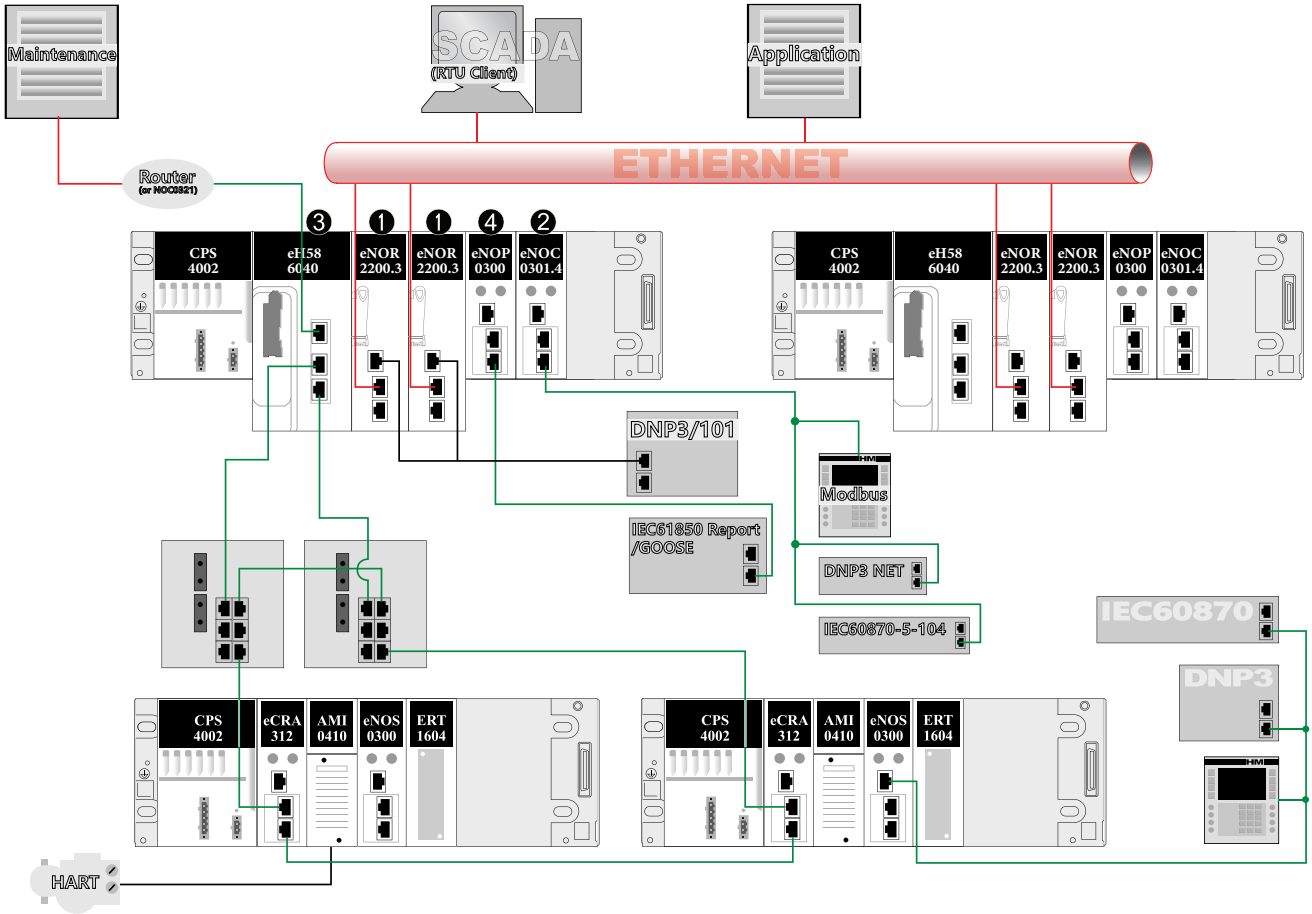
2 BMENOS0300 modules on the local racks connect distributed equipment (DNP3/IEC60870 devices, HMI) to the RIO main rings using redundant links

3 BMENOC0321 modules with IP forwarding enabled connect the RIO main rings and distributed equipment (DNP3/IEC60870 devices, HMI) to the blue network via the service port and the red network through the control network port using redundant links

Isolated Network under Standalone Controller

Sample Network

This sample isolated standalone network includes BMENOR2200H module on local racks. The BMENOR2200H module provides two different isolated subnets for control network (red) and backplane network (green).



Legend:

1 A BMENOR2200H module connects the upstream equipment (for example, the SCADA) via control port and connects the local rack to other ethernet devices (RTU devices, HMI) via the Ethernet backplane port or serial port.

2 BMENOC0301 modules on the local racks connect distributed equipment (RTU devices, Modbus devices, HMI).

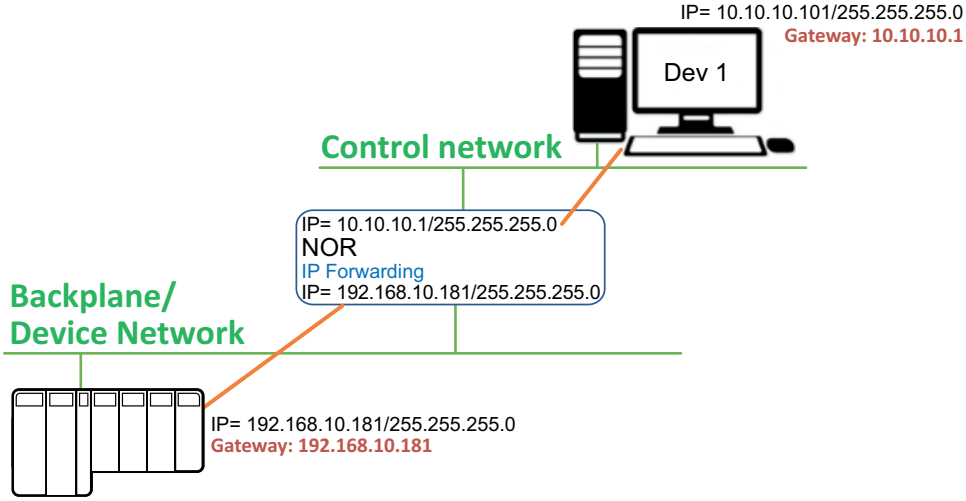
3 Network access to controller for Engineering/Maintenance application (Control Expert, Firmware upgrade tool etc.)

4 BMENOP0300 modules on the local racks connect IEC61850 devices (Server or Client).

Segmented Networks

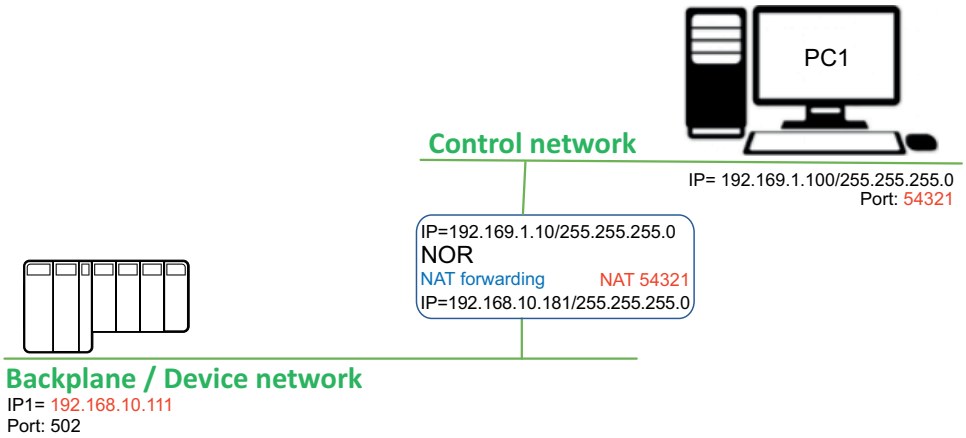
IP Forwarding

This sample segmented network builds upon the two-subnet example with distinct control and device networks. In this case, the BMENOR2200H module is configured with one interface in the control subnet and another interface in the device subnet, with IP forwarding enabled. The BMENOR2200H routes traffic between the subnets so that hosts in the control network can access devices in the device network using the BMENOR2200H address as the default gateway on each subnet, without performing address translation.



NAPT (NAT)

This sample segmented network builds upon the two-subnet example with distinct control and device networks. In this case, the BMENOR2200H module is configured for static NAT to expose a device-side service to the control network. A service port on the BMENOR2200H control-side address is mapped to the device-side address and service port (for example, control-side port 54321 to device-side port 502). This translation allows hosts in the control network to reach the device service while keeping the device subnet addressing private.



Redundant M580 Networks

Introduction

IP Address of the Module

Redundant systems contain separate primary and standby control networks. The configuration of the primary and standby racks is identical.

A redundant system that implements BMENOR2200H modules, therefore, includes one such module in both the primary and standby racks with these IP addresses:

- *IP address:* BMENOR2200H module in the primary configuration
- *IP address + 1:* BMENOR2200H module in the standby configuration

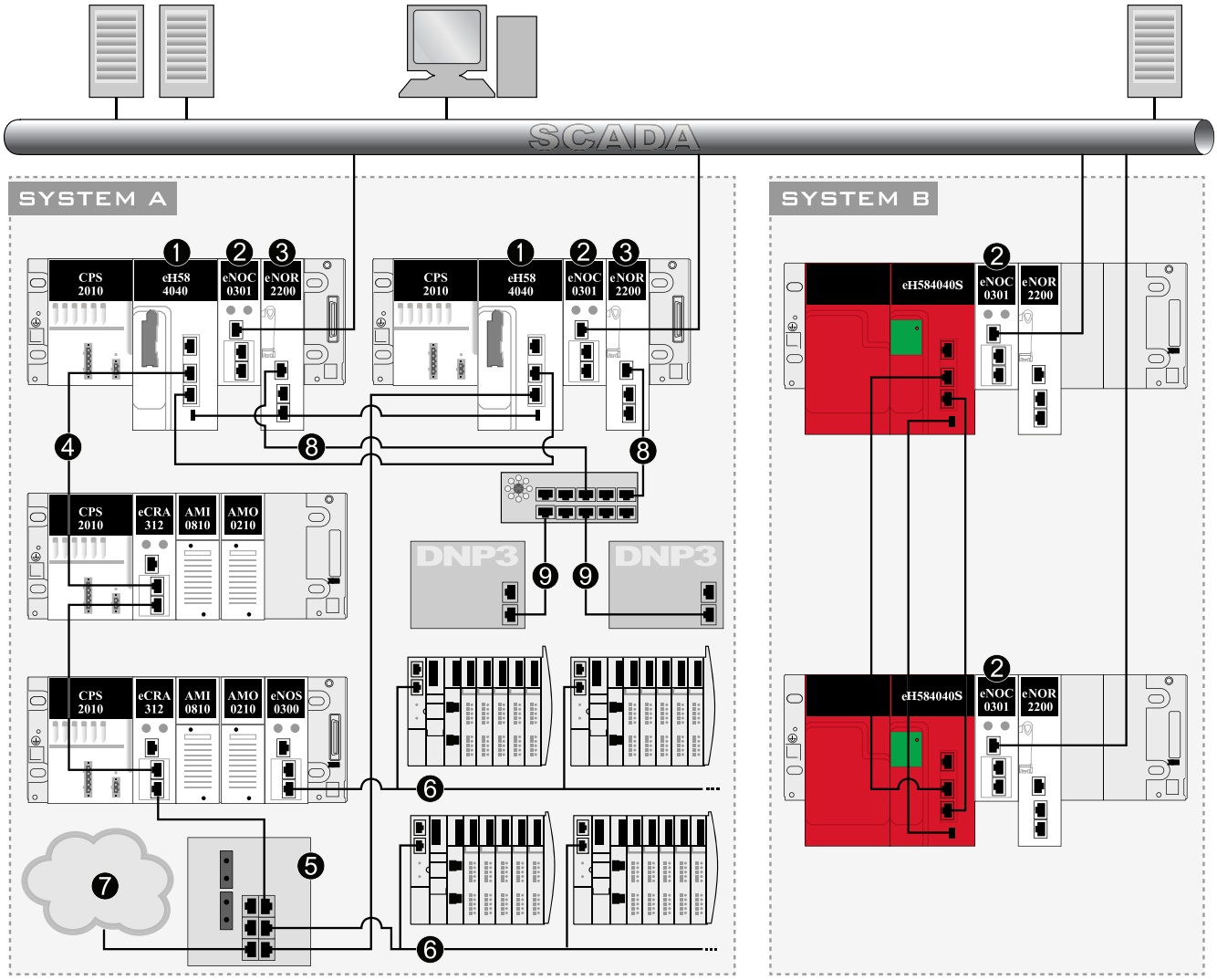
Upon a redundant switch-over, the IP address setting is automatically transferred from the (former) primary BMENOR2200H module to the (former) standby BMENOR2200H module. The *IP address + 1* setting is also transferred from the (former) standby BMENOR2200H module to the **new** standby BMENOR2200H module.

Redundant Architecture with One Subnet

Sample Network

This M580 architecture implements BMENOR2200H modules in two rack configurations, an M580 redundant system and an M580 Safety redundant system.

Both the redundant system (*SYSTEM A*) and the Safety redundant system (*SYSTEM B*) have primary and secondary rack configurations with routing functionality to support redundancy. The connected SCADA network is also equipped with switch routing:



Legend:

1 An M580 redundant PAC connects the main ring to the control network.

2 A BMENOC0301 module connects to the standalone and Safety Hot Standby PACs via the Ethernet backplane that supports distributed equipment.

3 A BMENOR2200H module acts as an RTU server to support DNP3, IEC60870-5-101, or IEC60870-5-104 communications.

4 RIO main ring

5 A dual-ring switch (DRS) connects distributed equipment to the RIO drop on the main ring.

6 Distributed equipment connects to the main ring via the DRS using DNP3, IEC60870-5-101, or IEC60870-5-104 communications.

7 A DIO cloud connects to the main ring via the DRS.

8 BMENOR2200H modules connect to a network splitter block for serial devices.

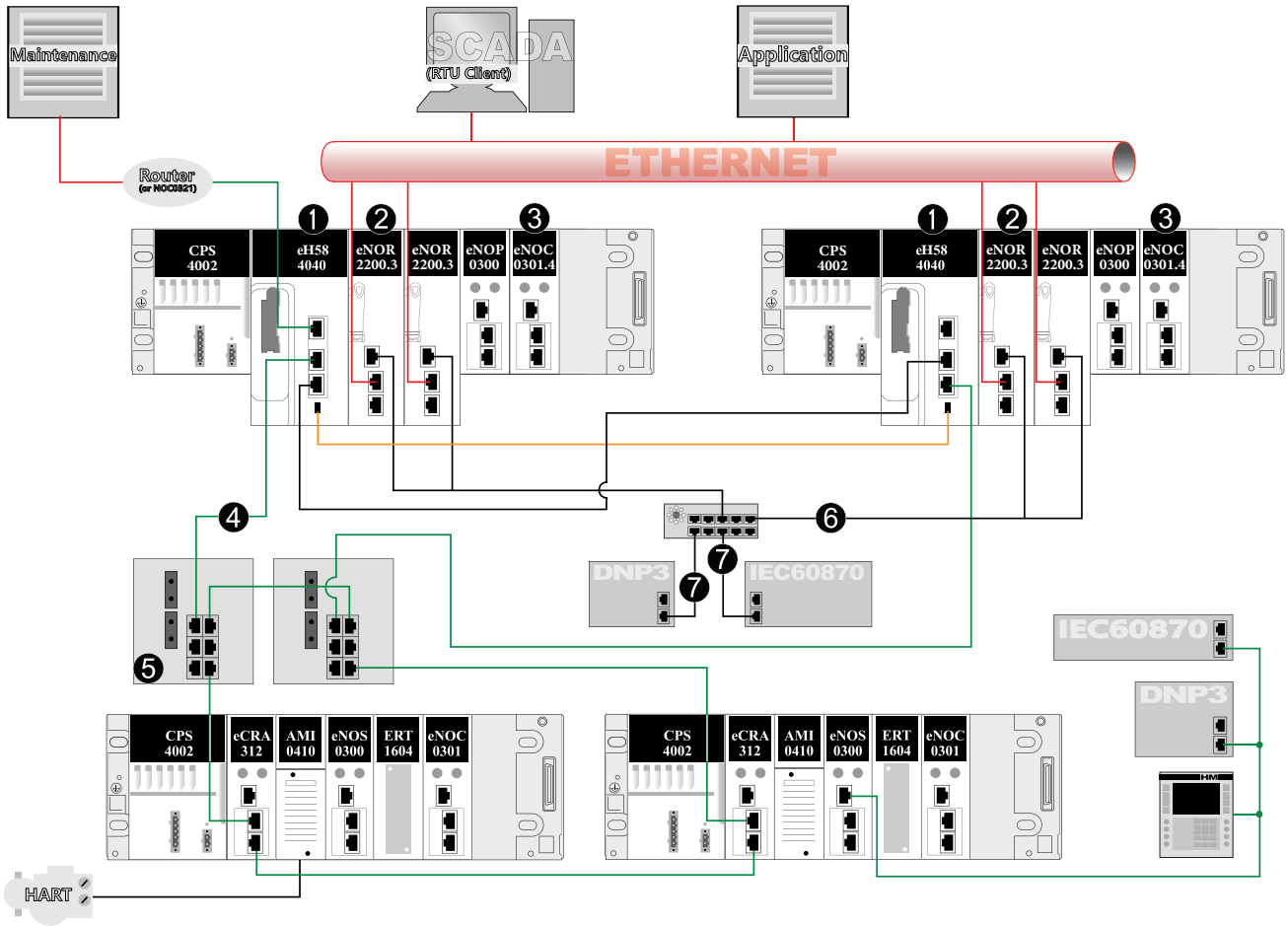
9 DNP3 serial devices have RS485 connections to the network splitter block.

NOTE: The primary and standby BMENOR2200H modules use the RIO network or the upstream network to synchronize data. Otherwise, the pair of modules cannot establish Hot Standby functionality.

Redundant Architecture with Isolated Network

Sample Network

This sample isolated redundant network includes BMENOR2200H modules on local racks. The BMENOR2200H module provides two different isolated subnets for control network (red) and backplane network (green).



Legend:

1 An M580 redundant PAC connects the main ring to the control network.

2 A BMENOR2200H module acts as an RTU server to support DNP3, IEC60870-5-101, or IEC60870-5-104 communications.

3 A BMENOC0301 module connects to the standalone and Safety Hot Standby PACs via the Ethernet backplane that supports distributed equipment.

4 RIO main ring

5 A dual-ring switch (DRS) connects distributed equipment to the RIO drop on the main ring.

6 BMENOR2200H modules connect to a network splitter block for serial devices.

7 DNP3 serial devices have RS485 connections to the network splitter block.

NOTE: The primary and standby BMENOR2200H modules use the RIO network or the upstream network to synchronize data. Otherwise, the pair of modules cannot establish Hot Standby functionality.

Hardware Installation

Mounting the Module on the Rack

Introduction

The BMENOR2200H module has a dual-bus connector, page 30 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

UNINTENDED EQUIPMENT OPERATION

The Modicon X80 racks must be mounted horizontally on a vertical plane to facilitate ventilation.

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, page 28 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 controller).

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

controller	BMENOR2200H
BMEP581020	2
BMEP582020	2
BMEP582040(S)	3
BMEP584020	4
BMEP584040(S)	4
BMEP586040	4
BMEH582040	2
BMEH584040	4
BMEH586040(S)	4

NOTE: Refer to the controller selection table in the *Modicon M580 Standalone, System Planning Guide for Frequently Used Architectures*. Also refer to *Modicon M580 – Hot Standby, System Planning Guide for Frequently Used Architectures; Modicon M580, Safety System Planning Guide* (Related Documents, page 11).

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

Backplane	Description
BMEXBP0400(H)	4-slot (hardened) Ethernet backplane
BMEXBP0800(H)	8-slot (hardened) Ethernet backplane
BMEXBP1200(H)	12-slot (hardened) 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	These slots do not support the BMENOR2200H module. **NOTE:** These slots are reserved for the controller 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 Standard configuration directly to the Advanced configuration or vice-versa.
- Always power up the module with the rotary switch in the Cybersecurity Reset position when you transition between the Standard and Advanced modes.

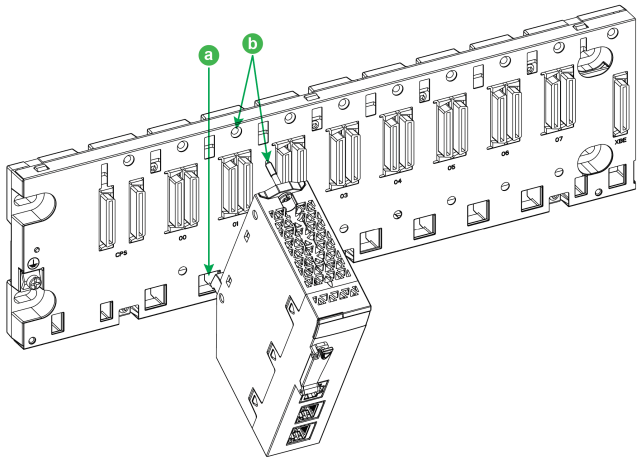
Failure to follow these instructions can result in equipment damage.

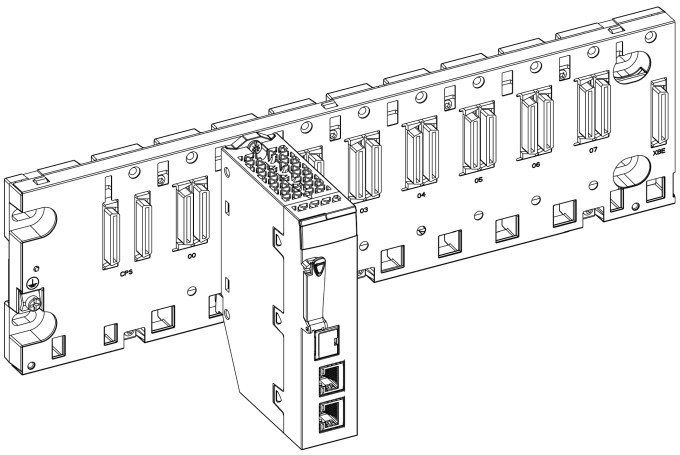
Follow these steps every time you insert a BMENOR2200H module on a powered rack:

Step	Action
1	Set the rotary switch, page 28 on the module to the **Cybersecurity Reset** position.
2	Insert the module in the rack to power it up.
3	Remove the module from the rack to power it down.
4	Set the rotary switch on the module to the **Advanced** 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, page 28.
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 controller. **NOTE:** Do not insert the BMENOR2200H module into X-bus only slot.

Step	Action
5	Tighten the retaining screw to hold the module in place on the rack:  **⚠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.** **NOTE:** Tightening torque: 1.1 ... 1.5 Nm (*0.81 ... 1.10 lbf-ft*).
6	Insert the SD card if you intend to use the data logging feature.

Grounding Considerations

This section describes the wiring guidelines and best practices to be respected when installing and cabling the BMENOR2200H Ethernet Communications Module.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables, or wires except under the specific conditions specified in the appropriate hardware guide for this equipment.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to the unit.
- Use only the specified voltage when operating this equipment and any associated products.

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

⚠ WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it into service.

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

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* and to NEMA ICS 7.1 (latest edition), *Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems* or their equivalent governing your particular location.

The following rules must be applied when cabling the Ethernet Communications module:

- Communication wiring must be kept separate from the power wiring. Route these two types of wiring in separate cable ducting.
- Verify that the operational conditions and environment are within the values cited in the present document and the other user guides associated with this equipment.
- Use twisted pair, shielded (ferrule) cables with the proper rating for your installation/environment.

If you do not use proper, shielded (ferrule) cables for these connections, electromagnetic interference can cause signal degradation. Degraded signals can cause the controller or other attached modules and equipment to perform in an unintended manner.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Use shielded (ferrule) cables for all communication signals.
- Ground (ferrule) cable shields for all communication signals at a single point[1].
- Route communication separately from power cables.

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

[1] Multipoint grounding is permissible if connections are made to an equipotential ground plane dimensioned to help avoid cable shield damage in the event of power system short-circuit currents.

Use fiber-optic cable to establish a communications link when it is not possible to equalize the potential between the two grounds.

NOTE: Refer to the ground protection information provided in the *Electrical installation guide* and *Control Panel Technical Guide, How to protect a machine from malfunctions due to electromagnetic disturbance* (Related Documents, page 11).

Replacing a Module

NOTICE

UNINTENDED EQUIPMENT OPERATION

- Do not switch from the Standard configuration directly to the Advanced configuration or vice-versa.
- Always power up the module with the rotary switch in the Cybersecurity Reset position when you transition between the Standard and Advanced 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 controller. The transfer occurs immediately at the next cycle to the device.

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

Export your cyber security configuration before you replace the module. When the rotary switch is set to the factory Cybersecurity 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, page 28 on the replacement module to the **Cybersecurity 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 **Advanced** 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 to create a backup configuration and import a stored cyber security configuration file to new module through the web page.

NOTE: The SD memory card contains the CSV files for the independent data logging service, page 166. When data logging is enabled, therefore, backup the data logging tables from the SD card before you replace the module.

Ethernet Communications

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
- DNP3 serial server with SAv2 or SAv5
- DNP3 serial client with SAv2 or SAv5
- IEC60870-5-104 client
- IEC60870-5-104 server
- IEC60870-5-101 client
- IEC60870-5-101 server

NOTE: Refer to the description of RTU protocols, page 64.

Ethernet Services

The module supports these Ethernet services:

- SNMPv1 and SNMPv3 Agents, page 56
- FDR client (basic service), page 60
- Modbus TCP server and client, page 61
- SNTPv1 client, page 157
- built-in HTTPS -based web pages, page 176
- Ping Function, page 63

Other Services

The BMENOR2200H module also supports these services:

- Firmware upgrade, page 59
- clock synchronization, page 82
- Cyber Security, page 197

SNMP Service

SNMP Overview

Introduction to SNMP

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

An SNMP agent runs on:

- Ethernet communication modules
- Controllers with embedded Ethernet communication ports

SNMP and the NMS

A network management system (NMS) uses SNMP to monitor and control Ethernet architecture components for the rapid network diagnosis.

The NMS allows a network manager to execute these tasks:

- 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 statuses.
- Obtain statistics about the networks to which they are attached.

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

SNMP Communication

Introduction

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

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, page 155.
- Refer also to the description of MIB support for SNMP, page 53.

SNMP Structure

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.

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`: This message obtains the value of one or more variables.
- `Get_Next_Request`: Obtain the value of the next variables.
- `Set_Request`: Set 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 Versions

Available Versions

The module runs multiple versions of the SNMP communications protocol:

- **SNMPv1:** Version 1 of SNMP extends the capabilities of the protocol to address ministration and security issues. With this version, simple-text password is shared between a *manager* and an *agent*. SNMPv1 commands are simple request-and-response protocol commands (*Get*, *Set*, *Trap*).

  NOTE: This version offers minimal security among users with access to the same network.

- **SNMPv3:** In terms of operations, SNMPv3 is functionally quite similar to SNMPv1. SNMPv3 does, however, offer enhanced security for a network that is accessed by multiple users through authentication and privacy controls. SNMPv3 re-brands the *managers* or *agents* in SNMPv1 as *entities*. Each *entity* in SNMPv3 is composed of an SNMP *engine* and at least one SNMP *application*. Such distinctions enable the protocol to implement security according to the relationships between these entities in a modular architecture. In addition, SNMPv3 facilitates the configuration of remote SNMP agents because each SNMP entity has a unique identifier (*engineID*) that corresponds to requests from a specific remote SNMP engine.

Security Level Summary

There is no native compatibility between SNMPv1 and SNMPv3 messages. Therefore, the SNMP agent provides these security levels:

- *standard mode:* Support SNMPv1 and SNMPv3. In this mode, SNMPv3 uses `NoAuthNoPriv`; there is no authorization and no encryption for packets sent between the network management station and the SNMP manager.
- *advanced mode:* Support SNMPv3 in advanced mode to enhance authentication and integrity (`AuthNoPriv`), and authentication, integrity, and confidentiality (`AuthPriv`).

SNMPv3 and HMAC

SNMPv3 authentication uses the Hash Message Authentication Code (HMAC) to authenticate each critical message by implementing a challenge-reply model.

Think of HMAC as a cryptographic checksum over the SNMP message that is combined with a secret key (derived from the user password). The HMAC and user name are transmitted within the packet. The device verifies the integrity and originator of the message by calculating a checksum over the received message with the secret key from its local user database. If the calculated HMAC and the one in the packet match, access is granted.

The Hashed Message Authentication Code (HMAC) security algorithm is used to *sign* security messages to confirm that they were not tampered with. HMAC SHA-256 algorithms are more secure than HMAC SHA-1 algorithms, but they require more RTU processing. Algorithms with more bytes are more secure, but create the longer messages that require more bandwidth for critical messages.

SNMPv3 and USM

SNMPv3 supports the user-based security model (USM) to create and associate authorized users with a specific SNMPv3 agent to enhance the authentication of users and the privacy and integrity of message.

SNMPv3 Encryption Libraries

The SNMPv3 agent uses these encryption libraries for authentication and encryption:

- encryption: CFB128-AES-128 (RFC3826)
- authentication: HMAC-SHA1-96 (RFC-2104)

SNMP Agent Details

Introduction

This module runs the Simple Network Management Protocol (SNMP). This protocol extends the capabilities of SNMP to address administration and security issues. In particular, the PDU contents can be encrypted.

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.

SNMP supports a framework architecture that can be easily extended with new user security protocols. It also uses the UDP transport-layer protocol through ports 161 (polling) and 162 (notifications, requests, traps). You can easily extend and adapt the SNMP framework architecture for new user-security protocols.

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 verify 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

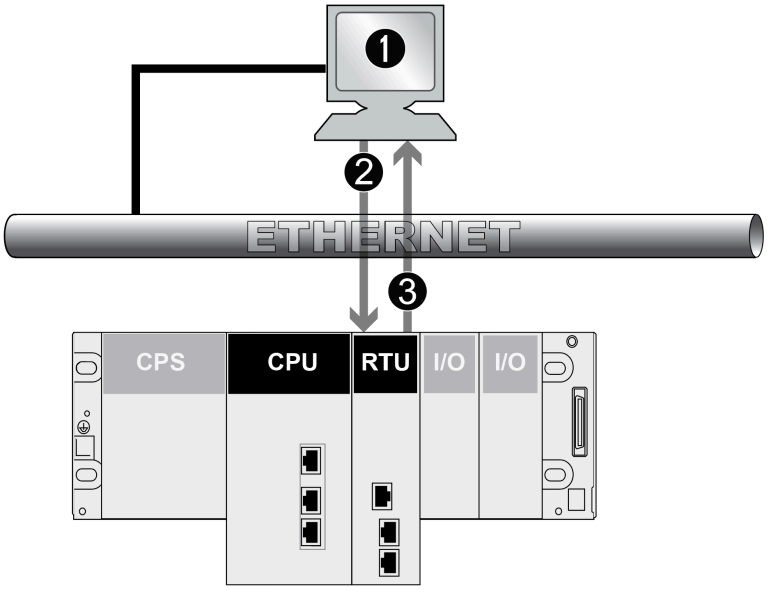
SNMP Operations Example

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 BMENOR2200H module.

Example

In this example, an SNMP manager on an Ethernet network sends a request to the SNMP agent in the BMENOR2200H module 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` (SNMP v1 only): 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.

MIB Support

About 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

MIB Versions

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

Standard MIB II: 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.

Firmware Upgrade

EcoStruxure™ Automation Device Maintenance Tool

Tool Functions

Use the EcoStruxure™ Automation Device Maintenance tool to upgrade the firmware of the BMENOR2200H module.

Perform these actions with this web-based tool:

- Manually discover one or more BMENOR2200H modules in your project, based on IP addresses.
- Upgrade the selected firmware version that is applicable to those modules.

For details on how to install and use this firmware upgrade tool, refer to the online help.

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

NOTE: The firmware version less than 4.0 cannot be downloaded to the BMENOR2200H module with control ports.

User Role

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

NOTE:

- Certification is invalid and the firmware upgrade process is blocked if the BMENOR2200H module's internal clock is earlier than 2019. The module updates the internal clock from the M580 controller. If no time is set for the controller, a default date is used (Jan 1, 1980). Therefore, it is good practice to confirm that the module's internal clock is set at the current time/date before you upgrade the firmware.
- When the module operates in **Standard** mode, the default user role is **INSTALLER**:
  - default username: *installer*
  - default password: *Inst@ller1*
- When the module operates in **Advanced** mode, the default user role is **SECADM**. In that case, log in to the security setting page to create a new user, page 176 as an **INSTALLER** and upgrade the firmware in that role.
- Refer to the description of the rotary switch positions and the corresponding modes, page 28.

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 controller 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 stored in the BMENOR2200H module.

Configuration Process

The service configures the IP parameters for the BMENOR2200H module:

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

Default IP Address

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 controller. Instead, it uses the default IP address 10.10.mac5.mac6 for control ports and the default IP address 10.20.mac5.mac6 for backplane port. In this case, the module detects a duplicated IP status and does not run.

NOTE: In rarely case, mac6 value is 00 (zero). Default IP address might not work properly. You can configure a M580 to set a valid IP address and download it to BMENOR2200H module.

Behavior

When you power up the BMENOR2200H module, the FDR client service uses the default IP. When the initialization is complete, the FDR client service gets the IP configuration from the controller. Then the service validates those IP parameters:

- *OK:* The FDR client uses the received parameters when they are valid and not duplicates.
- *not OK:* The FDR client service uses the default IP when any of the received IP parameters are not valid, missing, or duplicated.

  NOTE: When a duplicate IP address is found in the system, the BS and/or NS LED is solid red. Refer to the description of LED indications, page 23.

When the IP address parameters represent a duplicate IP address, the FDR client sends ARP requests to detect the IP. If the duplicate IP parameters disappear, the FDR client uses the configured IP parameters. After the IP configuration, the FDR client service sends gratuitous ARP requests.

Modbus TCP Messaging

Data Access

Introduction

The BMENOR2200H module supports Modbus TCP server and client features. In advanced mode, this service is disabled by default. (It can be enabled via web if the module is in **Advanced** mode, page 28.) In standard mode, this server is enabled always.The Modbus TCP server provides diagnostic data in the module's local register. The Modbus TCP Client can access this database via the module's IP address (unit ID 100).

NOTE: For details about diagnostic information for Modbus TCP, refer to the appendix of Modbus diagnostic codes, page 286.

You can also use the module service to transfer a Control Expert configuration file to the controller over X Bus. In this case, you do not have to connect an external engineering station directly to the controller.

Data Exchange

Exchanges

Data exchanges take place in one of two modes:

- **server mode**: The BMENOR2200H module supports all Modbus-over-TCP requests from the PLC or the external Modbus client.
- **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 information about data exchange functionality or the definition of the BMENOR2200H module as a host Modbus client, refer to the *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 for standard mode:

Feature		Maximum Capacity
client	simultaneous requests	16 requests in data exchange blocks
	message size	1024 bytes
	client connections	16 connections
server	server connections	32 connections
	message size	1024 bytes

Port 502 messaging paths for high performance mode:

Feature		Maximum Capacity
client	simultaneous requests	32 requests in data exchange blocks
	message size	1024 bytes
	client connections	16 connections
server	server connections	32 connections
	message size	1024 bytes

Ping Function

Overview

The Ping function allows you to verify network connectivity between the RTU and external devices. This diagnostic tool sends ICMP echo requests from the RTU to a specified IP address and records the response time. It is useful for troubleshooting communication issues and validating device reachability within the network.

Performing a Ping Test

Step	Action
1	Navigate to **Diagnostics > Module** from the web page
2	Select **Ping** in the left-hand menu. The Ping page displays the following fields: • **Module Rack Slot information**: Identifies the module location. • **Ping**: Shows the response times for each attempt.
3	Enter the IP address of the device you want to test in the **IP** field.
4	Click **Ping** to start the operation. **NOTE:** Each ping operation is performed three times, and the corresponding response times are displayed. The results are displayed in **Ping Result**: • **Response Time**: Indicates the time (in milliseconds) for each ping attempt. • **Status**: Displays **Ping OK** when the target device responds successfully, and **Ping Not OK** when the device is unreachable.

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.

Communication Protocols

Functions and Protocols

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

Protocols & Functionalities	Description
RTU protocols	built-in RTU protocols for serial or Ethernet communications
	IEC60870-5-101 (server or client)
	IEC60870-5-104 (server or client)
	DNP3 serial (server or client)
	DNP3 NET (server or client)
	Modbus TCP (server or client)
	NOTE: The number of communication connections affects the module performance (web page access, module start-up and data exchange through the backplane).
Main RTU protocol functions	time synchronization through a protocol facility or SNTP, page 83
	data synchronization on demand of the SCADA
	event management with time stamping, page 85 (Sequence of Event, SOE)
	event queue stored in RAM memory (up to 300,000 events)
	events data backfill to SCADA application via protocol facility, page 90
	event routing, page 87
	report by exception data exchanges
	unsolicited messaging data exchanges
	DNP3 secure authentication, page 80 SAv2 and SAv5 with pre-shared key, page 81
Other built-in functionality	web server to help security set-up and remote diagnostic

IEC60870-5-101/104 Protocols

Introduction

IEC60870-5 is an international standard released in the early 1990s by the International Electrotechnical Commission (IEC). This standard provides a communication profile for telecontrol, teleprotection, and associated telecommunications characteristics for electric power systems. It is used today for other infrastructures, including water applications in Europe and Asia.

The IEC60870-5-101 and IEC60870-5-104 protocols are designed for systems that have permanent direct connections between the controlling station (client) and the controlled station(s) (servers). The IEC60870-5-101 and IEC60870-5-104 standards are applicable for multiple network configurations like point-to-point, star, and multi-drop. The standard is suitable for power system monitoring, control communications, teleprotection, and associated telecommunications for electric power systems.

Protocol Distinctions

The IEC 60870-5-101 protocol is based on the Enhanced Performance Architecture (EPA). This protocol defines only the physical link and application layers of the OSI model. IEC 60870-5-101 is used primarily on serial links with relatively slow transmission media. This standard conforms to baud rates of up to 9600 bit/s, although baud rates of <115200 bit/s are being used.

The IEC60870-5-104 protocol is an extension of the IEC60870-5-101 protocol. There are changes in transport, network, link & physical layer to open networking.

IEC60870-5-104 enables communication between control stations and substations in a standard TCP/IP network. The TCP protocol is used for connection-oriented data transmission. To have connectivity to LANs and routers with different facilities (frame relay, etc.), connect it to the WAN. The application layer of IEC60870-5-104 is the same as that of IEC60870-5-101, except that some data types and facilities are not used. There are separate link layers defined in the standard, which facilitates the transfer of data over Ethernet and serial lines.

NOTE: When links from a central control station to multiple outstations use the same physical channel, the links operate properly only in unbalanced mode. This helps limit instances in which multiple outstations attempt to transmit on the channel at the same time.

Supported Protocol Features

Supported IEC60870–5–101/104 features:

Feature	IEC 60870-5-101	IEC60870-5-104	Description
link mode	✓	X	• **balanced**: There is a one-to-one full-duplex connection between a channel and a single server. • **unbalanced**: There is a half-duplex connection between a channel and one or more servers (for example, in a multi-drop setup).
data classification	✓	X	• Data is classified into different information objects. Each object receives a specific address. • Data can be classified into the following priority levels and transferred using separate mechanisms: ◦ high priority (class-1) ◦ low priority (class-2)
data group	✓	✓	Data can be classified into different groups (1–16) to issue specific group interrogation commands from the client and retrieve data for all groups by issuing a general interrogation.
data update	✓	✓	Cyclic and spontaneous updating methods can be used.
general interrogation	✓	✓	A general interrogation command retrieves a specified group of static data from a remote outstation. It is typically sent after device restart, loss of communication, or on a periodic basis so that no changes are missed in the spontaneous reporting of data.
time synchronization	✓	✓	The time synchronization service establishes time accuracy among devices clocks over a network.
events transmission (time-stamped or not)	✓	✓	Configure the transmission threshold based on the count or time since the last event transmission.
counter interrogation	✓	✓	Counter-interrogation commands retrieve counter values from the RTU.
command transmission modes (select and execute mode)	✓	✓	*select/execute:* Write operations with a dual command and response.
			execute: Write operations with a single command and response.
✓: supported features **X**: unsupported features			

Supported Protocol Data Types

This list shows the supported data types for the IEC60870-5-101/104 protocols:

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

Protocol Characteristics

The table lists the characteristics for the supported RTU protocols:

Protocol	Characteristics
IEC60870-5-104 server	Client IP address validation list (up to 10 IP addresses)
	Up to four concurrent client connections with configurable TCP service port (standard is 2404)
	Input and output maximum (module level): • *input:* 8 KB (16 KB in high performance mode) • *output:* 8 KB (16 KB in high performance mode) **NOTE:** Refer to the description of I/O data exchange with the controller, page 31.
	Up to 150,000 events (300,000 in high performance mode) in a queue for all data types in all servers (each server has a dedicated event buffer)
	Event time-stamping configurable by type (None, CP56)
	Channel redundancy
IEC60870-5-104 client	• *input:* 8 KB (16 KB in high performance mode) • *output:* 8 KB (16 KB in high performance mode) **NOTE:** Refer to the description of I/O data exchange with the controller, page 31.
	Up to 64 server connections supported
	Connections share common channel configuration
	Dedicated connection for each device configuration
	Dedicated destination IP address and port settings for each connection
IEC60870-5-101 server	• *input:* 8 KB (16 KB in high performance mode) • *output:* 8 KB (16 KB in high performance mode) **NOTE:** Refer to the description of I/O data exchange with the controller, page 31.
	Up to 150,000 events (300,000 in high performance mode) in a queue for all data types in all servers (each server has a dedicated event buffer)
	Event time-stamping configurable by type (None, CP24, CP56)
	Maximum number of active connections/sessions: 4 Maximum number of configured devices per session: 5
IEC60870-5-101 client	• *input:* 8 KB (16 KB in high performance mode) • *output:* 8 KB (16 KB in high performance mode) **NOTE:** Refer to the description of I/O data exchange with the controller, page 31.
	Maximum number of active connections: • RS232: 1 • RS485: 32
	Connections share common channel configuration
	Dedicated connection for each device configuration

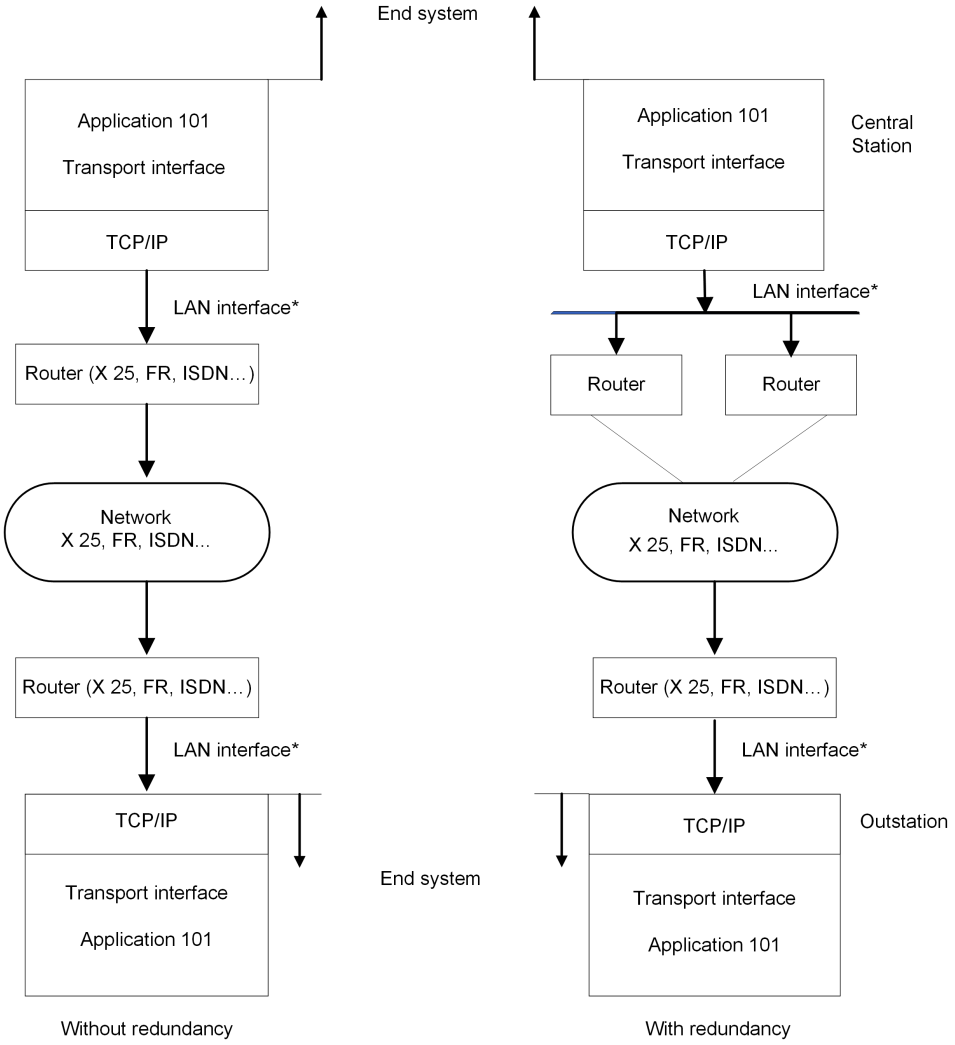
Channel Redundancy

Redundancy is sometimes necessary to increase the availability of the communication system. In these cases, confirm that you establish multiple redundant connections between the two stations. Redundant communication in a system using IEC60870-5-104 allows you to establish more than one logical connection between two stations. A logical connection is defined by a unique combination of two IP addresses and two port numbers, specifically the controlling station's IP address/port number pair and the controlled station's IP address/port number pair.

This table represents the redundancy software architecture within the BMENOR2200H module:

Application Layer		
Redundancy Group or Channel		
Channel 1	Channel 2	Channel 3

This flowchart shows the general architecture for a redundant configuration in the central station as well as a non-redundant system:



** The LAN interface may be redundant.*

Considerations:

- Every main or virtual channel can be configured as *None*, which indicates the independence of the channel. That is, it does not belong to any redundancy group.
- Every main or virtual channel can be configured as group *1/2*.
- There is only one *Active* channel in one redundant group. It performs all user application communications. All the other connected channels are inactive. (Inactive channels are monitored to confirm that they are operational.)
- If an active link control is configured as *External* and the active channel stops communicating, its communications move to the next operational channel by a remote client with a STARTDT message.
- If an active link control is configured as *Module* and the active channel stops communicating, the module automatically moves its communications to the next operational channel.

NOTE: For the *Event Backup* restore mode, you can select *All Channels* for the *Restore Mode* in the channel configuration, page 117.

Read Only Mode

For IEC60870-5-104 sever, the channels can be configured as "Read only".

On **Channel /Device > IEC104 Server > Server > Session Parameters**: Select the checkbox **Read Only** in the Server Session parameters. The variables "ReadOnly_Cmd" and "ReadOnly_Status", are displayed in the Device DDT.

Variable	Type	Bit	Description	Note
ReadOnly_Cmd	WORD	Bit 0/1/2/3: 1	The first IEC104 server channel is set in **Read Only** mode.	Bit 0-3 are the control bit for all the IEC104 Server channel (maximum 4 channels).
		Bit 0/1/2/3: 0	The first IEC104 server channel is not set in **Read Only** mode.	
		Bit 5/6/7...15	Reserved.	-
ReadOnly_Status	WORD	Bit 0/1/2/3: 1	The channel is in **Read Only** mode.	Bit 0-3 are for the values of IEC104 server channels **Read Only** mode.
		Bit 0/1/2/3: 0	The channel is not in **Read Only** mode.	

NOTE:

- If there is a redundancy group and one channel in it is set to be in **Read Only** mode, all channels in the group are in **Read Only** mode.
- When a channel is in Read Only mode, command types C_DC/C_SC/C_RC/ C_BO/C_SE_A/C_SE_B/C_SE_C/C_CS/C_RP/P_ME_A/P_ME_B/P_ME_C/P_AC from SCADA will be rejected and the module will give negative response, but other requests will be allowed.

Interoperability Lists

The interoperability list (defined by the standard) facilitates interoperability between devices from different manufacturers. In the list, the function range is described for each device by marking the applicable functions.

NOTE: The appendix includes the IEC60870-5-101/104 interoperability list for the BMENOR2200H module, page 230.

IEC60870-5-101/104 Supported Data Types

Process Information: Monitored Direction

IEC60870-5-101/104 servers support this process information in the monitored direction:

- M_SP: single-point information
- M_DP: double-point information
- M_ME_A: measurements value, normalized value
- M_ME_B: measurements value, scaled value
- M_ME_C: measurements value, short floating-point
- M_IT: integrated totals
- M_ST: step position information
- M_BO: bit and byte strings

Process Information: Control Direction

IEC60870-5-101/104 servers support this process information in the control direction:

- C_SC: single command
- C_DC: double command
- C_SE_A: set-point command, normalized value
- C_SE_B: set-point command, scaled
- C_SE_C: set-point command, short floating-point number
- C_RC: regulating step command
- C_BO: bit-string of 32 bits

System Information: Monitored Direction

IEC60870-5-101/104 servers support this system information in the monitored direction:

- M_EI: end of initialization with COT of initialized
- M_EI_NA: After receiving an M_EI_NA EOI message, you can configure these items:
  - general interrogation information
  - clock synchronization
  - counter-interrogation

System Information: Control Direction

IEC60870-5-101/104 servers support this system information in the control direction:

- C_IC: These interrogation command points support G/1~16 qualifiers and the **Deactivation**/**Activation** operation modes.
- C_CI: These counter-interrogation commands support G/1~4 qualifiers and **Read**/**Freeze**/**Freeze-With-Reset**/**Reset** operation modes.
- C_CS: clock synchronization commands
- C_TS: test commands

  C_RP: These reset process command points support the **General**/**Event** qualifiers.
- C_RD: read commands

Parameter Information: Control Direction

IEC60870-5-101/104 servers support these parameters in the control direction:

- P_ME_A: parameter for measurement, normalized value
- P_ME_B: parameter for measurement, scaled value
- P_ME_C: parameter for measurement, short-floating point number
- P_AC: parameter activation support for the **Deactivation**/**Activation** operation mode

M_CUSTOME_IT_D

IEC60870-5-101/104 servers support 64–bit M_CUSTOME_IT_D points, which support the mapping functions to the Device DDT variables of the controller.

IEC60870-5-101/104 Features

Event Support

IEC60870-5-101/104 servers support events:

- The event function can be disabled/enabled by a datatype ID.
- The event function can be disabled/enabled by a data point.
- The event time format can be configured by a datatype ID.
- The time format for events can be an option of None/CP24 (Only for IEC 60870-5-101)/CP56.
- The timestamp for the event is the local time with the summer/winter flag set.
- You can configure the event buffer size through the datatype ID and channel. The buffer capacity is up to 300,000 events for all channels. Only the newest events are saved when the buffer events consume more space than is configured for the buffer.
- The buffer retains events when a channel is disconnected. Events are expelled from the buffer when a SCADA systems is connected.
- The event buffer is cleared in this situations:
  - A clear-event point is set in the controller.
  - A remote command with a qualifier event is received.

Event Backup Support

IEC60870-5-101/104 servers support the backup of events:

- Events are backed up in these situations:
  - power loss
  - Hot Swap of the module
- The BMENOR2200H module supports the backup of up to 10,000 events upon a power loss. Only the newest events are saved if the number of events exceeds 10,000.
- The BMENOR2200H module supports the backup of at least 5,000 events when the module is Hot Swapped. Only the newest events are saved in the event buffer.
- Backup events are restored to the RTU protocol stack after power is restored only when the configuration matches the previous one. Otherwise, backed-up events are discarded.
- Backed-up events are cleared when the controller module cold restart (for example, when a new configuration is downloaded). In this case, communications are reset.
- You can enable or disable the event backup function.

On-Demand Mode

IEC60870-5-101/104 servers support on-demand mode for these set-point commands:

- C_SC
- C_DC
- C_RC
- C_SE_NA
- C_SE_NB
- C_SE_NC
- C_BO

NOTE:

- These points support the setting using the controller Device DDT variable or %MW register.
- These points support the setting using the IEC60870-5-101/104 command.

Local Cyclic Freeze (M_IT)

IEC60870-5-101/104 severs support the cyclic freeze function for M_IT points:

- You can disable this function.
- This function can start automatically after the modules starts up, or it can be controlled but a running controller Device DDT variable.
- This function supports the setting of a freeze period for every group.
- This function supports the Freeze-Only/Freeze-with-Reset operation mode.

Local Trigger Freeze (M_IT)

IEC60870-5-101/104 severs support the trigger freeze function for M_IT points:

- This function is controlled by a controller Device DDT variable. A change in the value of the variable triggers the operation.
- This function supports the Freeze-Only/Freeze-With-Reset operation mode.
- This function supports the freezing of a specified group.

DNP3 Protocol

Introduction

The distributed network protocol (DNP3) was developed to achieve an open, standard interoperability for communications between client 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 client-to-RTU/IED.

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

Protocol Characteristics

The table lists the characteristics for the supported RTU protocols:

Protocol	Characteristics
DNP3 NET client	up to 64 servers (one session for each server)
	input: 8 KB (16 KB in high performance mode) *output:* 8 KB (16 KB in high performance mode) **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 Controller, page 31.
DNP3 NET server	*input:* 8 KB (16 KB in high performance mode) *output:* 8 KB (16 KB in high performance mode) **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 Controller, page 31.
	up to 150,000-event (300,000 in high performance mode) queue for all data types
	clock synchronization from a client
	DNP3 secure authentication versions SAv2 and SAv5
	4 concurrent client connections
DNP3 serial client	up to 32 servers (one device/session for each server)
	input: 8 KB (16 KB in high performance mode) *output:* 8 KB (16 KB in high performance mode)
DNP3 serial server	*input:* 8 KB (16 KB in high performance mode) *output:* 8 KB (16 KB in high performance mode)
	up to 150,000-event (300,000 in high performance mode) queue for all data types
	clock synchronization from a client
	DNP3 secure authentication versions SAv2 and SAv5
	1 concurrent client connection

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, page 231 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 Supported Data Types

- Single-bit binary input point type object groups:

Group number	Used for
1	Reporting the present value of a single-bit binary input
2	Reporting single-bit binary input events or flag bit changes

- Double-bit binary input point type object groups:

Group number	Used for
3	Reporting present state value
4	Reporting double-bit binary input events or flag bit changes

- Binary output point type object groups:

Group number	Used for
10	Reporting the present output status
11	Reporting changes to the output status or flag bits
12	Issuing control commands

- Counter point type object groups:

Group number	Used for
20	Reporting the count value
21	Reporting the frozen count value or changed flag bits
22	Reporting counter events
23	Reporting frozen counter events

- Analog input point type object groups:

Group number	Used for
30	Reporting the present value
32	Reporting analog input events or changes to the flag bits
34	Reading and writing analog deadband values

- Analog output point type object groups:

Group number	Used for
40	Reporting the present value of analog outputs
41	Controlling analog output values
42	Reporting changes to the analog output or flag bits

- Time and data object groups:

Group number	Used for
50	Set or get the current time

- Class object groups:

Group number	Used for
60	Read request to specify that the outstation return some or all objects having a specified class event attribute.

- Octet string point type object groups:

Group number	Used for
110	To convey the present value

- Security statistics point type object groups:

Group number	Used for
121	Reporting the current value of the statistics
122	Reporting changes to the statistics

DNP3 Features

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
- client commands
- Multiple-session configuration for DNP3 Server

Event Support

DNP3 server supports events:

- The event function can be disabled/enabled by a datatype ID.
- The event function can be disabled/enabled by a data point.
- The event can be configured with or without timestamp by a data point.
- The timestamp for the event is absolute time when the event occurred.
- You can configure the event buffer size through the datatype ID and channel. The buffer capacity is up to 300,000 events for all channels. Each data type can support maximum 65,535 events. Only the newest events are saved when the buffer events consume more space than is configured for the buffer.
- The buffer retains events when a channel is disconnected. Events are expelled from the buffer when a SCADA system is connected.
- The event buffer is cleared when a clear-event point is set in the controller.

Event Backup Support

DNP3 server supports the backup of events:

- Events are backed up in these situations:
  - power loss
  - Hot Swap of the module
- The BMENOR2200H module supports the backup of up to 10,000 events upon a power loss. Only the newest events are saved if the number of events exceeds 10,000.
- The BMENOR2200H module supports the backup of at least 5,000 events when the module is hot swapped. Only the newest events are saved in the event buffer.
- Backup events are restored to the RTU protocol stack after power is restored only when the configuration matches the previous one. Otherwise, backed-up events are discarded.
- Backed-up events are cleared when the controller module cold restart (for example, when a new configuration is downloaded). In this case, communications are reset.
- You can enable or disable the event backup function.

On-Demand Mode

DNP3 server supports on-demand mode for these set-point commands:

- Binary output point type
- Analog output point type

NOTE:

- These points support the setting using controller Device DDT variable or %MW register.
- These points support the setting using DNP3 command.

Trip-Close Mode

DNP3 server supports specifying one or two binary output points to implement 'Trip and Close' function. (For more detail, refer to *Behavior of a Binary Output*, page 131).

- Double point mode: the contiguous two binary output points are grouped to implement the trip and close function. The first point is used as close function point, and the second point is used as trip function point.
- Single point mode: one binary output point contains 'trip' and 'close' variables to implement the function.

Multiple-Session for DNP3 Server

DNP3 server supports configuring the four channels session parameters respectively and independently.

- If the *Multiple-session* function is not enable, then only session 1 can be configured.
- Once the *Multiple-session* is enable, each session parameter is opened to configure.

DNP3 Secure Authentication Concepts

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.

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

- A DNP3 server uses DNP3 SA to unambiguously determine that it is communicating with a user who is authorized to access the services of the server.

  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 client uses DNP3 SA to unambiguously determine that it is communicating with the appropriate server.

  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).

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.
  - BMENOR2200H provides DNP3 security setting at build-in Web page.

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.
- For general information about pre-shared keys, refer to the *Modicon Controllers Platform Cyber Security, Reference Manual*.

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 (client) 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 or a reset for RTU protocol by Device DDT.

Clock Synchronization with the RTU Protocol

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
server	When acting as a server, the BMENOR2200H module can synchronize its clock with a client station (SCADA). When you update the clock to the controller, the module receives the clock synchronization command and it updates its internal clock, and posts the new value to the controller. This maintains a consistent time on the local rack.
client	When acting as a client, the BMENOR2200H module sends clock synchronization commands to connected servers. As with the case above, the clock is initialized from the controller when it starts up.

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, page 157.

Clock Synchronization with SNTP

Introduction

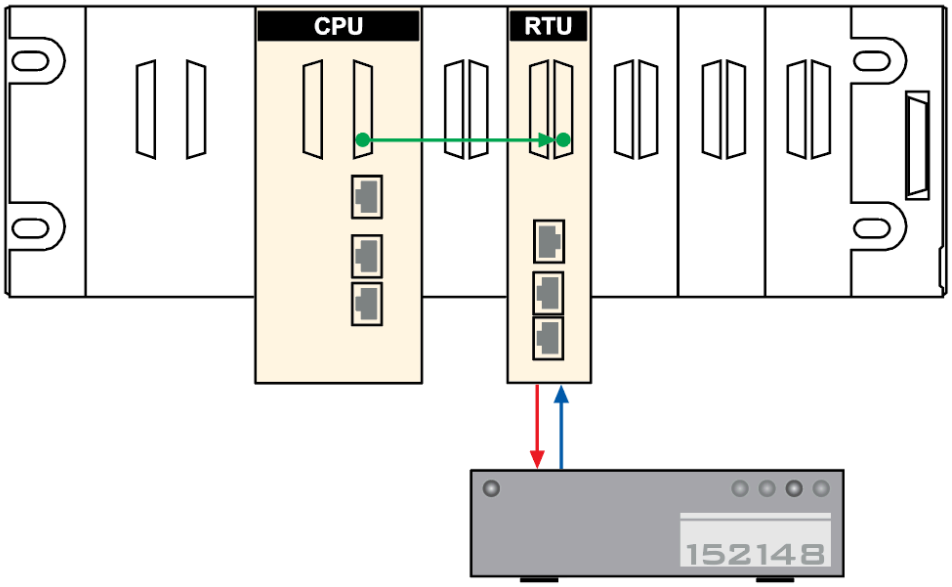
The BMENOR2200H module supports clock synchronization as an SNTP protocol client.

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, page 157.

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 ethernet port to the SNTP server.

blue line: The SNTP server sends a reply to the BMENOR2200H module via ethernet port.

green line: The BMENOR2200H module sends the source clock synchronization signal to the controller over X Bus.

NOTE:

- The BMENOR2200H module sends the signal to update the controller's internal clock only when you select **Update Clock to Controller** in the time synchronization parameters, page 158. Time signal updating to controller will be stopped automatically when module detects its time quality is invalid.
- The clock time accuracy of BMENOR2200H module 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 BMENOR2200H module updates its own clock every millisecond with its internal timer.

Clock Synchronization with the Controller

Introduction

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

Configure the Controller 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.
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 controller 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 controller NTP server.

Events Management

Introduction to Event Management

Overview

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 300,000 events. Each data type can support maximum 65,535 events.

  NOTE: One dedicated event buffer is managed per server application (up to four server applications are supported).
- Automatic event backfill to the SCADA or the client station with RTU protocol facility (on DNP3, IEC60870-5-101, or IEC60870-5-104).

For the RTU server configuration (DNP3, IEC60870-5-101, IEC60870-5-104), each object type has an independent event queue setting. To enable event generation, set an event queue for the corresponding object type.

Event Time Stamping

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

- Time stamping performed at source in the controller (requires controller programming).
- Time stamping performed in the BMENOR2200H module (does *not* require controller programming).

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

Event Buffer Capacity in RAM

The number of events in the buffer observes these limitations:

- The module records up to 150,000 (up to 300,000 in Ethernet High Performance mode) event in the event buffer. Each data type can support maximum 65,535 events.
- The event buffer is synchronized (if event sync, page 95 is enabled) between the primary and standby modules in a redundant system.
- The module records up to 10,000 security events per server channel in the event buffer.

NOTE: For more details about to set Ethernet High Performance mode see IP Address Configuration, page 110

Retain or Clear the RAM

The event buffer in RAM is retained in these situations:

- The controller 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 **Clear Events** command to clear the buffer in RAM.
- The controller 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.
- Change the DNP3 cybersecurity configuration on the web page to clear the buffer.
- A SCADA command specifically clears the buffer.
- Reset RTU protocol by Device DDT.

Hot Standby Event Performance

When a BMENOR2200H module generates up to 4,000 events per second, the module still supports a Hot Standby switch-over without event loss (depending on the configuration).

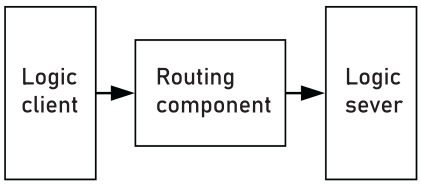
Event Routing

Introduction

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

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

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 server and a client) that are configured in the same station.

In a hierarchical architecture, time stamped events are automatically transferred from low-end server sub stations to the SCADA (or client) through the station. The automatic transfer uses path-through events functionality with a single BMENOR2200H module configured in both the client and server.

Configuration

Configure the BMENOR2200H module for event routing on the data mapping configuration page, page 123.

Considerations:

- The BMENOR2200H module does not detect events for event routing points in a server.
- In a valid configuration for event routing points, only one point is occupied in the database to reduce the data size stored in memory. Use the device DDT to see the point and its structure in the **Variables** list.

Point configuration considerations:

Configuration	Description
channel (See the note below.)	For routing events, configure one client channel and at least one server channel. One client channel is required so that the system can connect with more sub servers, and more server channels allow for more SCADA in the system. **NOTE:** Refer to the channel configuration instructions, page 114.
client data mapping (See the note below.)	Add data points in the client channel. These points show the mapping of client points in the sub server, which communicate with the client channel. **NOTE:** Refer to the DNP3 data object mapping instructions, page 123.
server point	After you configure the points in the client channel, the corresponding point is listed in the server channel. The points used to route are different from the normal points of the server. The parameters (CPU type, CPU address, variable name, and time stamp) of controller mapping are no longer available, and the available parameters are read only. *Their lifetime is consistent with peer point configuration in the client*.

NOTE: When you configure these routing points in the client channel, the module will select the events of the points to be routed, and route events to the corresponding server channel.

For example, if the client channel receives Binary Input point events from the sub server and routes them to the logic server channel, they become the Binary Input point events of logic server channel.

Considerations:

- When you specify one point in the client for event routing, such as the binary input point, one corresponding point configuration is automatically generated in the logic server channel. The point configuration for the logic server channel is read only; it cannot be changed or removed in its DB mapping panel. These points on sever side will not occupy memory usage (8 KB input/8 KB output and 16 KB input/16 KB output in high performance mode).
- If the channel number, session number, or point number mismatches in the server channel, an error page appears.
- If you choose the route to the channel as Disable, the point does not need to be routed to a server.

Channel Combination for Event Routing

To route events inside the BMENOR2200H module, use the configuration instructions to combine the client channel and server channel.

The supported combinations are:

Client Channel	Server Channel
DNP3 net client	DNP3 net server
DNP3 serial client	DNP3 net server
IEC60870-5-101 client	IEC60870-5-104 server
IEC60870-5-104 client	IEC60870-5-104 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 controller cannot get and process the events. (The controller can still get the point value in events just like the standalone client channel.)
- Only events are routed. Requests (commands) from SCADA are not routed to the sub server. This means that inside the BMENOR2200H module, there is no other data exchange or communication between the client channel and the server channel except for events. Not all client and server channel combinations are supported by the event routing function.
- In the system, SCADA cannot communicate with sub servers. The solution uses the logic server in the BMENOR2200H module to simulate sub servers, so SCADA can communicate only with the logic server in the BMENOR2200H module, and the sub server can communicate only with the logic client in the BMENOR2200H module.
- Some information related to events may be changed. Key information related to events like point value and time stamp is kept during event routing. The routed events quality depends on configuration. For example, if quality change is selected when routed device is offline, then the quality bit will become invalid once field device is offline. Other information related to events like point number, events class, and variation is changed according to the client channel configuration.

Events Buffer Size

Confirm that the events buffer of the server are greater than the events buffer in the sub server.

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 to record the events via data types upon a loss of power or a module hot-swap.

These are the storage capacities for events in flash memory for the BMENOR2200H module and the RTU protocol:

- The module records up to 10,000 events into flash memory upon a loss of power.
- The module records only the latest events when number of recorded events exceeds 10,000.
- The module reads events from flash memory when power is restored.

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	Records 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. • The BMENOR2200H receives a RTU reset command from Device DDT.	Does not record 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 records only the latest events.
- Hot Standby systems does not support the event backup feature.

RTU Protocol Data Flow

RTU Communications

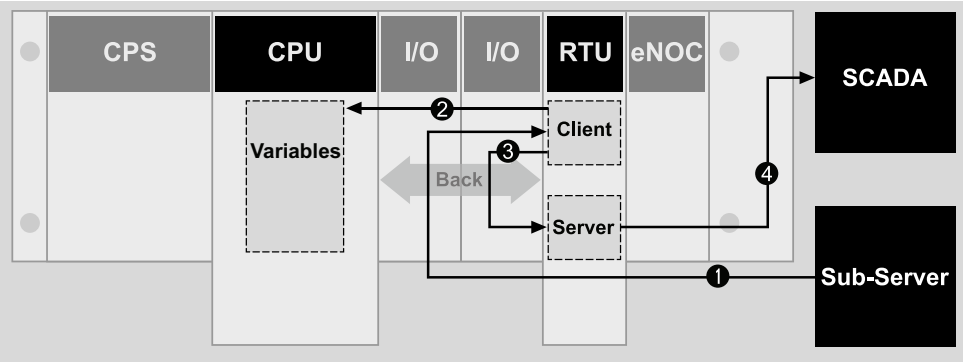
Communication Behavior

The BMENOR2200H module is equipped with a dual-bus connector, page 30 that supports both Ethernet and X Bus communications.

This Ethernet backplane port is used mainly to communicate with the remote client or server with RTU protocols. The backplane interface is used to communicate with other communication modules in rack and RIO. 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 Client Channel Receives Events from the Sub-Server

When something significant changes in the sub-server (like the value of a point), the sub-server 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-server sends events to the client channel of the BMENOR2200H module.

2 The client channel updates the point values in the module and the database of the logic server channel and synchronizes the value to CPU variables.

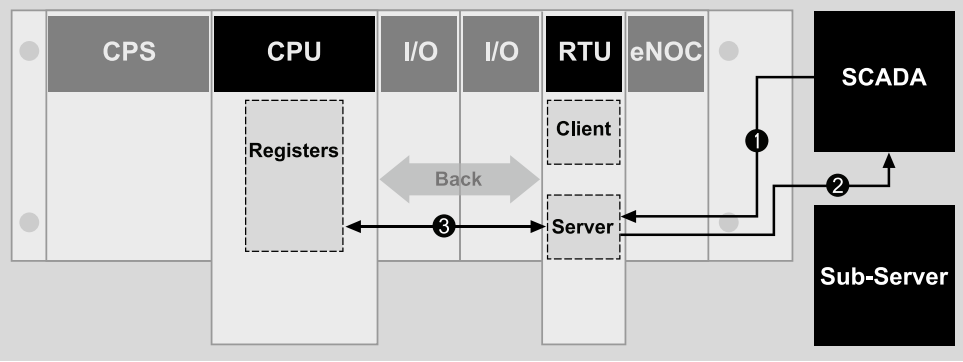
3 Events are routed to server channels according to point configuration.

4 The server channel buffers these events and sends events to SCADA when the communication link is established.

When the Server Channel Receives Request from SCADA

In the RTU system, a SCADA system sends requests (commands) like an Integrity Poll to the server connected to it. The server channel receives this request and sends a response to the SCADA system. With event routing, the behavior of the server channel is exactly the same as a standalone (no event routing) server channel. The client channel and sub-servers 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 server channel.

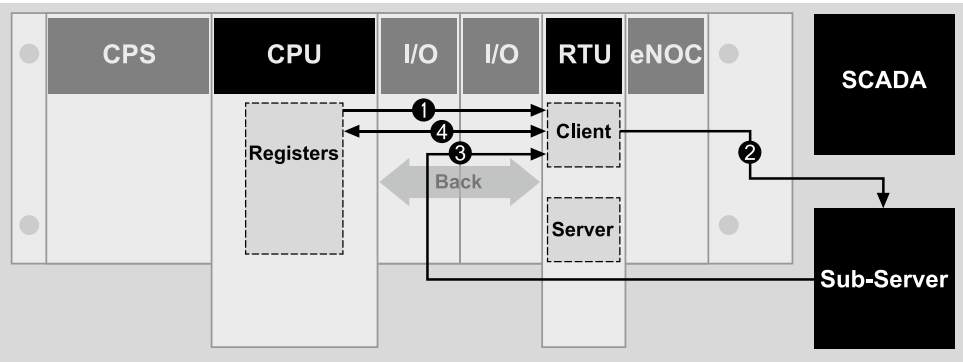
2 The server channel responds to the SCADA request with the point values in the database.

3 The point values are synchronized cyclically between the database of the server channel and CPU registers.

When the Client Channel Sends Request to the Sub-Server

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

Send request to a sub-server example:



1 The application in the M580 CPU sends an Integrity Poll command to the client channel.

2 The client channel sends Integrity Poll requests to the sub-server.

3 The sub-server responds to the request with the value of the latest points.

4 The logic server data base is synchronized while the client channel updates the database.

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

Connection Status

Connection Status

Introduction

The connection status of each channel of the BMENOR2200H module is put in a double-word descriptor in the Device DDT mapping:

- Sever: <DTM Name>_CONN.<Sever Name>.Error_Code
- Client: <DTM Name>_CONN.<Client Name>.Error_Code

Detected Error Codes

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

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 creation error, IPT initialization error, etc.).
3...14	These bits are reserved.
15	A TLS error is detected.

Client:

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 creation error IPT initialization error, etc.).
3	There is an authentication problem.
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	There is an authorization problem.
10	The update key change method is not permitted.
11	The signature is not valid.
12	The certification data are not valid.
13	An unknown user is detected.
14	The capacity of session key status requests is exceeded.
15	A TLS error is detected.

Reset Communication

Introduction

The BMENOR2200H module communicates with the other parties based on TCP/IP. The protocol is DNP3 or IEC104, and the other parties could be SCADA, RTU or other controllers. The network connection is various and combined with lots of switches/routers and other network devices.

In some abnormal cases (for example, the ethernet cable between remote device and switch is broken), the communication may be stopped due to the lost heartbeat packet from partner device, but the link status is still working well. In these cases, it needs some time to retry and timeout finally.

BMENOR2200H module provides a new Device DDT to allow manually reset communication for a quick recovery.

Reset RTU Communication by Variables

The TCP communication or protocol can be reset on the Device DDT.

In the **Project Browser**, expand the **Project > Variables & FB instances > Device DDT Variables > Variables**.

Expand the "CONN" parameters to see the variable **RESET_TCP**:

Name: RESET_TCP

Type: WORD

W: writable

Variable Name	Value	Description
RESET_TCP	0	0 is the initial value and it means no command.
	Change value to 1	If the value is changed to 1, the sever TCP channel and the client will be reset, which means that the TCP connection will close and reopen. There will be no impact on the protocol and events.
	Change value to 2	If the value is changed to 2, the client TCP channel and the sever will be reset, which means that the TCP connection will close and reopen. There will be no impact on the protocol and events.
	Change value to 3	If the value is changed to 3, the protocol will be rest. The reset protocol has two functions: • Close all the channel connections and then reopen them, with the associated configurations, points events, points values deleted and reconstructed. • After reset the protocol, the BMENOR2200H module will obtain the clock time from the M580 controller and then synchronize with it.

Hot Standby Capacity

Introduction

This section describes the functionality of BMENOR2200H redundant modules, including the operating state of redundant RTU modules, depending on the PAC state, Ethernet services, and the Hot Standby switch-over function.

Hot Standby Capacity

Overview

In a running Hot Standby system, you can perform the following actions (in either primary or standby rack, cabled or not cabled), and this action does not cause a Hot Standby switch-over or a duplicate IP address:

- hot-swap a BMENOR2200H module
- remove or reconnect a cable to a BMENOR2200H module

When you clear a detected fault on a BMENOR2200H in a standby rack (network cabling cut, power off, hot swap), this action does not affect the Hot Standby primary operation; in other words, no primary stop or shut down, no I/O bump, or no switch-over occur. The BMENOR2200H module can switch its servers or SCADA connections smoothly during a Hot Standby switch-over.

NOTE:

- During a Hot Standby swap of the BMENOR2200H module, all values are set to *0* in its Hot Standby diagnostics table, page 192.
- The controller automatically switches over under some conditions, but a detected error (for example, in the xxxx module) may stop the switchover. You may have to configure some logic to specifically detect the status of the module to trigger the intended switchover.
- Event backup is not supported in a Hot Standby system. When this function is enabled in a standalone system in which the controller is replaced with a Hot Standby controller, the event backup function is automatically disabled.
- For DNP3, IEC60870-5-101, and IEC60870-5-104, the event acknowledgement in the last cycle may not have synchronized from primary to standby. The acknowledgement also causes SCADA to receive the duplicate event, which has the same time stamp.
- For IEC60870-5-101 (via RS232) is not supported in a Hot Standby system.

Hot Standby Enable/Disable

The Hot Standby event synchronization can be enabled/disabled via DTM configuration in following steps:

Channel Configuration > Server > Advanced Settings > Event Buffer Sync Enable

Hot Standby Path Selection

Configure the Hot Standby communication port via the DTM. The default selection is through the backplane port and once the control ports are enabled, there are two options for path selection:

- Control port
- Backplane port

The Hot Standby service will apply the relevant IP address of different ports to make connection and all HTSB data will be exchanged via that port.

Hot Standby RTU Service

In a Hot Standby system, the input I/O image (••••_CONN Device DDT) is synchronized cyclically between the M580 primary and standby PACs.

The content of diagnostic Device DDT is not required to exchange between the primary and standby BMENOR2200H modules.

Confirm that only the first section in the standby controller is running.

NOTE: An error is detected if you update the RTU Ethernet variables in the first section in the standby controller.

DNP3/IEC60870-5-101/IEC60870-5-104 Server

With a DNP3, IEC60870-5-101, or IEC60870-5-104 server, only the primary module works as usual in a Hot Standby system, and the standby module has no communication with SCADA connections.

- When the DTM configuration of the primary module, as well as its security mode and firmware version are the same as that of the standby module, the two modules can synchronize. In this case, the primary module synchronizes the event history and internal data (unsolicited state, frozen counter....) with the standby module.

  NOTE: Confirm that the primary and standby modules have the same cyber security configurations. If they have different configurations, the modules could still synchronize, but they may not work properly because some channels are disabled due to a missing security policy.
- In run mode, if the primary and standby modules are synchronized, the following items are synchronized via internal protocol:
  - DNP/IEC event
  - DNP/IEC event acknowledgement
  - DNP frozen counter
  - DNP AII dead band
  - DNP enable/disable unsolicited
  - cold/warm start
  - DNP IIN
  - IEC MIT (frozen, sequential number)
  - IEC CRPNA
- When a Hot Standby switch-over occurs:
  - The primary module closes the connection with SCADA.
  - The secondary module gets the data in value from the PAC to the local database first (AO, BO, String, CMD status, P_ME_A, P_ME_B, P_ME_C, IEC P_AC) and then starts to take over and accept new SCADA connections.
  - During a switch-over, all server methods report any detected error codes.
  - With the DNP3 secure authentication enabled, the session key is forced time out.
  - For MIT:

    --> When Auto Local Freeze is set to auto freeze, the new primary module forces a freeze immediately after switch-over.

    --> When Auto Local Freeze is set to freeze by application, if the Freeze Cyclic point value is 1, the new primary module forces a freeze immediately after switch-over.
  - The new primary module handles the last two cycle's data and generates an event.
  - For AI, M_ME_A, M_ME_B, and M_ME_C:

    --> The second from last cycle before a switch-over is set as the base value, on which the data change check is based.

    --> Some of the last two cycle's events may already be synchronized with the standby module, which causes SCADA to receive duplicate events.
- If the module time source is set from the RTU protocol, time synchronizes cyclically between primary and standby BMENOR2200H modules via internal protocol.
- For the IEC60870-5-101 and IEC60870-5-104 message intervals and background periods, the primary and standby modules do not synchronize timer status information. After switch-over, the first cyclic/background message may not remain in time out. The second cyclic/background message remains in time out according to the user setting.

DNP3/IEC60870-5-101/IEC60870-5-104 Client

For a DNP/IEC client, the primary module typically communicates with the remote server, and the standby module does not establish a connection with the remote IED.

- The primary and secondary modules synchronize data from the PAC memory with the local database, but the standby module does not send data to the remote server. Therefore, the remote server receives output data from the primary module only.
- When a Hot Standby switch-over happens, the primary module closes the connection with the remote server, and the standby module takes the role of communicating with the remote server.
- During a switch-over, if some commands (read class, read group, polling command, control operation) are not finished, a detected error code is returned in DDT instance status. The user can manage the status to re-send commands that did not finish.

NOTE: For IEC60870-5-101 and IEC60870-5-104, the client does not immediately send an event acknowledgement, which depends on the W value (maximum unacknowledged received APDUs) and the T2 S frame period (the time to wait before sending a supervisory ADPU acknowledgement). During a Hot Standby module hot swap, the client may receive duplicate events because an event is not acknowledged before the hot swap.

Managing Ethernet Services

This table describes the status of the services that run in the primary and standby BMENOR2200H modules at the RUN and STOP PAC states:

Service List	**Primary BMENOR2200H Module**		**Standby BMENOR2200H Module**	
PAC State	**RUN**	**STOP**	**RUN**	**STOP**
DNP3/IEC server	*RUNNING*	*RUNNING*	*RUNNING* (synchronization from primary)	*RUNNING* (synchronization from primary)
Event routing	*RUNNING*	*RUNNING*	*RUNNING* (synchronization from primary)	*RUNNING* (synchronization from primary)
DNP3/IEC client	*RUNNING*	*RUNNING*	*STOPPED*	*STOPPED*
SNTP client	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*
Modbus TCP client	*RUNNING*	*RUNNING*	*STOPPED*	*STOPPED*
Syslog	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*
Modbus TCP server	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*
Firmware upgrade	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*
SNMPv1	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*
SNMPv3				
Web server (cyber security setting + diagnostic)	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*
OEB (FDR+LLDP)	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*
Data logging	*RUNNING*	*RUNNING*	*RUNNING*	*RUNNING*

Sequence Of Events

Introduction

Use the information in this chapter to configure a BMXERT1604 module's time stamping 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 RTU protocol in a Control Expert project that includes a BMENOR2200H module.

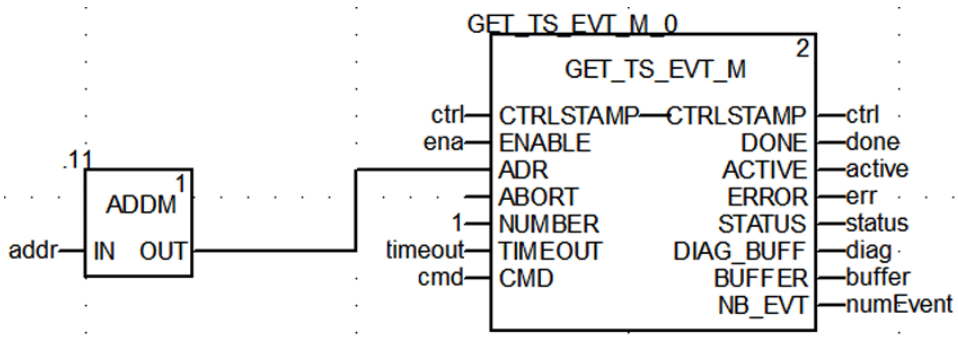
Process Overview

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.

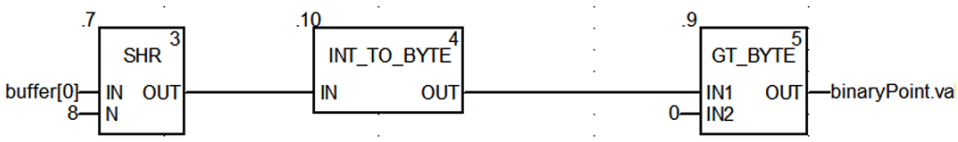
Event Format in Response Buffer

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

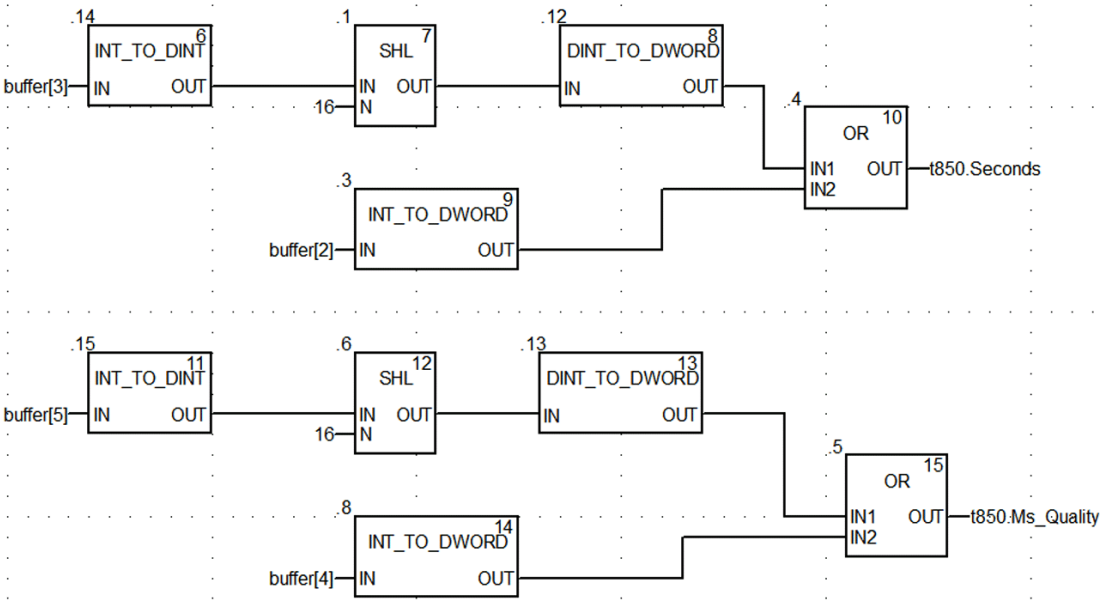
Extract the Time Stamp Event

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]`:



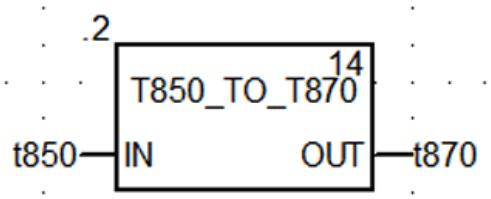
Extract the T850 Data

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	BYTE	Year: 0-99
	reserved	BYTE	Reserved
TIME_850_FORMAT	Seconds	DWORD	Seconds since 1970, confirm the time stamp is later than 2000.

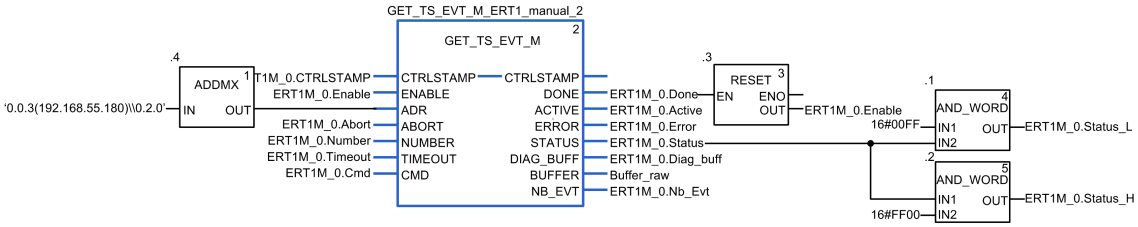
Data Structure	Element	Type	Definition
	Ms_Quality	DWORD	• Bit 0-23: The fraction of the current second when the value of the TimeStamp has been determined. The fraction of second is calculated as (SUM from i = 0 to 23 of bi*2**—(i+1) s). • Bit 24-31: Time Quality • Bit 31: LeapSecondsKnown (not supported) • 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 the 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_Quality:= 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;
```

Configuring the Module

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, page 105.

Configuration Environment Components

Select the appropriate component in the configuration environment with the intended configuration role:

Component	Functional Feature
Control Expert Configuration Overview	BMENOR2200H module name definition, page 109
	adding the module to a Control Expert project, page 109
	IP address assignment, page 110
	basic online diagnostics, page 178
Device DTM	RTU protocol configuration, page 64
	IEC60870-5-104 client/server, page 137
	version selection, page 113
	channel configuration, page 114
	DNP3 Net Client/Server, page 114
	RTU point configuration, page 124
	SNMP agent, SNMP client, page 155
	Network Timing Service (SNTP), page 157
	Control Ports Configuration, page 161
	Export / Import, page 163
	Module Information, page 165
	fast-access link to the diagnostic web pages, page 178
	serial port configuration, page 159
HTTPS web pages	DNP3 Secure Authentication configuration, page 217
	security configuration, page 197
	TLS configuration: • DNP3, page 215 • IEC60870, page 219
	RBAC configuration, page 229
Automation Device Maintenance	firmware upgrade, page 59
project migration	project migration considerations, page 276
	located variables with addresses (DNP3 AO/BO point “On Demand” mode)

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.

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 their 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 record the changes.

  – or –

  Select **OK** to record 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:

Computer Configuration	Requirements
Controller	2.4 GHz, 3.0 GHz or higher recommended.
	Core i3 or higher. Core i7 or higher recommended.
RAM	8 GB, 16 GB recommended.
	16 GB minimum for Windows Server.
Storage	8 GB including the space for the software installation, execution, and for saving applications.
	20 GB recommended.
	SSD drive are recommended.
Operating system and version	Microsoft Windows 10 64-bit, version 21H1 or newer.
	Microsoft Windows 10 64-bit Enterprise 2019 LTSC, version 1809.
	Microsoft Windows Server 2019, standard 1809 version.
	Microsoft Windows 11 64-bit, version 21H1 or newer.
	Microsoft Windows Server 2022, version 21H1 or newer.
Drive	DVD R to install the software. DVD RW recommended.
Display	VGA (800 x 600) minimum resolution.
	Maximum supported resolution 2560 x 1440 with Scale and Layout at 125%.
Input devices	Keyboard and mouse or compatible pointing device.
Web access	License activation on the Internet is recommended.
	Offline activation remains possible (please refer to License Manager or Floating License Manager).
Other	USB port.

NOTE: Windows 10 32-bit is not supported.

The minimum and recommended version of Microsoft Excel to execute the Bulk Configuration, page 164 is Microsoft Excel 2007 and later.

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:

- *client (communication) DTMs*: This DTM is both a device DTM and a communication DTM. The client 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 (client)	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.
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:

```
<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:

```
<172.168.12.1>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 Controller Bus

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

Step	Action
1	Open a project in EcoStruxure 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 scroll to select a **New Device**. **NOTE:** Select a rack position that conforms to the module's slot restrictions, page 46.
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. **NOTE:** There are several BMENOR2200H modules under the **Device List**. The later versions correspond to the newer features from the software version.
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 BMENOR2200H modules to the **PLC bus**. **NOTE:** The local rack in an M580 system can hold a maximum of four communication modules, including the BMENOR2200H modules.

Configuration with Control Expert

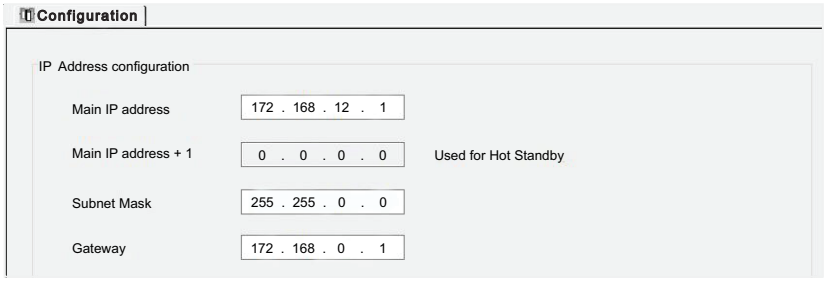
IP Address Configuration

Introduction

Use these instructions to configure the IP address parameters for a BMENOR2200H module. There are two different IP addresses that can be assigned to the module. The IP address of backplane port is configured by Control Expert, and that of control ports is configured by DTM.

Configure IP Address for Backplane Ethernet Port

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. **NOTE:** The **Main IP address + 1** field is used for configuring a redundant system.
4	Click **Function** to select: • **Ethernet**: to choose normal mode • **Ethernet High Performance**: to choose the high performance mode
5	• Click **Apply** to implement your configuration changes. • Click **OK** to implement your changes and close the dialog box.

Configure IP Address for Control Ports

Two control ports share a same IP address. The IP address should be configured manually in the DTM. For details, you can refer to Control Ports Configuration, page 161.

Limitations

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

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, page 60.

Debugging with Control Expert

Overview

This section describes procedures for debugging the configuration of an BMENOR2200H module with Control Expert.

Module Debugging Screen

Introduction

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

Address Information

Parameters

These debugging parameters for TCP/IP utilities in the BMENOR2200H module appear on the module **Debug** screen:

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

LED Display

Observe these LEDs in the upper-right window corner 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.

Observe the LED in the Fault tab for conditions related to the module:

Location	LED	Description
Fault tab	**Fault**	Problem descriptions: • detected internal problem • detected configuration problem • detected communication error • detected application problem • detected configuration error • Ethernet disabled • duplicate IP address • link disconnection • awaiting IP address • storm detection

Configuration in the DTM

Introduction

Use the instructions in this section to configure services through the DTM after you access the services configuration link, page 112.

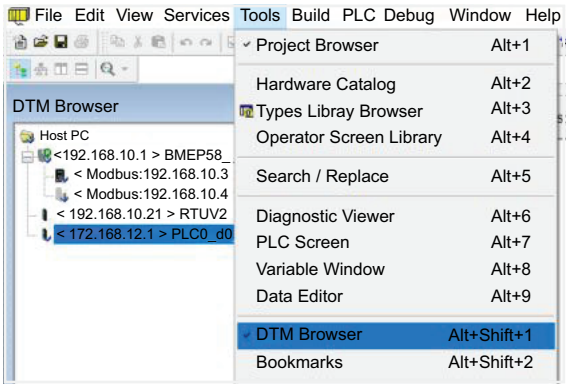
Access the DTM

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.

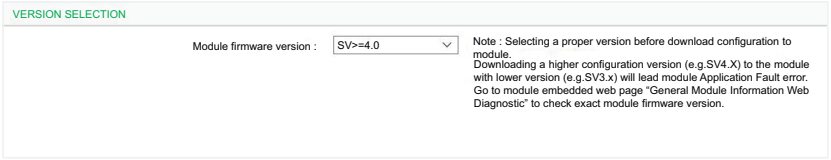
Step	Action
1	Open the Control Expert project that includes the appropriate module.
2	Open the **DTM Browser** (**Tools** > **DTM Browser**). 
3	In the **DTM Browser**, double-click the name that you assigned to the module, page 109 to open the configuration window.

– 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.

Version Selection

Before you configure the module in the DTM, select the DTM template that corresponds to the firmware for your module:

Step	Action
1	Left-click **Version Selection** in the **CONFIGURATION** menu. 
2	Scroll to the appropriate version in the **Module firmware version** pull-down menu.
3	Press the **OK** or **Apply** Button.

NOTE:

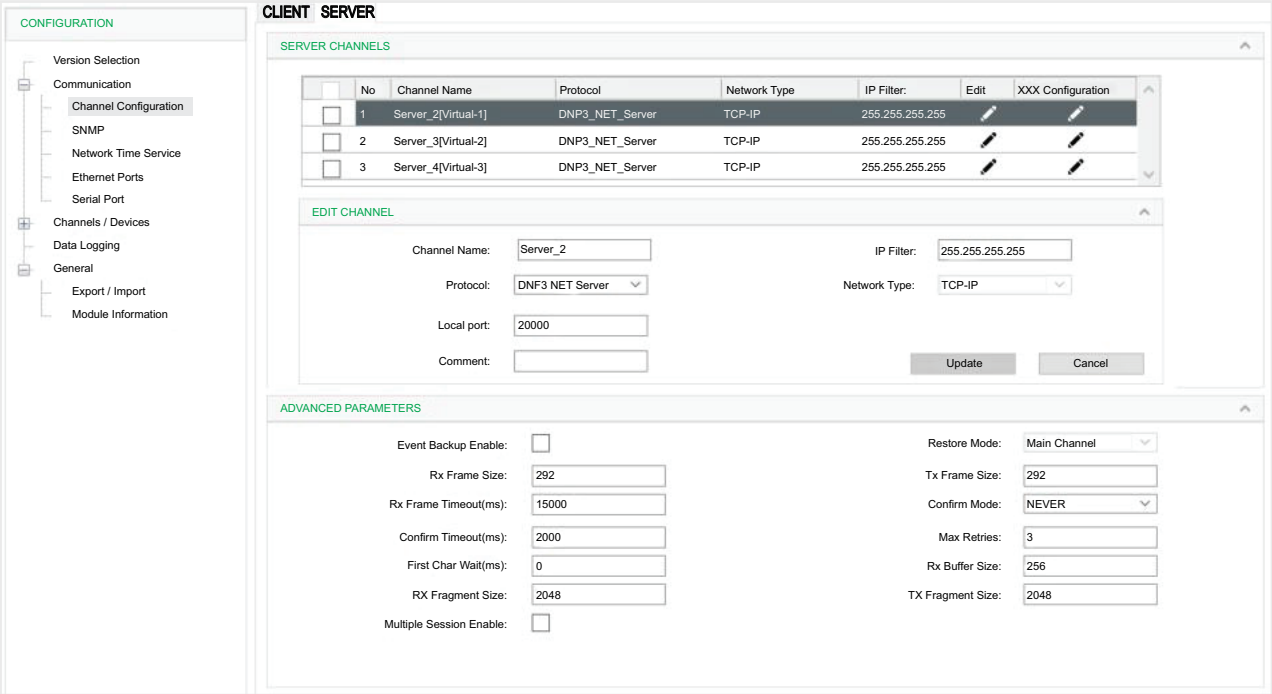
- Select a proper version before downloading configuration to the module. Downloading a higher configuration version to the module with a lower version will cause the module an Application Fault error.
- Go to the module embedded web page *General Module Information Web Diagnostic* to check the exact module firmware version.

DNP3 Channel Configuration

Introduction

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

In the following configuration instructions, make selections that are appropriate for the channel type (server or client).



Configure NET or Serial Channels

Configure *CLIENT* or *SERVER* NET channels:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the open ***CONFIGURATION*** window, expand (**+**) ***Communication*** and select ***Channel Configuration***.
3	Select the appropriate tab: • Select the ***CLIENT*** tab to add client channels. • Select the ***SERVER*** 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, page 115.
6	Select the ***Add*** button to see the newly configured channel in the table.
7	After you create a *server* channel on the ***SERVER*** tab, repeat the above steps to create the corresponding *client* channel on the ***CLIENT*** tab. – or – After you create a *client* channel on ***CLIENT*** tab, repeat the above steps to create the corresponding *server* channel on the ***SERVER*** tab. **NOTE:** • Only one type of RTU protocol can be configured in the module (either DNP3 or IEC60870). The module cannot support multiple RTU protocols configured at the same time. • If the DNP3 Secure Authentication is configured in the web cybersecurity setting, confirm that the configured name of the RTU channel matches the channel name in the DTM. Otherwise, the DNP3 Secure Authentication setting does not map to the corresponding channel in the DTM.

Step	Action
8	• Select *Apply* to implement the changes • Select *OK* to implement the changes and close the dialog box. **NOTE:** When you create the first channel, the expandable ***Channels/Devices*** sub-menu appears on the ***CONFIGURATION*** screen.
9	Repeat these steps to create additional channels while observing these limitations for the module's role: • *RTU Ethernet client:* 64 connections • *RTU Ethernet server:* 4 connections • *RTU serial client:* 32 connections • *RTU serial server:* 1 connection **NOTE:** The serial client supports the signal from serial field devices to the upper-level network through Ethernet.

NOTE: At any time, you can edit or delete a channel, page 118.

Channel Parameter Descriptions

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

These parameters in the ***ADD NEW CHANNEL*** fields are available for the DNP3/ IEC60870 client and server channel configurations:

Field	Client	Server	Description
Channel Name	✓	✓	Assign a name to the server or client on their respective tabs. **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, page 217.
Protocol	✓	✓	*DNP3 NET Client:* Configure the new channel as a DNP3 NET client.
			DNP3 NET Server: Configure the new channel as a DNP3 NET server.
			DNP3 Serial Client: Configure the new channel as a DNP3 serial client.
			DNP3 Serial Server: Configure the new channel as a DNP3 serial server.
			IEC60870-5-101 client: Configure the new channel as a IEC60870-5-101 client.
			IEC60870-5-101 server: Configure the new channel as a IEC60870-5-101 serer.
			IEC60870-5-104 client: Configure the new channel as a IEC60870-5-104 client.
			IEC60870-5-104 server: Configure the new channel as a IEC60870-5-104 serer.
Dest Port	✓	X	Define the destination port. **NOTE:** This parameter is available for DNP3 NET and IEC60870-5-104 configurations only.
Local Port	X	✓	Define the local port for network communications. **NOTE:** This parameter is available for DNP3 NET and IEC60870-5-104 configurations only.
IP Address	✓	X	The IP address in this field is the IP address of the source of the communications packets. **NOTE:** This parameter is available for DNP3 NET and IEC60870-5-104 configurations only.
IP Filter	X	✓	Enter the IP address of the remote device. **NOTE:** • This parameter is available for DNP3 NET and IEC60870-5-104 configurations. • The default value is 255.255.255.255 (present disable IP filter).

Field	Client	Server	Description
Network Type	✓	✓	Select a network protocol: • *TCP-IP* • *UDP-IP* • *TCP-UDP* **NOTE:** This parameter is available for DNP3 NET configurations only.
✓: Available **X**: Unavailable			

Advanced Parameter Configuration

After you create a channel with the instructions above, the new channel appears in the table on the ***CLIENT*** tab or ***SERVER*** 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 ***CLIENT*** tab. • Select the ***SERVER*** tab.
3	Select a row in the table.
4	Click ***Advanced Settings***.
5	Configure the parameters according to the Advanced Parameter Descriptions, page 117.
6	• Select ***Apply*** to implement the changes. • Select ***OK*** to implement the changes and close the dialog box.

Advanced Parameter Descriptions

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

Field	Client	Server	Description
Event Buffer Sync Enable	X	✓	• Enable (value: 1) ◦ Primary BMENOR2200H synchronizes DNP/IEC events to standby BMENOR2200H in runtime. ◦ When HSBY is switched over, SCADA will retrieve events from the new primary BMENOR2200H. If the runtime event generate rate does not exceed the maximum events supported, events are not lost. • Disable (value: 0) ◦ Primary BMENOR2200H does not synchronize DNP/IEC events to standby BMENOR2200H in runtime. ◦ Primary BMENOR2200H synchronizes the time and other data to standby BMENOR2200H in runtime. ◦ When HSBY is switched over: – Standby BMENOR2200H clears the events generated. – Primary BMENOR2200H starts to generate events. – If there are events not reported, those events are lost, and SCADA will not retrieve those events from the primary BMENOR2200H.
Event Buffer Sync Ports	X	✓	Select network path to transfer event sync data. • Backplane Port (default). Generally, the internal sync data should be transferred using the backplane port. • Control Port(s). Event sync data is transferred through front control ports. There are some use cases as below. ◦ The backplane network is not available between Primary controller/ BMENOR2200H and Secondary controller/BMENOR2200H. ◦ The RIO Ring is working under high traffic data.
Event Backup Enable	X	✓	*enabled (selected):* Events are backed up upon a power outage.
			disabled (empty): Events are not backed up upon a power outage.
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 synchronization.
Confirm Timeout	✓	✓	Configure the maximum wait time for link level confirmation.
Offline Poll Period	✓	X	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	✓	X	Configure the wait time for the DNP3 client's response to a transmitted request.
Inhibit command when CPU stop	✓	X	Select this check box to stop sending commands when the controller stops.
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.
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	X	✓	**Main Channel:** Restore events for the main channel or main redundancy group.
			All Channels: Restore all events.
Max Queue Size	✓	X	Configure the maximum number of requests that are queued on a DNP3 client.
Exlude value 0 for BO Pulse_Trip commands	✓	X	Select this check box to stop sending BO Pulse_Trip commands (*Select, Operate, Direct, DirectNoAct, Auto*) when the variable value changes to 0.

Field	Client	Server	Description
Multiple-Session Enable	X	✓	Select this check box to enable the multiple-session configuration for DNP3 Server. Once the multiple-session is enabled, all supported parameters can be configured independently. **NOTE:** When the multiple-session is enabled, check that each channel is assigned with its unique *IP address* and *port number*.
✓: Available **X**: Unavailable			

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

NOTE: When the EcoStruxure 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.

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	Re-configure the parameters in the **EDIT CHANNEL** and **ADVANCED PARAMETERS** fields (described above, page 117).
3	Click **Update** to update the configuration.
4	Click **OK** or **Apply** to record 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 **Delete**.
3	• Select **Apply** to record the changes. –or– • Select **OK** to record the changes and close the dialog box.

DNP3 Device Configuration

Introduction

To facilitate communications with the BMENOR2200H module, configure parameters for the DNP3 communication protocols in the CLIENT PARAMETERS or SEVER PARAMETERS tab in the DTM.

Access the Configuration Tab

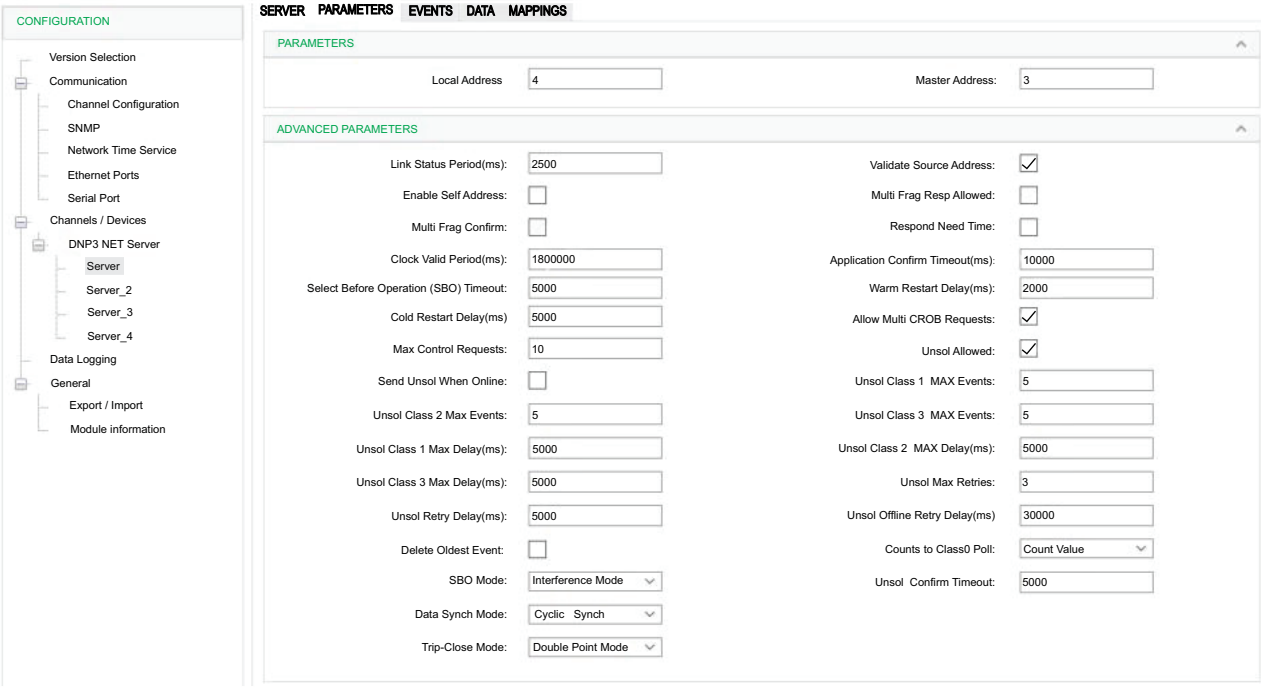
Access the configuration parameters in Control Expert:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	Confirm that you already created client or server channels, page 114.
3	In the **CONFIGURATION** menu, expand (**+**) the **Channels/Devices** sub-menu.
4	Make a selection in the **Channels/Devices** sub-menu: • **DNP3 NET Server** • **DNP3 NET Client** • **DNP3 Serial Server** • **DNP3 Serial Client**
5	Select a specific channel/device in the sub-menu.
6	Select the **CLIENT PARAMETERS** or **SEVER PARAMETERS** tab for the channel.
7	Configure the parameters.
8	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

DNP3 Device Parameters Description

The tables below describe the DNP3 net client/server parameters that appear on the CLIENT/SEVER PARAMETERS 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	Client	Sever	Channel Independence[1]	Description
Local Address	✓	✓	✓	This field contains the source address for this session.
Client Address	✓	✓	✓	This field contains the remote client (destination) address for this session.
Default Response Timeout	✓			Enter a value for the default timeout for the confirmation of request. • The value scope is 0...4294967295. • The default value is 3000.

ADVANCED PARAMETERS:

Parameter	Client	Sever	Channel Independence[1]	Description
Link Status Period	✓	✓	✓	Configure the frequency (ms) for the transmission of status requests when no DNP3 frames are received during this session. **NOTE:** Confirm that the link status period of client and server is set to a non-zero value, such as 2s. If the link status period is set to zero, during a Hot Standby switch-over, the module cannot create a new connection because the old connection is not in time out.
Auto Integrity Local	✓			Issue integrity data poll after local IIN bit was set and cleared. • (Default: Selected)
Auto Integrity Timeout	✓			Issue integrity data poll on time out. • (Default: Deselected)
Auto Event Poll	✓			Issue event data poll when class 1,2, or 3 IIN bit is set. • (Default: Deselected)
Auto Delay Measure	✓			Use delay measurement in time sync. • (Default: Deselected)
Auto Time Sync	✓			Perform time sync on need time (IIN bit set). • None: don't perform time sync. • Serial: using serial method. • LAN: using LAN method. • (Default: None)
Auto Unsolicited	✓			Automatically send unsolicited command upon remote device startup. • None: don't send unsolicited command. • Disable: send disable command. • (Default: None)
Auto Enable Unsol Class1	✓			Indicate which event classes should be enabled for unsolicited reporting. • (Default: None)
Auto Enable Unsol Class2	✓			Indicate which event classes should be enabled for unsolicited reporting. • (Default: None)
Auto Enable Unsol Class3	✓			Indicate which event classes should be enabled for unsolicited reporting. • (Default: Selected)
Read Timeout Allowed	✓			Number of times a read request is allowed to timeout before the session is considered offline. • (Min:0, Max:255, Default:0)
Auto Integrity Overflow	✓			Auto Integrity Overflow. • (Default: Selected)
Validate Source Address		✓	✓	Select this box to validate the source address in received frames.
Enable Self Address		✓	✓	Select this box to have the server respond to address 0xfffc as if it received a request at its configured address. The server responds with its own address so that the client can automatically discover the server address.
Multi Frag Resp Allowed		✓	✓	Select this box to allow the application to send multi-fragment responses.
Multi Frag Confirm		✓	✓	Select 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		✓	✓	Select 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 server DNP3 device waits for an application layer confirmation from the client 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 client 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 client 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		✓	✓	Select this box to allow multiple control relay block objects (CROBs) in a single request.

Parameter	Client	Sever	Channel Independence[1]	Description
Max Control Requests		✓	✓	Configure the maximum number of binary (CROB) or analog control outputs that are allowed in a single request.
Unsol Allowed		✓	✓	Select this box to allow unsolicited responses.
Send Unsol When Online		✓	✓	Select 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.
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: • *Selected:* Delete the oldest event. • *Deselected:* 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 server cancels the selection if the next received request is not an operate request. (Only read requests are processed.) • **Noninterference Mode:** The server 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).
Trip-Close Mode		✓		Select an option: • **Single Point Mode** • **Double Point Mode**
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 **Sync On Demand** mode, client-side routing points for the analog or binary output status do not support server-side mapping. • An underscore (_) is not a valid 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.

NOTE: 1 The parameters ticked in the column *Channel Independence* can be configured independently and respectively on each sever channel, once the multiple-session function is enabled.

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.

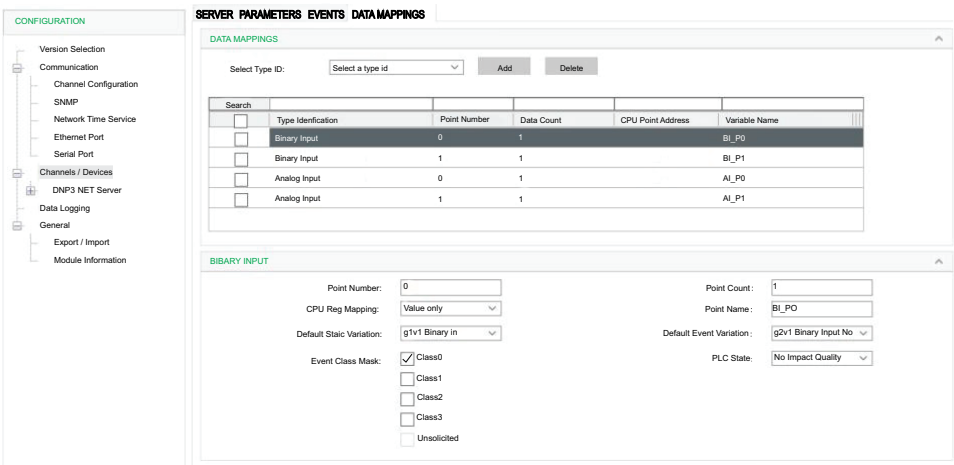
Access the Configuration Tab

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

Step	Action
1	Access the DTM configuration for your module, page 112.
2	Confirm that you already created client or server channels, page 114.
3	In the **CONFIGURATION** menu, expand (**+**) the **Channels**/Devices sub-menu.
4	Make a selection in the **Channels**/Devices sub-menu: • **DNP3 NET Server** • **DNP3 NET Client** • **DNP3 Serial Server** • **DNP3 Serial 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 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 '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.
5	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

Exchangeable Controller 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 select the corresponding box in the **Property value** column. **NOTE:** Select 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	If **Only HMI variables** is selected in the **Data label** (unselected by default), ensure that RTU Device DDT variables are all configured as HMI variables. Otherwise the RTU can report **0x0002** (**"Unlocated variable initialize detected"**) and RTU communication may not operate.
6	• 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 controller and the BMENOR2200H module after you define and manage the memory map of the controller to exchange data with the module.

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

Data Exchange

To sustain a high rate of data exchange, the user can 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. Inconsecutive point number will cause some DNP3 points unavailable to work.

Predefined Command List

The required input fields are requested to define a predefined command item for DNP3 client/DNP3 NET client, page 231.

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
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 server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count		Indicates the number of points.
Store to Controller		Choose a source for the event time stamp and flag: • **Value only:** module time • **Value with time:** controller register time • **Value with flag:** point flag information from the controller registers • **Value with flag and time:** flag and time from the controller 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 Without Events:** Set the flag to offline when the routing channel is offline. • **Invalid Quality With Event:** ◦ Set the point flag to invalid in the event when the routing channel is offline. ◦ Generate event with received flag value when the routing channel is online. The general integrity will be firstly started (if general integrity is enabled in the client).

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 server mode. If this is not the case, the nonconsecutive points do not work normally.
Point Count	indicates the number of points.
Controller Reg Mapping	Choose a source for the event time stamp and flag: • **Value only:** module time • **Value with time:** controller register time • **Value with flag:** point flag information from the controller registers • **Value with flag and time:** flag and time from the controller registers **NOTE:** Select one of these values to implement SOE for time stamping, page 100.
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.
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 server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count		Indicates the number of points.
Store to Controller		Choose a source for the event time stamp and flag: • **Value only:** module time • **Value with time:** controller register time • **Value with flag:** point flag information from the controller registers • **Value with flag and time:** flag and time from the controller 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.
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 for normal operations.
	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 Without Events:** Set the flag to offline when the routing channel is offline. • **Invalid Quality With Event:** ◦ Set the point flag to invalid in the event when the routing channel is offline. ◦ Generate event with received flag value when the routing channel is online. The general integrity will be firstly started (if general integrity is enabled in the client).

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 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. In client, confirm that `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.
Controller Reg Mapping	Choose a source for the event time stamp and flag: • **Value only:** module time • **Value with time:** controller register time • **Value with flag:** point flag information from the controller registers • **Value with flag and time:** flag and time from the controller registers **NOTE:** Select one of these values to implement SOE for time stamping, page 100.
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 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_On:** Change the value. **NOTE:** Refer to the description of binary output behavior, page 131.
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 server mode. If this is not applied, the nonconsecutive points cannot work normally.
Point Count	Indicates the number of points.
TCC	It is used to create Trip Close Control Code of CROB. If it is enabled, the odd point in this configuration is close output and the following point is trip out, when outstation receives close or trip command. Be sure that the point count should be even if enabled. • Default value is *None*.
Short Pulse Duration	Indicates the pre-configured pulse duration of the server
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.
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`.
Controller Register Type	The only available option for the binary output is %MW.
Controller Register Address	This is the start %MW address in the controller. 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 controller %MW register range (default 2048).

NOTE: The **Binary_Output_Status** is applied in the client, which records the latest value, state (flag), and time stamp.

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 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 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	The 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`
Controller Register Type	The only available option for the analog output is %MW.
CPU Register Address	This is the start %MW address in the controller. 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 controller %MW register range (default 2048).

NOTE:

- The **Analog_Output_Status** is applied in the client, which records 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, page 129.

The configuration applies **latch on/off**, **pulse on**, and **Pulse/Trip close**.

Depending on the situation, three control types are available for binary outputs. This table shows examples of Trip/close point numbers in the client and server sides for the BMENOR2200H module.

CROB sent in DNP3 client	Point number in DNP3 client	Point number in DNP3 server
Close/Pulse on (double mode)	*n*	*n*
Trip/Pulse on (double mode)	*n*	*n* + 1
Close/Pulse on (single mode)	*n*	first element of *n*
Trip/Pulse on (single mode)		second element of *n*

Refer to these trigger mechanisms for the corresponding type of control code:

Op type field	Trigger mechanism	Description
Pulse_on	any value change (0...65535)	pulse on if value change
Latch_on	even-to-odd value change, for example: • *0* to *1* • *2* to *3*	latch on
Latch off	odd-to-even value change, for example: • *1* to *0* • *3* to *2*	latch off
Close/Pulse_on	even-to-odd value change, for example: • *0* to *1* • *2* to *3*	pulse on for close output
Trip/Pulse_on	odd-to-even value change, for example: • *1* to *0* • *3* to *2*	pulse on for trip output

Long and Short Pulses of Binary Outputs

This configuration depends on the selection you made for these parameters in the binary output client parameters, page 129:

- **Pulse Duration**: It is the pulse duration setting of the client.
- **Short Pulse Duration**: It is the pre-configured pulse duration of the server.

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

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 server receives the request from the DNP3 client.

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 client and the DNP3 server. 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, page 128.

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 client uses a Read_Group command to read the Octet String.

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

- **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 server:

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

Octet String lengths:

- *maximum:* 255 characters
- *default:* 16 characters

Event Generation

Access the event command configuration in Control Expert:

Step	Action
1	Follow the directions to configure a server channel, page 114.
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 **Apply** to implement your configuration changes. • Click **OK** to implement your changes and close the dialog box.

NOTE: IEC60870-5-101/104 protocols do not support event generation.

Clearing Events in the Server

Clear_Events supports a new point type which clears the event buffer in DNP3 and IEC60870-5-101/104 servers. It enables the user to clear the events buffer in a local or remote SCADA through mapping memory.

To create *Clear_Events* for these servers, 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 ObjectsBinary InputDouble InputBinary CounterAnalog InputBinary OutputAnalog Output*	Specifies the object group whose event is cleared o. demand
Variable Name	—	Indicates the name of the located register.

DNP3 Event Parameters

The event-generation parameters in the following tables are available after you create an instance of the corresponding type ID, page 85. Select the instance of *Generate Events* or *Clear Events* in the **Data Mappings** table to view the parameters.

Generate Events parameters:

Parameter	Description
Point Number	Start point number of the point (min: 0, max: 65535, default: 0)
Point Count	Number of the points (min: 0, max: 7000, default: 1)
Object Group	Object group to read (default: binary input)
Point Name	Name of located or unlocated register (default: –, forbidden symbol: {} “ [], max length: 50) default: CE_P0_P0
Add CMD_STATUS	*selected:* Specify a CMD_STATUS variable name.
	deselected: A CMD_STATUS variable name is not specified.

Clear Events: parameters:

Parameter	Description	
Object Group	Object group to read (default: binary input)	
Point Name	Name of located or unlocated register (default: –, forbidden symbol: {} “ [], max length: 50) default: CE_P0_P0	
Add CMD_STATUS	*selected:* Specify a CMD_STATUS variable name.	
	deselected: A CMD_STATUS variable name is not specified.	
Channel Mask	*Main Channel*	Select the appropriate *Channel Mask* box to specify the channel number to clear an object group. **NOTE:** This functionality is configuration dependent.
	Virtual Channel-1	
	Virtual Channel-2	
	Virtual Channel-3	

Event Queue Setting Page

Configure the parameters on the **Events** tab to map the event queue status to the Device DDT registers in the controller. 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/Devices** > **<DNP3 NET Server>** > **<ServerName>**
2	Make a selection in the **Select Type Id** pull-down menu on the **EVENTS** tab
3	Select **Add** 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 **Apply** to implement your configuration changes. • Click **OK** to implement your changes and close the dialog box.

DNP3 Events

Introduction

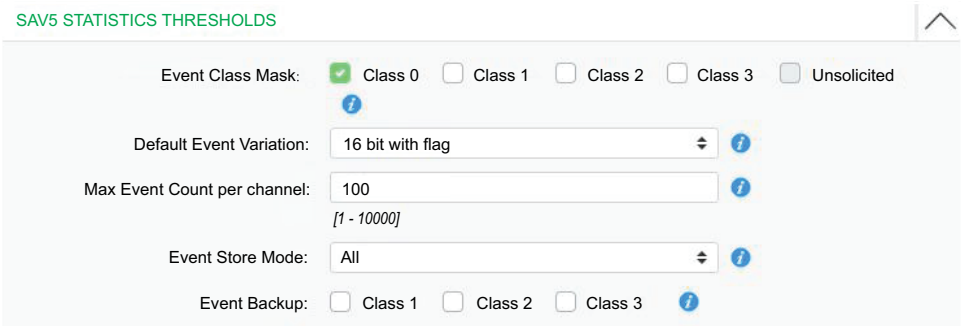
You can configure the **Events** tab for DNP3 NET server channels.

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, page 112.
2	Confirm that you already created client or server channels.
3	In the **CONFIGURATION** menu, expand (**+**) the **Channels/Devices** sub-menu.
4	Select **DNP3 NET Server** from the **Channels/Devices** 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, page 124.
7	Click the **OK** or **Apply** button to implement your configuration changes.

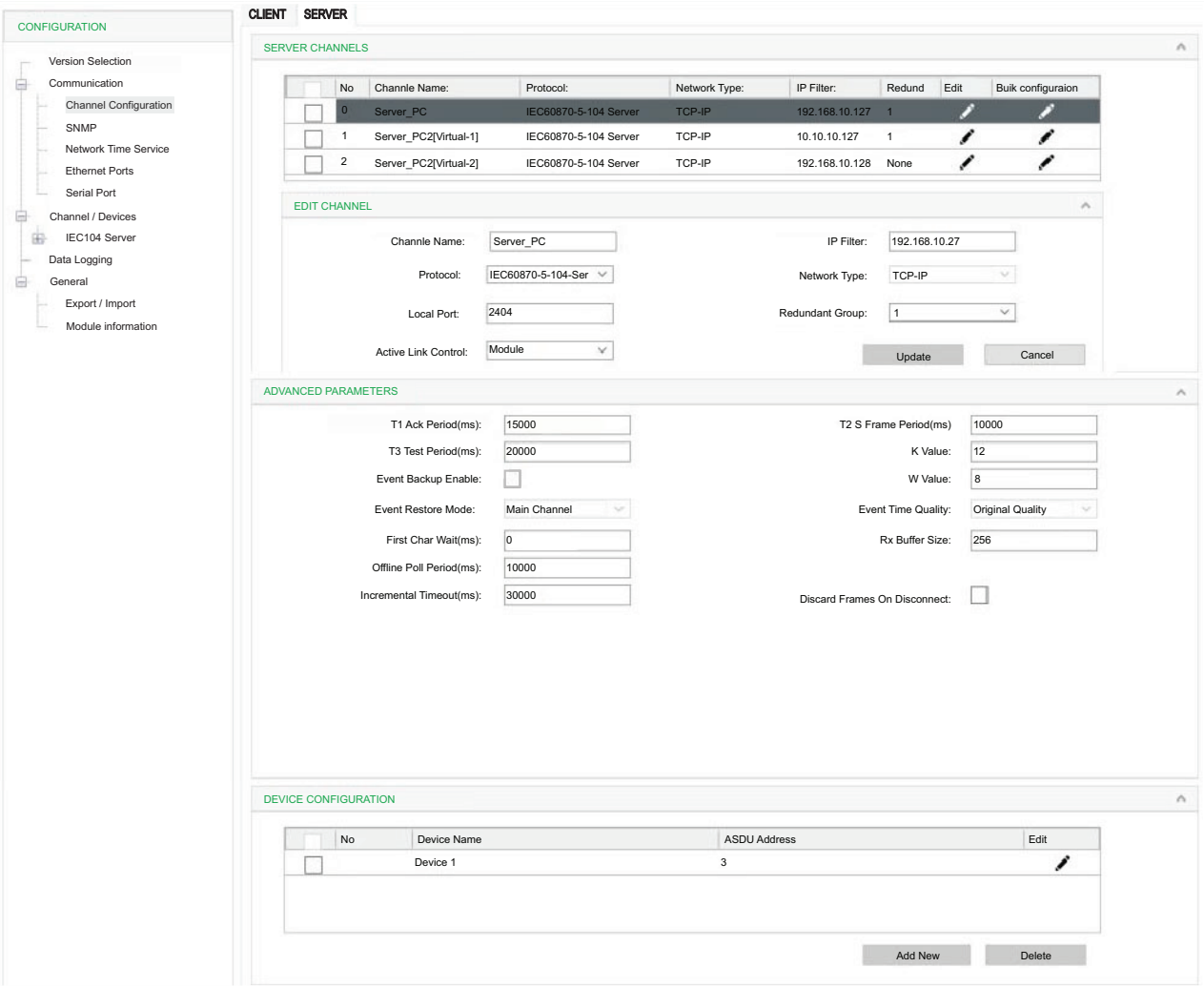
NOTE: Configure the DNP3 SAv5 security events (object 121/122) on the web pages.



IEC60870 Channel Configuration

Introduction

Configure the IEC60870-5-101 and IEC 60870-5-104 communications for your module in the Control Expert DTM.



Basic Parameter Configuration

Configure the **CLIENT** or **SERVER** channels:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the open **CONFIGURATION** window, expand (+) **Communication** and select **Channel Configuration**. **NOTE:** The **Channels/Devices** menu item cannot be expanded because there are no configured channels.
3	Select the appropriate tab: • **CLIENT**: Add client channels. • **SERVER**: 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.
6	Select the **Add** button to see the newly configured channel in the table. **NOTE:** The **Devices** menu can now be expanded because there is at least one configured device. All configured devices appear in this menu.

Step	Action
7	After you create a *server* channel on the **SERVER** tab, repeat steps 1-6 to create the corresponding *client* channel on the **CLIENT** tab (or vice versa). **NOTE:** Only one client and one server are supported.
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/Devices** sub-menu appears on the **CONFIGURATION** screen.
9	Repeat steps 1-8 to create additional channels while observing these limitations: • *client*: ◦ *IEC60870-5-104*: 64 connections ◦ *IEC60870-5-101*: 32 connections • *server*: 4 connections

Basic 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 IEC60870-5-101/104 client and server channel configurations:

Field	Client	Server	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.
Protocol	✓	✓	IEC60870-5-104 client IEC60870-5-104 server IEC60870-5-101 client IEC60870-5-101 server
IP Address	✓		Enter the IP address of the server with which the client communicates. **NOTE:** This field applies to IEC60870-5-104 only.
Dest Port	✓		Define the destination port. **NOTE:** This field applies to IEC60870-5-104 only.
IP Filter		✓	When you select the **IP Filter** field, the **IP Filter Panel** dialog box opens. Enter the IP address of the remote device. Select the **Ok** button. **NOTE:** This field applies to IEC60870-5-104 only.
Local Port		✓	Define the local port for network communications. • This field applies to IEC60870-5-104 only. • The default value is 2404.
Redundant Group		✓	Select None, 1, 2 from the drop-down list. **NOTE:** This field applies to IEC60870-5-104 only.

Advanced Parameter Configuration

After you create a channel using the instructions above, the new channel appears in the table on the **CLIENT** or the **SERVER** tab. You can configure **ADVANCED PARAMETERS** for the channel. These advanced parameters are global settings that are implemented on all server or client channels.

Step	Action
1	Select **Channel Configuration** from the **Communication** menu.
2	Select the appropriate tab: • **CLIENT**: View the **CLIENT CHANNEL** table. • **SERVER**: View the **SERVER CHANNEL** table.
3	Select a row in the table.
4	Select 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 PARAMETER** fields.
5	Configure the parameters according to the advanced parameter descriptions below.
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

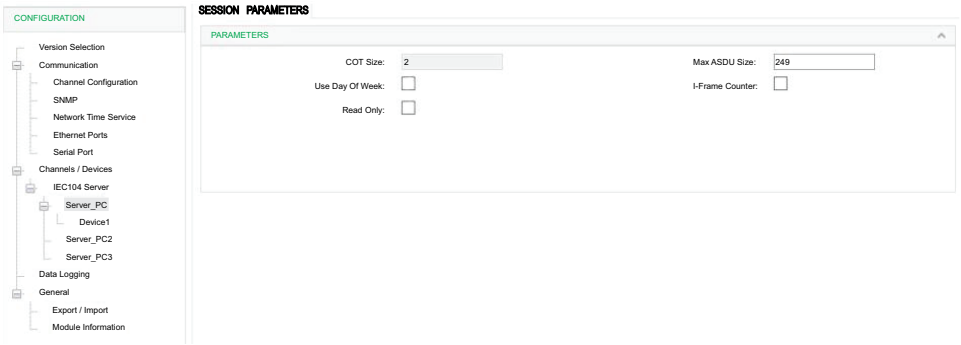
Field	Client	Server	Description
T1 Ack Period (ms)	✓	✓	Enter a value for timeout of waiting for ACK to a transmitted APDU. T1 of server should be greater than T2 of client. • The value scope is 0…4294967295. • The default value is 15000.
T2 S Frame Period (ms)	✓	✓	Enter a value for time to wait before sending supervisory APDU ACK. • The value scope is 0…4294967295. • The default value is 10000.
T3 Test Period (ms)	✓	✓	Enter a value for Idle before sending TEST APDU. • The value scope is 0…4294967295. • The default value is 20000.
K Value	✓	✓	Enter a value for the max unacknowledged transmitted APDUs. • The value scope is 1…12. • The default value is 12.
First Char Wait (ms)	✓	✓	Enter a value for the minimum time between reception and transmission. • The value scope is 0...65535. • The default value is 0.
W Value	✓	✓	Enter a value for the max unacknowledged received APDUs. • The value scope is 0…32767. • The default value is 8.
Rx Buffer Size	✓	✓	Enter a value for the receive buffer size of serial port (bytes). • The value scope is 0...256. • The default value is 256.
Offline Poll Period (ms)	✓	✓	Enter a value for the period to re-establish transfer of an offline session. • The value scope is 0...4294967295. • The default value is 10000.
Max Queue Size	✓		Enter a value for the maximum request message number with a specific application specific data unit (ASDU) type and destination matching an outstanding request that will be queued on a client. • The value scope is 0...65535 (unlimited queue). • The default value is 0 (disabled queue).
Incremental Timeout (ms)	✓	✓	Enter a value for the incremental application layer time-out. • The value scope is 0...4294967295. • The default value is 30000.
Inhibit command when CPU stop	✓		Select this box to stop sending commands when the controller stops.
Event Backup Enable		✓	Specify whether to back up events when a power outage is detected. By default, the check box is deselected.

Field	Client	Server	Description
Event Buffer Sync Enable		✓	• Enable (value: 1) ◦ Primary NOR synchronizes DNP/IEC events to standby NOR in runtime. ◦ When HSBY is switched over, SCADA could retrieve events from the new primary NOR. If the runtime event generate rate doesn’t exceed the maximum events supported, events won't lost. • Disable (value: 0) ◦ Primary NOR doesn't synchronize DNP/IEC events to standby NOR in runtime. ◦ Primary NOR synchronizes the time and other data to standby NOR in runtime. ◦ When HSBY is switched over: – Standby NOR clears the events generated. – Primary NOR starts to generate events. – If there are events not reported, those events will get lost, and SCADA could not retrieve those events from the primary NOR.
Event Buffer Sync Ports		✓	Select network path to transfer event sync data. • Backplane Port (default) Generally, the internal sync data should be transferred via backplane port. • Control Port(s) For cases below, the sync path could be changed from backplane port to front ports. ◦ The backplane network is not available between Primary controller/NOR and Secondary controller/NOR. ◦ The RIO Ring is running heavily and to avoid more traffic data.

IEC60870 Session/Device Configuration

Introduction

To facilitate communications with the BMENOR2200H module, configure parameters for the IEC60870 communication protocols in the SESSION PARAMETERS or DEVICE PARAMETERS tab in the DTM.



Access the Configuration Tab

Access the configuration parameters in Control Expert:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	Confirm that you already created client or server channels, page 114.
3	In the **CONFIGURATION** menu, expand (**+**) the **Channels/Devices** sub-menu.
4	Make a selection in the **Channels/Devices** sub-menu: • **IEC60870-5-104 Server** • **IEC60870-5-104 Client** • **IEC60870-5-101 Server** • **IEC60870-5-101 Client**
5	Select a specific channel/device in the sub-menu to see the session parameters or device parameters.
6	Select the **SESSION PARAMETERS** or **DEVICE PARAMETERS** tab for the channel.
7	Configure the parameters.
8	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

IEC60870 Session Parameters Description

Access the client and server session parameters.

Client: Select the client session parameters from the **CONFIGURATION** menu (**Channels / Devices > IEC101/104 Client > Client**):

Parameter	Description
COT Size	Configure the bytes of COT.
Original address for COT	Use as a second COT byte if the COT length is 2.
Default Response Timeout	This is the timeout value for deleted responses. **NOTE:** Configure this value to delete old responses in the queue that are no longer relevant.
Use Day of Week	Deselect this box to ignore dayOfWeek from IEC60870. **NOTE:** Some devices cannot receive the dayOfWeek input.
Strict Cot Checking	Select this box to enforce COT checking.

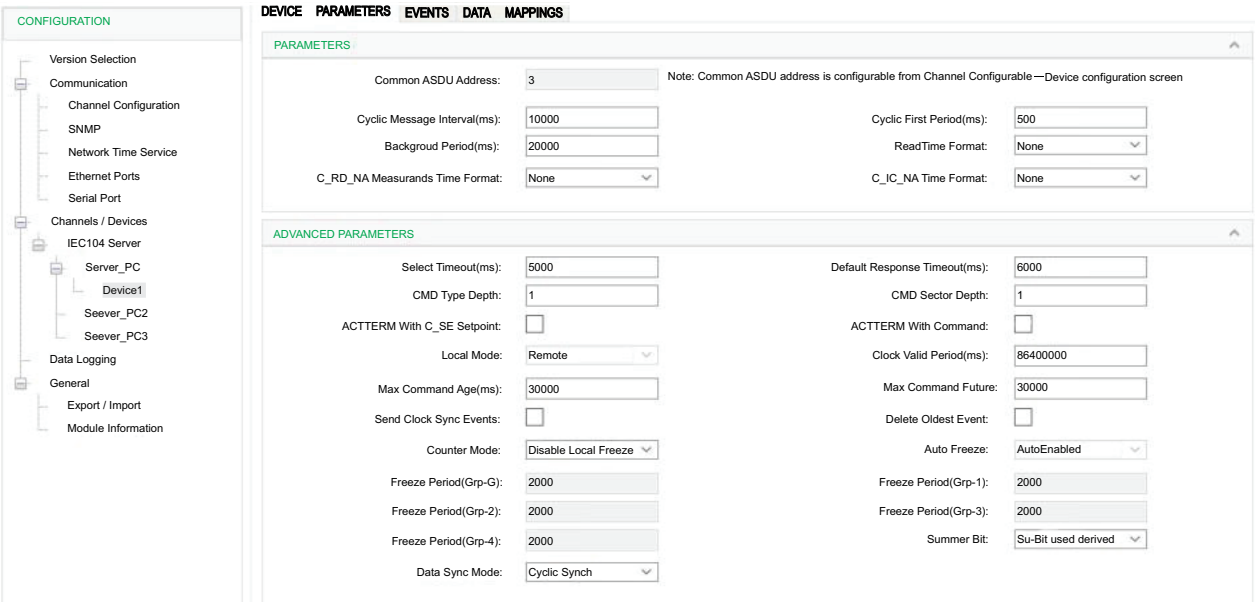
Server: Select the server session parameters from the **CONFIGURATION** menu (**Channels / Devices > IEC101/104 Server > Server**):

Parameter	Description
COT Size	Configure the bytes of COT.
Use Day of Week	Deselect this box to ignore dayOfWeek from IEC60870. **NOTE:** Some devices cannot receive the dayOfWeek input.
Max ASDU Size	Configure the maximum size of an Application Specific Data Unit.
Read Only	Select this box to enable read only mode for IEC104 Server channel(s).

IEC60870 Device Parameters Description

The tables below describe the IEC60870 client/server parameters that appear on the DEVICE PARAMETERS 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	Client	Sever	Description
Common ASDU Address	✓	✓	Enter a value for the common address of an ASDU. • The value scope is 1...65535. • 65535 is the broadcast address. • The default value is 3. **NOTE:** Common ASDU address is configurable from **Channel Configuration > Device Configuration** screen.
Cyclic Message Interval (ms)		✓	Enter a value for the number of milliseconds between cyclic updates. • The value scope is 1...4294967295. • The default value is 10000.
Cyclic First Period (ms)		✓	Enter a value for the period to generate the first cyclic data response. • The value scope is 1...4294937295. • The default value is 500.
Background Period (ms)		✓	Enter a value for the period allowed to generate background scan data on a particular sector. • The value scope is 1...4294967295. • The default value is 20000.
Read Time Format		✓	Select the completeness time format for responding to C_RD_NA from the drop-down list: • None • CP24 only for IEC60870-5-101 • CP56 The default value is None.

Parameter	Client	Sever	Description
C_RD_NA Measure and Time Format		✓	Select the time stamp format in the response to read command from the drop-down list: • None • CP24 only for IEC60870-5-101 • CP56 **NOTE**: • This field is used for measured points. • The default value is None.
C_IC_NA Time Format		✓	Select the time stamp format in the response to read command from the drop-down list: • None • CP24 only for IEC60870-5-101 • CP56 **NOTE**: • This field is used for counters. • The default value is None.

NOTE: When the module receives a C_RD command, it responds to the information object with the requested information-object address (IOA). When multiple data points have the same IOA, the module returns the first information object according to this priority: M_SP, M_DP, M_ST, M_BO, M_ME_A, M_ME_B, M_ME_C, P_ME_A, P_ME_B, P_ME_C, CUSTOM_M_IT_D. Consider these points when you configure IEC60870-5-104 server communications.

ADVANCED PARAMETERS:

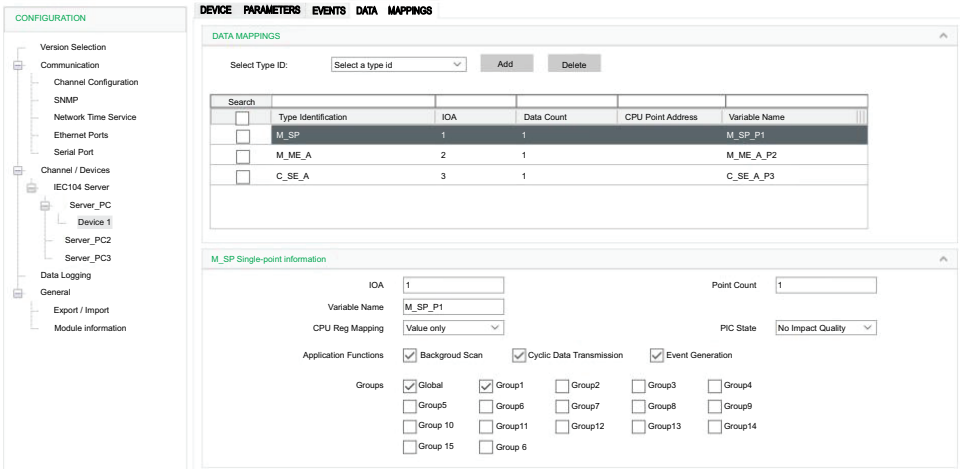
Parameter	Client	Sever	Description
Select Timeout (ms)		✓	Enter a value for the period after which a previously received selection is timed out. Confirm that an executed command is received before the time-out in order to be valid. • The value scope is 0...4294967295. • The default value is 5000.
Default Response Timeout (ms)		✓	Enter a value for the default timeout for the confirmation of request. • The value scope is 0...4294967295. • The default value is 60000.
CMD Type Depth		✓	Enter a value for the size of a command queue to process in parallel for each point type. • The value scope is 1...128. • The default value is 1.
CMD Sector Depth		✓	Enter a value for the total number of simultaneous commands supported by the sector. • The value scope is 1...128. • The default value is 1.
ACTTERM with C_SE Setpoint	✓	✓	Select the check box for ACT TERM to be transmitted upon completion of the set point commands: • C_SE_NA, C_SE_NB, C_SE_TA, C_SE_TB, C_SE_TC **NOTE:** The check box is selected by default.
ACTTERM with Command	✓	✓	Select the check box for ACT TERM to be transmitted upon completion of commands, other than the set point commands. **NOTE:** The check box is selected by default.
Clock Valid Period (ms)		✓	Enter a value for the period for which the system clock remains valid after a clock synchronization. If this period expires without a clock synchronization, all times are reported invalid. • The value scope is 0...4294967295. • The default value is 86400000.
Max Command Age (ms)		✓	Enter a value for the maximum time delta at which commands are accepted. The command time tag is selected and if the elapsed time is greater than `MAX Command Age (ms)`, the command gets no response. • The value 0 indicates that the command time tag is not selected. • The value scope is 0...600000. • The default value is 30000.

Parameter	Client	Sever	Description
Max Command Future		✓	Enter a value for the maximum delta at which commands are accepted with future time. There is a conformance test that says time in the future by one hour also fails. If a time tag command is received with a time before that current time plus the `Max Command Future`, the command will be discarded, with no response sent. • The value scope is 0...600000. • The default value is 30000.
Send Clock Sync Events		✓	Select the check box to send spontaneous clock synchronization events to the client. **NOTE:** The check box is de-selected by default.
Delete Oldest Event		✓	Indicates whether or not the oldest event is removed from the event queue when the buffer is full and a new event arrives. • Select the check box to remove the oldest event. • De-select the check box to ignore the new event. • The check box is de-selected by default.
Counter Mode		✓	Specify the mode of freezing counter: • Disable Local Freeze: freeze by counter - interrogation command only (Mode C or Mode D). • Enable Local Freeze without Reset: enable local freeze counter automatically (Mode A or Mode B) and freeze by counter - interrogation command (Mode C or Mode D). • Enable Local Freeze with Reset: enable local freeze with reset counter automatically (Mode A or Mode B) and freeze by counter - interrogation command (Mode C or Mode D). • The default value is *Disable Local Freeze* (Mode C or Mode D).
Summer Bit		✓	Select this check box to manage the summer bit of time stamp that comes from an external device or the controller. • This feature is effective only if Daylight Saving Time is enabled. • The check box is de-selected by default.
Data Sync Mode		✓	Select a data synchronization mode: • **Cyclic Sync**: Use the default (cyclic) synchronization. • **Sync On Demand**: Allow the PAC application to implement local changes on the binary or analog output. **NOTE:** Enabling a Sync On Demand point changes the variable structure (out of the Device DDT).
M_EI_NA GI	✓		Select the check box for general interrogation to be performed after receiving an M_EI_NA EOI message. **NOTE:** The check box is selected by default.
M_EI_NA Time sync	✓		Select the check box to indicate that Clock Sync is performed after receiving an M_EI_NA EOI message. **NOTE:** The check box is selected by default.
M_EI_NA CI	✓		Select the check box to indicate that counter interrogation is performed after receiving an M_EI_NA EOI message. **NOTE:** The check box is de-selected by default.
Online GI	✓		Select the check box to indicate that general interrogation is performed when a remote device has come online and is available for devices that do not generate an M_EI_NA EOI message. **NOTE:** The check box is selected by default.
Online Time Sync	✓		Select the check box to indicate that Clock Sync is performed when a remote device has come online and is available for devices that do not generate an M_EI_NA EOI message. **NOTE:** The check box is selected by default.
Online CI	✓		Select the check box to indicate that counter interrogation is performed when a remote device has come online and is available for devices that do not generate an M_EI_NA EOI message. **NOTE:** The check box is de-selected by default.
Command with Time Tag	✓		Select the check box to indicate that the control command follows the time tag. **NOTE:** The check box is de-selected by default.

IEC60870 Data Object Mapping

Introduction

To facilitate communications with the BMENOR2200H module, create data points for the IEC60870-5-101/104 communication protocols 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, page 112.
2	Confirm that you already created client and/or server channels, page 115.
3	In the **CONFIGURATION** menu, expand (+) the **Channels** sub-menu.
4	Make one of the following selections in the **Channels/Devices** sub-menu: • **IEC104 Client** • **IEC104 Server** • **IEC101 Client** • **IEC101 Server**
5	Select the desired device 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.

IEC60870 Data Mappings

Edit the data point configuration on the **DATA MAPPINGS** tab:

Step	Action
1	Select a type ID in the **Select Type Id** drop-down list.
2	Select **Add** to configure the data object type.
3	Configure the data object type. Depending on the data object type and the selected protocol profile, different configuration fields are required to define a data object mapping item.
4	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

IEC60870 Data Mapping Parameters

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.

This table describes parameters that appear on the DATA MAPPINGS tab for both client and sever:

Client & sever Parameter	Description
IOA	Indicates the information object address of the object.
Point Count	Indicates the number of objects defined. The IOA of each object defined. The IOA of each object is in sequence from the first object address.
Variable Name	Indicates the variable name.
CPU Reg Mapping	Indicates the choice of the stored time or flag; follows the value in the controller Device DDT variable: • **Value only:** module time • **Value with time:** controller register time • **Value with flag:** point flag information from the controller registers • **Value with flag and time:** flag and time from the controller registers
Threshold	Indicates the default threshold value for M_ME_A/M_ME_B point to trigger event.
	Indicates the default threshold value for M_ME_C point to trigger event.
Low Limit	Indicates the low limit value for M_ME_A/M_ME_B point to trigger event.
	Indicates the low limit value for M_ME_C point to trigger event.
High Limit	Indicates the high limit value for M_ME_C point to trigger event.
	Indicates the high limit value for M_ME_A/M_ME_B point to trigger event.
Add CMD_STATUS	Specify the CMD_STATUS variable name.

This table describes parameters that appear on the DATA MAPPINGS tab for sever:

Sever Parameter	Value Scope	Description
Associate Point Number	104 max.: 16777215 101 max.: based on IOA size	Starting point number of the point.
Channel Mask	Check boxes	For each check box, specify the channel number to clear object group (dependent on the channel configuration).
Default Qualifier	• Short Pulse • Long Pulse • Persistent Output	Default qualifier of the command if the controlling station does not specify a qualifier.
Freeze Period	0...4294967295	Specify the width of the pulse (ms).
M_ME_*X* Point Number	1...16777215	Specify the associated M_ME_*X* point parameter.
PLC State	No Impact Quality Impact Quality	Specify whether the quality of monitoring points are impacted by the PLC state.
Type	(command types)	Select a command type.
Short Pulse Duration	0...4294967295 ms	Indicates the short pulse duration for C_SC/C_DC/C_RC control point.
Long Pulse Duration	0...4294967295 ms	Indicates the long pulse duration for C_SC/C_DC/C_RC control point.
Need Select	Check box	Indicates the need to select before operation for C_SC/C_DC/C_RC/C_SE_A/C_SE_B/C_SE_C control command.
Cdc Mode	• Determinate state • Indeterminate state	Indicates the pulse recovery state for C_DC command. In determinate state mode, it recovers to the previous on (2)/off (1) state. In indeterminate state mode, it recovers to the fixed intermediate (0) state.
Global 1/2/3/4/5/6/7/8/910/11/12/13/14/15/16	Check box	Defines the data object group responding to the interrogation command from the client. It can be a combination of options.

This table describes parameters that appear on the DATA MAPPINGS tab for client:

Client Parameter	Value Scope	Description
Operation Mode	• Auto • Select • Execute • Deselect	Indicates the operation mode for C_SC/C_DC/C_RC/C_SE_A/C_SE_B/C_SE_C control command.

Client Parameter		Value Scope	Description
		• Activation • Deactivation	Indicates the active/deactive operation for the C_IC/P_AC point.
		• Read • Freeze • Freeze with reset • Reset	Indicates the operation mode for C_CI control command.
Qualifier		• Default • Short Pulse • Long Pulse • Persistent Output	Indicates the qualifier for C_SC/C_DC/C_RC control command. When it is received, a C_SC/C_DC/C_RC command with 'default qualifier,' the server operates the command with this configured qualifier.
		G/1/2/3/4/5/6/7/8/9/10/11/12/13/14/15/16	Indicates the interrogation group for C_IC control command.
		1/2/3/4/G	Indicates the counter interrogation group for C_CI control command.
		• General • Event	Indicates general reset or event clear for C_RP control command.
		• Threshold • Low limits • High limits	Indicates the parameter type to set for P_ME_A/P_ME_B/P_ME_C point.
Read Number		1...16777215	Indicates the information object address of the point to be read.
Qualifier		• Threshold • Low limits • High limits	Indicates the parameter type to set for P_ME_A/P_ME_B/P_ME_C point.
Event Routing	**Route Channel**	Disable/Enable	Indicates whether the event routing function is disabled or enabled.
	Route Session	0	Indicates the session number to route.
	Route Sector	Server device list	Indicates the device to route.
	Route Point	1...16777215	Indicates the information object address to route.
	Routing Offline	Valid Quality	Use any available routing channel connection.
		Invalid Quality Without Events	Set the flag to offline when the routing channel is offline.
		Invalid Quality With Event:	• Set the point flag to invalid in the event when the routing channel is offline. • Generate event with received flag value when the routing channel is online. The general integrity will be firstly started (if general integrity is enabled in the client).
	Background Scan	Check box	Indicates the background scan is enabled. (The check box is selected.)
	Cyclic Data Transmission	Check box	Indicates the cyclic data transmission is enabled. (The check box is selected.)
	Event Generation	Check box	Indicates that events for points can be configured.

Data Point Mapping with DDDT Variable Definition

This table describe the IEC60870-104 Client DDDT points definition, including Value and Flag.

IEC data point	DDDT Name	DDDT Data Type	Comments
M_SP/M_DP/M_ST	.Flags	BYTE	Read-only points
	.Timestamp	CP56Time2a	
	.value	BYTE	
M_BO	.Flags	BYTE	
	.Timestamp	CP56Time2a	
	.Value	DWORD	
M_ME_A/M_ME_B	.Flags	BYTE	
	.Timestamp	CP56Time2a	
	.Value	INT	
M_ME_C	.Flags	BYTE	
	.Timestamp	CP56Time2a	
	.Value	REAL	
M_IT	.Flags	BYTE	
	.Timestamp	CP56Time2a	
	.Value	DINT	
C_SC	.Value	BYTE	When value changed: If the bit 0 is 0, an OFF C_SC command is sent out If the bit 0 is 1, an ON C_SC command is sent out.
	.Status	WORD	
C_DC	.Value	BYTE	When value changed: If bit 1:bit 0 is 01, an OFF C_DC command is sent out If bit 1:bit 0 is 10, an ON C_SC command is sent out.
	.Status	WORD	
C_RC	.Value	BYTE	When value changed: if the value is bigger than previous, a higher C_RC command is sent; if the value is lower than previous, a lower C_RC command is sent out.
	.Status	WORD	
C_SE_A/C_SE_B	.Value	INT	When value changed, and the difference value is bigger than dead-band or the value exceeds low-limit/high-limit, a C_SE command with value is sent out.
	.Status	WORD	
C_SE_C	.Value	REAL	
	.Status	WORD	
C_BO	.Value	DWORD	When value changed, a C_BO command with value is sent out.
	.Status	WORD	
C_IC/C_CI/C_RD/ C_CS/C_TS/C_RP	.Value	BYTE	When value changed, a related command is sent out.
	.Status	WORD	
P_ME_A	.Value	INT	When value changed, a P_ME command with value is sent out.
	.Status	WORD	
P_ME_B	.Value	INT	
	.Status	WORD	
P_ME_C	.Value	REAL	
	.Status	WORD	
P_AC	.Value	BYTE	When value changed, a P_AC command is sent out.
	.Status	WORD	
	.Status	WORD	

IEC data point	DDDT Name	DDDT Data Type	Comments
CUSTOM_M_IT_D	.Flags	BYTE	Read-only points
	.Timestamp	CP56Time2a	
	.Value0	INT	
	.Value1	INT	
	.Value2	INT	
	.Value3	INT	

This table describe the IEC60870-104 Server DDDT points definition, including Value and Flag.

IEC data point	DDDT Name	DDDT Data Type	Comments
M_SP	.Flags	BYTE	M_SP Value: Bit0: 0 (Off) / 1 (On) Bit1...Bit7: Reserved
	.Timestamp	CP56Time2a	
	.value	BYTE	
M_DP	.Flags	BYTE	M_DP Value: Bit0...Bit1: 0 (Intermediate) / 1 (Off) / 2 (On) / 3 (Indeterminate) Bit2...Bit7: Reserved Flag: Bit0...Bit3: Reserved Bit4: Blocked Bit5: Substituted Bit6: Not Topical Bit7: Invalid
	.Timestamp	CP56Time2a	
	.value	BYTE	
M_ST	.Flags	BYTE	Flag: Bit0: Overflow Bit1...Bit3: Reserved Bit4: Blocked Bit5: Substituted Bit6: Not Topical Bit7: Invalid
	.Timestamp	CP56Time2a	
	.value	BYTE	
M_BO	.Flags	BYTE	
	.Timestamp	CP56Time2a	
	.Value	DWORD	
M_ME_A/M_ME_B	.Flags	BYTE	
	.Timestamp	CP56Time2a	
	.Value	INT	
M_ME_C	.Flags	BYTE	
	.Timestamp	CP56Time2a	
	.Value	REAL	
M_IT	.Flags	BYTE	Flag: Bit0...Bit4: Sequence number (Reserved in DDDT and calculated by BMENOR2200H) Bit5: Counter has overflowed Bit6: Counter was adjusted Bit7: Counter reading is invalid
	.Timestamp	CP56Time2a	
	.Value	DINT	
C_SC/C_DC/C_RC	.Value	BYTE	Read-Only points
C_SE_A/C_SE_B	.Value	INT	
C_SE_C	.Value	REAL	
C_BO	.Value	DWORD	
P_ME_A	.Value	INT	
P_ME_B	.Value	INT	
P_ME_C	.Value	REAL	
P_AC	.Value	BYTE	
Freeze Cyclic	.Cmd	BYTE	Cmd value: 0: Disable cyclic M_IT freeze 1: Enable cyclic M_IT freeze
	.Status	WORD	

IEC data point	DDDT Name	DDDT Data Type	Comments
Freeze Trigger/ Clear Events	.Cmd	BYTE	Cmd value change will cause the operation.
	.Status	WORD	
Cmd_quality	.Cmd	BYTE	Cmd value: Bit0...Bit3: Reserved Bit4: Blocked Bit5...Bit6: Reserved Bit7: Invalid When cmd value set to blocked/invalid, remote associated control command will be failed, as the control point is blocked by local.
CUSTOM_M_IT_D	.Flags	BYTE	Flag: Bit0: Overflow Bit1...Bit3: Reserved Bit4: Blocked Bit5: Substituted Bit6: Not Topical Bit7: Invalid
	.Timestamp	CP56Time2a	
	.Value0	INT	
	.Value1	INT	
	.Value2	INT	
	.Value3	INT	
Event State for M_ SP/M_DP/M_ST/ M_BO/M_ME_A/ M_ME_B /M_ME_C/M_IT/ CUSTOM_M_IT_D	.Count	WORD	Read Only points for event buffer diagnostics.

Clearing Events in the Server

Clear_Events supports a new point type which clears the event buffer in DNP3 and IEC60870-5-101/104 servers. It enables the user to clear the events buffer in a local or remote SCADA through mapping memory.

To create *Clear_Events* for these servers, 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 ObjectsBinary InputDouble InputBinary CounterAnalog InputBinary OutputAnalog Output*	Specifies the object group whose event is cleared o. demand
Variable Name	–	Indicates the name of the located register.

Event Queue Setting Page

Configure the parameters on the **Events** tab to map the event queue status to the Device DDT registers in the controller. 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: **IEC10• Server<ServerName><DeviceName>**
2	Make a selection in the **Select Type Id** pull-down menu on the **EVENTS** tab
3	Select **Add** 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 **Apply** to implement your configuration changes. • Click **OK** to implement your changes and close the dialog box.

IEC60870 Events

Access the Configuration Tab

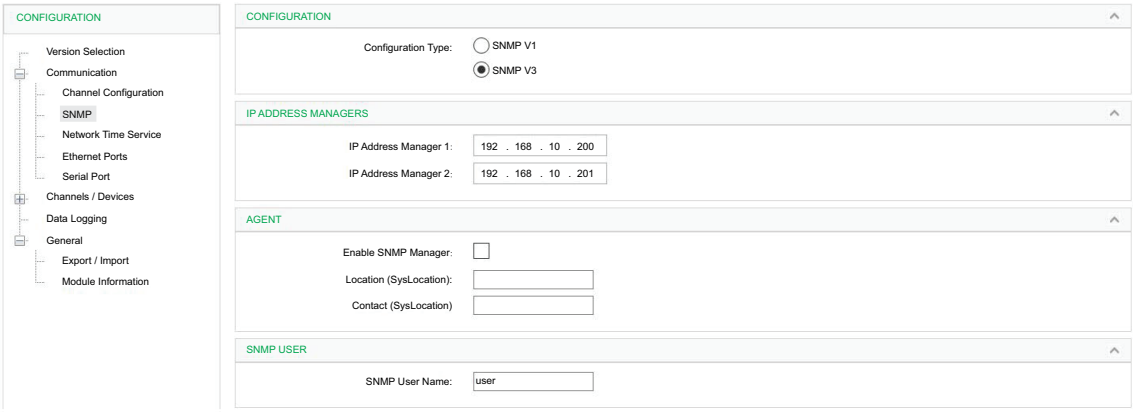
Access the configuration parameters for IEC60870-5-101 and IEC60870-5-104 events on the **EVENTS** tab in Control Expert:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	Confirm that you already created client and/or server channels for IEC60870 communications, page 115.
3	In the **CONFIGURATION** menu, expand (+) the **Channels/Devices** sub-menu.
4	Make one of the following selections in the **Channels/Devices** sub-menu: • **IEC101/IEC104 Client** • **IEC101/IEC104 Server**
5	• Select the specific channel in the sub-menu. • Select the specific device in the sub-menu.
6	Select the **EVENTS** tab.
7	Configure the event parameters. **NOTE:** The event parameters are similar to the data mapping parameters, page 147.
8	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

SNMP Configuration

Access the SNMP Configuration

Access the SNMP parameters in the Control Expert DTM:

Step	Action
1	Access the DTM configuration for your module, page 112.
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.

Field	Parameter	Description
CONFIGURATION	*SNMP V1*	Click the radial button that conforms to your application design. **NOTE:** SNMP versions are not compatible between each other.
	SNMP V3	
IP ADDRESS MANAGERS	*IP Address Manager 1*	IP address of the primary SNMP manager.
	IP Address Manager 2	IP address of the secondary SNMP manager.
AGENT	*Enable SNMP Manager*	*selected*: Select this box to enable the SNMP manager.
		deselected: Leave this box empty to disable the SNMP manager.
	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 (*SNMP V1* only)	*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 162. • Confirm whether you configure trap settings on the SNMP manager that are consistent with those on the processor.
SECURITY (*SNMP V1* only)	*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.
SNMP USER (*SNMP V3* only)	*SNMP User Name*	Enter a user name for the SNMP version 3 (maximum length: 32 characters).

NOTE: The characteristics and details of the SNMP service are described in the Ethernet services chapter, page 53.

Secure Mode

In Secure mode, SNMP v3 must complete configuration in Web page Cybersecurity page. Otherwise SNMP service will not start.

Network Time Service Configuration

Introduction

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

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, page 83.

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

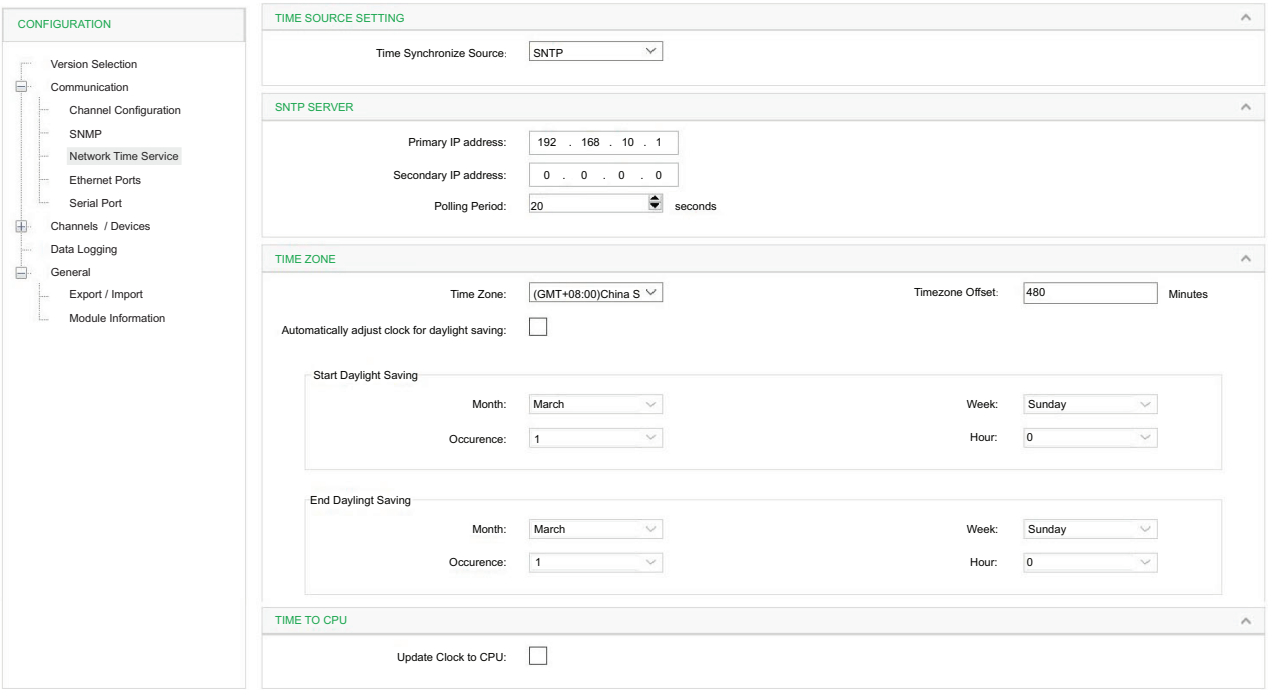
Access the SNTP Configuration

Access the SNTP parameters in the Control Expert DTM:

Step	Action
1	Access the DTM configuration for your module, page 112.
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

These SNTP parameters are available for your module:



Field	Parameter	Description
Time Source Setting	**Time Synchronize Source**	Select a value from the drop-down list to identify the time source of synchronization: • **RTU Protocol**: If SCADA or the client synchronizes time with the BMENOR2200H module, its time source is the Controlling Station. • **SNTP Server**: If the NTP client is enabled and connected with the NTP server, its time source is the NTP server when it synchronizes the BMENOR2200H module's clock.
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: The clock is not adjusted 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 time to the controller.
		*deselected:*The clock time is not updated to the controller.

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

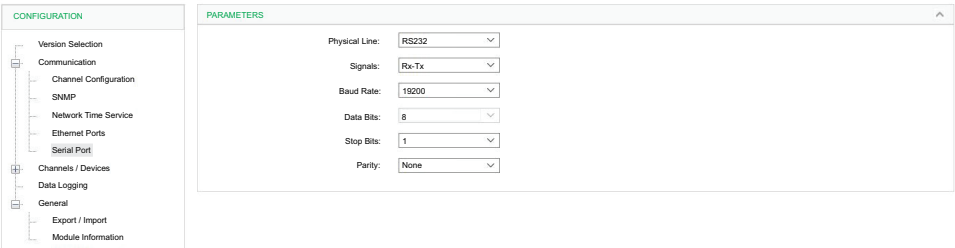
SNTP terms:

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.
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.

Serial Port Configuration

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the **CONFIGURATION** menu, expand (**+**) the **Communication** sub-menu.
3	Select **Serial Port**.
4	Configure the serial port 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.

Serial Port Parameters



These parameters apply to the serial port for your module:

Parameter	Description
Physical Line	Select the type of physical line for the port.
Signals	Select the type of signal that is supported by the physical line.
Baud Rate	Select a transmission speed for the port.
Data Bits	Adjust the number of data bits to correspond to the remote device in use.
Stop Bits	Select the number of bits to stop in a single transmission.
Parity	Configure the addition (or not) of the parity bit.

Obtaining and Maintaining Accuracy

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

The M580's clock is synchronized when the module starts. This is the default start time in the display:

Model	Starting Date
M580	January 1, 1980 00:00:00.00

Later, the module will look for the SNTP time source or wait for the RTU time synchronization command from the client. The default date of the M580 is as follows.

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 have no effect on the accuracy of the Ethernet network.

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

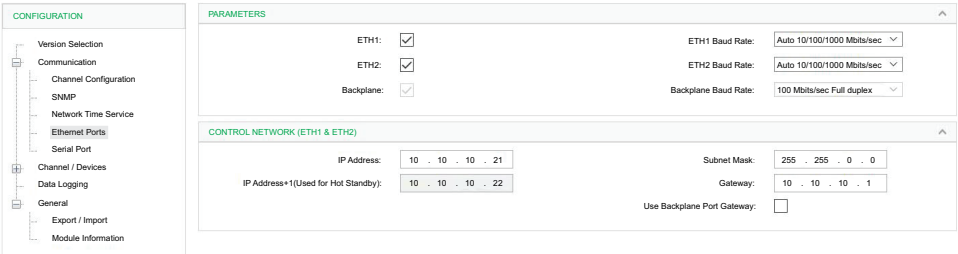
General Time Synchronization Terms

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 BMENOR2200H module sends the source clock synchronization signal to the controller over X Bus.

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.

Control Ports Configuration



NOTE: This option is only available and take effect on the module PV>=04 (with front ethernet port) and using BMENOR2200H.3 from Device list for configuration.

Enable/Disable Control Ports

When the **Version Selection** is *firmware version >=4.0*, follow the below steps to enable the control ports:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the **CONFIGURATION** menu, expand (**+**) the **Communication** sub-menu.
3	Click the **Ethernet Ports** sub-men to see the PARAMETERS: • **ETH1** • **ETH2** **NOTE:** The default value of the two front control ports is set to disabled (deselected). Backplane port is mandatory enabled as 100M bits/sec.
4	Enable the ports by checking the corresponding boxes..
5	• Select **Apply** to implement your configuration changes. • Select **OK** to implement your changes and close the dialog box.

Control Network (ETH1 & ETH2)

The parameters below can be configured manually once the control ports have been enabled:

Parameters	Description
IP Address	Enter the IP address: two control ports share a same IP address.
Subnet Mask	Enter a subnet mask for control ports that corresponds to the IP address.
Default Gateway	This is the IP address of the default gateway for control ports/ back Ethernet port to which messages for other networks are transmitted
IP address + 1	The **IP address + 1** field is used for configuring a redundant system.
Use Backplane Port Gateway	If this check box is selected, the gateway is set in backplane port domain.
• Click the **Apply** button to implement your configuration changes. • Click the **OK** button to implement your changes and close the dialog box.	

NOTE: There are two MAC addresses, but only one gateway can be configured, and which could work for either front control ports (if set in front control ports domain) or backplane ports (if set in backplane port domain)

NOTE: IP range of control ports cannot be the same as backplane port's, otherwise, it will lead to invalid status for module running. (RUN LED: off, ERR LED: red flashing)

Baud Rate Setting

Once the two front control ports have been enabled, baud rate setting is allowed and the options are:

- Auto 10/100/1000 Mbits/sec
- 100 Mbits/sec Half duplex
- 100 Mbits/sec full duplex
- 10 Mbits/sec Half duplex
- 10 Mbits/sec full duplex

NOTE: *Auto 10/100/1000 Mbits/sec* is the default option once the ports are enabled.

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 back up/recover and share that file among different modules to implement the same configuration.

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

- *export:* Record the module and protocol configurations into 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	
Backup/ Recovery and Batch 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, page 276.	

Import

Import an .xml configuration file:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the **CONFIGURATION** menu, expand (**+**) the **General** sub-menu.
3	Select **Export / Import**.
4	In the **Import / Export** dialog, click the **Browse** button in the **Import File Name** field to find the .xml configuration file name path you want to import, located on your local or network drive.
5	Select the respective configuration file and click the **Open** button to enter the file name path for the **Import File Name** field.
6	Select or deselect the **Use system defined data mapping point names** check box: • *selected:* The import setting allows you to import user-defined mapping point names. • *deselected:* Data mapping point name is assigned based on point type, point number, and point count.
7	Select the **Import** button. **NOTE:** Once you apply the *import*, all existing configuration data will be overwritten by import and all existing backup files of this table will move to Archive folder.
8	Select **Apply** to record your changes, or select **OK** to record your changes and close the dialog.

Export

Export an .xml configuration file:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the **CONFIGURATION** menu, expand (**+**) the **General** sub-menu.
3	Select **Export / Import**.
4	In the **Import / Export** dialog, copy/paste the path file name of the .xml configuration file saved from the BMENOR module and protocol parameters, which you want to export to a local drive, in the **Import File Name** field.
5	Select or deselect the **Use system defined data mapping point names** check box: • *selected:* The import setting allows you to import user-defined mapping point names. • *deselected:* Data mapping point name is assigned based on point type, point number, and point count.
6	Select the **Export** button. **NOTE:** The .xml configuration file is exported to a pre-determined location on your local or network drive.
7	Select **Apply** to record your changes, or select **OK** to record your changes and close the dialog.

Bulk Configuration

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the **CONFIGURATION** menu, expand (**+**) the **Communication** sub-menu.
3	Select **Channel Configuration**.
4	To edit, double-click the pencil in the **Bulk Configuration** tab of the **CLIENT CHANNELS** dialog. **Result**: An **Open** dialog box appears where you can navigate to the required bulk configuration file.
5	Select the **DataMapping_BulkConfiguration.xlsm** file to the required folder required in step 4 and open the Excel worksheet or CSV file.
6	Based on the requirement, (data points for server and client for IEC or DNP3), copy the respective data to the IEC Client or IEC Server worksheet.
7	Open the corresponding data mapping, and the data should be successfully imported.
8	Record your changes and import the Excel worksheet or CSV file.

Excel worksheet details:

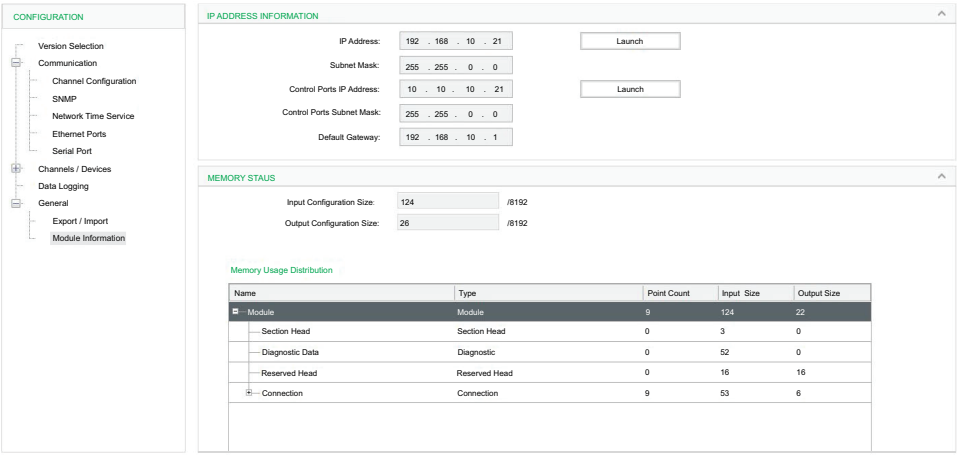
- IEC Server: IECDataPoint_Ref sheet to IECServer
- IEC Client: IECDataPoint_Ref sheet to IECClient
- DNP3 Server: DNP3DataPoints_Ref to DNP3Server
- DNP3 Client: DNP3DataPoints_Ref to DNP3Client

Module Information in the DTM

Access the Information

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

Step	Action
1	Access the DTM configuration for your module, page 112.
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:**
  - **Input:** The level indicator displays the memory usage (in bytes) for input memory type.
  - **Output:** The level indicator displays the memory usage (in bytes) for output memory type.

Limitations

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

Type	Memory
Input	8 K bytes (16 KB in high performance mode)
Output	8 K bytes (16 KB in high performance mode)

NOTE: For details, refer to the description of the I/O data exchange with the controller, page 31.

Data Logging

About Data Logging

Introduction

The data logging service allows application data archiving (events, alarms, process data, devices status, measures, etc.) in the internal memory of the module. This service allows you to log data in .csv files in the ASCII format. These files are stored locally in the SD memory card of the module.

You can configure the data logging service to execute upon the detection of one of these events:

- A configured interval (period) elapses.
- The CPU or the user triggers an event.

File Format

This data logging service logs data in .csv (comma-separated value) files. These files provide flexibility of use:

- Port the file directly to a Microsoft Excel spreadsheet or a database management system (DBMS) for analysis.
- These files can be accessed by HTTPS clients.

Data Logging Tables

A data logging table occupies a chunk of the module’s memory (RAM).

The value of logged variables is stored in this table. A new record appears in the table for each logged event. The record can contain a timestamp or value for all selected variables. You can configure the number of records that the table can hold.

When the data logging backup event occurs, the table in RAM is saved as a backup file in the SD card and all table records are cleared.

Memory Usage

The data logging service can manage up to 10 tables that are independent of each other. That means each table can have a unique size and a different triggering mechanism. The service can also manage up to 10 groups of data logging files (backups). This mean you can create several different data tables, each of which can be associated with different logging periods.

For example, the folder *Table_n* represents the backup that corresponds to *table_n*. The table backup files on the SD memory card can be purged (or deleted) as configured (event n triggered by the CPU). When the module experiences a loss of power during data logging, the records in the RAM table that have not been backed up are lost while the backup files are retained.

These events occur when you download a new project or configuration to the PLC:

- The data logging tables in RAM are cleared and expelled.
- The table's corresponding backup files on the SD card are archived if the table's configuration is changed.

Before You Begin

Data Logging and the DTM

The data logging service is configured in Control Expert through the DTM that corresponds to the BMENOR2200H module.

Data Logging and the SD Card

Confirm that an SD card is in the slot on the front of the module before you download the Control Expert project that includes the data logging service to the module.

NOTE: The module recognizes the SD card about seven seconds after it is inserted in the memory card slot.

NOTE: Don't remove the SD card when the data logging service is running.

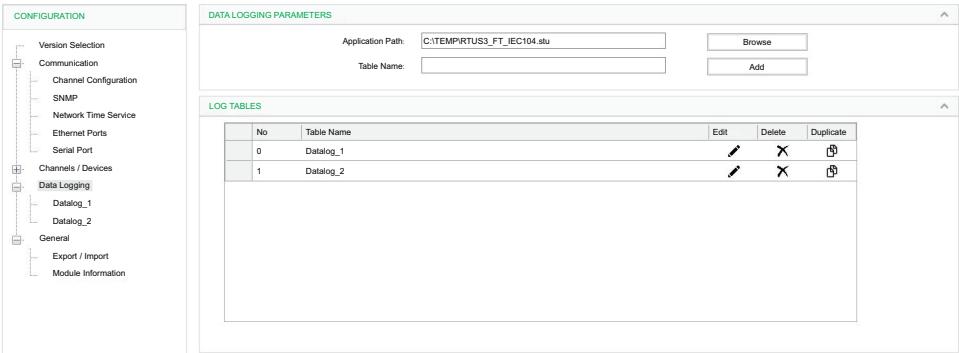
The use of the data logging service requires that you enable the Data Dictionary in the project settings, page 124.

Data Logging Control Expert Configuration

Access the Configuration

Access the data logging parameters:

Step	Action
1	Access the DTM configuration for your module, page 112.
2	In the *DTM Browser*, double-click the DTM that corresponds to the BMENOR2200H module to access its configuration parameters.
3	In the **CONFIGURATION** menu, select **Data Logging**.

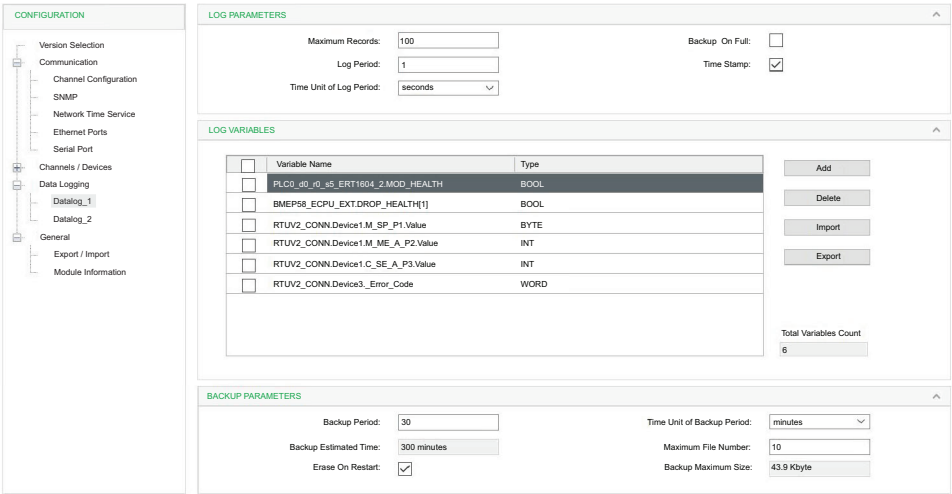


Configuration Instructions

Configure data logging in the *DATA LOGGING PARAMETERS* fields:

Step	Action
1	Enter the destination of the .stu file in the *Application Path* field. **NOTE:** You can use the **Browse** button to navigate to a file destination.
2	Assign a name in the *Table Name* field. **NOTE:** You can enter a maximum of 31 characters in this field.
3	Press the **Add** button to create the log table.
4	Confirm that the new log table is created: • The new table appears in the *LOG TABLES* field. • Expand the structure (**CONFIGURATION > Data Logging**) to see the name of the new table.
5	Click the **OK** or **Apply** button to implement the changes.

Data Logging Parameters



LOG PARAMETERS: Expand (+) **Data Logging** in the **CONFIGURATION** menu and select a table to access these parameters:

Parameter	Description
Maximum Records	Enter the maximum number of records that can be stored in a log table. **NOTE:** When the configured number of records are logged, the newest records overwrite the oldest records.
Log Period	Use these values to enter an interval after which the backup is triggered: • Disable the period backup: 0 • Configure the interval. • Configure the time unit of log period.
Time Unit of Log Period	Select the unit of time to apply.
Backup On Full	Select this check box to trigger a backup when the log table is full (at its maximum configured capacity).
Time Stamp	Select this check box to add a time stamp for each log record.

LOG VARIABLES: You can access these parameters only after you create a data logging table (above).

Parameter	Description
Add	Click this button to open the *Global Variables* dialog box and add new variables to the *LOG VARIABLES* table.
Variable Name	This column shows the names of the added variables.
Type	This column shows the type that corresponds to the configured variables.
Delete	Click this button to remove the selected variable from the table.
Import	Import the selected variable.
Export	Export the selected variable.
Total Variable Count	This field shows the total number of variables in the table.

BACKUP PARAMETERS:

Parameter	Description
Backup Period	Use these values to trigger the table backup or configure a periodic event. In this case, configure the time base: • Disable the period backup: 0 • Configure the interval: 30 min ... 100 days
Backup Estimated Time	This is the maximum estimated amount of time that elapses before the backup data is lost (overwritten by new backup data).
Erase on Restart	Select this check box to delete the table log files in the SD card upon a restart of the module.
Time Unit of Backup Period	Select the unit of time to apply.
Maximum File Number	Use these values to define the maximum number of backup files for this table: • default value: 10 • maximum backup file count: 200
Backup Maximum Size	Data logging files are stored in the SD card, and the maximum size of an SD card is 4GB. When you build a new data logging table, the maximum size of the table is fixed. This number comes from the DTM, which uses the following assessments to calculate the maximum folder size (backup folder in this case): • data type in table • the number of recorders in each file • the number of files in the SD card

Variables in the Device DDT

To access the variables in the device DDT for the module, open the **Variables** tab in the **Project Browser** (**Project > Variables & FB instances > Device DDT Variables**).

Value	Action
1	Open the **Variables** tab in the **Project Browser** (**Project > Variables & FB instances > Device DDT Variables**).
2	In the **Name** column, expand (**+**) the name of a module that is associated with a data logging table.
3	Find the name of the table and expand (**+**) it to access the structural elements that are described in the next table.

Structural elements:

Element	Description
Enable	This value controls the data logging service for the selected table: • *0:* disabled • *1:* enabled
Records_count	This value represents the number of records in the selected table.
Backup_count	This value represents the number of backup files in the selected table.
Last_Log_Status	*byte 0:* trigger value (The action finished without the detection of an error.)
	byte 1: trigger result (The SD card is not available.)
Last_Backup_Status	*byte 0:* trigger value (The action finished without the detection of an error.)
	byte 1: trigger result (The SD card is not available.)
Log	Trigger a log action and view the trigger result. **NOTE:** Refer to the description of byte values for *Trigger_S*, below.
Backup	Trigger a backup action and view the trigger result. **NOTE:** Refer to the description of byte values for *Trigger_S*, below.
Purge	Trigger a purge action to delete the backup file and view the trigger result. **NOTE:** Refer to the description of byte values for *Trigger_S*, below.

Trigger_S

The *Trigger_S* type has two variables when it is associated with the *log*, *backup*, or *purge* variables:

- *Trigger*: Every change in value triggers the corresponding action.
- *Status*: The high byte of the *Status* variable contains the result of the executed action, as indicated by these values:

Byte	Description
0	The execution of the action completed without any detected errors:
1	The SD card is not available.: ◦ *possible reason:* The slot does not contain a compatible SD card. ◦ *suggested action:* Insert a compatible SD card in the slot.
2	A file system error is detected: ◦ *possible reason:* It is not possible to write files to the SD card. ◦ *suggested action:* Verify the write-protection on the card, reboot the module, or swap out the SD card.
3	The available space on the SD card is not sufficient to execute the action: ◦ *possible reason:* The SD card is full. ◦ *suggested action:* Replace the SD card or purge the files on the card.
4	The available RAM is not sufficient for logging or backup: ◦ *possible reason:* Too many services or data points are configured. ◦ *suggested action:* Reduce the size of the configuration.
5	The variable is not available: ◦ *possible reason:* The data dictionary is not enabled in the project or one or more variables that are configured in table are missing from the user's project. ◦ *suggested action:* Enable the data dictionary in the project settings or re-configure the data logging table to remove the missing variables.
6	The table is full: ◦ *possible reason:* There are too many log records. ◦ The high byte of the *Status* variable contains the result of the executed action, as indicated by these values *Status* va ◦ *suggested action:* Trigger a backup action.
7	The SD card is busy.
8	A system error is detected: ◦ *possible reason:* The data transfer between the module and the controller is interrupted. ◦ *suggested action:* Verify the hardware connections, or reboot the entire system.

- The low byte of the *Status* variable identifies the action that the result effects. When the execution of an action is completed, the value of the low byte is updated to the value of the *Trigger* byte that triggered the action.

  NOTE:

  Confirm that the *Status* is updated before the next action is triggered.

1. This is an example of a log action that is triggered with its result verified for a selected table:
   - *BME_NOR_2200H_DATALOG.Table0.enable = 1* (The table is enabled.)
   - *BME_NOR_2200H_DATALOG.Table0.log.Trigger = 0*
   - *BME_NOR_2200H_DATALOG.Table0.log.Status = 0*
2. The action is triggered by a change in the value of *BME_NOR_2200H_DATALOG.Table0.log.Trigger* from *0* to *1* to start this sequence:
   a. The module adds a log record to the table.
   b. The module updates the value of *BME_NOR_2200H_DATALOG.Table0.log.Status*.
3. The user's application program continues to monitor the value of *BME_NOR_2200H_DATALOG.Table0.log.Status*:
   - If the low byte changes to 1, the log action finishes executing.
   - If the high byte changes to 0, the log action is finished successfully.
   - Any other value indicated an unsuccessful execution.
4. The user's application program can again change the value of *BME_NOR_2200H_DATALOG.Table0.log.Trigger* to fire another log action.
5. Repeat these steps to verify the result.

Module Diagnostic Device DDT

The module diagnostic Device DDT includes the status of the SD (*SD_STATUS*) card and data logging service (*DATALOGING*). These are the possible bit values for *SD_STATUS*:

- *bit 0 STATUS*: This bit is set when the SD card is normal.
- *bit 1 BUSY:* This bit is set when the SD card is busy.
- *bit 2 LOW_SPACE_ALARM:* This bit is set when the free-space rate of the SD card is less than 20 percent.

Variable Selection

You can add existing unlocated variables (in your current project) to the *Variable selection* table when you configure the data logging table. The data logging service supports these variable types:

Variable Type	Logging format (backup files)
BOOL	0, 1
EBOOL	0, 1
BYTE	0 ... 255 (decimal)
INT	-32768 ... 32767 (decimal)
UINT	0 ... 65535 (decimal)
WORD	0 ... 65535 (decimal)
DINT	-2147483648 ... 2147483647 (decimal)
UDINT	0 ... 4294967295 (decimal)
DWORD	0 ... 4294967295 (decimal)
REAL	-1.2345678e-99 (scientific notation)
TIME	49D_17H_20M_47S_295MS
DATE	1990-02-02
TOD	23:10:59

When you click the **Add** button in the *Log Variable* section, the *Variable selection* window opens. From here you can select from the variables that are defined in the current Control Expert project.

When a new backup event occurs (owing to a trigger or period expiration), a new record that contains all of the variable values is added to the log table (with optional time stamping). When the user-configured maximum number of records is reached, the newest records overwrite the oldest.

Backup File Format

The data logging service supports an SD card with a 4-GB capacity. Backup files are stored in the data log folder at the root of the card. Each table includes a dedicated sub-folder for this storing action. The name of the sub-folder is the same as that of the user-configured table name.

When a new log event occurs (owing to a trigger or period expiration), a new file is generated in this folder and the records in the log table are stored in the file. At this time, the log table itself is flushed. When the user-configured maximum number of files is reached, the oldest backup files are deleted.

The generated file assumes the event timestamp as its own name in this format:
`yyyy-mm-dd_hh-mm-ss`

The file format is fixed. You cannot modify it.

The file is encoded in pure ASCII format in a text file with the .csv extension. This is an example of the content of a log file:

```
Date,plc.plc1.height,plc.plc1.length,plc.plc1.width,
2003-10-01 02:44:55,150,200,50,
2003-10-01 03:48:08,140,150,30,
2003-10-01 04:55:10,220,280,80,
2003-10-01 06:01:05,170,220,60,
```

You can open the .csv file in Microsoft Excel to separate the data in columns:

Date	plc.plc1.height	plc.plc1.length	plc.plc1.width
10/1/2003 2:44	150	200	50
10/1/2003 3:48	140	150	30
10/1/2003 4:55	220	280	80
10/1/2003 6:01	170	220	60

Purge

A controller-triggered purge erases all backup files for the table from the SD card. In this case, the table folder is emptied.

To trigger the purge action every time the module restarts, select *Erase on restart*.

NOTE:

- This variable is available only after you configure the data logging service.
- The purge does not affect the log table in memory.

Name		Type	Description
Purge_Archive		Trigger_S	Clear archived backup file.
	Trigger	BYTE	Change the value of this byte to trigger the action.
	Status	WORD	*0:* Trigger value without a detected error.
			1: The SD card is not available.
			2: A file system error is detected.
			3: The SD card has insufficient space.
			4: There is insufficient memory space.
			5: The variable is not available.
			6: The table is full.
			7: The SD card is busy.
			8: A system error is detected.
<table name>		T_BME_NOR_2200H_TABLE	The table name is assigned when you create a data logging table.
	Enable	BOOL	*0:* Disable the datalogging service.
			1: Enable the datalogging service.
	Records_count	UINT	Records count in this table.
	Backup_count	UINT	Backup records count of this table.
	Last_Log_Status	BYTE	*0:* Trigger value without a detected error.
			1: The SD card is not available.
			2: A file system error is detected.
			3: The SD card has insufficient space.
			4: There is insufficient memory space.
			5: The variable is not available.
			6: The table is full.
			7: The SD card is busy.
			8: A system error is detected.
	Last_Backup_Status	BYTE	*0:* Trigger value without a detected error.
			1: The SD card is not available.
			2: A file system error is detected.
			3: The SD card has insufficient space.
			4: There is insufficient memory space.
			5: The variable is not available.
			6: The table is full.
			7: The SD card is busy.
			8: A system error is detected.

Data Logging and Hot Standby

The data logging service for the module runs in the primary and standby modes in a Hot Standby system. Both models respond when you trigger a log, backup, or purge action.

The Device DDT always displays the result of the trigger for the module in the primary role. During a Hot Standby swap, the status of the module that assumes the primary role is overwritten.

You can download the primary and standby backup data logging files from the web. The two modules do not necessarily have the same log data, time stamping, and SD card statuses.

Web Page and Device DDT Diagnostics

Introduction

This chapter describes diagnostics for the BMENOR2200H Web pages and Device DDT as configured in a Control Expert application.

Web Page Access

Introduction

The BMENOR2200H module has a built-in web server that provides various web pages offering setup, diagnostic, cybersecurity, and monitoring features.

These are the main tabs on the **Home** page:

- **DIAGNOSTICS**, page 176: Access this tab to configure diagnostics for the BMENOR2200H web pages and the device DDT as configured in a Sur un des liens vers une page, je dois mettre UI, mais ce n'est pas possible, je mets juste en gras ? Control Expert application.
- **FILE EXPLORER**, page 194: Access data logging information.
- **SETUP**, page 198: Access this tab to define security right and access rights for the module.

Browser Requirements

Observe these browser version requirements to use the web pages:

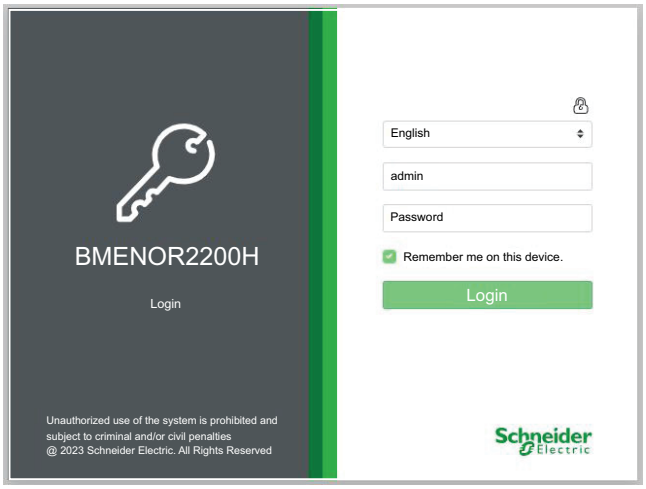
Browser	Requirememt
Google Chrome	50+
Mozilla Firefox	40+
Microsoft Edge	14+
Internet Explorer	11

Connecting via the HTTPS Protocol

If your application experiences connection problems, verify with your local IT support that your network configuration and security policies are consistent with HTTPS (port 443) access to the BMENOR2200H module IP address.

The BMENOR2200H module accepts the HTTPS connections with transport layer security (TLS) protocol v1.2 or later.

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 high communications load, the web page may not open immediately. In this case, refresh your browser.
2	In the pull-down menu, select the appropriate language.
3	Enter the default user name and password that conforms to the selected cybersecurity mode, page 22 the first time you access the web: • **Advanced** cyber security mode: ◦ *user name:* **admin** ◦ *password:* **password** • **Standard** cyber security mode: ◦ *user name:* **installer** ◦ *password:* **Inst@ller1**
4	Click **Login**.
5	Change your user name and password when prompted.

Web Page Diagnostics

Introduction

This section describes diagnostics for the BMENOR2200H Web pages as configured in a Control Expert application.

Web Page Diagnostics

Accessing Diagnostics

Access diagnostic information for the BMENOR2200H module using the Web pages:

Step	Action
1	Select **Tools > DTM Browser** to open your project DTM.
2	Double-click the DTM for the BMENOR2200H module.
3	In the DTM **Configuration** dialog, expand **General**, and select **Module Information**.
4	In the right-side pane, scroll to the bottom of the dialog to display **Web Diagnostics**.
5	Click **IP Address** to access the diagnostic Web pages.
6	Select **Diagnostics**.
7	Expand the **MENU** to display the available diagnostic pages: • **MODULE** ◦ **Status Summary** ◦ **HSBY Status** ◦ **Event Buffer Status** ◦ **Port Statistics** ◦ **Ping** • **CONNECTED DEVICES** ◦ **RTU Protocol** ◦ **Messaging** • **SERVICES** ◦ **SNTP** ◦ **Clock** ◦ **Datalogging** ◦ **SNMP** ◦ **802.1x Authentication**

Module Diagnostics

Status Summary

Monitor the status of the module through these parameters:

Field	Description
RUN, **ERR**	• *green* • *red* For more information, refer to the diagnostics information is explained in the description of LED activity and indications, page 23
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 the service. • *black:* The service is not present or not configured.
NETWORK INFORMATION	**Host Name:** This field displays the host name for the module (**BMENOR2200H**).
	Backplane Port IP Address: This field displaysthe IP address of the backplane port.
	Backplane Port Subnet Address: This field displaysthe subnet address of the backplane port.
	Backplane Port MAC Address: This field displaysthe MAC address of the backplane port.
	Control Port IP Address: This field displaysthe IP address of the control port. **NOTE:** When both ports are disabled, or the cable is not connected on the enabled port, the IP Address is 0.0.0.0.
	Control Port Subnet Address: This field displaysthe subnet address of the control port.
	Control Port MAC Address: This field displaysthe MAC address of the control port.
	Gateway Address: This field displaysthe gateway address of the control port.
VERSION INFORMATION	View the software versions that run on the module: • **SV** • **Web Server Version** • **Web Page Version**
MISCELLANEOUS	**Cybersecurity Mode:** The status of the security service (enabled or disables) is reported.
	Rack ID: This field identifies the local rack (0).
	Slot ID: This field shows the slot number in which the BMENOR2200H module is installed.
	Date: This field displays the date of the BMENOR2200H module.
	Time: This field displays the time of the BMENOR2200H module
MANUFACTURING INFORMATION	Displays the serial number for the device.

Hot Standby Diagnostics

These fields are on the diagnostics page for Hot Standby performance:

- **SERVICE STATUS**: Defines whether or not the HSBY service is working properly.
- **SYNC STATUS**: Defines whether or not the HSBY status is synchronizing properly.

  NOTE: When no RTU client or server channels are configured in the DTM for this module, page 112, this synchronization status remains in the *In Progress* state and the ERR (detected error) LED flashes, page 23.
- **PARAMETER VALIDITY**: Defines whether or not any partner devices are valid in a HSBY system.
- **SYNC COUNTER**: Describes the numerical value of the synchronization counter.
- **LAST SYNC**: Defines the last time the HSBY status was synchronized in date/time format.
- **PACKET STATISTICS**: Defines the status of each packet set:
  - Inbound Packets
  - Outbound Packets
  - Inbound Packet Errors
  - Outbound Packet Errors
- **DETECTED ERRORS**: Describes error codes that are detected in the HSBY system.
- **EVENT SYNC STATUS**: Defines whether or not the events synchronization for BMENOR2200H modules in HSBY system is enabled.
- **LOCAL MODULE/REMOTE MODULE**: Defines the status of these parameters for local and remote modules:
  - Role: Primary or Standby
  - IP Address
  - Firmware Version

Event Buffer Status

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

Parameter	Description
EVENT BUFFER USAGE	This parameter indicates the percentage of the event buffer consumed.
EVENT OVERFLOW	This parameter indicates if the capacity of the event buffer is exceeded.
EVENT RESOURCE USAGE	This parameter indicates the percentage of event resources consumed.
EVENT BACKUP	**Enabled:** Events are backed up.
	Disabled: Events are not backed up.
CHANNEL/POINT EVENT STATUS	**No.:** This number represents the sequence of device connections.
	Channel Name: This parameter is the configured DNP3 channel name, page 115.
	Current Event Buffer Usage%: This parameter indicates the percentage of the event buffer that is consumed.
	Current Event Quantity: This parameter is the number of events in the buffer.
	Configured Event Quantity: This parameter is the configured size of the event buffer.
	Current Overflow Event Quantity: This parameter is the number of events that are not in the buffer owing to an overflow.
	Total Current Overflow: This parameter is the total number of 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 display status details from the perspective of the module.

Port Statistics

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

Parameter	Description
Ports	*green:* The port is active.
Speed	This field displaysthe configured port speed (0, 100, 1000 Mbps).
Duplex, **Half**	The 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.).
Total Errors	This field displays the number of detected errors.
Success Rate	This field displays the percentage of successful requests out of the total number of requests.
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 displays the number of frames successfully transmitted from the port.
Frames Received	This field displays the number of frames successfully received from the port.
Excessive Collisions	This field displays 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 displays the number of times a collision is detected after the slot time of the channel elapses. **NOTE:** A value appears in this field only when the hardware provides the information.
CRC Errors	This field displays 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 displays the number of bytes received on the port.
Inbound Packet Errors	This field displays the number of packets received on the port for which errors are detected. **NOTE:** Does not include Out Discards.
Inbound Packets Discarded	The field displays the number of inbound packets received on the port but discarded.
Bytes Transmitted	This field displays the number of bytes that are sent on the port.
Outbound Packet Errors	This field displays the number of packets sent on the port for which errors are detected. **NOTE:** Does not include Out Discards.
Outbound Packets Discarded	The field displays the number of outbound packets sent on the port but discarded.
Carrier Sense Errors	This field displays 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 displays the number of frames received on this port that are an integral number of bytes but do not pass the FCS check.
Alignment Errors	This field displays the number of frames received on this port that are not an integral number of bytes in length and do not pass the FCS check.
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 transmission 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 reception error.
SQE Test Errors	This field displays 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

The **Port Statistics** page reports the statistics for the module's serial ports connection, once it is enabled:

Parameter	Description
Serial RJ45 Port Status	Green: the port is active.
	Black: the port is inactive.
BAUD Rate	This field displays configured baud rate of serial port (300..115200).
Physical Line	This field displays the configuration of physical interface (RS485 or RS232).
Bytes Received	This field displays the number of received frames.
Bytes Transmitted	This field displays the number of transmitted frames.
Error Frame Counter	This field displays the number of detected error frames.

Ping

For more information, refer to Ping Function, page 63.

Connected Device Diagnostics

RTU Protocol

This table shows the RTU 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/IEC60870 channel name, page 115.
	Protocol: This field shows the implemented connection protocol.
	Channel Mode: This field shows the channel mode (Read-only or Standard) of IEC60870-5-104 Server.
	Redundant Group: This field shows the number of redundant group ID.
	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: Refer to Detailed statistics for details on a specific Secure authentication version, page 80.
	Error Code: Refer to Error code, page 320 for details on a specific 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.
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

Expand the **MENU** on the **DIAGNOSTICS** tab to access and configure the service parameters for these **SERVICES**:

- SNTP, page 184
- Clock, page 184
- Datalogging, page 185
- SNMP, page 186

SNTP Service Diagnostics

This table describes the SNTP parameters for service diagnostics:

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 client time server for the current time.
	Secondary: A secondary server polls a client 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: A server error is detected.
	gray: The status of the server 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 for the module.

Clock Service Diagnostics

This table describes the clock parameters for service diagnostics:

Parameter	Description
CURRENT DATE AND TIME	**Date** (module date)
	Time (module time)
TIME ZONE	(module time zone)
LATEST TIME SYNCHRONIZATION	**Date** (synchronization timestamp)
	Time (synchronization timestamp)
	Time Source (synchronization timestamp): • **CPU:** If the RTU protocol is configured, the RTU can get its initial time from the controller when the RTU protocol starts or restarts. • **RTU:** This field shows the time source when a SCADA system or a client synchronizes its time with the RTU. • **SNTP:** 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.

Data Logging Service Diagnostics

This table describes the data logging parameters for service diagnostics:

Parameter	Description
SERVICE STATUS	*Enabled:* The data logging service is enabled.
	Working properly: The data logging service is enabled and runs properly.
	Disabled: The data logging service is not enabled.
	Not Configured: The data logging service is not configured.
	At Least One Connection is Bad: An incorrect hardware connection stops the data logging service.
	Enabled (On): The data logging service is enabled.
	Enabled (Off): The data logging service is disabled.
SD CARD STATUS	*Card is Present:* The SD card is present in the module and available for data logging functions.
	Low Space Alarm: The free-space rate of the SD card is less than 20 percent.
	Card is Busy: The SD card is busy.
	Card is Missing: The SD card is not available.
SD FREE SPACE	This is the amount of available space in KB on the SD card.

The data logging table contains these columns:

Column	Description
Table Name	This column shows the names of the created tables. **NOTE:** The name of the table is generated by the Modbus response.
Table Status	*Enabled:* The table is enabled.
	Disabled: The table is disabled.
Backup Count (SD Card)	When this number of incremental backups is reached, new data overwrites old data on the SD card.
Record Count	This value represents the number of records that contribute the result.
Last Log Status	*Success:* No errors were detected during the last execution of the data logging service.
	No Memory Space: The available memory was not sufficient to execute the data logging service.
	Variable Not Available: The data logging service requires a variable that is not available.
	Table Full: The logging function wraps when the table reaches the capacity indicated by this value.
	System Error: The detection of a system error blocked the execution of the data logging service.
Last Backup Status	*Success:* No errors were detected during the last backup of data logging files.
	No Compatible SD Card: The SD card is not compatible with the data logging backup.
	File System Error: The detection of a file system error blocked the execution of the backup.
	Not Enough Space on SD Card: The available memory on the SD card was not sufficient to execute the backup.
	SD Card Busy: The SD card is locked or write protected.
	System Error: The backup was not possible owing to the detection of a processing error.
Last Successful Backup	This column shows the date and time of the last successful backup of the data log file.

SNMP Service Diagnostics

This table shows the possible states for SNMP service diagnostics:

Parameter	Description
SERVICE STATUS	*working properly:* The SNMP agent is enabled for network services and running correctly.
	disabled: The SNMP agent is disabled for network services.
	not configured: The version configured in the DTM is a mismatch for the version in the web configuration.
SNMP VERSION	*V1:* Select version 1 (SNMPv1).
	V3: Select version 3 (SNMPv3).
	Unknown: The SNMP version is not known.
DIAGNOSTIC	*Packets In:* This value represents the number of received SNMP packets.
	Packets Out: This value represents the number of sent SNMP packets.
	Bad Versions In: This value represents the number of received SNMP packets from an unsupported SNMP version.
	USM Stats - Unknown User Names (SNMPv3 only): This value represents the number of packets for which the SNMPv3 function is polled that is not recognized according to the user-based security model (USM).
	USM Stats - Wrong Digests (SNMPv3 only): This value represents the number of packets for which the SNMPv3 polling function uses the wrong password or digest algorithm, according to the user-based security model (USM).
	USM - Unknown Security Models (SNMPv3 only): This value represents the number of SNMP packets that are requested from an unknown security level, according to the user-based security model (USM).

802.1X Authentication Service Diagnostics

Parameter	Description
SERVICE INFORMATION	*Port Number:* The NOR port name in 802.1X exchange.
	Service Status: 802.1X state for this port.
	Last Authentication Status: Result of the most recent 802.1X exchange on this port. For more details, see Authentication Status.
MAC INFORMATION	*Supplicant Mac:* Mac address of BMENOR2200H port in 802.1X exchange.
	Authenticator Mac: Mac address of Authenticator.
	Last Frame Source MAC: Source Mac address of last frame.
TIMER INFOMRATION	*Auth While Timer:* Timer value for Authentication.
	Held While Timer: Timer value for Held.
	Start While Timer: Timer value for Start.
	Start Count Start Count.
EAP INFORMATION	*Rx Frames:* Receive Frames counts.
	Tx Frames: Send Frames counts.
	Tx Start Frames: Send Start Frames counts.
	Tx Logoff Frames: Send Logoff Frames counts.
	Tx Resp Id Frames: Send Response Id Frames counts.
	Tx Resp Frames: Send Response Frames counts.
	Rx Resp Frames: Receive Response Frames counts.
	Rx Req Id Frames: Receive Response Id Frames counts.
	Rx Invalid Frames: Receive Invalid Frames counts.
	Rx Length Error Frames: Receive Length error Frames counts.
	Outer State: Outer State.
	*Negotiated Outer EAP Type:*Negotiated Outer EAP Type

Authentication Status:

Authentication state	Description
Undefined	802.1X function is disabled.
Logoff	An EAPOL LOGOFF message has been received.
Disconnected	The supplicant is not connected.
Connecting	The supplicant has sent an EAPOL start message and is awaiting subsequent EAP response messages.
Acquired	The supplicant has sent an EAP identity reply and is awaiting subsequent EAP authentication request messages.
Authenticating	The supplicant is performing EAP authentication exchanges.
Held	Authentication failed. The supplicant failed its EAP authentication.
Authenticated	Authentication succeeded. The EAP exchange is complete.

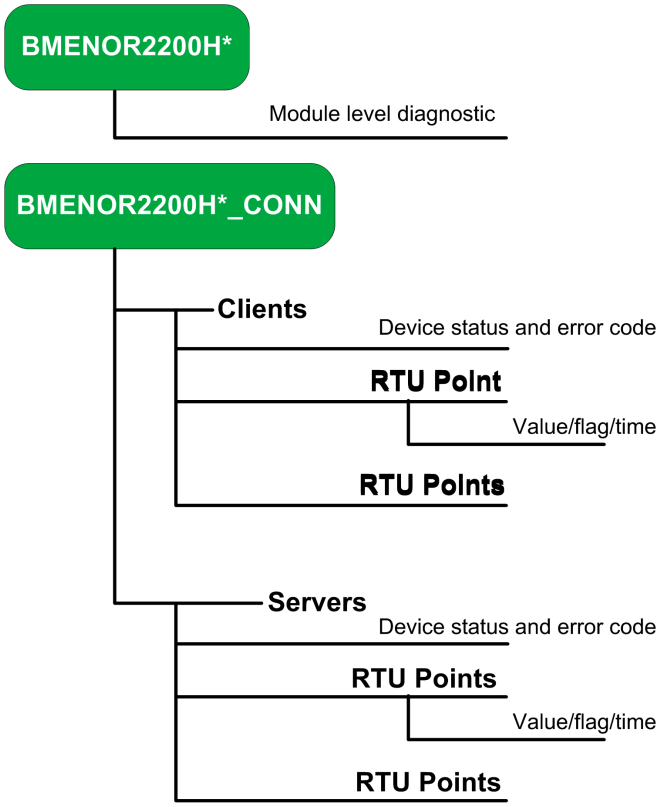
Device DDT Diagnostics

Introduction

This section describes Device DDT diagnostics for the BMENOR2200H module in a Hot Standby configuration.

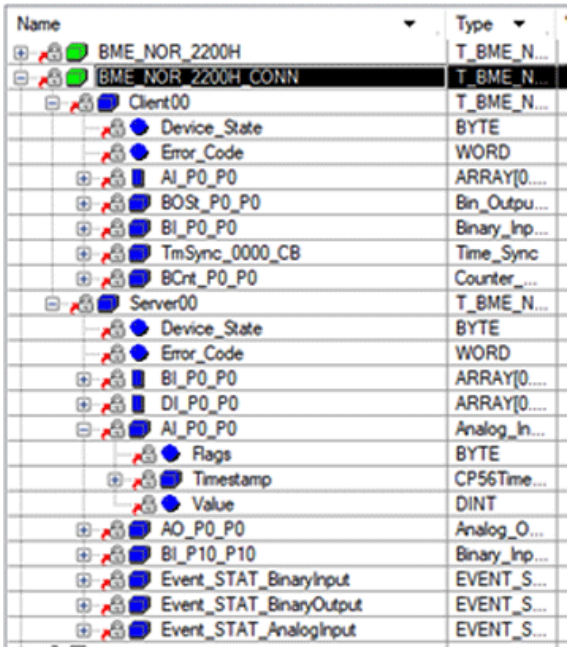
Device DDT Structure

Graphical Representation



**** customer-defined name***

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



Correspondences

These correspondences apply to the above DDT structure and graphical representation:

- 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 these 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)

Device DDT Diagnostics

Access the Diagnostics

View the device DDT diagnostics for the BMENOR2200H module:

1. Access the **Variables** tab in the **Data Editor** (**Project Browser > Project > Variables & FB instances**).
2. Select the **Device DDT** checkbox.

NOTE: The **Name** column shows the name that is assigned when you add the module to the project, page 108.

Module Diagnostics

View the Device DDT for BMENOR2200H module diagnostics:

Diagnostic Name		Comment
ETH_STATUS		Ethernet status
	ETH_BKP_PORT_LINK	Link up/down for Ethernet backplane port
	SCANNER_OK	Scanner OK and scanning at least one device (if at least one device configured)
	GLOBAL _STATUS	0: One or more services not operating normally.
		1: all operational
	NETWORK_HEALTH	1: No traffic overload detected 0: Traffic overload detected (ex: broadcast storm) **NOTE:** Check your network topology and configuration.
	PORT1_LINK	Link up/down for control port 1
	PORT2_LINK	Link up/down for control port 2
IN_PACKETS		Number of packets received on interface
IN_ERRORS		Number of inbound packets that contain errors
OUT_PACKETS		Number of packets sent on interface
OUT_ERRORS		Number of outbound packets that contain errors
SERVICE_STATUS		One bit for each user-observable feature

Diagnostic Name		Comment
	PORT502_SERVICE	0: Service not operating normally
		1: Service operating normally or disabled
	SNMP_SERVICE	0: Service not operating normally
		1: Service operating normally or disabled
	IP_ADDRESS_STATUS	IP address status (0 in case of duplicate IP or no IP assigned)
	SNTP_CLIENT	0: Service not operating normally
		1: Service operating normally or disabled
	WEB_SERVER	0: Service not operating normally
		1: Service operating normally or disabled
	FIRMWARE_UPGRADE	0: Service not operating normally
		1: Service operating normally or disabled
	CONTROL_NETWORK_MAIN_IP_ADDR	Main IP address status (0 in case of duplicate IP or no IP assigned)
	TIME_VALID	0: Time invalid
		1: Time valid
	LLDP_SERVICE	IP address A/B status (0 in case of duplicate IP or no IP assigned)
	SYSLOG_STATUS	0: Syslog service not operating normally
		1: Syslog service operating normally or disabled
	SYSLOG_SERVER_NOT_REACHABLE	1: No acknowledgement received from the syslog server
		0: otherwise
	SMTP_SERVICE	0: Service not operating normally
		1: Service operating normally or disabled
	DATALOGING	0: Service not operating normally
		1: Service operating normally or disabled
	RTU_DNP3	0: Service not operating normally
		1: Service operating normally or disabled
	RTU_IEC60870	0: Service not operating normally
		1: Service operating normally or disabled
	IEEE8021_SERVICE	0: Service not operating normally
		1: Service operating normally or disabled
	IP_FORWARDING_SERVICE	0: Service not operating normally
		1: Service operating normally or disabled
SD_STATUS		Bit 0 (STATUS): Set when card is normal
		Bit 1 (BUSY): Set when card is busy
		Bit 2 (LOW_SPACE_ALARM): Set when free space on card is less than 2%
FIRMWARE_VERSION		MSB: Major revision [HEX]
		LSB: Minor revision [HEX]
HW_VERSION		Hardware Version [HEX]
ETH_PORT1_2_STATUS		Control port 1 and 2 status
PROTOCOL_STATUS		General variable for RTU protocol status
	EVENT_OVERFLOW__COUNT	Number of total event overflows
	EVENT_BUFFER_USAGE	%Event buffer used in configured size
	DNP3_CLIENT_CONNECTION_COUNT	Number of total DNP3 client connections
	DNP3_SERVER_CONNECTION_COUNT	Number of total DNP3 server connections
	IEC60870_CLIENT_CONNECTION_COUNT	Number of total IEC60870 client connections
	IEC60870_SERVER_CONNECTION_COUNT	Number of total IEC60870 server connections
	MODBUS_CLIENT_CONNECTION_COUNT	Number of total Modbus client connections
	MODBUS_SERVER_CONNECTION_COUNT	Number of total Modbus server connections
CS_STATUS		—

Diagnostic Name	Comment
SECURE_MODE	Coding wheel state: • 0: Standard • 1: Advanced
CS_LED_STATUS	Cybersecurity LED status

Hot Standby Diagnostics

You can view all of the dedicated Device DDT diagnostics for a BMENOR2200H module in a Hot Standby system only after you configure at least one RTU channel in the DTM, page 114:

Diagnostic	Value	Type	Comment
HTSB_DIAG		T_HTSB_DIAG	—
SERVICE_STATE	0	BYTE	HTSB service state: • 0: Detected problem • 1: Running
SYNC_STATE	0	BYTE	HTSB synchronization status: • 0: In progress • 1: OK
INTERNAL_STATE	0	BYTE	Internal HTSB state: • 0: Init • 1: Link establish • 2: Reserved • 3: Integrity • 4: Wait synchronization • 5: Synchronized
PARTNER_VALIDITY	0	BYTE	Partner validity: • 0: Not reachable • 1: OK
ERROR_CODE	0	WORD	Bit 0: Firmware mismatch
			Bit 1: DTM configuration mismatch
			Bit 2: Security Mode mismatch
			Bit 3: DTLS certification error
			Bit 4: CS configuration mismatch (Reserved)
			Bit 5...15: Reserved
FW_VERSION_MISMATCH	0	BOOL	Application of the primary and standby are running with different firmware version
DTM_CFG_MISMATCH	0	BOOL	Application of the primary and standby are running with different DTM configuration
CS_CFG_MISMATCH	0	BOOL	Application of the primary and standby are running with different CS configuration
CERTIFICATION_ERROR	0	BOOL	DTLS certification error
SYNC_COUNT	0	UDINT	HTSB synchronization counter
DIN_PACKETS	0	UDINT	HTSB Input Packets Counter
N_ERRORS	0	UDINT	HTSB Input Error Packets Counter
OUT_PACKETS	0	UDINT	HTSB Output Packets Counter
OUT_ERRORS	0	UDINT	HTSB Output Error Packets Counter

RTU Diagnostics

You can view the Device DDT for BMENOR2200H RTU communication diagnostics only after you configure at least one RTU channel in the DTM, page 114:

Diagnostic Name	Value	Type	Comment
RTU Protocol Diagnostics			
Freshness	0	BOOL	All Device DDT variables of module are freshness
Scan_State	0	BYTE	0: Idle
			1: Busy
HSBY_Event_Index	0	UDINT	Index number of the current event generated in the module
HSBY_EventSync_Index	0	UDINT	Index number of the current event synchronized to standby module
Channel/Device Diagnostics			
<client_channel>	—	—	The channel name (*<client_channel>*, *<server_channel>*) corresponds to the name assigned in the channel configuration phase, page 114.
<server_channel>	—	—	
Device_state	0	BYTE	0: Unconnected
			1: Connected
			3: Active (Only for IEC 60870-104 in redundancy mode)
			4: Inactive (Only for IEC 60870-104 in redundancy mode)
Error_Code	0	WORD	Bit 0 (security_not_configured): Security not configured.
			Bit 1 (variable_initialize_error): Variable initialized error
			Bit 2 (internal_error): Internal error
			Bit 3 (authentication_failed): Detected authentication problem
			Bit 4 (unexpected_response): Unexpected response
			Bit 5 (no_response): No response
			Bit 6 (aggressive_mode_not_supported): Aggressive mode not supported
			Bit 7 (MAC_algorithm_not_supported): MAC algorithm not supported
			Bit 8 (key_Wrap_algorithm_not_supported): Key wrap algorithm not supported
			Bit 9 (authorization_failed): Detected authorization problem
			Bit 10 (update_key_change_method_not_permitted): Update key change method not permitted
			Bit 11 (invalid_signature): Invalid signature
			Bit 12 (invalid_certification_data): Invalid certification data
			Bit 13 (unknown_user): Unknown user
			Bit 14 (max_session_key_status_requests_exceed): Max session key status requests exceeded
			Bit 15 (TLS_error): TLS error
Unsol_Enabled (server channel only)	—	BYTE	0: Unsolicited Disable
			1: Unsolicited Enable
Event_STAT_AuthSecStats (server channel only)	—	—	
Count	0	WORD	
Overflow	0	BYTE	0: normal
			1: Overflow

File Explorer

Data Logging

Introduction

Access the **FILE EXPLORER** tab for the module to access data logging information through the BMENOR2200H web page. There are two tabs within the **Data Logging**:

- **DATALOGS**: This tab shows the list of saved data logging files.
- **ARCHIVES**: When the module receives its configuration, it compares the checksum with the one on the SD card. If they differ, the module archives the old files (including changed or unconfigured tables) in this dedicated archive folder.

Data Logs

This table describes the columns in the table on the **DATALOGS** tab:

Parameter	Description
Name	This column shows the names of the created tables. **NOTE:** The name of the table is generated by the Modbus response.
Date Modified	This column shows the day, date, and time that the table was last modified.
Size	This column shows the size (KB) of the selected table.

NOTE: Click the plus sign (+) button at the end of any row to expand and view the component .csv files of the logged table.

Archives

This table describes the parameters on the **ARCHIVES** tab:

Parameter	Description
Name	This column shows the names of the created tables. **NOTE:** The name of the table is generated by the Modbus response.
Date Modified	This column shows the day, date, and time that the table was last modified.
Size	This column shows the size (kilobytes) of the selected table.

Buttons

This table describes buttons of the **DATALOGS** and **ARCHIVES** tabs:

Button	Description
Delete	Press this button and follow the prompts to delete the selected table.
Download	Press this button and follow the prompts to download the selected table.
Download & Delete	Press this button and follow the prompts to download and delete the selected table.

Module Log

Introduction

The **Module Log** page provides access to diagnostic files generated by the Remote Terminal Unit (RTU). These files record system events, configuration changes, and when the application stops responding. They are essential for troubleshooting and for advanced analysis by support teams.

Accessing Module Logs

Navigate to **File explorer** page from module web page.

The page displays the log module table with a list of log files stored in the RTU, including:

- File name
- Last modified time
- File size

Available Actions

The **Module Log** page provides several actions to manage log files stored in the RTU, including refreshing the list, downloading files for analysis, and deleting unnecessary logs.

- **Refresh** Updates the list of available log files.
- **Upload** Transfers log files from the RTU to your PC for analysis.
- **Delete** Removes selected log files from the RTU.
- **Delete All** Deletes all log files from the RTU.

For details on the actions available for each user type, refer to RBAC, page 229.

Log File Details

The following table lists the log files available in the **Module Log** page and describes their purpose.

File Name	Description
nat_diag.txt	Diagnostic information related to NAT configuration and operations.
firewall_diag.txt	Logs related to firewall rules and ACL operations.
<dump file name>.vxcore.txt	Log indicating that the firmware stopped responding (text summary).
<dump file name>.vxcore	Detailed stop responding data for advanced analysis.

Cyber Security Configuration

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, page 23.

NOTE: Web page access is available only when the module is in advanced mode. Refer to the directions for configuring the appropriate level of cyber setting with the rotary switch, page 28.

Before You Begin

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

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

- If you want to configure cyber security on RTU protocol, you need to have configured at least one communications channel for the module in the Control Expert DTM.
- You have configured the appropriate setting (**Advanced**) on the rotary switch, page 28.

Login

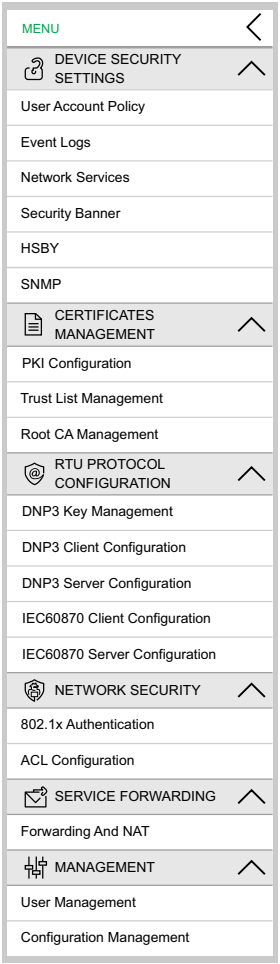
The first time you log in to advanced mode, the cyber security file is not valid. Therefore, follow these steps to configure the file:

Stage	Description
1	Log in to the web pages as an administrator, page 177.
2	Access the cyber security setting page, page 176.
3	Configure the event log with a valid IP address (or disable event log), page 200.
4	Configure a valid pre-shared key or disable DTLS in HSBY, page 203.
5	Apply the configuration to the module.

Setup Web Pages

Introduction

Use the setup web pages to communicate with a web server in the BMENOR2200H module to set all cybersecurity configuration aspects for the device.



User Account Policy Web Page

Access the Page

Access the **User Account Policy** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > DEVICE SECURITY SETTINGS > User Account Policy**).

Settings

Configure these settings on the on the **User Account Policy** web page:

Parameter		Description
USER ACCOUNT SETTINGS	*Session Maximum Inactivity*	This is the idle session timeout period (minutes) for HTTPS connections. **NOTE:** If a connection is inactive for this period, the user session is automatically closed.
	Maximum login attempts	This value represents the number of allowed login attempts that could not be accomplished. **NOTE:** When this configured maximum is reached, no additional logins are allowed for the configured period.
	Login attempt timer	This value represents the maximum amount of time (minutes) that is allotted for the login period.
	Account locking duration	This value represents the period of time (minutes) durin which no additional login attempts are allowed after the configured maximum login attempts is reached. Upon the expiration of this period, a locked user account is automatically unlocked.
Submit		Click this button to apply the new settings.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

Event Logs Web Page

Introduction

The BMENOR2200H module provides cyber security Syslog when the Advanced mode is enabled.

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

Access the Page

Access the **Event Logs** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > DEVICE SECURITY SETTINGS > Event Logs**).

Parameters

Find these parameters and settings on the **Event Logs** web page:

Parameter	Description
Service activation	Click these buttons to turn the Syslog client services on and off. **NOTE:** This service is *on* by default. Enter a valid IP address the first time the module runs in advanced mode to turn the Event Logs service *off*. Otherwise, the module remains in "invalid configuration" mode.
Syslog server IP address	This field contains the IPv4 address of the remote Syslog server. **NOTE:** If you configure the Syslog server, all events are forwarded to this IP address.
Syslog server port	This field shows the port number that is used by the Syslog client service.
Submit	Click this button to apply the new settings.

NOTE: Refer to the instructions for setting up a cyber security audit for event logging in the Modicon Controllers Platform Cyber Security, Reference Manual.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

Network Services Web Page

Introduction

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 BMENOR2200H module.

Access the Page

Access the **Network Services** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > DEVICE SECURITY SETTINGS > Network Services**).

Parameters

Parameter		Description
GLOBAL POLICY	*Enforce Security*	Click this button to disable all network services, except IPsec which is enabled.
	Unlock Security	Click this button to enable all network services, except IPsec which is disabled.
NETWORK SERVICES ACTIVATION	*SNMP Agent*	Use the pull-down menu to enable and disable SNMP agent communications.
	Modbus TCP Server	Use the pull-down menu to enable and disable the Modbus TCP server.
	DNP3 Server	Use the pull-down menu to enable and disable the DNP3 server.
	IEC60870 Server	Use the pull-down menu to enable and disable the IEC60870 server.
Submit		Click this button to apply the new settings.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

Security Banner Web Page

Access the Page

This page contains editable text that is displayed when a user accesses the web pages for the BMENOR2200H module:

Access the **Security Banner** web page through the **SETUP** tab for the module (**SETUP > MENU > DEVICE SECURITY SETTINGS > Security Banner**).

Parameters

Find these parameters and settings on the on the **Security Banner** web page:

Parameter		Description
LEGAL SECURITY BANNER	*Banner text*	A string of characters is displayed to a user on the login page. This editable text is displayed by default: *Unauthorized use of the system is prohibited and subject to criminal and/or civil penalties.* **NOTE:** The maximum string length is 128 characters.
Submit		Click this button to apply the new settings.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

HSBY Web Page

Introduction

In a Hot Standby system, the BMENOR2200H module supports datagram transport layer security (DTLS). This cyber security feature helps defend against attacks by hiding Hot Standby communication in encrypted traffic. Use these settings:

- *Enable DTLS*
- *Pre-shared key*

You can enable or disable the DTLS protocol for each module. The feature is enabled by default when the module is in advanced mode. Enter the pre-shared key or disable DTLS when the BMENOR2200H module initially boots (like the Syslog function).

Access the Page

Access the **HSBY** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > DEVICE SECURITY SETTINGS > HSBY**).

Parameters

Parameter	Description
Enable DTLS	Select (check) this box to enable DTLS.
	Deselect (uncheck) this box to disable DTLS.
	NOTE: The Hot Standby DTLS is on by default. The first time you use the module in advanced mode, enter a valid pre-shared key or turn it off. Otherwise, the module remains in "invalid configuration" mode.
Pre-Shared Key	Enter a key value (in hexidecimal). **NOTE:** There is no default value for the *Pre-shared Key*. User must record this key manually or back up the cybersecurity configuration after any change applied.
Generate	As an option, click this button to use a randomly generated key.
Submit	Click this button to apply the new settings.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

SNMP Web Page

Access the Page

Access the **SNMP** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > DEVICE SECURITY SETTINGS > SNMP**).

Parameters

Find these parameters and settings on the on the **SNMP** web page:

Parameter	Description
SNMP Version	SNMPv1
	SNMPv3
Security Level (SNMPv3 only)	*No Authentication, No Privacy*
	Authentication, No Privacy
	Authentication, Privacy: This selection activates two required password fields: • *Authentication Password* • *Privacy Password*

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

Certificates Management

Authentication Overview

A BMENOR2200H module can be authenticated in two ways:

- Self-signed certificate
- Certificate Authority (CA)

The BMENOR2200H module creates a self-signed certificate for:

- Configuration of the cyber security settings via the module web pages
- Diagnostic of the module via its web pages
- Firmware upgrade

Certificate Limitations

To support communication with the BMENOR2200H module, note the self-signed and CA certificate limitations, as follows:

Self-Signed Certificates:

- KeyUsage (marked as critical):
  - DigitalSignature
  - KeyEncipherment (No usage for TLS suite based on ephemeral keys such as TLS_ECDHE_xxxx; usage for TLS_RSA_xxxx)
  - KeyCertSign: when the subject public key is used for verifying signatures on public key certificates (Value TRUE)
  - nonRepudiation
  - dataEncipherment
- Subject Alt Name: In the SAN field the following values can be specified: IPAddress V4/V6, URI
- Basic Constraints:
  - cA field: whether the certified public key may be used to verify certificate signatures (Value TRUE) and pathLenConstraint=0
- Subject Key Identifier:
  - means of identifying certificates that contain a particular public 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
- Extended Key Usage extension:
  - id-kp-serverAuth if TLS Web server authentication
  - id-kp-clientAuth if TLS Web client authentication

CA Certificates:

- KeyUsage (marked as critical):
  - DigitalSignature
  - KeyEncipherment (No usage for TLS suite based on ephemeral keys such as TLS_ECDHE_xxxx; usage for TLS_RSA_xxxx)
  - KeyCertSign: when the subject public key is used for verifying signatures on public key certificates (value FALSE)
  - nonRepudiation
  - dataEncipherment
- Subject Alt Name: In the SAN field the following values can be specified: IPAddress V4/V6, URI
- Basic Constraints:
  - cA field: whether the certified public key may be used to verify certificate signatures (value FALSE)
- Extended Key Usage extension:
  - id-kp-serverAuth if TLS Web server authentication
  - id-kp-clientAuth if TLS Web client authentication
- CRL Distribution points
- Authority Key Identifier:
  - Identification of the public key corresponding to the private key used to sign a certificate.

PKI Configuration Web Page

Certificates Management and PKI

NOTE: Before you begin working on the **PKI Configuration** web page, familiarize yourself with the general description of certificates management, page 207.

The BMENOR2200H module relies upon certificates for authentication. To provide cyber security, each entity manages a trust list of all certificates of devices and applications that communicate with it. The method of certificate management depends on your system design, which may or may not apply a public key infrastructure (PKI) with a certificate authority (CA):

- **Certificates Management without PKI:** Use this certificate management method if your system does not include a CA. Manage certificates in the certificates management web pages as follows:
  - Self-signed only is the system default PKI mode.
  - You can only switch the device factory reset mode to self-signed only mode.
  - Manage the Certificate Trust List using the Add and Delete functions to create an allowed list that is authorized to communicate with the BMENOR2200H module.
  - Click the **Download** button (below) to export the BMENOR2200H module certificate to communicated devices.
- **Certificates Management with PKI:** Access the **PKI Configuration** web page and configure the parameters as described below.

Access the Page

Access the **PKI Configuration** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > CERTIFICATES MANAGEMENT > PKI Configuration**).

PKI Parameters

Manage the allotment and acceptance of certificates with the following PKI parameters if your system includes a CA.

PUBLIC KEY INFRASTRUCTURE SETTINGS parameters:

Parameter	Description
PKI Mode	*Self-Signed only:* This is the default PKI mode for the system.
	CA only: All installed devices support PKI. Manually enroll each BMENOR2200H module with the CA.
	Self-Signed & CA: Some installed devices do not support PKI. Considerations: • The certificate for the BMENOR2200H module is issued by a CA. • Certificates for devices that support PKI are issued by a CA. • Certificates for devices that do not support PKI are self-signed. Manually enroll each BMENOR2200H module with the CA. Manage the trusted list to create an allowed list that is authorized to communicate with the BMENOR2200H module. **NOTE:** Only certificates in the **Trusted List Management** list need to be managed.
Submit	Click this button to assign the PKI mode.

DEVICE CERTIFICATION parameters:

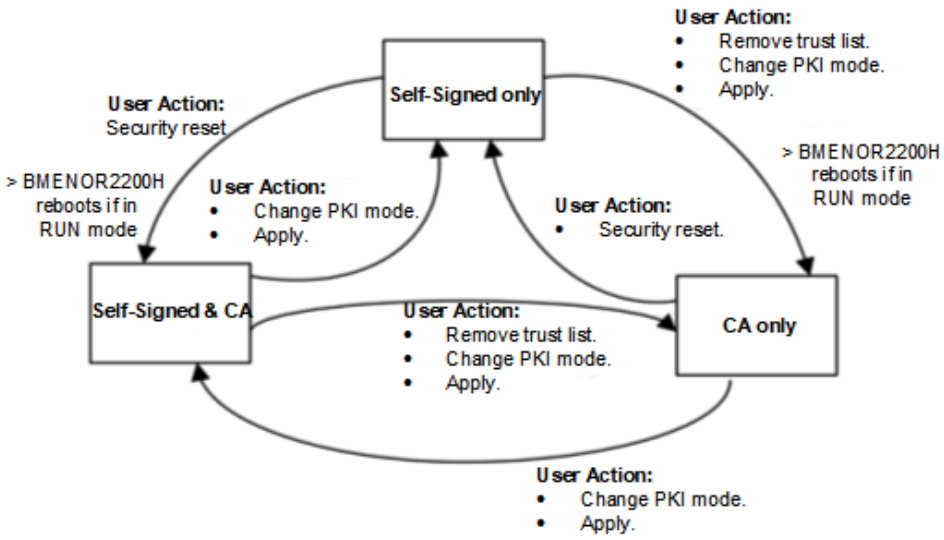
Parameter	Description
Subject	This line identifies the host or party that controls the private key certification.
Subject Alternative Name	The structured name in this field includes the domain and sub-domain names and the IP addresses that the certificate secures.
Issuer	This field shows the entity that issued the certificate.
Expiration Date	This field shows the expiration date of the certificate.
Download	Click this button to export the BMENOR2200H module certificate for HTTPS on your PC.

ENROLLMENT parameters:

Parameter	Description
1. Generate CSR	Click this button to download on your PC a Certificate Signing Request (CSR) in the Privacy Enhanced Mail (.pem) format.
2. Select the certificate file to upload	Enter an X.509v3 certificate that is encoded in ASN.1 (DER). A CA installed in the device produced this certificate from the downloaded CSR for the device. **NOTE:** You can use the **Browse** button to navigate to the file.
Upload	Click this button to upload on the module an offline file that contains a configuration for communications with the CA by receiving the certificate through the CSR.
NOTE: Refer to the description of the manual certificate-enrollment process, page 210.	

PKI Mode Setting Flowchart

This diagram illustrates the user actions and events related to changing the PKI mode setting:



Execute Changes

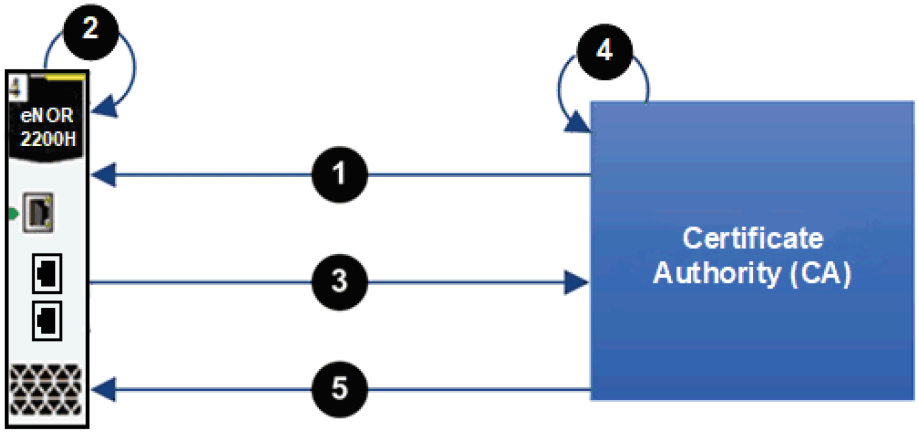
After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

Manual Enrollment

After configuring the BMENOR2200H module in Control Expert, you can use the **PKI Configuration MENU, ENROLLMENT** section to *get* a CSR file to be submitted to a CA. After submitting the CSR file, you can then extract the correspondent CA certificate. Thereafter, you can push this CA Certificate into the BMENOR2200H module. The combined get and push operations manually enroll a certificate issued by a third-party CA. After the certificate is pushed, the server applies this certificate for the purpose of signing and encrypting its communication with the client.

The following is an overview of the manual certificate enrollment process:



1 The BMENOR2200H imports a Root CA Management MENU from the certificate authority (CA).

2 The BMENOR2200H generates a certificate signing request (CSR).

3 The BMENOR2200H exports the CSR to the CA.

4 The CA executes the CSR and generates a certificate.

5 The BMENOR2200H imports the certificate from the CA.

Trust List Management Web Page

Introduction

To provide the required level of cyber security, each entity BMENOR2200H module manages a trust list of all certificates of devices/applications that communicate with it.

Only devices that have provided the BMENOR2200H module with an application instance certificate can communicate with RTU. The module implements local (module-based) management of application instance certificates, which are stored in a trust list. Use the commands on the **Certificates Management** web pages to add, download, or delete a certificate.

NOTE:

- Application instance trust list certificates are encoded in ANSI CRT.
- Before you begin working on the **PKI Configuration** web page, familiarize yourself with the general description of certificates management, page 207.

Access the Page

Access the **Trust List Management** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > CERTIFICATES MANAGEMENT > Trust List Management**).

Parameters

Use these parameters and settings on the on the **Trust List Management** web page to create a truts list:

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. **NOTE:** The expiration dates of the trusted certificates are made by reference to the internal Date and Time settings of the BMENOR2200H module. To help avoid inconsistency, use the NTP service to update the date and time settings of the RTU module, and verify that the NTP server is accessible and has an updated time and date settings. The BMENOR2200H module does not automatically manage the expiration dates of certificates. • For a self-signed certificate file, it is determined by the device. • For a CA certificate file, it depends on the CA agent.
Browse	Click this button to navigate to and select the certificate you want to add to the list.
Submit	Click this button to add the selected file to the list.
Apply	Click this button to record your configuration changes.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

Root CA Management Web Page

Introduction

The CA certificate is a public key certificate that identifies the certificate authority (CA) in a public key infrastructure (PKI). Use the **Root CA Management** page to push CA certificate(s) in the device.

NOTE: Before you begin working on the **PKI Configuration** web page, familiarize yourself with the general description of certificates management, page 207.

Access the Page

Access the **Root CA Management** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > CERTIFICATES MANAGEMENT > Root CA Management**).

Parameters

Find these parameters and settings on the on the **Root CA Management** web page:

Parameter	Description
Name (CN)	This column shows the name of the certificate.
Distinguished Name (DN)	The column corresponds to the name of the certificate.
Expiration Date	This field shows the expiration date of the certificate. **NOTE:** • The expiration dates of the trusted certificates are made by reference to the internal Date and Time settings of the BMENOR2200H module. To help avoid inconsistency, use the NTP service to update the date and time settings of the BMENOR2200H module, and verify that the NTP server is accessible and has an updated time and date settings. • The BMENOR2200H module does not automatically manage the expiration dates of certificates. ◦ For a self-signed certificate file, it is determined by the device. ◦ For a CA certificate file, it depends on the CA agent.
Browse	Click this button to navigate to and select the certificate you want to add to the list.
Submit	Click this button to add the selected file to the list.
Apply	Click this button to record your configuration changes.

NOTE: You can add a maximum of 10 CA certificates.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

DNP3 Key Management Web Page

Access the Page

Access the **CLIENT** and **SERVER** tabs for the **DNP3 Key Management** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > MANAGEMENT > DNP3 Key Management**).

Client Parameters

Find these parameters and settings on the on the **CLIENT** tab on the **DNP3 Key Management** web page:

Parameter	Description
User Number	This number corresponds to the current DNP3 user.
User Name	This name corresponds to the current DNP3 user.
Key Wrap	Select AES-128 or AES-256 from the pull-down menu.
Update Key	The column contains the value of the pre-shared key.
Generate	For the pre-shared key field (*Update Key*), you have the option to click the **Generate** button to use a randomly generated key.
Submit	Click this button to apply the modifications to the selected channel.
Add User	Click this button to open the **Add User** dialog box. In the screen you can configure the above parameters to create an additional user with defined roles and click the **OK** button to add the user to the table on the main **KEY MANAGEMENT > CLIENT** page.

Server Parameters

The server parameters are visible only after you have created a table on the **SERVER** tab on the **DNP3 Key Management** web page:

Step	Action
1	Click the **Create Table** button to open the **Create User Table** dialog box.
2	Assign a name to the table in the **Table Name** field.
3	Click the **OK** button to see the new table in the **KEY MANAGEMENT** list. **NOTE:** You can now see the name of the table in the pull-down menu next to the **Remove Table** button.
4	Additional steps: • To add additional tables to the **KEY MANAGEMENT** list, repeat the above steps. • To delete this table, select the table in the pull-down list, click the **Remove Table** button, and follow the prompts to delete the table. **NOTE:** The **Remove Table** button is visible only after you create at least one table. • To remove specific users from a table, select the table in the **KEY MANAGEMENT** list, click the trash can icon, and follow the prompts to remove the user from the table.

Parameters descriptions:

Parameter	Description
User Number	This number corresponds to the current DNP3 user.
User Name	This name corresponds to the current DNP3 user.
User Role	Select a role for the user according to the role descriptions, page 229.
Key Wrap	Select the appropriate wrap algorithm (AES-128 or AES-256).
Update Key	The column contains the value of the pre-shared key.
Generate	For the pre-shared key field (*Update Key*), you have the option to click the **Generate** button to use a randomly generated key.
Add User	Click this button to open the **Add User** dialog box. In the screen you can configure the above parameters to create an additional user with defined roles and click the **OK** button to add the user to the table on the main **KEY MANAGEMENT > SERVER** page.
Submit	Click this button to apply the modifications to the selected channel.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

DNP3 Client Configuration Web Page

Access the Page

Access the **DNP3 Client Configuration** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > RTU PROTOCOL CONFIGURATION > DNP3 Client Configuration**).

Parameters

Find these parameters and settings on the **DNP3 Client Configuration** web page:

Parameter	Description
Channel Name	This is the name of the selected channel.
Enable TLS	Select (check) this box to enable TLS.
	Deselect (uncheck) this box to disable TLS.
Secure Authentication	SAv2
	SAv5
	Disabled
Enable Aggressive Mode	Select (check) this box to enable aggressive mode.
	Deselect (uncheck) this box to disable aggressive.
Current User	Click the **Select** button to open the **Current User** dialog box to define the active user. **NOTE:** You can click the **Key Management** link in the **Current User** dialog box to go directly to the *DNP3 Key Management* web page, page 213.
Advanced Settings	Click the **Configure** button to open the **Advanced Settings** dialog box and configure these parameters: • *GENERAL AUTHENTICATION PARAMETERS* • *SAV2/SAV5 PARAMETERS* **NOTE:** There are several parameters in the **Advanced Settings** dialog box. Click the information icon (*i*) to the right of any parameter field to see a description of the acceptable values.
Submit	Click this button to apply the modifications to the selected channel.
Add Channel	Click this button to open the **Add Channel** dialog box on which you can create an additional channel using the above-listed parameters. Click the **OK** button to add an entry to the table (with the new **User Name**).

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

DNP3 Server Configuration Web Page

Access the Page

Access the **DNP3 Server Configuration** web page through the **SETUP** tab for theBMENOR2200H module (**SETUP > MENU > RTU PROTOCOL CONFIGURATION > DNP3 Server Configuration**).

Parameters

Find these parameters and settings on the **DNP3 Server Configuration** web page:

Parameter	Description
Channel Name	This is the name of the selected channel.
TLS Enabled	Select (check) this box to enable TLS for all server channels.
	Deselect (uncheck) this box to disable TLS for all server channels.
Secure Authentication Enabled	SAv2
	SAv5
MAC Algorithm (HMAC)	Select the MAC algorithm to be applied in challenges.
Key/Account Table	This table lists these client/server options: • *User Number* • *User Name* • *User Role* (operator, viewer, single user) • *Key Wrap:* Select AES-128 or AES-256. • *Key:* Enter the key wrap algorithm (hexadecimal format). • *Apply:* Click this button to record your modifications.
Enable Aggressive Mode	Select (check) this box to enable aggressive mode.
	Deselect (uncheck) this box to disable aggressive.
Advanced Settings	Click the **Configure** button to access these advanced parameters for the selected channel: • *GERNERAL AUTHENTICATION PARAMETERS* • *SAV2/SAV5 PARAMETERS* **NOTE:** Click any information icon (*i*) to see a description of the corresponding parameter.
Submit	Click this button to apply the modifications to the selected channel.
Add Channel	Click this button to create a channel with this configuration.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

DNP3 Secure Authentication Setup

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, page 177.
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: • **Client Configuration** • **Server Configuration** • **Key Management** **NOTE:** These security settings are described individually below.

Refer to these discussions:

- DNP3 client channel configuration web page, page 215
- DNP3 server channel configuration web page, page 216

NOTE: The implemented HMAC setting is the main difference between networked and serial DNP3 authentication:

Communications Protocol	HMAC Setting
serial	HMAC SHA-1 (8 bytes)
	HMAC SHA-256 (8 bytes)
networked	HMAC SHA-1 (10 bytes)
	HMAC SHA-256 (16 bytes)

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.

NOTE: Observe these maximums for the number of DNP3 users that can participate in key management configuration:

- DNP3 SAv2: 10
- DNP3 SAv5: 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
CLIENT (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 module acts as a data concentrator, the current user role on the **CLIENT** 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.
SERVER (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.

IEC60870 Client and Server Web Pages

Access the Page

Access the client and server web pages for the IEC60870 standard through the **SETUP** tab for the BMENOR2200H module.

Client Parameters

View the IEC60870 client configuration (**SETUP > MENU > RTU PROTOCOL CONFIGURATION > IEC60870 Client Configuration**):

Parameter	Description
Channel Name	This is the name of the selected channel.
Enable TLS	*enabled:* Select (check) this box to enable TLS.
	disabled: Deselect (uncheck) this box to disable TLS.
Submit	Click this button to apply the modifications to the selected channel.
Add Channel	Click this button to create an additional channel.

Server Parameters

View the IEC60870 server configuration (**SETUP > MENU > RTU PROTOCOL CONFIGURATION > IEC60870 Server Configuration**):

Parameter	Description
TLS Enabled	*enabled:* Select (check) this box to enable TLS.
	disabled: Deselect (uncheck) this box to disable TLS.
Submit	Click this button to apply the modifications to the selected channel.

Execute Changes

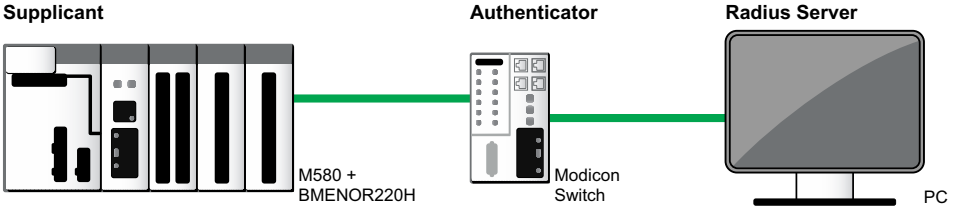
After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

IEEE 802.1x Authentication

Introduction

This chapter describes how to help secure network access to the module using IEEE 802.1X. In this architecture, the module acts as the supplicant, an 802.1X compatible industrial Ethernet switch acts as the authenticator, and an external RADIUS server provides the authentication decision. The chapter focuses on what must be configured in the module Web UI and the minimal settings that must exist on the switch (global 802.1X enablement, per-port 802.1X mode, RADIUS server IP and shared secret).



Configuration Parameters

Parameter	Type	Description
Authentication Enable	Boolean	Turns 802.1X authentication on / off for the selected BMENOR2200H port.
Port	Enum	Displays the currently targeted port for authentication. One port per action (Control Port 1, Control Port 2, or Backplane).
EAP Method	Enum	Selects the outer EAP method.
Internal EAP Method	Enum	Inner method used with tunneled methods. **NOTE:** Used with PEAPv0 / TTLS, not used with MD5 / TLS / MSCHAPv2.
Identity	Text	Supplicant identity.
Password	Text	Supplicant password. **NOTE:** Used with MD5 / MSCHAPv2 / PEAPv0 / TTLS, not used with TLS.
Submit / Cancel	Boolean	Applies or discards current settings.

Procedure Example

TTLS (with certificate):

This procedure is for perform password-based authentication inside a TTLS tunnel.

The BMENOR2200H needs to trust the RADIUS server.

Firstly, ensure the RADIUS server is properly configured (TTLS enabled, valid server certificate, user/realm as required).

On the Modicon managed switch:

Step	Action
1	Log in • Switch user: admin • Default Password: private
2	On **Network security** > **Port security** > **802.1x** > **Global**: Enable 802.1X.
3	On **Network security** > **Port security** > **802.1x** > **Port Configuration**: Select ports and set type from **forceAuthorized** to **Auto**
4	On **Network security** > **Port security** > **RADIUS** > **Authentication Server**: Add radius server IP address and associated secret.

On BMENOR2200H:

Step	Action
1	On **Setup** > **Certificate Management** > **Root CA management**: Import root certificate of Radius to NOR.
2	On **Setup** > **802.1X Authentication**: Set **Authentication Enable** = **ON**.
3	On **Setup** > **802.1X Authentication**: Select the **Port**.
4	On **Setup** > **802.1X Authentication**: Set **EAP Method** = **TTLS**.
5	On **Setup** > **802.1X Authentication**: Set **Internal EAP Method**.
6	On **Setup** > **802.1X Authentication**: Enter **Identity** and **Password**.
7	On **Setup** > **802.1X Authentication**: Click **Submit**.
8	On **Diagnostics** > **802.1X Authentication**: Check **Last Authentication Status** becomes **Authenticated**.

ACL Configuration

Introduction

Access Control Lists (ACL) restrict network access to RTU services by IP address and port number. On X80 Advanced RTU, ACL rules can be applied to:

- the **Control Port**
- the **Backplane Port**

When ACL is **enabled**, only traffic that matches a configured **Service** and a permitted **Source IP** is allowed. Other IP addresses are blocked for this service. The UI provides status icons per service:

- Red: blocked (no client can access the service)
- Yellow: partially allowed (only the white listed sources can access)
- Green: allowed (all sources can access)

NOTE: For system availability, HTTPS on the backplane is forced open to prevent lock-out of the web interface.

All settings saved in the **ACL Configuration** are recorded in the **Module Log**. For more information, see Module Log, page 196.

Service List

Defines the services (protocol/port) that ACL can control. Typical entries include HTTPS (TCP/443), Modbus-TCP (TCP/502), ICMP Echo, SNMP, and custom services (Customer TCP-1/...). The NBMENOR2200H module will block listed service when ACL is enabled. The services not in this list are allowed to access the module.

Parameter	Type	Description
Service Name	Enum	Logical name displayed in tables created from the Service Label (for example HTTPS, Modbus-TCP, Customer TCP-1).
Protocol	Enum	Transport protocol used by the service.
Port Number	Integer	Listening port associated with the service. (value range: 1...65535). Not used for ICMP.
Service Label	Enum	Optional display name shown in the Service List.
Service Access (Control Port) Status	-	Real-time accessibility of the service through **Control Port**.
Service Access (Backplane Port)	-	Real-time accessibility of the service through **Backplane Port**.

The **Service List** supports the following actions to manage ACL-controlled services:

- **Add Service**: Create a custom entry.
- **Delete**: Remove a service from ACL control only if it is not referenced by any rule.

ACL Source IP

Defines who (which IPs or ranges) may access services when ACL is enabled.

Parameter	Type	Description
IP Mode	Enum	Select addressing mode for the source definition.
IP / Range / Subnet	IPv4	Enter the address(es) according to the selected **IP Mode**. For **Single IP**, provide the host address and for **Range IP**, provide the start and end of the address range.
SubMask	IPv4 mask	Defines the network boundary used to compute the permitted source range.
Address Label	Text	Label used later when selecting sources in rules. Concatenation of the IP address and submask.

The **ACL Source IP** table supports the following actions to define and maintain the set of permitted sources referenced by ACL rules:

- **Add ACL Source**: Create a new source definition using **Single IP** or **Range IP**.
- **Edit**: Modify an existing source. Changes apply to **Control**/**Backplane** rules that reference it.
- **Delete**: Remove a source definition. **Control**/**Backplane** access list rules that reference this source are cleared automatically.

Control/Backplane Port Rule - Access List

The **Control/Backplane Port Rule - Access List** section defines which source IP addresses are allowed to access specific services through the Control/Backplane Port when ACL is enabled.

In the **Control/Backplane Port Rule - Access List** section you can perform the following actions:

- **Enable / Disable Control Port ACL**: Activate or deactivate access list enforcement on the **Control**/**Backplane Port**.
- **Add Control/Backplane Port Rule**: Create a new rule by selecting a defined source IP and a service from the **Service List**.

Parameter	Type	Description
Control/Backplane Port ACL Enable	Boolean	When enabled, only listed rules are allowed on **Control**/**Backplane Port**.
ACL Source IP	Enum	Source set permitted to access the selected service(s).
Service	Enum	The service endpoint accessible from that source on **Control**/**Backplane Port**.

- **Delete**: Remove an existing rule. Once deleted, the associated source and service pair is no longer permitted on the Control/Backplanel Port.

Forwarding and NAT

Introduction

Forwarding and NAT are different functions: IP Forwarding routes IP traffic between RTU connected subnets (no address translation), whereas NAT (Port Forwarding) translates incoming connections on the Control Port to a specific Internal Port Number.

- **Forward On** (IP forwarding): the RTU routes traffic between the control port network and the backplane/internal network, allowing devices in different subnets to communicate when they use the RTU interface IP as their gateway.
- **NAT On** (port forwarding): the RTU translates connections received on the external port numbers of the control port and forwards them to a specific Internal IP: Internal Port Number .

NOTE:

- IPSEC messages cannot be forwarded.
- The optional FTP ALG component is fully supported in NAT.

NAT Rules

The following settings need to be configured in order to create a NAT rule:

Parameter	Type	Description
External Port Number	Integer	This is the port to which clients connect. It must be unique across all rules (value range 1...65535).
Service Name	Enum	Logical name to identify the rule in the UI. Standard services may imply internal ports, custom services allow flexible mapping.
Protocol	Enum	Transport protocol of the forwarded connection.
Internal IP	IPv4	Destination host on the internal/ backplane network.
Internal Port Number	Integer	Destination service port on the internal host (value range 1...65535).

When the **NAT On** is selected you can perform the following actions:

- **Add Rule**: Create a port-forwarding rule by entering **External Port Number**, **Service Name**, **Protocol**, **Internal IP**, and **Internal Port Number**.
- **Edit**: Modify an existing rule; changes take effect after **Apply**.
- **Delete**: Remove a rule; the external port mapping is no longer available.

Block All

When **Block All** is selected, neither IP forwarding nor port forwarding is active.

Procedure Example

Purpose: Allow an external client to reach a DNP3 device on the internal network through the RTU using a dedicated external port.

Example data (replace with your own):

- Mode: NAT On
- Service: HTTPS
- Protocol: TCP
- Internal Port: 443
- Internal IP: 192.168.10.101
- External Port Number: 444 (client connects to RTU Control Port on 444)

Step	Action
1	Select **NAT On** in the mode selector.
2	Click **Add Rule** to open the **Add Rule** dialog.
3	Enter **External Port Number** = 444.
4	Set **Service Name** = HTTPS.
5	Select **Protocol** = TCP
6	Enter **Internal IP** = 192.168.10.101.
7	Enter **Internal Port Number** = 443.
8	Click **OK**.
9	Click **Apply** in the top banner to save your changes.

User Management Web Page

Access the Page

Access the **User Management** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > MANAGEMENT > User Management**).

Parameters

Parameter		Description
USER MANAGEMENT	*User Name*	This field shows the current user.
	Roles	This field shows the role for the current user.
ROLES		Select the role performed by the user (**OPERATOR**, **ENGINEER**, **INSTALLER**, **SECURITY ADMINISTRATOR**) **NOTE:** A single user can perform multiple roles.
CHANGE PASSWORD	*New Password*	Enter the new password.
	Confirm Password	Re-enter the new password.
	Submit	Apply the new password.
	NOTE: • There is no default value for the *PASSWORD*. User must record the password manually or back up the cybersecurity configuration after any change applied. • If the user forget the password, use the factory reset to erase all cybersecurity configuration, details refer to Set the Switch, page 29	
Add User	Click this button to create additional users with defined roles. **NOTE:** You can create a maximum of 15 new users.	

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

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

Configuration Management Web Page

Introduction

You can use the **Configuration Management** web page to export the cyber security settings for a BMENOR2200H module to import that configuration into another module.

NOTE: Only a security administrator with SECADM credentials can perform these configuration management tasks.

Access the Page

Access the **Configuration Management** web page through the **SETUP** tab for the BMENOR2200H module (**SETUP > MENU > MANAGEMENT > Configuration Management**).

Export the Configuration

Export the cyber security configuration file with the **EXPORT CONFIGURATION** parameters on the **Configuration Management** tab. The applied settings immediately overwrite the existing settings.

Configure these parameters for the export action:

Parameter	Description
Password	Enter your Password, which is an encryption key to archive the exported configuration file. **NOTE:** This same password is used to archive an imported configuration file.
Confirm Password	Re-enter your password.
Export	Click this button to exmport the configuration.

Import the Configuration

Import the cyber security management configuration and apply it to the module with the **IMPORT CONFIGURATION** parameters on the **Configuration Management** tab.

Configure these parameters for the import action:

Parameter	Description
Configuration Archive	Select the configuration file you want to import and follow the prompt(s) to confirm your selection. **NOTE:** You can use the **Browse** button to navigate to the appropriate file.
Password	Enter the configuration file password that was assigned to the file when the file was exported.
Save	Select this check box to automatically apply the imported configuration immediately after it is uploaded.
Import	Click this button to import the configuration.

Reset the Configuration

Click the **Reset** button in the *RESET CONFIGURATION* field to restore the factory default cyber security settings for the module.

NOTE: Restart the module to implement the reset action.

Execute Changes

After you configure any of these parameters, press the **Apply** button in the page banner to implement your changes.

NOTE: The **Apply** and **Discard** buttons are disabled (grayed out) when the configuration is not valid.

RBAC

Introduction

Role-based access control (RBAC) is a method to help reduce the risk of cybersecurity 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 five.

Available Functionalities

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

		DNP3 SAv2/v5		Firm-ware	Web Page (HTTPS)						
Value	Name	Monitor Data	Operator Control	Upgrade	Cybersecurity Settings	Diagnostic	Data Logging - Download	Data Logging - Delete	Module Log - Query	Module Log - Upload	Module Log - Delete
1	**OPERATOR**	✓	✓	X	X	✓	✓	X	✓	X	X
2	**ENGINEER**	✓	X	X	X	✓	✓	✓	✓	✓	X
3	**INSTALLER**	✓	X	✓	X	✓	✓	X	✓	✓	X
4	**SECADM**	X	X	X	✓	✓	✓	X	✓	✓	✓
32768	**SINGLEUSER (COMMON)**	✓	✓	X	X	X	X	X	X	X	X
	NOTE: The **SINGLEUSER** functionality is dedicated to DNP3 security authentication functions, not web access.										

✓: Available

X: Unavailable

Appendices

Interoperability

About this Chapter

This chapter describes the specific implementation of protocols with the BMXNOR0200H module.

It includes these topics:

- DNP3 server device profile, page 232
- DNP3 client device profile, page 236
- DNP3 device profile implementation table, page 240
- IEC60870-5-104 server device profile, page 248
- IEC60870-5-104 client device profile, page 257
- IEC60870-5-101 client and server device profiles, page 266

DNP3 Interoperability

Introduction

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

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 client via the DNP3 protocol.

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

This section contains this information:

- DNP3 server device profile, page 232
- DNP3 client device profile, page 236
- DNP3 device profile implementation table, page 240

DNP3 Server Device Profile

Profile Parameters

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 client as an example. (Your module may be different.)

Parameter	Capabilities	Value
Device Identification		
Device Function	Server	Server
Vendor Name	—	Schneider Electric Industries SAS
Device Name	—	BMENOR2200H
Device Manufacturer Hardware Version	—	1.0
Device Manufacturer Software Version	—	1.0
Device Profile Document Version Number	—	1
DNP3 Levels Supported	For both requests and responses: None, Level 1, Level 2, Level 3	Level 3
Supported Function Blocks	Self Address Support Secure Authentication	Secure Authentication
Notable Additions	—	—
Methods to set Configurable Parameters	Software Protocol, set via DNP3	Software (EcoStruxure Control Expert)
DNP3 XML files available On-line	N/A	N/A
External DNP3 XML files available Off-line	dnpDP.xml (read)	dnpDP.xml (read)
Connections Supported	Serial IP Networking	IP Networking
Conformance Testing	Independently tested	—
Serial Connections		
Port Name	—	Serial Port
Serial Connection Parameters	Asynchronous - 8 Data Bits, 1 Start Bit, 1 Stop Bit, No Parity Other	Asynchronous
Baud Rate	Configurable, selectable from 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	19200
Hardware Flow Control (Handshaking)	**RS-232/V.24/V.28 Options:** Asserts: • RTS Before Rx • DTR Before Rx Requires Before Tx: • CTS (Asserted) • DCD (Asserted)	**RS-232/V.24/V.28 Options:** • Asserts RTS before Rx • Asserts DTR before Rx • Before Tx, Requires CTS asserted • Before Tx, Requires DCD asserted
	RS-485 Options: Requires Rx inactive before Tx	**RS-485 Options:** Requires Rx inactive before Tx
Interval to Request Link Status	Configurable range 0...4294967295 ms	2500 ms
Supports DNP3 Collision Avoidance	No	No
Receiver Inter-character Timeout	Not checked	Not checked
Inter-character gaps in transmission	None	None
IP Networking		
Port Name	—	Ethernet
Type of End Point	TCP Listening TCP Datagram	TCP Listening
IP Address of this device	—	0.0.0.0

Parameter	Capabilities	Value
Subnet Mask	—	255.255.255.0
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...65535	20000
Destination UDP Port for DNP3 Requests	Configurable range 1...65535	20000
Destination UDP Port for initial unsolicited null responses	Fixed at 20000	20000
Destination UDP Port for DNP3 Responses	Configurable range 1...65536	20000
Multiple server connections	N/A	N/A
Multiple client connections	Supports multiple clients	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
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_CLIENT	
	18 DOWNSTREAM_FAIL	
	126 RESERVED	
	127 UNDEFINED	
Server Only Properties		
Timeout waiting for Application Confirm of solicited response message	Configurable range 0...2147483647 ms	10000 ms
How often is time synchronization required from the client	Never needs time	Periodically, every 1800 sec
	between 0 and 4294967295 seconds	
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
Last Fragment Confirmation	Sometimes	Sometimes
DNP Command Settings preserved through a device restart	—	—
Supports configuration signature	Not supported	Not supported
Requests application confirmation	For event responses: Yes	Yes
	For non-final fragments: Configurable	Yes
Supports DNP3 Clock Management	Yes	Yes
	No	
Server Unsolicited Response Support Properties		
Supports unsolicited reporting	Configurable (On/Off)	On
Client Data Link Address	Configurable range 0...65519	3
Unsolicited Response Confirmation Timeout	Configurable range 0...2147483647	5000 ms
Number of Unsolicited Retries	Configurable range 0...65535	3
Server Unsolicited Response Trigger Conditions		
Number of class 1 events	Configurable range 0...255	5
Number of class 2 events	Configurable range 0...255	5
Number of class 3 events	Configurable range 0...255	5
Total number of events from any class	Total Number of Events not used to trigger Unsolicited Responses	—
Hold time after class 1 event	Configurable range 0 to 4294967295 ms	5000 ms

Parameter	Capabilities	Value
Hold time after class 2 event	Configurable range 0 to 4294967295 ms	5000 ms
Hold time after class 3 event	Configurable range 0 to 4294967295 ms	5000 ms
Hold time after event assigned to any class	Fixed at 0 ms	0 ms
Retrigger Hold Time	Hold-time timer is not retriggered for each new detected event (enabled update time)	Not retriggered
Other Unsolicited Response Trigger Conditions	—	N/A
Server Performance Properties		
Maximum Time Base Drift	—	—
When does server set IIN1.4	Never	Never
	Asserted at startup until first Time Synchronization request received	
	Range 1 to 4294967 seconds after the last time synchronization	
Maximum Internal Time Reference Error when set via DNP	Other	Other
Maximum Delay Measurement Error	Other	Other
Maximum Response Time	Other	Other
Maximum time from start-up to IIN 1.4 assertion	Other	Other
Maximum Event Time-tag error for local Binary and Double Bit I/O	Other	Other
Maximum Event Time-tag error for local I/O other than Binary and Double Bit data types	Other	Other
Individual Field Server 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 server (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)	v 2 5
	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
Aggressive mode of operation (issuing)	—	No
Session key change interval	Configurable range 60...604800 sec (when enabled	Enabled at 900 sec
Session key change message count	Configurable range 0...65535	1000
Maximum error count (SAv2 only)	Configurable range 0...255	2
MAC algorithm requested in a challenge exchange	SHA-1 (truncated to the leftmost 4 bytes)	SHA-256 (16)
	SHA-1 (truncated to the leftmost 8 bytes)	
	SHA-1 (truncated to the leftmost 10 bytes)	
	SHA-256 (truncated to the leftmost 8 bytes)	
	SHA-256 (truncated to the leftmost 16 bytes)	
Key-wrap algorithm to encrypt session keys	AES-128	AES-128
	AES-256	
Cipher Suites used with DNP implementations using TLS	TLS_RSA encrypted with AES-128	TLS_RSA encrypted with AES-128
Change cipher request timeout	Fixed at 30 sec	30 sec
Number of Certificate Authorities supported	—	No limit
Certificate Revocation check time	Not relevant - CRL is not used	Not relevant

Parameter	Capabilities	Value
Additional critical function codes	None	None
Other critical fragments	None	N/A
Support for remote update key changes	None	N/A
Default user credentials are permitted to expire	No	No
Secure Authentication enabled	Configurable: On or Off	Off
Length of the challenge data	Configurable range 4...60 bytes	4 bytes
Maximum statistic counts (SAv5):		
Max Detected 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 Client Device Profile

Profile Parameters

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 client as an example. (Your module may be different.)

Parameter	Capabilities	Value
Device Identification		
Device Function	Client	Client
Vendor Name	—	Schneider Electric Industries SAS
Device Name	Device Name	BMENOR2200H
Device Manufacturer Hardware Version	—	1.0
Device Manufacturer Software Version	—	1.0
Device Profile Document Version Number	—	1
DNP3 Levels Supported	For both requests and responses: None, Level 1, Level 2, Level 3	For requests: Level 3
		For responses: Level 3
Supported Function Blocks	Self Address Support	Secure Authentication
	Secure Authentication	
Notable Additions	Refer to the DNP3 implementation table, page 240	
Methods to set Configurable Parameters	Software	Software (EcoStruxure Control Expert)
	Proprietary file loaded via other transport mechanism	
DNP3 XML files available On-line	N/A	Software (EcoStruxure Control Expert)
External DNP3 XML files available Off-line	dnpDP.xml (read)	dnpDP.xml (read)
Connections Supported	Serial	IP Networking
	IP Networking	
Conformance Testing	Independently tested	—
Serial Connections		
Port Name	—	Serial Port
Serial Connection Parameters	Asynchronous - 8 Data Bits, 1 Start Bit, 1 Stop Bit, No Parity	Asynchronous
	Other, explain *configurable*	

Parameter	Capabilities	Value
Baud Rate	Configurable, selectable from 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	19200
Hardware Flow Control (Handshaking)	**RS-232/V.24/V.28 Options:** Asserts: • RTS Before Rx • DTR Before Rx Requires Before Tx: • CTS (Asserted) • DCD (Asserted)	**RS-232/V.24/V.28 Options:** • Asserts RTS before Rx • Asserts DTR before Rx • Before Tx, Requires CTS asserted • Before Tx, Requires DCD asserted
	RS-485 Options: Requires Rx inactive before Tx	**RS-485 Options:** Requires Rx inactive before Tx
Interval to Request Link Status	Configurable, range 0...4294967295 ms	2500 ms
Supports DNP3 Collision Avoidance	No	No
Receiver Inter-character Timeout	Not checked	Not checked
Inter-character gaps in transmission	None	None
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	—	255.255.255.0
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...65535	20000
TCP Keep-alive timer	Fixed at 75000 ms	75000 ms
Local UDP Port	Configurable range 1...65535	20000
	Let system choose (client only)	
Destination UDP Port for DNP3 Requests	Configurable range 1...65535	20000
Destination UDP Port for initial unsolicited null responses	None	None
Destination UDP Port for DNP3 Responses	Configurable range 1...65536	20000
Multiple server connections	Supports multiple servers	TRUE
Multiple client connections	Not supported	Not supported
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, one address allowed	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

Parameter	Capabilities	Value
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
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	
Client-Only Properties		
Timeout waiting for Complete Application Layer Responses (ms)	Configurable range 0...4294967295 ms	30000 ms
Maximum Application Layer Retries for Request Messages	None	None
Timeout waiting for First or Next Fragment of an Application Layer Response	Configurable range 0...4294967295 ms	10000 ms
Issuing controls to Off-line devices	No	No
Issuing controls to off-scan devices	No	No
Maximum Application Layer Retries for Control Select Messages (same sequence number)	None	None
Maximum Application Layer Retries for Control Select Messages (new sequence number)	None	None
Security Parameters		
DNP3 device support for secure authentication	Configurable, selectable from 2, 5	v 2 5
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
Aggressive mode of operation (issuing)	—	No
Session key change interval	Configurable range 60...604800 sec (when enabled)	Enabled at 900 sec
Session key change message count	Configurable range 0...65535	1000
Maximum error count (SAv2 only)	Configurable range 0...255	2
MAC algorithm requested in a challenge exchange	SHA-1 (truncated to the leftmost 4 bytes)	SHA-256 (16)
	SHA-1 (truncated to the leftmost 8 bytes)	
	SHA-1 (truncated to the leftmost 10 bytes)	
	SHA-256 (truncated to the leftmost 8 bytes)	
	SHA-256 (truncated to the leftmost 16 bytes)	
Key-wrap algorithm to encrypt session keys	AES-128	AES-128
	AES-256	

Parameter	Capabilities	Value
Cipher Suites used with DNP implementations using TLS	TLS_RSA encrypted with AES-128	TLS_RSA encrypted with AES-128
Change cipher request timeout	Fixed at 30 sec	30 sec
Number of Certificate Authorities supported	—	No limit
Certificate Revocation check time	Not relevant - CRL 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	No	No
Secure Authentication enabled	Configurable: On or Off	Off
Length of the challenge data	Configurable range 4...60 bytes	4 bytes
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 Implementation

Implementation Table

This 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 client or all requests that are parsed by a server. The *Response* columns identify all responses that are parsed by a client or all responses that may be sent by a server:

DNP OBJECT GROUP & VARIATION			**REQUEST** **Client may issue** **Server parses**		**RESPONSE** **Client parses** **Server 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)		
1	0	Binary Input - any variation		00, 01 (start-stop), 06 (no range, or all)		
1	1	Binary Input - Single-bit packed	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
1	2	Binary Input - Single-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop),
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)
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)		
3	0	Double-bit Input - any variation		00, 01 (start-stop), 06 (no range, or all)		
3	1	Double-bit Input - Double-bit packed	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop),
3	2	Double-bit Input - with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop),
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)
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)

DNP OBJECT GROUP & VARIATION			REQUEST Client may issue Server parses		RESPONSE Client parses Server 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			(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)		
10	0	Binary Output - any variation		00, 01 (start-stop), 06 (no range, or all)		
10	1	Binary Output - packed format	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
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)	(Response)	00, 01 (start-stop)
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)
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		00, 01 (start-stop), 06 (no range, or all)		
12	1	Binary Output Command (CROB) - control relay output block	3(select)	17, 28 (index)	(Response)	echo of request
12	1	Binary Output Command (CROB) - control relay output block	4(operate)	17, 28 (index)	(Response)	echo of request
12	1	Binary Output Command (CROB) - control relay output block	5(direct op.)	17, 28 (index)	(Response)	echo of request
12	1	Binary Output Command (CROB) - control relay output block	6(direct op, no ack)	17, 28 (index)		echo of request
20	0	Counter - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all)		
20	0	Counter - any variation		00, 01 (start-stop), 06 (no range, or all)		
20	0	Counter - any variation	7(freeze)	00, 01 (start-stop), 06 (no range, or all)		
20	0	Counter - any variation	8(freeze, no ack)	00, 01 (start-stop), 06 (no range, or all)		

DNP OBJECT GROUP & VARIATION			REQUEST Client may issue Server parses		RESPONSE Client parses Server 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	9(freeze & clear)	00, 01 (start-stop), 06 (no range, or all)		
20	0	Counter - any variation	10(frz & clr, no ack)	00, 01 (start-stop), 06 (no range, or all)		
20	1	Counter - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
20	2	Counter - 16-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
20	5	Counter - 32-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
20	6	Counter - 16-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
21	0	Frozen Counter - any variation	1(read)	00, 01 (start-stop), 06 (no range, or all)		
21	0	Frozen Counter - any variation		00, 01 (start-stop), 06 (no range, or all)		
21	1	Frozen Counter - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
21	2	Frozen Counter - 16-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
21	5	Frozen Counter - 32-bit with flag and time	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
21	6	Frozen Counter - 16-bit with flag and time	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
21	9	Frozen Counter - 32-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
21	10	Frozen Counter - 16-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
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)
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)

DNP OBJECT GROUP & VARIATION			REQUEST Client may issue Server parses		RESPONSE Client parses Server may issue	
Object Group Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifier Codes (hex)**	**Function Codes (dec)**	**Qualifier Codes (hex)**
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)
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		00, 01 (start-stop), 06 (no range, or all)		
30	3	Analog Input - 32-bit without flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
30	1	Analog Input - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(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)	(Response)	00, 01 (start-stop), 17, 28 (index)
30	3	Analog Input - 32-bit with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(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)	(Response)	00, 01 (start-stop), 17, 28 (index)
30	5	Analog Input - single-precision, floating-point with flag	1(read)	00, 01 (start-stop), 06 (no range, or all)	(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)

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

DNP OBJECT GROUP & VARIATION			REQUEST Client may issue Server parses		RESPONSE Client parses Server 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)		
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)

DNP OBJECT GROUP & VARIATION			REQUEST Client may issue Server parses		RESPONSE Client parses Server may issue	
Object Group Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifier Codes (hex)**	**Function Codes (dec)**	**Qualifier Codes (hex)**
42	5	Analog Output Change Event - single-precision, floating-point without time			(Unsol. Resp.)	17, 28 (index)
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)		
60	1	Class Objects - class 0 data		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		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		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		06 (no range, or all)		

DNP OBJECT GROUP & VARIATION			REQUEST Client may issue Server parses		RESPONSE Client parses Server may issue	
Object Group Number	**Variation Number**	**Description**	**Function Codes (dec)**	**Qualifier Codes (hex)**	**Function Codes (dec)**	**Qualifier Codes (hex)**
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)			
110	string length	Octet String	1(read)	00, 01 (start-stop), 06 (no range, or all)	(Response)	00, 01 (start-stop)
110	string length	Octet String	2(write)	00, 01 (start-stop), 17, 28 (index)		
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
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)
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)

IEC60870-5-104 Interoperability

IEC60870-5-104 Server Profiles

Introduction

This companion standard presents sets of parameters and alternatives from which subsets have to be selected to implement particular telecontrol systems. Certain parameter values, such as the choice of *structured* or *unstructured* fields of the information object address of ASDUs, represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in the command and monitor directions, allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment from different manufacturers, it is necessary that all partners agree on the selected parameters.

This interoperability list is defined as in IEC60870-5-101 and extended with parameters used in this standard. The text descriptions of parameters that are not applicable to this companion standard are strike-through (the corresponding checkbox is marked black).

The selected parameters should be marked in the white boxes:

☐	The function or ASDU is not used.
X	The function or ASDU is used as standardized (default).
R	The function or ASDU is used in reverse mode.
B	The function or ASDU is used in standard and reverse mode.

The possible selection (*empty*, **X**, **R**, or **B**) is specified for each specific clause or parameter.

NOTE: A black checkbox indicates that the option cannot be selected in this companion standard.

System or Device

System-specific parameters indicate the definition of a system or a device by marking these boxes with an *X*:

☐	system definition
☐	controlling station definition (client)
X	controlling station definition (server)

Application Layer

For all application layer functions, mark each parameter accordingly:

- *X:* The parameter is used in only the standard direction.
- *R:* The parameter is used in only the reverse direction.
- *B:* The parameter is used in both directions.
- (*empty*): The function is not available in this companion standard.

Transmission mode for application data

Mode 1 (least significant byte first), as defined in 4.10 of IEC60870-5-4, is used exclusively in this companion standard.

Common address of ASDU

For system-specific parameters, all implemented configurations are marked with an *X*:

[X] two bytes

Information object address

For system-specific parameters, all implemented configurations are marked with an *X*:

[ ] structured

[X] three bytes [ ] structured

Cause of transmission

For system-specific parameters, all implemented configurations are marked with an *X*:

[X] two bytes (with originator address

NOTE: The originator address is set to *0* if not used.

Length of APDU: For system-specific parameters, specify the maximum length of the APDU per system.

NOTE: The maximum length of APDU for both directions is 253. It is a fixed system parameter.

Process Information in Monitor Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

X	<1>	:=	single-point information	M_SP_NA_1
X	<3>	:=	double-point information	M_DP_NA_1
X	<5>	:=	step position information	M_ST_NA_1
X	<7>	:=	bitstring of 32 bits	M_BO_NA_1
X	<9>	:=	measured value, normalized value	M_ME_NA_1
X	<11>	:=	measured value, scaled value	M_ME_NB_1
X	<13>	:=	measured value, short floating point value	M_ME_NC_1
X	<14>	:=	measured value, short floating point value with time tag	M_ME_TC_1
X	<15>	:=	integrated totals	M_IT_NA_1
	<20>	:=	packed single-point information with status change detection	M_PS_NA_1
	<21>	:=	measured value, normalized value without quality descriptor	M_ME_ND_1
X	<30>	:=	single-point information with time tag CP56Time2a	M_SP_TB_1
X	<31>	:=	double-point information with time tag CP56Time2a	M_DP_TB_1
X	<32>	:=	step position information with time tag CP56Time2a	M_ST_TB_1

X	<33>	:=	bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
X	<34>	:=	measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
X	<35>	:=	measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
X	<36>	:=	measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
X	<37>	:=	integrated totals with time tag CP56Time2a	M_IT_TB_1
	<38>	:=	event of protection equipment with time tag CP56Time2a	M_EP_TD_1
	<39>	:=	packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
	<40>	:=	packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

NOTE: This companion standard uses only the set <30> to <40> for ASDUs with permitted time tags.

Process Information in Control Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

X	<45>	:=	single command	C_SC_NA_1
X	<46>	:=	double command	C_DC_NA_1
X	<47>	:=	regulating step command	C_RC_NA_1
X	<48>	:=	set point command, normalized value	C_SE_NA_1
X	<49>	:=	set point command, scaled value	C_SE_NB_1
X	<50>	:=	set point command, short floating point value	C_SE_NC_1
X	<51>	:=	bitstring of 32 bits	C_BO_NA_1
X	<58>	:=	single command with time tag CP56Time2a	C_SC_TA_1
X	<59>	:=	double command with time tag CP56Time2a	C_DC_TA_1
X	<60>	:=	regulating step command with time tag CP56Time2a	C_RC_TA_1
X	<61>	:=	set point command, normalized value, with time tag CP56Time2a	C_SE_TA_1
X	<62>	:=	set point command, scaled value, with time tag CP56Time2a	C_SE_TB_1
X	<63>	:=	set point command, short floating point value, with time tag CP56Time2a	C_SE_TC_1
X	<64>	:=	bitstring of 32 bits with time tag CP56Time2a	C_BO_TA_1

NOTE: This companion standard uses either of these ASDU sets:

- <45> ... <50>
- <58> ... <64>

System Information in Monitor Direction

Mark each station-specific parameter appropriately (*X*, *R*, *B*): M_EI_NA_1

X	<70>	:=	end of initialization	

System Information in Control Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*): C_IC_NA_1

X	<100>	:=	interrogation command	
X	<101>	:=	counter interrogation command	C_CI_NA_1
X	<102>	:=	read command	C_RD_NA_1
X	<103>	:=	clock synchronization command	C_CS_NA_1
X	<105>	:=	reset process command	C_RP_NA_1
X	<107>	:=	test command with time tag with time tag CP56Time2a	C_TS_TA_1

Parameter in Control Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

X	<110>	:=	This is the parameter of the measured value, normalized value.	P_ME_NA_1
X	<111>	:=	This is the parameter of the measured value, scaled value.	P_ME_NB_1
X	<112>	:=	This is the parameter of the measured value, short floating point value.	P_ME_NC_1
X	<113>	:=	This is the parameter activation.	P_AC_NA_1

File Transfer

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

	<120>	:=	file ready	
	<121>	:=	section ready	F_SR_NA_1
	<122>	:=	call directory, select file, call file, call section	F_SC_NA_1
	<123>	:=	last section, last segment	F_LS_NA_1
	<124>	:=	ack file, ack section	F_AF_NA_1
	<125>	:=	segment	F_SG_NA_1
	<126>	:=	directory {blank or X, only available in monitor (standard) direction}	F_DR_TA_1
	<127>	:=	query log — request archive log	F_SC_NB_1

Type Identifier and Cause of Transmission Assignments (station-specific parameters)

- *(shaded):* These boxes are not required.
- *(black):* This option is not permitted in this companion standard.
- *(blank):* The function or ASDU is not used.

Mark each type identification/cause of transmission combination appropriately (*X*, *R*, *B*):

Type Identification		Cause of Transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 ... 36	37 ... 41	44	45	46	47
<1>	M_SP_NA_1		X	X		X									X					
<3>	M_DP_NA_1		X	X		X									X					
<5>	M_ST_NA_1		X	X		X									X					
<7>	M_BO_NA_1		X	X		X									X					
<9>	M_ME_NA_1	X	X	X		X									X					
<11>	M_ME_NB_1	X	X	X		X									X					
<13>	M_ME_NC_1	X	X	X		X									X					
<15>	M_IT_NA_1			X												X				
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X		X														
<31>	M_DP_TB_1			X		X														
<32>	M_ST_TB_1			X		X														
<33>	M_BO_TB_1			X		X														
<34>	M_ME_TD_1			X		X														
<35>	M_ME_TE_1			X		X														
<36>	M_ME_TF_1			X		X														
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<51>	C_BO_NA_1						X	X			X						X	X	X	X
<58>	C_SC_TA_1						X	X	X	X	X						X	X	X	X
<59>	C_DC_TA_1						X	X	X	X	X						X	X	X	X
<60>	C_RC_TA_1						X	X	X	X	X						X	X	X	X
<61>	C_SE_TA_1						X	X	X	X	X						X	X	X	X
<62>	C_SE_TB_1						X	X	X	X	X						X	X	X	X
<63>	C_SE_TC_1						X	X	X	X	X						X	X	X	X
<64>	C_BO_TA_1						X	X			X						X	X	X	X
<70>	M_EI_NA_1 See note (below).				X															
<100>	C_IC_NA_1						X	X	X	X	X						X	X	X	X
<101>	C_CI_NA_1						X	X			X						X	X	X	X
<102>	C_RD_NA_1					X											X	X	X	X
<103>	C_CS_NA_1						X	X									X	X	X	X
<105>	C_RP_NA_1						X	X									X	X	X	X
<107>	C_TS_TA_1						X	X									X	X	X	X

Type Identification		Cause of Transmission																		
<110>	P_ME_NA_1						X	X							X		X	X	X	X
<111>	P_ME_NB_1						X	X							X		X	X	X	X
<112>	P_ME_NC_1						X	X							X		X	X	X	X
<113>	P_AC_NA_1						X	X	X	X							X	X	X	X
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1 See note (below).																			
<127>	F_SC_NB_1 See note (below).																			

NOTE: *Blank* or *X* only.

Basic Application Functions

Mark each basic application function accordingly:

- *X:* The parameter is used in only the standard direction.
- *R:* The parameter is used in only the reverse direction.
- *B:* The parameter is used in both directions.
- (*empty*): The function is not available in this companion standard.

Station Initialization

For station-specific parameters, all implemented functions are marked with an *X*:

X remote initialization

Cyclic Data Transmission

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

X cyclic data transmission

Read Procedure

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

X read procedure

Spontaneous Transmission

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

X spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous

For station-specific parameters, mark each function *X* when a type ID without time and a corresponding type ID with time are both issued in response to a single spontaneous change of a monitored object:

- [ ] single-point information (M_SP_NA_1, M_SP_TA_1, M_SP_TB_1, M_PS_NA_1)
- [ ] double-point information (M_DP_NA_1, M_DP_TA_1, M_DP_TB_1)
- [ ] step position information (M_ST_NA_1, M_ST_TA_1, M_ST_TB_1)
- [ ] bitstring of 32 bits (M_BO_NA_1, M_BO_TA_1, M_BO_TB_1) if defined for a specific project.
- [ ] measured value, nomalized value (M_ME_NA_1, M_ME_TA_1, M_ME_ND_1, M_ME_TD_1)
- [ ] measured value, scaled value (M_ME_NB_1, M_ME_TB_1, M_ME_TE_1)
- [ ] measured value, short floating point number (M_ME_NC_1, M_ME_TC_1, M_ME_TF_1)

Station Interrogation

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] global

[X] group 1	[X] group 7	[X] group 13
[X] group 2	[X] group 8	[X] group 14
[X] group 3	[X] group 9	[X] group 15
[X] group 4	[X] group 10	[X] group 16
[X] group 5	[X] group 11	
[X] group 6	[X] group 12	

NOTE: Show information object addresses that are assigned to each group in a separate table.

Clock Synchronization

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] clock synchronization
- [X] day of week used
- [X] RES1, GEN (time tag substituted/not substituted) used
- [X] SU-bit (summertime) used

Transmission of Integrated Totals

For station- or object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] Mode A: local freeze with spontaneous transmission
- [X] Mode B: local freeze with counter interrogation
- [X] Mode C: freeze and transmit by counter interrogation commands
- [ ] Mode D: freeze by counter-interrogation command, frozen values reported spontaneously
- [X] counter read
- [X] counter freeze without reset
- [X] counter freeze with reset
- [X] counter reset
- [X] general request counter
- [X] request counter group 1
- [X] request counter group 2
- [X] request counter group 3
- [X] request counter group 4

Parameter Loading

For object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] threshold value
- [ ] smoothing factor
- [X] low limit for transmission of measured value
- [X] high limit for transmission of measured value

Parameter Activation

For object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] activate/deactivate the persistent cyclic or periodic transmission of the addressed object

Test Procedure

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] test procedure

File Transfer

For station-specific parameters, mark *X* when the function is used.
File transfer in monitor direction:

- [ ] transparent file
- [ ] transmission of disturbance data of protection equipment
- [ ] transmission of sequences of events
- [ ] transmission of sequences of recorded analog values

File transfer in control direction:

- [ ] transparent file

Background Scan

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] background scan

Definition of Timeouts

Parameter	Default Value	Remarks	Selected Value
t_0	30 sec	timeout of connection establishment	configurable
t_1	15 sec	timeout of send or test APDUs	configurable
t_2	10 sec	timeout for acknowledges in case of no data messages $t_2 < t_1$	configurable
t_3	20 sec	timeout for sending test frames in case of a long idle state	configurable

Ranges:

- maximum range for timeouts t_0 to t_2: 1...255 sec (accuracy: 1 sec)
- maximum range for timeout t_3: 1...48 hours (resolution: 1 sec)
- long timeouts for t_3 may be needed for special cases in which satellite links or dial-up connections are used (for instance, to establish a connection and collect values only once per day or week)

Maximum number of outstanding I-format APDUs *k* and latest acknowledge APDUs (*w*)

Parameter	Default Value	Remarks	Selected Value
k	12 APDUs	maximum difference receive sequence number to send state variable	configurable
w	8 APDUs	latest acknowledge after receiving *w* I format APDUs	configurable

Range of values:

- *k:* 1...12 APDUs (accuracy: 1 APDU)
- *w:* 1...32767 APDUs (accuracy: 1 APDU) (*w* should not exceed two-thirds of *k*).

NOTE: In most of the cases, the value of *w* does not exceed two-thirds of *k*.

Port Number

Parameter	Value	Remarks
Portnumber	2404	configurable

Redundant Connections

4 number *N* of redundancy group connections used

RFC 2200 Suite

RFC 2200 is an official internet standard that describes the state of standardization of protocols used in the internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

☐ Ethernet 802.3

☐ serial X.21 interface

☐ another selection from RFC 2200

IEC60870-5-104 Client Profiles

Introduction

This companion standard presents sets of parameters and alternatives from which subsets must be selected to implement particular telecontrol systems. Certain parameter values, such as the choice of *structured* or *unstructured* fields of the information object address of ASDUs represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturers, it is necessary that all partners agree on the selected parameters.

This interoperability list is defined as in IEC60870-5-101 and extended with parameters used in this standard. The text descriptions of parameters that are not applicable to this companion standard are strike-through (the corresponding checkbox is marked black).

The selected parameters should be marked in the white boxes:

☐	The function or ASDU is not used.
X	The function or ASDU is used as standardized (default).
R	The function or ASDU is used in reverse mode.
B	The function or ASDU is used in standard and reverse mode.

The possible selection (*empty*, **X**, **R**, or **B**) is specified for each specific clause or parameter.

NOTE: A black checkbox indicates that the option cannot be selected in this companion standard.

System or Device

System-specific parameters indicate the definition of a system or a device by marking these boxes with an *X*:

☐	system definition
X	controlling station definition (client)
☐	controlling station definition (server)

Application Layer

For all application layer functions, mark each parameter accordingly:

- *X:* The parameter is used in only the standard direction.
- *R:* The parameter is used in only the reverse direction.
- *B:* The parameter is used in both directions.
- (*empty*): The function is not available in this companion standard.

Transmission mode for application data

Mode 1 (least significant byte first), as defined in 4.10 of IEC60870-5-4, is used exclusively in this companion standard.

Common address of ASDU

For system-specific parameters, all implemented configurations are marked with an *X*:

[X] two bytes

Information object address

For system-specific parameters, all implemented configurations are marked with an *X*:

[ ] structured

[X] three bytes [ ] structured

Cause of transmission

For system-specific parameters, all implemented configurations are marked with an *X*:

[X] two bytes (with originator address

NOTE: The originator address is set to *0* if not used.

Length of APDU: For system-specific parameters, specify the maximum length of the APDU per system.

NOTE: The maximum length of APDU for both directions is 253. It is a fixed system parameter.

Process Information in Monitor Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

[X]	<1>	:=	single-point information	M_SP_NA_1
[X]	<3>	:=	double-point information	M_DP_NA_1
[X]	<5>	:=	step position information	M_ST_NA_1
[X]	<7>	:=	bitstring of 32 bits	M_BO_NA_1
[X]	<9>	:=	measured value, normalized value	M_ME_NA_1
[X]	<11>	:=	measured value, scaled value	M_ME_NB_1
[X]	<13>	:=	measured value, short floating point value	M_ME_NC_1
[X]	<15>	:=	integrated totals	M_IT_NA_1
[ ]	<20>	:=	packed single-point information with status change detection	M_PS_NA_1
[ ]	<21>	:=	measured value, normalized value without quality descriptor	M_ME_ND_1
[X]	<30>	:=	single-point information with time tag CP56Time2a	M_SP_TB_1
[X]	<31>	:=	double-point information with time tag CP56Time2a	M_DP_TB_1
[X]	<32>	:=	step position information with time tag CP56Time2a	M_ST_TB_1
[X]	<33>	:=	bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
[X]	<34>	:=	measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
[X]	<35>	:=	measured value, scaled value with time tag CP56Time2a	M_ME_TE_1

X	<36>	:=	measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
X	<37>	:=	integrated totals with time tag CP56Time2a	M_IT_TB_1
	<38>	:=	event of protection equipment with time tag CP56Time2a	M_EP_TD_1
	<39>	:=	packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
	<40>	:=	packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

NOTE: This companion standard uses only the set <30> to <40> for ASDUs with permitted time tags.

Process Information in Control Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

X	<45>	:=	single command	C_SC_NA_1
X	<46>	:=	double command	C_DC_NA_1
X	<47>	:=	regulating step command	C_RC_NA_1
X	<48>	:=	set point command, normalized value	C_SE_NA_1
X	<49>	:=	set point command, scaled value	C_SE_NB_1
X	<50>	:=	set point command, short floating point value	C_SE_NC_1
X	<51>	:=	bitstring of 32 bits	C_BO_NA_1
X	<58>	:=	single command with time tag CP56Time2a	C_SC_TA_1
X	<59>	:=	double command with time tag CP56Time2a	C_DC_TA_1
X	<60>	:=	regulating step command with time tag CP56Time2a	C_RC_TA_1
X	<61>	:=	set point command, normalized value, with time tag CP56Time2a	C_SE_TA_1
X	<62>	:=	set point command, scaled value, with time tag CP56Time2a	C_SE_TB_1
X	<63>	:=	set point command, short floating point value, with time tag CP56Time2a	C_SE_TC_1
X	<64>	:=	bitstring of 32 bits with time tag CP56Time2a	C_BO_TA_1

NOTE: This companion standard uses either of these ASDU sets:

- <45> ... <50>
- <58> ... <64>

System Information in Monitor Direction

Mark each station-specific parameter appropriately (*X*, *R*, *B*): M_EI_NA_1

X	<70>	:=	end of initialization

System Information in Control Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*): C_IC_NA_1

X	<100>	:=	interrogation command	
X	<101>	:=	counter interrogation command	C_CI_NA_1
X	<102>	:=	read command	C_RD_NA_1
X	<103>	:=	clock synchronization command	C_CS_NA_1
X	<105>	:=	reset process command	C_RP_NA_1
X	<107>	:=	test command with time tag with time tag CP56Time2a	C_TS_TA_1

Parameter in Control Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

X	<110>	:=	This is the parameter of the measured value, normalized value.	P_ME_NA_1
X	<111>	:=	This is the parameter of the measured value, scaled value.	P_ME_NB_1
X	<112>	:=	This is the parameter of the measured value, short floating point value.	P_ME_NC_1
X	<113>	:=	This is the parameter activation.	P_AC_NA_1

File Transfer

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

	<120>	:=	file ready	
	<121>	:=	section ready	F_SR_NA_1
	<122>	:=	call directory, select file, call file, call section	F_SC_NA_1
	<123>	:=	last section, last segment	F_LS_NA_1
	<124>	:=	ack file, ack section	F_AF_NA_1
	<125>	:=	segment	F_SG_NA_1
	<126>	:=	directory {blank or X, only available in monitor (standard) direction}	F_DR_TA_1
	<127>	:=	query log — request archive log	F_SC_NB_1

Type Identifier and Cause of Transmission Assignments (station-specific parameters)

- *(shaded):* These boxes are not required.
- *(black):* This option is not permitted in this companion standard.
- *(blank):* The function or ASDU is not used.

Mark each type identification/cause of transmission combination appropriately (*X*, *R*, *B*):

Type Identification		Cause of Transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 ... 36	37 ... 41	44	45	46	47
<1>	M_SP_NA_1		X	X		X						X	X		X					
<3>	M_DP_NA_1		X	X		X						X	X		X					
<5>	M_ST_NA_1		X	X		X						X	X		X					
<7>	M_BO_NA_1		X	X		X									X					
<9>	M_ME_NA_1	X	X	X		X									X					
<11>	M_ME_NB_1	X	X	X		X									X					
<13>	M_ME_NC_1	X	X	X		X									X					
<15>	M_IT_NA_1			X												X				
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X		X						X	X							
<31>	M_DP_TB_1			X		X						X	X							
<32>	M_ST_TB_1			X		X						X	X							
<33>	M_BO_TB_1			X		X														
<34>	M_ME_TD_1			X		X														
<35>	M_ME_TE_1			X		X														
<36>	M_ME_TF_1			X		X														
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<51>	C_BO_NA_1						X	X			X						X	X	X	X
<58>	C_SC_TA_1						X	X	X	X	X						X	X	X	X
<59>	C_DC_TA_1						X	X	X	X	X						X	X	X	X
<60>	C_RC_TA_1						X	X	X	X	X						X	X	X	X
<61>	C_SE_TA_1						X	X	X	X	X						X	X	X	X
<62>	C_SE_TB_1						X	X	X	X	X						X	X	X	X
<63>	C_SE_TC_1						X	X	X	X	X						X	X	X	X
<64>	C_BO_TA_1						X	X			X						X	X	X	X
<70>	M_EI_NA_1 See note (below).				X															
<100->	C_IC_NA_1						X	X	X	X	X						X	X	X	X
<101->	C_CI_NA_1						X	X			X						X	X	X	X
<102->	C_RD_NA_1					X											X	X	X	X
<103->	C_CS_NA_1						X	X									X	X	X	X
<105->	C_RP_NA_1						X	X									X	X	X	X

Type Identification		Cause of Transmission																		
<107->	C_TS_TA_1						X	X									X	X	X	X
<110->	P_ME_NA_1						X	X							X		X	X	X	X
<111>	P_ME_NB_1						X	X							X		X	X	X	X
<112->	P_ME_NC_1						X	X							X		X	X	X	X
<113->	P_AC_NA_1						X	X	X	X							X	X	X	X
<120->	F_FR_NA_1																			
<121->	F_SR_NA_1																			
<122->	F_SC_NA_1																			
<123->	F_LS_NA_1																			
<124->	F_AF_NA_1																			
<125->	F_SG_NA_1																			
<126->	F_DR_TA_1 See note (below).																			
<127->	F_SC_NB_1 See note (below).																			

NOTE: *Blank* or *X* only.

Basic Application Functions

Mark each basic application function accordingly:

- *X:* The parameter is used in only the standard direction.
- *R:* The parameter is used in only the reverse direction.
- *B:* The parameter is used in both directions.
- (*empty*): The function is not available in this companion standard.

Station Initialization

For station-specific parameters, all implemented functions are marked with an *X*:

X remote initialization

Cyclic Data Transmission

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

X cyclic data transmission

Read Procedure

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

X read procedure

Spontaneous Transmission

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

X spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous

For station-specific parameters, mark each function *X* when a type ID without time and a corresponding type ID with time are both issued in response to a single spontaneous change of a monitored object:

- [X] single-point information (M_SP_NA_1, M_SP_TA_1, M_SP_TB_1, M_PS_NA_1)
- [X] double-point information (M_DP_NA_1, M_DP_TA_1, M_DP_TB_1)
- [X] step position information (M_ST_NA_1, M_ST_TA_1, M_ST_TB_1)
- [X] bitstring of 32 bits (M_BO_NA_1, M_BO_TA_1, M_BO_TB_1) if defined for a specific project.
- [X] measured value, nomalized value (M_ME_NA_1, M_ME_TA_1, M_ME_ND_1, M_ME_TD_1)
- [X] measured value, scaled value (M_ME_NB_1, M_ME_TB_1, M_ME_TE_1)
- [X] measured value, short floating point number (M_ME_NC_1, M_ME_TC_1, M_ME_TF_1)

Station Interrogation

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

[X] global

[X] group 1	[X] group 7	[X] group 13
[X] group 2	[X] group 8	[X] group 14
[X] group 3	[X] group 9	[X] group 15
[X] group 4	[X] group 10	[X] group 16
[X] group 5	[X] group 11	
[X] group 6	[X] group 12	

NOTE: Show information object addresses that are assigned to each group in a separate table.

Clock Synchronization

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] clock synchronization
- [X] day of week used
- [X] RES1, GEN (time tag substituted/not substituted) used
- [X] SU-bit (summertime) used

Command Transmission

- [X] direct command transmission
- [X] direct set point command transmission
- [X] select and execute command
- [X] select and execute set point command
- [X] C_SE ACTTERM used
- [X] no additional definition
- [X] short-pulse duration (determined by a system parameter in the server)
- [X] long-pulse duration (determined by a system parameter in the server)
- [X] persistent output
- [ ] supervision of maximum delay in command direction of commands and set point commands

Configurable maximum allowable delay of commands and set point commands

Transmission of Integrated Totals

For station- or object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] Mode A: local freeze with spontaneous transmission
- [X] Mode B: local freeze with counter interrogation
- [X] Mode C: freeze and transmit by counter interrogation commands
- [ ] Mode D: freeze by counter-interrogation command, frozen values reported spontaneously
- [X] counter read
- [X] counter freeze without reset
- [X] counter freeze with reset
- [X] counter reset
- [X] general request counter
- [X] request counter group 1
- [X] request counter group 2
- [X] request counter group 3
- [X] request counter group 4

Parameter Loading

For object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] threshold value
- [ ] smoothing factor
- [X] low limit for transmission of measured value
- [X] high limit for transmission of measured value

Parameter Activation

For object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] activate/deactivate the persistent cyclic or periodic transmission of the addressed object

Test Procedure

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] test procedure

File Transfer

For station-specific parameters, mark *X* when the function is used.
File transfer in monitor direction:

- [ ] transparent file
- [ ] transmission of disturbance data of protection equipment
- [ ] transmission of sequences of events
- [ ] transmission of sequences of recorded analog values

File transfer in control direction:

- [ ] transparent file

Background Scan

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] background scan

Definition of Timeouts

Parameter	Default Value	Remarks	Selected Value
t_0	30 sec	timeout of connection establishment	configurable
t_1	15 sec	timeout of send or test APDUs	configurable
t_2	10 sec	timeout for acknowledges in case of no data messages $t_2 < t_1$	configurable
t_3	20 sec	timeout for sending test frames in case of a long idle state	configurable

Ranges:

- maximum range for timeouts t_0 to t_2: 1...255 sec (accuracy: 1 sec)
- maximum range for timeout t_3: 1...48 hours (resolution: 1 sec)
- long timeouts for t_3 may be needed for special cases in which satellite links or dial-up connections are used (for instance, to establish a connection and collect values only once per day or week)

Maximum number of outstanding I-format APDUs *k* and latest acknowledge APDUs (*w*)

Parameter	Default Value	Remarks	Selected Value
k	12 APDUs	maximum difference receive sequence number to send state variable	configurable
w	8 APDUs	latest acknowledge after receiving *w* I format APDUs	configurable

Range of values:

- *k:* 1...12 APDUs (accuracy: 1 APDU)
- *w:* 1...32767 APDUs (accuracy: 1 APDU) (*w* should not exceed two-thirds of *k*).

NOTE: In most of the cases, the value of *w* does not exceed two-thirds of *k*.

Port Number

Parameter	Value	Remarks
Portnumber	2404	configurable

Redundant Connections

[4] number *N* of redundancy group connections used

RFC 2200 Suite

RFC 2200 is an official internet standard that describes the state of standardization of protocols used in the internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

[X] Ethernet 802.3

[ ] serial X.21 interface

[ ] another selection from RFC 2200

IEC60870-5-101 Server and Client Device Profiles

Introduction

This topic contains the information that is used to configure devices from other providers for interoperability. It is based on the standard IEC60870-5-101 interoperability template (*IEC60870-5-101:2003, Clause 8*).

This companion standard presents sets of parameters and alternatives from which subsets have to be selected to implement particular telecontrol systems. Certain parameter values, such as the number of bytes in the common address of ASDUs, represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in the command and monitor directions, allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment from different manufacturers, it is necessary that all partners agree on the selected parameters.

The selected parameters should be marked in the white boxes:

- ☐ The function or ASDU is not used.
- **X** The function or ASDU is used as standardized (default).
- **R** The function or ASDU is used in reverse mode.
- **B** The function or ASDU is used in standard and reverse mode.

The possible selection (*empty*, **X**, **R**, or **B**) is specified for each specific clause or parameter.

NOTE: In addition, the full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

System or Device

System-specific parameters indicate the definition of a system or a device by marking these boxes with an *X*:

- ☐ system definition
- **X** controlling station definition (client)
- **X** controlling station definition (server)

Network Configuration

For network-specific parameters, all implemented configurations are marked with an *X*:

- **X** point to point
- ☐ multi-point partyline
- **X** multiple point to point
- ☐ multi-point star

Physical Layer

For network-specific parameters, all implemented interfaces and data rates are marked with an *X*:

Transmission speed (control direction):

Unbalanced Interchange Circuit V.24/V.28 Standard	Unbalanced Interchange Circuit V.24/V.28 Recommended if >1200 bit/s	Balanced Interchange Circuit V.24/V.27	
☐ 100 bit/s	☒ 2400 bit/s	☒ 2400 bit/s	☒ 57600 bit/s
☐ 200 bit/s	☒ 4800 bit/s	☒ 4800 bit/s	☒ 115200 bit/s
☒ 300 bit/s	☒ 9600 bit/s	☒ 9600 bit/s	
☒ 600 bit/s		☒ 19200 bit/s	
☒ 1200 bit/s		☒ 38400 bit/s	

Transmission speed (monitor direction):

Unbalanced Interchange Circuit V.24/V.28 Standard	Unbalanced Interchange Circuit V.24/V.28 Recommended if >1200 bit/s	Balanced Interchange Circuit V.24/V.27	
☐ 100 bit/s	☒ 2400 bit/s	☒ 2400 bit/s	☒ 57600 bit/s
☐ 200 bit/s	☒ 4800 bit/s	☒ 4800 bit/s	☒ 115200 bit/s
☒ 300 bit/s	☒ 9600 bit/s	☒ 9600 bit/s	
☒ 600 bit/s		☒ 19200 bit/s	
☒ 1200 bit/s		☒ 38400 bit/s	

Link Layer

For network-specific parameters, all implemented options are marked with an *X*. Specify the maximum frame length. If a non-standard assignment of class 2 messages is implemented for unbalanced transmission, indicate the type ID and COT of all messages assigned to class 2.

Frame format FT 1.2, single character 1, and the fixed timeout interval are used exclusively in this companion standard.

Link Transmission Procedure

☒ balanced transmission

☒ unbalanced transmission

Frame Length

256 maximum length L (control direction)

256 maximum length L (monitor direction)

3 time during which repetitions are permitted (Trp) or number of repetitions

Address Field of the Link

☐ not present (balanced transmission only)

☒ one byte

☒ two bytes

☐ structured

☐ unstructured

When using an unbalanced link layer, these ASDU types are returned in class 2 messages (low priority) with the indicated causes of transmission (*X*).

[X] This is the standard assignment of ASDUs to class 2 messages:

Type Identification	Cause of Transmissions
9, 11, 13, 21	<1>

[X] This is the special assignment of ASDUs to class 2 messages:

Type Identification	Cause of Transmissions
1, 3, 5, 7, 9, 11, 13	<2>

NOTE: In response to a class 2 poll, a controlled station may respond with class 1 data when there is no class 2 data available.

Application Layer

Transmission mode for application data

Mode 1 (least significant byte first), as defined in 4.10 of IEC60870-5-4, is used exclusively in this companion standard.

Common address of ASDU

For system-specific parameters, all implemented configurations are marked with an *X*:

[X] one byte [X] two bytes

Information object address

For system-specific parameters, all implemented configurations are marked with an *X*:

[X] one byte [ ] structured

[X] two bytes [ ] unstructured

[X] three bytes

Cause of transmission

For system-specific parameters, all implemented configurations are marked with an *X*:

[X] one byte [X] two bytes (with originator address)

NOTE: The originator address is set to *0* if not used.

Selection of Standard ASDUs

Process Information in Monitor Direction

For station-specific parameters, mark each type ID accordingly:

- *X:* The parameter is used in only the standard direction.
- *R:* The parameter is used in only the reverse direction.
- *B:* The parameter is used in both directions.

[X]	<1>	:=	single-point information	M_SP_NA_1
[X]	<2>	:=	single-point information with time tag	M_SP_TA_1
[X]	<3>	:=	double-point information	M_DP_NA_1
[X]	<4>	:=	step position information	M_ST_NA_1
[X]	<5>	:=	bitstring of 32 bits	M_BO_NA_1

X	<6>	:=	step position information with time tag	M_ST_TA_1
X	<7>	:=	bitstring of 32 bits	M_BO_NA_1
X	<8>	:=	bitstring of 32 bits with time tag	M_BO_TA_1
X	<9>	:=	measured value, normalized value	M_ME_NA_1
X	<10>	:=	measured value, normalized value with time tag	M_ME_TA_1
X	<11>	:=	measured value, scaled value	M_ME_NB_1
X	<12>	:=	measured value, scaled value with time tag	M_ME_TB_1
X	<13>	:=	measured value, short floating point value	M_ME_NC_1
X	<14>	:=	measured value, short floating point value with time tag	M_ME_TC_1
X	<15>	:=	integrated totals	M_IT_NA_1
X	<16>	:=	integrated totals with time tag	M_IT_TA_1
	<17>	:=	event of protection equipment with time tag	M_EP_TA_1
	<18>	:=	packed start events of protection equipment with time tag	M_EP_TB_1
	<19>	:=	packed output circuit information of protection equipment with time tag	M_EP_TC_1
	<20>	:=	packed single-point information with status change detection	M_PS_NA_1
	<21>	:=	measured value, normalized value without quality descriptor	M_ME_ND_1
X	<30>	:=	single-point information with time tag CP56Time2a	M_SP_TB_1
X	<31>	:=	double-point information with time tag CP56Time2a	M_DP_TB_1
X	<32>	:=	step position information with time tag CP56Time2a	M_ST_TB_1
X	<33>	:=	bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
X	<34>	:=	measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
X	<35>	:=	measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
X	<36>	:=	measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
X	<37>	:=	integrated totals with time tag CP56Time2a	M_IT_TB_1
	<38>	:=	event of protection equipment with time tag CP56Time2a	M_EP_TD_1
	<39>	:=	packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
	<40>	:=	packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

The ASDUs for one of these sets is used:

- <2>, <4>, <6>, <8>, <10>, <12>, <14>, <16>, <18>, <19>
- <30>...<40>

Process Information in Control Direction

For station-specific parameters, mark each type ID accordingly:

- *X:* The parameter is used in only the standard direction.
- *R:* The parameter is used in only the reverse direction.
- *B:* The parameter is used in both directions.

X	<45>	:=	single command	C_SC_NA_1
X	<46>	:=	double command	C_DC_NA_1
X	<47>	:=	regulating step command	C_RC_NA_1
X	<48>	:=	set point command, normalized value	C_SE_NA_1
X	<49>	:=	set point command, scaled value	C_SE_NB_1
X	<50>	:=	set point command, short floating point value	C_SE_NC_1
X	<51>	:=	bitstring of 32 bits	C_BO_NA_1

System Information in Monitor Direction

Mark each station-specific parameter appropriately (*X*, *R*, *B*): M_EI_NA_1

X	<70>	:=	end of initialization

System Information in Control Direction C_IC_NA_1

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

X	<100>	:=	interrogation command	
X	<101>	:=	counter interrogation command	C_CI_NA_1
X	<102>	:=	read command	C_RD_NA_1
X	<103>	:=	clock synchronization command	C_CS_NA_1
X	<105>	:=	reset process command	C_RP_NA_1
X	<107>	:=	test command with time tag with time tag CP56Time2a	C_TS_TA_1

Parameter in Control Direction

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

X	<110>	:=	This is the parameter of the measured value, normalized value.	P_ME_NA_1
X	<111>	:=	This is the parameter of the measured value, scaled value.	P_ME_NB_1
X	<112>	:=	This is the parameter of the measured value, short floating point value.	P_ME_NC_1
X	<113>	:=	This is the parameter activation.	P_AC_NA_1

File Transfer

For station-specific parameters, mark each type ID appropriately (*X*, *R*, *B*):

☐	<120>	:=	file ready	
☐	<121>	:=	section ready	F_SR_NA_1
☐	<122>	:=	call directory, select file, call file, call section	F_SC_NA_1

☐	<123>	:=	last section, last segment	F_LS_NA_1
☐	<124>	:=	ack file, ack section	F_AF_NA_1
☐	<125>	:=	segment	F_SG_NA_1
☐	<126>	:=	directory {blank or X, only available in monitor (standard) direction}	F_DR_TA_1

Type Identifier and Cause of Transmission Assignments (station-specific parameters):

- *(shaded):* These boxes are not required.
- *(blank):* The function or ASDU is not used.

Mark each type identification/cause of transmission combination appropriately (*X*, *R*, *B*):

Type Identification		Cause of Transmission																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 ... 36	37 ... 41	44	45	46	47
<1>	M_SP_NA_1		X	X		X									X					
<2>	M_SP_TA_1			X		X														
<3>	M_DP_NA_1		X	X		X									X					
<4>	M_DP_TA_1			X		X														
<5>	M_ST_NA_1		X	X		X									X					
<6>	M_ST_TA_1			X		X														
<7>	M_BO_NA_1		X	X		X									X					
<8>	M_BO_TA_1			X		X														
<9>	M_ME_NA_1	X	X	X		X									X					
<10>	M_ME_TA_1			X		X														
<11>	M_ME_NB_1	X	X	X		X									X					
<12>	M_ME_TB_1			X		X														
<13>	M_ME_NC_1	X	X	X		X									X					
<14>	M_ME_TC_1			X		X														
<15>	M_IT_NA_1			X												X				
<16>	M_IT_TA_1			X																
<17>	M_EP_TA_1																			
<18>	M_EP_TB_1																			
<19>	M_EP_TC_1																			
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X		X														
<31>	M_DP_TB_1			X		X														
<32>	M_ST_TB_1			X		X														
<33>	M_BO_TB_1			X		X														
<34>	M_ME_TD_1			X		X														
<35>	M_ME_TE_1			X		X														
<36>	M_ME_TF_1			X		X														
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1																			
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<51>	C_BO_NA_1						X	X			X						X	X	X	X
<70>	M_EI_NA_1				X															
<100>	C_IC_NA_1						X	X	X	X	X						X	X	X	X
<101>	C_CI_NA_1						X	X			X						X	X	X	X
<102>	C_RD_NA_1					X											X	X	X	X
<103>	C_CS_NA_1						X	X									X	X	X	X

Type Identification		Cause of Transmission																		
<104>	C_TS_NA_1						X	X									X	X	X	X
<105>	C_RP_NA_1						X	X									X	X	X	X
<106>	C_CD_NA_1						X	X									X	X	X	X
<110>	P_ME_NA_1						X	X							X		X	X	X	X
<111>	P_ME_NB_1						X	X							X		X	X	X	X
<112>	P_ME_NC_1						X	X							X		X	X	X	X
<113>	P_AC_NA_1						X	X	X	X							X	X	X	X
<120>	F_FR_NA_1																			
<121>	F_SR_NA_1																			
<122>	F_SC_NA_1																			
<123>	F_LS_NA_1																			
<124>	F_AF_NA_1																			
<125>	F_SG_NA_1																			
<126>	F_DR_TA_1 See note (below).																			

NOTE: *Blank* or *X* only.

Basic Application Functions

Mark each basic application function accordingly:

- *X:* The parameter is used in only the standard direction.
- *R:* The parameter is used in only the reverse direction.
- *B:* The parameter is used in both directions.
- (*empty*): The function is not available in this companion standard.

Station Initialization

For station-specific parameters, all implemented functions are marked with an *X*:

☒ remote initialization

Cyclic Data Transmission

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

☒ cyclic data transmission

Read Procedure

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

☒ read procedure

Spontaneous Transmission

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

☒ spontaneous transmission

Double transmission of information objects with cause of transmission spontaneous

For station-specific parameters, mark each function *X* when a type ID without time and a corresponding type ID with time are both issued in response to a single spontaneous change of a monitored object:

☐ single-point information (M_SP_NA_1, M_SP_TA_1, M_SP_TB_1, M_PS_NA_1)

☐ double-point information (M_DP_NA_1, M_DP_TA_1, M_DP_TB_1)

- [ ] step position information (M_ST_NA_1, M_ST_TA_1, M_ST_TB_1)
- [ ] bitstring of 32 bits (M_BO_NA_1, M_BO_TA_1, M_BO_TB_1) if defined for a specific project.
- [ ] measured value, nomalized value (M_ME_NA_1, M_ME_TA_1, M_ME_ND_1, M_ME_TD_1)
- [ ] measured value, scaled value (M_ME_NB_1, M_ME_TB_1, M_ME_TE_1)
- [ ] measured value, short floating point number (M_ME_NC_1, M_ME_TC_1, M_ME_TF_1)

Station Interrogation

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] global

[X] group 1	[X] group 7	[X] group 13
[X] group 2	[X] group 8	[X] group 14
[X] group 3	[X] group 9	[X] group 15
[X] group 4	[X] group 10	[X] group 16
[X] group 5	[X] group 11	
[X] group 6	[X] group 12	

NOTE: Show information object addresses that are assigned to each group in a separate table.

Clock Synchronization

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] clock synchronization
- [X] day of week used
- [X] RES1, GEN (time tag substituted/not substituted) used
- [X] SU-bit (summertime) used

Command Transmission

- [X] direct command transmission
- [X] direct set point command transmission
- [X] select and execute command
- [X] select and execute set point command
- [X] C_SE ACTTERM used
- [X] no additional definition
- [X] short-pulse duration (determined by a system parameter in the server)
- [X] long-pulse duration (determined by a system parameter in the server)
- [X] persistent output

Transmission of Integrated Totals

For station- or object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] Mode A: local freeze with spontaneous transmission
- [X] Mode B: local freeze with counter interrogation
- [X] Mode C: freeze and transmit by counter interrogation commands
- [ ] Mode D: freeze by counter-interrogation command, frozen values reported spontaneously
- [X] counter read
- [X] counter freeze without reset
- [X] counter freeze with reset
- [X] counter reset

- [X] general request counter
- [X] request counter group 1
- [X] request counter group 2
- [X] request counter group 3
- [X] request counter group 4

Parameter Loading

For object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] threshold value
- [ ] smoothing factor
- [X] low limit for transmission of measured value
- [X] high limit for transmission of measured value

Parameter Activation

For object-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] activate/deactivate the persistent cyclic or periodic transmission of the addressed object

Test Procedure

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] test procedure

File Transfer

For station-specific parameters, mark *X* when the function is used.

File transfer in monitor direction:

- [ ] transparent file
- [ ] transmission of disturbance data of protection equipment
- [ ] transmission of sequences of events
- [ ] transmission of sequences of recorded analog values

File transfer in control direction:

- [ ] transparent file

Background Scan

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] background scan

Acquisition of Transmission Data

For station-specific parameters, mark each function appropriately (*X*, *R*, *B*):

- [X] acquisition of transmission delay

Project Migration

Introduction

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

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, page 163.

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, page 277.

DNP3 Data Type Migration

Introduction

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

These tables follow:

- DNP3 Server RTU Point Data Type Migration, page 277
- DNP3 Client RTU Point Data Type Migration, page 278

Apply this information when you configure DNP3 communications in the BMENOR2200H DTM, page 114.

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, page 133 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
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	—	.Command	WORD	.Command	BYTE

Object Type (Default Variable Name)	Object Element	BMXNOR0200H		BMENOR2200H	
		Parameter	Data Type	Parameter	Data Type
(GE_xxxx)	—	.Status	WORD	.Status	WORD
Clear_Event	—	.Command	WORD	.Command	BYTE
(CE_xxxx_CB)	—	.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]
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	.flags	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	.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
Analog_Input_Deadband	Value - 16 bit	.value	WORD	.Value	WORD

Object Type (Default Variable Name)	Object Element	BMXNOR0200H		BMENOR2200H	
		Parameter	Data Type	Parameter	Data Type
(AI_Px_Dband)	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
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

IEC60870 Data Type Migration

Introduction

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

These tables follow:

- IEC60870-5-104 Server RTU Point Data Type Migration
- IEC60870-5-104 Client RTU Point Data Type Migration

Apply this information when you configure IEC60870-5-104 communications in the BMENOR2200H module.

IEC60870 Client RTU Point Data Type Migration

The client RTU point data types that may change in the migration:

Object Type	CPU Register Type	Data Type	Parameter Name	Data Type in BMXNOR0200	Parameter Name in BMENOR2200H	Data Type in BMENOR2200H
M_SP	%M	Value	.value	WORD	.value	BYTE
	%MW	Flag	.quality	WORD	.flags	BYTE
	Unlocated	Time	.timestamp	CP56	.timestamp	CP56
M_DP	%MW	Value	.value	WORD	.value	BYTE
	Unlocated	Flag	.quality	WORD	.flags	BYTE
		Time	.timestamp	CP56	.timestamp	CP56
M_ST	%MW	Value	.value	WORD	.value	BYTE
	Unlocated	Flag	.quality	WORD	.flags	BYTE
		Time	.timestamp	CP56	.timestamp	CP56
M_BO	%MW	Value	.value	DWORD	.value	DWORD
	Unlocated	Flag	.quality	DWORD	.flags	BYTE
		Time	.timestamp	CP56	.timestamp	CP56
M_ME_A	%MW	Value	.value	INT	.Value	INT
	Unlocated	Flag	.quality	WORD	.flags	BYTE
		Time	.timestamp	CP56	.Timestamp	CP56
M_ME_B	%MW	Value	.value	INT	.Value	INT
	Unlocated	Flag	.quality	WORD	.flags	BYTE
		Time	.timestamp	CP56	.Timestamp	CP56
M_ME_C	%MW	Value	.value	REAL	.Value	REAL
	Unlocated	Flag	.quality	DWORD	.flags	BYTE
		Time	.timestamp	CP56	.Timestamp	CP56
M_IT	%MW	Value	.value	DINT	.Value	DINT
	Unlocated	Flag	.quality	DWORD	.flags	BYTE
		Time	.timestamp	CP56	.Timestamp	CP56
C_SC	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	BYTE
C_DC	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
C_RC	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
C_SE_A	%MW	Value	.value	INT	.value	INT
		Flag	.status	WORD	.status	WORD
C_SE_B	%MW	Value	.value	INT	.value	INT
		Flag	.status	WORD	.status	WORD
C_SE_C	%MW	Value	.value	REAL	.value	REAL
		Flag	.status	DWORD	.status	WORD
C_BO	%MW	Value	.value	DWORD	.value	DWORD
		Flag	.status	DWORD	.status	WORD
C_IC	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD

Object Type	CPU Register Type	Data Type	Parameter Name	Data Type in BMXNOR0200	Parameter Name in BMENOR2200H	Data Type in BMENOR2200H
C_CI	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
C_RD	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
C_CS	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
C_TS	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
C_RP	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
P_ME_A	%MW	Value	.value	WORD	.value	INT
		Flag	.status	WORD	.status	WORD
P_ME_B	%MW	Value	.value	WORD	.value	INT
		Flag	.status	WORD	.status	WORD
P_ME_C	%MW	Value	.value	REAL	.value	REAL
		Flag	.status	DWORD	.status	WORD
P_AC	%MW	Value	.value	WORD	.value	BYTE
		Flag	.status	WORD	.status	WORD
M_IT_D		Value	.value0	INT	.value0	INT
		Value	.value1	INT	.value1	INT
		Value	.value2	INT	.value2	INT
		Value	.value3	INT	.value3	INT
		Flag	.flag	BYTE	.flags	BYTE
		Time	.timestamp	CP56	.timestamp	CP56

NOTE: When the module receives a C_RD command, it responds to the information object with the requested information-object address (IOA). When multiple data points have the same IOA, the module returns the first information object according to this priority: M_SP, M_DP, M_ST, M_BO, M_ME_A, M_ME_B, M_ME_C, P_ME_A, P_ME_B, P_ME_C, CUSTOM_M_IT_D. Consider these points when you configure IEC60870-5-104 server communications.

IEC60870 Server RTU Point Data Type Migration

The server RTU point data types that may change in the migration:

Object Type	CPU Register Type	Data Type	Parameter Name	Data Type in BMXNOR0200	Parameter Name in BMENOR2200H	Data Type in BMENOR2200H
M_SP	%M	Value	.value	WORD	.value	BYTE
	%M	Flag	.quality	WORD	.flags	BYTE
	%S Unlocated	Time	.timestamp	CP56	.timestamp	CP56
M_DP	%MW Unlocated	Value	.value	WORD	.value	BYTE
		Flag	.quality	WORD	.flags	BYTE
		Time	.timestamp	CP56	.timestamp	CP56

Object Type	CPU Register Type	Data Type	Parameter Name	Data Type in BMXNOR0200	Parameter Name in BMENOR2200H	Data Type in BMENOR2200H
M_ST	%MW Unlocated	Value	.value	WORD	.value	BYTE
		Flag	.quality	WORD	.flags	BYTE
		Time	.timestamp	CP56	.timestamp	CP56
M_BO	%MW Unlocated	Value	.value	DWORD	.value	DWORD
		Flag	.quality	DWORD	.flags	BYTE
		Time	.timestamp	CP56	.timestamp	CP56
M_ME_A	%MW %SW Unlocated	Value	.value	INT	.Value	INT
		Flag	.quality	WORD	.Flags	BYTE
		Time	.timestamp	CP56	.Timestamp	CP56
M_ME_B	%MW Unlocated	Value	.value	INT	.Value	INT
		Flag	.quality	WORD	.Flags	BYTE
		Time	.timestamp	CP56	.Timestamp	CP56
M_ME_C	%MW Unlocated	Value	.value	REAL	.Value	REAL
		Flag	.quality	DWORD	.Flags	BYTE
		Time	.timestamp	CP56	.Timestamp	CP56
M_IT	%MW Unlocated	Value	.value	DINT	.Value	DINT
		Time	.timestamp	CP56	.Timestamp	CP56
C_SC	%MW %M Unlocated	—	.value	WORD	.value	BYTE
C_DC	%MW Unlocated	Value	.value	WORD	.value	BYTE
C_RC	%MW Unlocated	Value	.value	WORD	.value	BYTE
C_SE_A	%MW Unlocated	Value	.value	INT	.value	INT
C_SE_B	%MW Unlocated	Value	.value	INT	.value	INT
C_SE_C	%MW Unlocated	Value	.value	REAL	.value	REAL
C_BO	%MW Unlocated	Value	.value	DWORD	.value	DWORD
P_ME_A	%MW Unlocated	Value	—	WORD	.value	INT
P_ME_B	%MW Unlocated	Value	—	WORD	.value	INT
P_ME_C	%MW Unlocated	Value	—	REAL	.value	REAL
P_AC	%MW Unlocated	Value	—	WORD	.value	BYTE

Object Type	CPU Register Type	Data Type	Parameter Name	Data Type in BMXNOR0200	Parameter Name in BMENOR2200H	Data Type in BMENOR2200H
M_IT_D	%MW Unlocated	—	.value0	INT	.value0	INT
			.value1	INT	.value1	INT
			.value2	INT	.value2	INT
			.value3	INT	.value3	INT
			.flag	BYTE	.flags	BYTE
			.timestamp	CP56	.timestamp	CP56
Clear Events	%MW	—	.cmd	WORD	.cmd	BYTE
			.status	WORD	.status	WORD
CUSTOM_CMD	%MW Unlocated	FreezeCyclic (auto freeze)	Cmd	WORD	cmd	BYTE
			Status	WORD	.status	WORD
		freeze Trigger (local freeze)	Cmd	WORD	.cmd	BYTE
			Status	WORD	.status	WORD
CMD_QUALITY	%MW Unlocated	—	Cmd	WORD	.cmd	BYTE

Logged Events

Introduction

For more details about the logged events and secured statistics for the BMENOR2200H module, you can refer to the chapter *How to Help Secure the Architecture* in the *Modicon Controllers Platform Cyber Security Reference Manual*.

Modbus Diagnostic Codes

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 (Internal port)	39	103
Ethernet Port Diagnostic Data (Eth 1)	142	103
Ethernet Port Diagnostic Data (Eth 2)	245	103
Ethernet Port Diagnostic Data (Eth 3)	348	103
Ethernet Port Diagnostic Data (Eth 4 backplane port)	451	103
Modbus TCP/Port 502 Diagnostic Data	554	114
Modbus TCP/Port 502 Connection Table Data	668	515
SMTP Diagnostic Data	1183	130
SNTP Diagnostics	1313	43
DNP/IEC Connection Information	1356	6
DNP/IEC Server Diagnostic	1362	1141
DNP/IEC Client Diagnostic	2503	1281
DNP Server Security Diagnostic	3784	157
DNP Client Security Diagnostic	3961	2497
Clock Diagnostic	6458	13
SNMP Diagnostic	6471	1
Web Service Diagnostic	6472	1
LLDP Service Diagnostic	6473	1
Firmware Upgrade Service Diagnostic	6474	1
Syslog Service Diagnostic	6475	1
SD Diagnostic	6476	1
ipAddrStatus Diagnostic	6477	1
Reserved	6478	13
HSBY Diagnostic	6491	35
Datalogging Table General Diagnostic	6526	171
Datalogging Service Diagnostic	6697	230
SNMP Service Diagnostic	6927	23
Module Diagnostic	6950	15
Basic Networks Diagnostic Data (Front-face port)	6965	39
Serial Port Diagnostic Data	7004	20
802.1x Diagnostic Data	7024	40

Basic Networks Diagnostic Data (Offset 0)

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	
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	Ethernet 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 of open client connections
Offset + 22	MS Byte	LS Byte	Number of open server connections
Offset + 23	C00	C01	Number of messages sent regarding detected Modbus errors
Offset + 24	C02	C03	
Offset + 25	C00	C01	Number of sent Modbus messages
Offset + 26	C02	C03	
Offset + 27	C00	C01	Number of received Modbus messages
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 (Offset 39)

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	Ethernet control capability
Offset + 3	MS Byte	LS Byte	Link speed capability
Offset + 4	MS Byte	LS Byte	Ethernet control configuration
Offset + 5	MS Byte	LS Byte	Link speed configuration
Offset + 6	MS Byte	LS Byte	Ethernet 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 of bytes transmitted successfully
Offset + 14	C02	LSB - C03	
Offset + 15	MSB - C00	C01	Number of bytes received successfully
Offset + 16	C02	LSB - C03	
Offset + 17	MSB - C00	C01	Number of Ethernet collisions
Offset + 18	C02	LSB - C03	
Offset + 19	MSB - C00	C01	Carrier sense detected errors
Offset + 20	C02	LSB - C03	
Offset + 21	MSB - C00	C01	Number of excessive Ethernet collisions
Offset + 22	C02	LSB - C03	
Offset + 23	MSB - C00	C01	CRC detected errors
Offset + 24	C02	LSB - C03	
Offset + 25	MSB - C00	C01	FSC detected errors
Offset + 26	C02	LSB - C03	
Offset + 27	MSB - C00	C01	Alignment detected errors
Offset + 28	C02	LSB - C03	
Offset + 29	MSB - C00	C01	Number of detected internal MAC transmission errors
Offset + 30	C02	LSB - C03	
Offset + 31	MSB - C00	C01	Late collisions
Offset + 32	C02	LSB - C03	
Offset + 33	MSB - C00	C01	Number of detected internal MAC reception errors
Offset + 34	C02	LSB - C03	
Offset + 35	MSB - C00	C01	Multiple collisions
Offset + 36	C02	LSB - C03	
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	Detected SQE test error
Offset + 46	C02	LSB - C03	

Address	MS Byte	LS Byte	Comments
Offset + 47	MS Byte	LS Byte	Interface label length
Offset + 48	IL_char64	IL_char63	Interface label characters
Offset + ...	...	...	Interface label characters
Offset + 79	IL_char2	IL_char1	Interface label characters
Offset + 80	MS Byte	LS Byte	Interface counters diagnostic validity
Offset + 81	MSB - C00	C01	Number of received bytes
Offset + 82	C02	LSB - C03	
Offset + 83	MSB - C00	C01	Number of received unicast packets
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 of discarded inbound packets
Offset + 88	C02	LSB - C03	
Offset + 89	MSB - C00	C01	Number of inbound errors packets
Offset + 90	C02	LSB - C03	
Offset + 91	MSB - C00	C01	Number of unknown inbound packets
Offset + 92	C02	LSB - C03	
Offset + 93	MSB - C00	C01	Number of sent bytes
Offset + 94	C02	LSB - C03	
Offset + 95	MSB - C00	C01	Number of sent unicast packets
Offset + 96	C02	LSB - C03	
Offset + 97	MSB - C00	C01	Number of sent non-unicast packets
Offset + 98	C02	LSB - C03	
Offset + 99	MSB - C00	C01	Number of discarded outbound packets
Offset + 100	C02	LSB - C03	
Offset + 101	MSB - C00	C01	Number of outbound error packets
Offset + 102	C02	LSB - C03	

Modbus TCP/Port 502 Diagnostic Data (Offset 554)

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 of open connections
Offset + 4	MSB - C00	C01	Number of sent Modbus messages
Offset + 5	C02	LSB - C03	
Offset + 6	MSB - C00	C01	Number of received Modbus messages
Offset + 7	C02	LSB - C03	
Offset + 8	MS Byte	LS Byte	Number of open Modbus client connections
Offset + 9	MS Byte	LS Byte	Number of open Modbus server connections
Offset + 10	MS Byte	LS Byte	Maximum number of connections
Offset + 11	MS Byte	LS Byte	Maximum number of client connections
Offset + 12	MS Byte	LS Byte	Maximum number of server connections
Offset + 13	MSB - C00	C01	Number of messages sent regarding detected Modbus errors
Offset + 14	C02	LSB - C03	
Offset + 15	MS Byte	LS Byte	Number of open priority connections
Offset + 16	MS Byte	LS Byte	Maximum number of priority connections
Offset + 17	MS Byte	LS Byte	Number of entries in an unauthorized table
Offset + 18	MSB - IP1	IP2	Remote IP address 1
Offset + 19	IP3	LSB - IP4	
Offset + 20	MS Byte	LS Byte	Number of attempts to open an unauthorized connection 1
...			
Offset + 111	MSB - IP1	IP2	Remote IP address 32
Offset + 112	IP3	LSB - IP4	
Offset + 113	MS Byte	LS Byte	Number of attempts to open an unauthorized connection 32

Modbus TCP/Port 502 Connection Table Data (Offset 668)

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 of Modbus messages sent on the connection
Offset + 9	MS Byte	LS Byte	Number of Modbus messages received on the connection
Offset + 10	MS Byte	LS Byte	Number of Modbus detected error messages sent on the connection
...			
Offset + 3 + (8 * (N–1))	MS Byte	LS Byte	Connection index
Offset + 4 + (8 * (N–1))	IP 1	IP 2	Remote port address
Offset + 5 + (8 * (N–1))	IP 3	IP 4	
Offset + 6 + (8 * (N–1))	MS Byte	LS Byte	Remote port number
Offset + 7 + (8 * (N–1))	MS Byte	LS Byte	Local port number
Offset + 8 + (8 * (N–1))	MS Byte	LS Byte	Number of Modbus messages sent on the connection
Offset + 9 + (8 * (N–1))	MS Byte	LS Byte	Number of Modbus messages received on the connection
Offset + 10 + (8 * (N–1))	MS Byte	LS Byte	Number of detected Modbus error messages sent on the connection

SNTP Diagnostic Data (Offset 1313)

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 controller with module time
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 type
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 sent NTP requests
Offset + 30	LSW - MSB	LSW - LSB		
Offset + 31	MSW - MSB	MSW - LSB	UDINT	Number of detected communication errors
Offset + 32	LSW - MSB	LSW - LSB		
Offset + 33	MSW - MSB	MSW - LSB	UDINT	Number of received NTP responses
Offset + 34	LSW - MSB	LSW - LSB		
Offset + 35	MS Byte	LS Byte	UINT	Last detected 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		
Offset + 41	MSW - MSB	MSW - LSB	UINT	Time since last update
Offset + 42	LSW - MSB	LSW - LSB		

DNP/IEC Connection Information (Offset 1356)

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 Connection Diagnostic (Offset 1362)

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
Offset + 3	C01	LSB - C00	Configured event Buffer size
Offset + 4	MSB - C03	C02	Module total
Offset + 5	C01	LSB - C00	Current event buffer used
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 server DNP3 NET server IEC 101 server IEC 104 server
Offset + 11	MS Byte	LS Byte	LS Byte connection state 0: disconnected 1: connected 2: connecting 3: active 4: inactive MS Byte authentication type 0: none 1: SAv2 2: SAv5 3: TLS_ONLY 4: TLS_SAv2 5: T:LS_SAv5

Address	MS Byte	LS Byte	Comments
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: Bit 0: Channel security not configured Bit 1: Unlocated variable initialize error Bit 2: Internal error (pipe creation error, IPC init error, etc.) Bits 3-14: Reserved Bit 15: TLS error
Offset + 25	C03	C02	Channel total
Offset + 26	C01	C00	Configured event Buffer size
Offset + 27	C03	C02	Channel total
Offset + 28	C01	C00	Current event Buffer used
Offset + 29	C03	C02	Channel total
Offset + 30	C01	C00	Current overflow
Offset + 31	MS Byte	LS Byte	MS Byte: Reserved LS Byte: Event buffer overflow
Offset + 32	C01	C00	TLS error code
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
Offset + 36	MS Byte	LS Byte	MS Byte Bit 0: Validity Bit 1: Event buffer overflow Bits 2-7: Reserved LS Byte: Index

Address	MS Byte	LS Byte	Comments
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. Reserved 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. Reserved
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
Offset + 47	C01	C00	Buffer size
Offset + 48	C03	C02	Current event
Offset + 49	C01	C00	Buffer used
Offset + 50	C03	C02	Current overflow
Offset + 51	C01	C00	
Offset + 36 + (X-1) *16	MS Byte	LS Byte	MS Byte: Bit 0: Validity Bit 1: Event buffer overflow Bits 2-7: Reserved LS Byte: Index

Address	MS Byte	LS Byte	Comments
Offset + 37 + (X-1) *16	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. Reserved 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. Reserved
Offset + 38 + (X-1) *16	Char 1	Char 2	Data type name
Offset + 39 + (X-1) *16	Char 3	Char 4	
Offset + 40 + (X-1) *16	Char 5	Char 6	
Offset + 41 + (X-1) *16	Char 7	Char 8	
Offset + 42 + (X-1) *16	Char 9	Char 10	
Offset + 43 + (X-1) *16	Char 11	Char 12	
Offset + 44 + (X-1) *16	Char 13	Char 14	
Offset + 45 + (X-1) *16	Char 15	Char 16	
Offset + 46 + (X-1) *16	Char 03	Char 02	Configured event Buffer size
Offset + 47 + (X-1) *16	Char 01	Char 00	
Offset + 48 + (X-1) *16	Char 03	Char 02	Current event Buffer used
Offset + 49 + (X-1) *16	Char 01	Char 00	
Offset + 50 + (X-1) *16	Char 03	Char 02	Current overflow
Offset + 51 + (X-1) *16	Char 01	Char 00	
...			
Offset + 09 + (N-1) *(27 + 16*16)	MS Byte	LS Byte	Channel index
Offset + (N-1)*283 + 10	MS Byte Reserved	LS Byte: 1: DNP3 serial 3: DNP3 NET 5: IEC 101 7: IEC 104	Protocol: DNP3 serial server DNP3 NET server IEC 101 server IEC 104 server

Address	MS Byte	LS Byte	Comments
Offset + (N-1)*283 + 11	MS Byte	LS Byte	LS Byte Connection State: 0: Disconnected 1: Connected 2: Connecting 3: Active 4: Inactive MS Byte Authentication type: 5: None 6: SAv2 7: SAv5 8: TLS_ONLY 9: TLS_SAv2 10: TLS_SAv5
Offset + (N-1)*283 + 12	Char 1	Char 2	Channel name
Offset + (N-1)*283 + 13	Char 3	Char 4	
Offset + (N-1)*283 + 14	Char 5	Char 6	
Offset + (N-1)*283 + 15	Char 7	Char 8	
Offset + (N-1)*283 + 16	Char 9	Char 10	
Offset + (N-1)*283 + 17	Char 11	Char 12	
Offset + (N-1)*283 + 18	Char 13	Char 14	
Offset + (N-1)*283 + 19	Char 15	Char 16	
Offset + (N-1)*283 + 20	IP 1	IP 2	Remote IP address
Offset + (N-1)*283 + 21	IP 3	IP 4	
Offset + (N-1)*283 + 22	MS Byte	LS Byte	Remote port number
Offset + (N-1)*283 + 23	MS Byte	LS Byte	Local port number
Offset + (N-1)*283 + 24	MS Byte	LS Byte	Error code: Bit 0: Channel security not configured Bit 1: Unlocated variable initialize error Bit 2: Internal error (pipe creation error, IPC init error, etc.) Bits 3-14: Reserved Bit 15: TLS error
Offset + (N-1)*283 + 25	C03	C02	Channel total Configured event Buffer size
Offset + (N-1)*283 + 26	C01	C00	
Offset + (N-1)*283 + 27	C03	C02	Channel total Current event Buffer used
Offset + (N-1)*283 + 28	C01	C00	
Offset + (N-1)*283 + 29	C03	C02	Channel total Current overflow
Offset + (N-1)*283 + 30	C01	C00	
Offset + (N-1)*283 + 31	MS Byte	LS Byte	MS Byte: Reserved LS Byte: Event buffer overflow

Address	MS Byte	LS Byte	Comments
Offset + (N-1)*283 + 32	C01	C00	TLS error code
Offset + (N-1)*283 + 33	MS Byte	LS Byte	Reserved 2
Offset + (N-1)*283 + 34	MS Byte	LS Byte	Reserved 3
Offset + (N-1)*283 + 35	MS Byte	LS Byte	Number of data type Event status Always 16
Offset + (N-1)*283 + 36	MS Byte	LS Byte	MS Byte: Bit 0: Validity Bit 1: Event buffer overflow Bits 2-7: Reserved LS Byte: Index
Offset + (N-1)*283 + 37	MS Byte	LS Byte	DNP data typs: 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. Reserved 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. Reserved
Offset + (N-1)*283 + 38	Char 1	Char 2	Data type name
Offset + (N-1)*283 + 39	Char 3	Char 4	
Offset + (N-1)*283 + 40	Char 5	Char 6	
Offset + (N-1)*283 + 41	Char 7	Char 8	
Offset + (N-1)*283 + 42	Char 9	Char 10	
Offset + (N-1)*283 + 43	Char 11	Char 12	
Offset + (N-1)*283 + 44	Char 13	Char 14	
Offset + (N-1)*283 + 45	Char 17	Char 16	

Address	MS Byte	LS Byte	Comments
Offset + (N-1)*283 + 46	C03	C02	Configured event
Offset + (N-1)*283 + 47	C01	C00	Buffer size
Offset + (N-1)*283 + 48	C03	C02	Current event
Offset + (N-1)*283 + 49	C01	C00	Buffer used
Offset + (N-1)*283 + 50	C03	C02	Current overflow
Offset + (N-1)*283 + 51	C01	C00	
...			
Offset + (N-1)*283 + 36 + (X-1)*16	MS Byte	LS Byte	MS Byte: Bit 0: Validity Bit 1: Event buffer overflow Bits 2-7: Reserved LS Byte: Index
Offset + (N-1)*283 + 37 + (X-1)*16	MS Byte	LS Byte	DNP data type: 1. Binary input 2. Double input 3. Binary output 4. Binary counter 5. Frozen counter 6. Analog output 7. Analog output 8-16. Reserved 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. Reserved
Offset + (N-1)*283 + 38 + (X-1)*16	Char 1	Char 2	Data type name
Offset + (N-1)*283 + 39 + (X-1)*16	Char 3	Char 4	
Offset + (N-1)*283 + 40 + (X-1)*16	Char 5	Char 6	
Offset + (N-1)*283 + 41 + (X-1)*16	Char 7	Char 8	
Offset + (N-1)*283 + 42 + (X-1)*16	Char 9	Char 10	
Offset + (N-1)*283 + 43 + (X-1)*16	Char 11	Char 12	
Offset + (N-1)*283 + 44 + (X-1)*16	Char 13	Char 14	
Offset + (N-1)*283 + 45 + (X-1)*16	Char 15	Char 16	

Address	MS Byte	LS Byte	Comments
Offset + (N-1)*283 + 46 + (X-1)*16	C03	C02	Configured event Buffer size
Offset + (N-1)*283 + 47 + (X-1)*16	C01	C00	
Offset + (N-1)*283 + 48 + (X-1)*16	C03	C02	Current event Buffer used
Offset + (N-1)*283 + 49 + (X-1)*16	C01	C00	
Offset + (N-1)*283 + 50 + (X-1)*16	C03	C02	Current overflow
Offset + (N-1)*283 + 51 + (X-1)*16	C01	C00	

DNP/IEC Client Connection Diagnostic (Offset 2503)

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 client DNP3 NET client IEC 101 client IEC 104 client
Offset + 3	MS Byte	LS Byte	LS Byte connection state: 0: Disconnected 1: Connected 2: Connecting 3: Active 4: Inactive MS Byte authentication type: 5: None 6: SAv2 7: SAv5 8: TLS_ONLY 9: TLS_SAv2 10: TLS_SAv5
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

Address	MS Byte	LS Byte	Comments
Offset + 16	Bit 15~8	Bit 7~0	Error code Bit 0: Channel security not configured Bit 1: Unlocated variable initialize error Bit 2: Internal error (pipe creation error, IPC init error, etc.) Bit 3: authentication not performed Bit 4: Unexpected response Bit 5: No response Bit 6: Aggressive mode not supported Bit 7: MAC algorithm not supported Bit 8: Key wrap algorithm not supported Bit 9: Authorization not performed Bit 10: Update key change method not permitted Bit 11: Invalid signature Bit 12: Invalid certification data Bit 13: Unknown user Bit 14: Max session key status requests exceed Bit 15: TLS error
Offset + 17	C01	C02	TLS error code
Offset + 18	MS Byte	LS Byte	Reserved 1
Offset + 19	MS Byte	LS Byte	Reserved 2
Offset + 20	MS Byte	LS Byte	Reserved 3
...			
Offset + 01 + (N-1)*20	MS Byte	LS Byte	Channel index
Offset + 02 + (N-1)*20	MS Byte reserved	LS Byte: 2: DNP3 serial 4: DNP3 NET 6: IEC 101 8: IEC 104	Protocol: DNP3 serial client DNP3 NET client IEC 101 client IEC 104 client
Offset + 03 + (N-1)*20	MS Byte	LS Byte	LS Byte connection state: 0: Disconnected 1: Connected 2: Connecting 3: Active 4: Inactive MS Byte authentication type: 5: None 6: SAv2 7: SAv5 8: TLS_ONLY 9: TLS_SAv2 10: TLS_SAv5

Address	MS Byte	LS Byte	Comments
Offset + 04 + (N-1)*20	Char 1	Char 2	Channel name
Offset + 05 + (N-1)*20	Char 3	Char 4	
Offset + 06 + (N-1)*20	Char 5	Char 6	
Offset + 07 + (N-1)*20	Char 7	Char 8	
Offset + 08 + (N-1)*20	Char 9	Char 10	
Offset + 09 + (N-1)*20	Char 11	Char 12	
Offset + 10 + (N-1)*20	Char 13	Char 14	
Offset + 11 + (N-1)*20	Char 15	Char 16	
Offset + 12 + (N-1)*20	IP 1	IP 2	Remote IP address
Offset + 13 + (N-1)*20	IP 3	IP 4	
Offset + 14 + (N-1)*20	MS Byte	LS Byte	Remote port number
Offset + 15 + (N-1)*20	MS Byte	LS Byte	Local port number
Offset + 16 + (N-1)*20	Bit 15~8	Bit7~0	Error code: Bit 0: Channel security not configured Bit 1: Unlocated variable initialize error Bit 2: Internal error (pipe creation error, IPC init error, etc.) Bit 3: Authentication not performed Bit 4: Unexpected response Bit 5: No response Bit 6: Aggressive mode not supported Bit 7: MAC algorithm not supported Bit 8: Key wrap algorithm not supported Bit 9: Authorization not performed Bit 10: Update key change method not permitted Bit 11: Invalid signature Bit 12: Invalid certification data Bit 13: Unknown user Bit 14: Max session key status requests exceed Bit 15: TLS error
Offset + 17 + (N-1)*20	C01	C00	TLS error code
Offset + 18 + (N-1)*20	MS Byte	LS Byte	Reserved 1
Offset + 19 + (N-1)*20	MS Byte	LS Byte	Reserved 2
Offset + 20 + (N-1)*20	MS Byte	LS Byte	Reserved 3

DNP Server/Server Security Diagnostic (Offset 3784)

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 (SAv2, SAv5)
Offset + 3	C01	C00	
Offset + 4	C03	C02	Authorization problems (SAv2, SAv5)
Offset + 5	C01	C00	
Offset + 6	C03	C02	Authentication problems (SAv2, SAv5)
Offset + 7	C01	C00	
Offset + 8	C03	C02	Reply timeout (SAv2, SAv5)
Offset + 9	C01	C00	
Offset + 10	C03	C02	Re-keys due to authentication problem (SAv5 only)
Offset + 11	C01	C00	
Offset + 12	C03	C02	Total message sent (SAv5 only)
Offset + 13	C01	C00	
Offset + 14	C03	C02	Total messages received (SAv5 only)
Offset + 15	C01	C00	
Offset + 16	C03	C02	Critical message sent (SAv2, SAv5)
Offset + 17	C01	C00	
Offset + 18	C03	C02	Critical message received (SAv2, SAv5)
Offset + 19	C01	C00	
Offset + 20	C03	C02	Discarded messages (SAv5 only)
Offset + 21	C01	C00	
Offset + 22	C03	C02	Detected error message sent (SAv2, SAv5)
Offset + 23	C01	C00	
Offset + 24	C03	C02	Detected error message received (SAv2, SAv5)
Offset + 25	C01	C00	
Offset + 26	C03	C02	Successful authentications (SAv2, SAv5)
Offset + 27	C01	C00	
Offset + 28	C03	C02	Session key changes (SAv2, SAv5)
Offset + 29	C01	C00	
Offset + 30	C03	C02	Not performed session key changes (SAv2, SAv5)
Offset + 31	C01	C00	
Offset + 32	C03	C02	Update key changes (SAv5 only)
Offset + 33	C01	C00	
Offset + 34	C03	C02	Not performed update key changes (SAv5 only)
Offset + 35	C01	C00	
Offset + 36	C03	C02	Re-keys due to restart (SAv5 only)
Offset + 37	C01	C00	
Offset + 38	C01	C00	Reserved 0
Offset + 39	C01	C00	Reserved 1
...			
Offset + (N-1)*39 + 01	MS Byte reserved	LS Byte Channel index	Channel index
Offset + (N-1)*39 + 02	C03	C02	Unexpected messages (SAv2, SAv5)
Offset + (N-1)*39 + 03	C01	C00	
Offset + (N-1)*39 + 04	C03	C02	Authorization problems (SAv2, SAv5)
Offset + (N-1)*39 + 05	C01	C00	

Address	MS Byte	LS Byte	Comments
Offset + (N-1)*39 + 06	C03	C02	Authentication problems (SAv2, SAv5)
Offset + (N-1)*39 + 07	C01	C00	
Offset + (N-1)*39 + 08	C03	C02	Reply time out (SAv2, SAv5)
Offset + (N-1)*39 + 09	C01	C00	
Offset + (N-1)*39 + 10	C03	C02	Re-keys due to authentication problem (SAv5 only)
Offset + (N-1)*39 + 11	C01	C00	
Offset + (N-1)*39 + 12	C03	C02	Total messages sent (SAv5 only)
Offset + (N-1)*39 + 13	C01	C00	
Offset + (N-1)*39 + 14	C03	C02	Total messages received (SAv5 only)
Offset + (N-1)*39 + 15	C01	C00	
Offset + (N-1)*39 + 16	C03	C02	Critical messages sent (SAv2, SAv5)
Offset + (N-1)*39 + 17	C01	C00	
Offset + (N-1)*39 + 18	C03	C02	Critical messages received (SAv2, SAv5)
Offset + (N-1)*39 + 19	C01	C00	
Offset + (N-1)*39 + 20	C03	C02	Discarded messages (SAv5 only)
Offset + (N-1)*39 + 21	C01	C00	
Offset + (N-1)*39 + 22	C03	C02	Detected error messages sent (SAv2, SAv5)
Offset + (N-1)*39 + 23	C01	C00	
Offset + (N-1)*39 + 24	C03	C02	Detected error messages received (SAv2, SAv5)
Offset + (N-1)*39 + 25	C01	C00	
Offset + (N-1)*39 + 26	C03	C02	Successful authentications (SAv2, SAv5)
Offset + (N-1)*39 + 27	C01	C00	
Offset + (N-1)*39 + 28	C03	C02	Session key changes (SAv2, SAv5)
Offset + (N-1)*39 + 29	C01	C00	
Offset + (N-1)*39 + 30	C03	C02	Not performed session key changes (SAv2, SAv5)
Offset + (N-1)*39 + 31	C01	C00	
Offset + (N-1)*39 + 32	C03	C02	Update key changes (SAv5 only)
Offset + (N-1)*39 + 33	C01	C00	
Offset + (N-1)*39 + 34	C03	C02	Not performed update key changes (SAv5 only)
Offset + (N-1)*39 + 35	C01	C00	
Offset + (N-1)*39 + 36	C03	C02	Re-keys due to restart (SAv5 only)
Offset + (N-1)*39 + 37	C01	C00	
Offset + (N-1)*39 + 38	C03	C02	Reserved 0
Offset + (N-1)*39 + 39	C01	C00	Reserved 1

DNP Client/Client Security Diagnostic (Offset 3961)

Address	MS Byte	LS Byte	Comments
Offset			Number of entries
Offset + 01	MS Byte reserved	LS Byte Channel index	Channel index
Offset + 02	C03	C02	Unexpected messages (SAv2, SAv5)
Offset + 03	C01	C00	
Offset + 04	C03	C02	Authorization problems (SAv2, SAv5)
Offset + 05	C01	C00	
Offset + 06	C03	C02	Authentication problems (SAv2, SAv5)
Offset + 07	C01	C00	
Offset + 08	C03	C02	Reply timeout (SAv2, SAv5)
Offset + 09	C01	C00	
Offset + 10	C03	C02	Re-keys due to authentication problem (SAv5 only)
Offset + 11	C01	C00	
Offset + 12	C03	C02	Total message sent (SAv5 only)
Offset + 13	C01	C00	
Offset + 14	C03	C02	Total messages received (SAv5 only)
Offset + 15	C01	C00	
Offset + 16	C03	C02	Critical message sent (SAv2, SAv5)
Offset + 17	C01	C00	
Offset + 18	C03	C02	Critical messages received (SAv2, SAv5)
Offset + 19	C01	C00	
Offset + 20	C03	C02	Discarded messages (SAv5 only)
Offset + 21	C01	C00	
Offset + 22	C03	C02	Detected error message sent (SAv2, SAv5)
Offset + 23	C01	C00	
Offset + 24	C03	C02	Detected error message received (SAv2, SAv5)
Offset + 25	C01	C00	
Offset + 26	C03	C02	Successful authentications (SAv2, SAv5)
Offset + 27	C01	C00	
Offset + 28	C03	C02	Session key changes (SAv2, SAv5)
Offset + 29	C01	C00	
Offset + 30	C03	C02	Not performed session key changes (SAv2, SAv5)
Offset + 31	C01	C00	
Offset + 32	C03	C02	Update key changes (SAv5 only)
Offset + 33	C01	C00	
Offset + 34	C03	C02	Not performed update key changes (SAv5 only)
Offset + 35	C01	C00	
Offset + 36	C03	C02	Re-keys due to restart (SAv5 only)
Offset + 37	C01	C00	
Offset + 38	C01	C00	Reserved 0
Offset + 39	C01	C00	Reserved 1
...			
Offset = (N-1)*39 + 01	MS Byte reserved	LS Byte Channel index	Channel index
Offset = (N-1)*39 + 02	C03	C02	Unexpected messages (SAv2, SAv5)
Offset = (N-1)*39 + 03	C01	C00	

Address	MS Byte	LS Byte	Comments
Offset = (N-1)*39 + 04	C03	C02	Authorization problems (SAv2, SAv5)
Offset = (N-1)*39 + 05	C01	C00	
Offset = (N-1)*39 + 06	C03	C02	Authentication problems (SAv2, SAv5)
Offset = (N-1)*39 + 07	C01	C00	
Offset = (N-1)*39 + 08	C03	C02	Reply timeout (SAv2, SAv5)
Offset = (N-1)*39 + 09	C01	C00	
Offset = (N-1)*39 + 10	C03	C02	Re-keys due to authentication problem (SAv5 only)
Offset = (N-1)*39 + 11	C01	C00	
Offset = (N-1)*39 + 12	C03	C02	Total messages sent (SAv5 only)
Offset = (N-1)*39 + 13	C01	C00	
Offset =3(N-1)*39 + 14	C03	C02	Total messages received (SAv5 only)
Offset = (N-1)*39 + 15	C01	C00	
Offset = (N-1)*39 + 16	C03	C02	Critical messages sent (SAv2, SAv5)
Offset = (N-1)*39 + 17	C01	C00	
Offset = (N-1)*39 + 18	C03	C02	Critical messages received (SAv2, SAv5)
Offset = (N-1)*39 + 19	C01	C00	
Offset = (N-1)*39 + 20	C03	C02	Discarded messages (SAv5 only)
Offset = (N-1)*39 + 21	C01	C00	
Offset = (N-1)*39 + 22	C03	C02	Detected error messages sent (SAv2, SAv5)
Offset = (N-1)*39 + 23	C01	C00	
Offset = (N-1)*39 + 24	C03	C02	Detected error messages received (SAv2, SAv5)
Offset = (N-1)*39 + 25	C01	C00	
Offset = (N-1)*39 + 26	C03	C02	Successful authentication (SAv2, SAv5)
Offset = (N-1)*39 + 27	C01	C00	
Offset = (N-1)*39 + 28	C03	C02	Session key changes (SAv2, SAv5)
Offset = (N-1)*39 + 29	C01	C00	
Offset = (N-1)*39 + 30	C03	C02	Not performed session key changes (SAv2, SAv5)
Offset = (N-1)*39 + 31	C01	C00	
Offset = (N-1)*39 + 32	C03	C02	Update key changes (SAv5 only)
Offset = (N-1)*39 + 33	C01	C00	
Offset = (N-1)*39 + 34	C03	C02	Not performed update key changes (SAv5 only)
Offset = (N-1)*39 + 35	C01	C00	
Offset = (N-1)*39 + 36	C03	C02	Re-keys due to restart (SAv5 only)
Offset = (N-1)*39 + 37	C01	C00	
Offset = (N-1)*39 + 38	C01	C00	Reserved 0
Offset = (N-1)*39 + 39	C01	C00	Reserved 1

Clock Diagnostic (Offset 6458)

Address	MS Byte	LS Byte	Comments
Offset			Number of entries
Offset + 01	MS Byte reserved	LS Byte clock status 1: Synchronized 0: Unsynchronized	Clock status
Offset + 02	C03	C02	Current time
Offset + 03	C01	C00	
Offset + 04	C01	C00	Current date
Offset + 05	—	—	Reserved
Offset + 06	C03	C02	Time zone
Offset + 07	C01	C00	
Offset + 08	C03	C02	Time of last time synchronization
Offset + 09	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 3: controller 4: IEC60870 5: partner module ...	Time source of last time synchronization

SNMP Diagnostic (Offset 6471)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	SNMP_service 0: Service not operating correctly 1: Service operating normally or disabled

Web Service Diagnostic (Offset 6472)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	Web_service 0: Service not operating correctly 1: Service operating normally or disabled

LLDP Service Diagnostic (Offset 6473)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	LLDP_service status FW_upgrade service status 0: Service not operating correctly 1: Service operating normally or disabled

Firmware Upgrade Service Diagnostic (Offset 6474)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	FW_upgrade service status 0: Service not operating correctly 1: Service operating normally or disabled

Syslog Service Diagnostic (Offset 6475)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	MS Byte: Syslog service status: 0: Syslog service not operating correctly 1: Syslog service operating correctly or disabled LS Byte: Syslog server not reachable: 1: No acknowledgment received from the Syslog server 0: Acknowledge received from the Syslog Server successfully

SD Service Diagnostic (Offset 6476)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	SD status: 0: SD card missing or unusable 1: SD card normal

IP Address Status Diagnostic (Offset 6477)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte	LS Byte	IP address status: 0: Duplicate or no IP 1: Normal IP configured

HSBY Diagnostic (Offset 6491)

Address	MS Byte	LS Byte	Comments
Offset	MS Byte HSBY function state	LS Byte HSBY service	HSBY function: 0: Disabled **NOTE:** If it is disabled, other diagnostic data are at zero. In this case the web page does not display HSBY diagnostics. 1: Enabled HSBY Service: 0: Not performed 1: Running
Offset + 01	MS Byte Synchronization Status	LS Byte Internal HSBY state	Synchronization Status: 0: In progress 1: OK Internal HSBY state: 0: Init 1: Link established 2: Reserved 3: Integrity 4: Wait Synchronization 5. Synchronized (not shown on the web page)
Offset + 02	MS Byte Partner validity	LS Byte reserved Event Sync Status	Partner validity: 0: Not reachable 1: OK Event sync status: 0: Disabled 1: Enabled
Offset + 03	Bit 31 - Bit 24	Bit 23 - Bit 16	Error code Bit 0: Firmware mismatch Bit 1: DTM configuration mismatch Bit 2: Security mode mismatch Bit 3: Certification error Bit 4: CS configuration mismatch (reserved) Bit 5-31: Reserved
Offset + 04	Bit 15 - Bit 8	Bit 7 - Bit 0	
Offset + 05	C03	C02	Synchronization Counter
Offset + 06	C01	C00	
Offset + 07	C03	C02	Time of last time synchronization
Offset + 08	C01	C00	
Offset + 09	C01	C00	Date of last time synchronization
Offset + 10	C01	C00	Reserved
Offset + 11	C03	C02	HSBY input packets
Offset + 12	C01	C00	
Offset + 13	C03	C02	HSBY input error packets
Offset + 14	C01	C00	
Offset + 15	C03	C02	HSBY output packets
Offset + 16	C01	C00	
Offset + 17	C03	C02	HSBY output error packets
Offset + 18	C01	C00	

Address	MS Byte	LS Byte	Comments
Offset + 19	IP 1	IP 2	Local IP address
Offset + 20	IP 3	IP 4	
Offset + 21	C03 Reserved	C02 Major version	Local FW version
Offset + 22	C01 Minor version	C00 Internal revision	
Offset + 23	MS Byte Remote Role	LS Byte Reserved	Local role: 0: Unknown 1: Primary 2: Standby
Offset + 24	C1	C0	Reserved
Offset + 25	C1	C0	Reserved
Offset + 26	IP 1	IP 2	Remote IP address
Offset + 27	IP 3	IP 4	
Offset + 28	C03 Reserved	C02 Major version	Remote FW version
Offset + 29	C01 Minor version	C00 Internal revision	
Offset + 30	MS Byte Remote Role	LS Byte Reserved	Remote role: 0: Primary 1: Standby
Offset + 31	C01	C00	Reserved
Offset + 32	C01	C00	Reserved
Offset + 33	C01	C00	Reserved
Offset + 34	C01	C00	Reserved

Data Logging Service Diagnostic (Offset 6526)

Address	MS Byte	LS Byte	Comments
Offset + 0	MS Byte	LS Byte	MS Byte: Configured table count: LS Byte: Service status.
Offset + 1	MS Byte	LS Byte	Enable table count.
Offset + 2	C03	C02	SD card free space (KB)
Offset + 3	C01	C00	
Offset + 4	MS Byte	LS Byte	SD Card Status: Bit 0: 1/0: SD card is working correctly / missing Bit 1: 1/0: SD card is busy/not busy Bit 2: 1/0: Low space alarm is set/not set.
Offset + 5	C01	C00	Reserved
Offset + 6	C01	C00	Reserved
Offset + 7	C01	C00	Reserved
Offset + 8	C01	C00	Reserved
Offset + 9	C01	C00	Reserved
Offset + 10	MS Byte	LS Byte	Table ID
Offset + 11	MS Byte	LS Byte	Table Status: 0: disabled 1: enabled
Offset + 12	MS Byte	LS Byte	Log status: 0: no error 4: no memory space, 5: variable not available 6: table full 8: detected system error
Offset + 13	MS Byte	LS Byte	Backup status: 0: no detected error 1: no compatible SD card 2: detected file system error 3: not enough space in SD card 7: SD card busy 8: detected system error
Offset + 14	C03	C02	Time of last time backup
Offset + 15	C01	C00	
Offset + 16	C01	C00	Date of last time backup
Offset + 17	C01	C00	Reserved
Offset + 18	MS Byte	LS Byte	Records count in RAM
Offset + 19	MS Byte	LS Byte	Backup count in the SD card
Offset + 20	C01	C00	Reserved
Offset + 21	C01	C00	Reserved
Offset + 22	C01	C00	Reserved
Offset + 23	C01	C00	Reserved
Offset + 24	C01	C00	Reserved
Offset + 25	C01	C00	Reserved
Offset + 26	C01	C00	Reserved
Offset + 27	C01	C00	Reserved
Offset + 28	C01	C00	Reserved

Address	MS Byte	LS Byte	Comments
Offset + 29	C01	C00	Reserved
Offset + 30	C01	C00	Reserved
Offset + 31	C01	C00	Reserved
...			
Offset + 10 + (X-1) * 22	MS Byte	LS Byte	Table ID
Offset + 11 + (X-1) * 22	MS Byte	LS Byte	Table Status: 0: disabled 1: enabled
Offset + 12 + (X-1) * 22	MS Byte	LS Byte	Log status: 0: no detected error 4: no memory space, 5: variable not available, 6: table full 7: detected transfer error 8: detected system error
Offset + 13 + (X-1) * 22	MS Byte	LS Byte	Backup status: 0: no detected error 1: no SD card 2: detected file system error 3: not enough space in SD card 8: detected system error
Offset + 14 + (X-1) * 22	C03	C02	Time of last time backup
Offset + 15 + (X-1) * 22	C01	C00	
Offset + 16 + (X-1) * 22	C01	C00	Date of last time backup
Offset + 17 + (X-1) * 22	C01	C00	Reserved
Offset + 18 + (X-1) * 22	MS Byte	LS Byte	Records count in TAM
Offset + 19 + (X-1) * 22	MS Byte	LS Byte	Backup count in the SD card
Offset + 20 + (X-1) * 22	C01	C00	Reserved
Offset + 21 + (X-1) * 22	C01	C00	Reserved
Offset + 22 + (X-1) * 22	C01	C00	Reserved
Offset + 23 + (X-1) * 22	C01	C00	Reserved
Offset + 24 + (X-1) * 22	C01	C00	Reserved
Offset + 25 + (X-1) * 22	C01	C00	Reserved
Offset + 26 + (X-1) * 22	C01	C00	Reserved
Offset + 27 + (X-1) * 22	C01	C00	Reserved
Offset + 28 + (X-1) * 22	C01	C00	Reserved
Offset + 29 + (X-1) * 22	C01	C00	Reserved
Offset + 30+ (X-1) * 22	C01	C00	Reserved

SNMP Service Diagnostic (Offset 6471)

Address	MS Byte	LS Byte	Comments
Offset + 0	MS Byte: Error code	LS Byte: Service Status	Service Status: 0: Unknown 1: Enabled 2: Working Properly 3: Disabled 4: Not Configured 5: At Least One Connection is Bad 6: Enabled On 7: Enabled Off Detected error Code: Bit 8-Mismatch snmp DTM version
Offset + 1	MS Byte	LS Byte	Snmp Version: 0: V1 1:V3 3:Unknown
Offset + 2	C03	C02	Snmp Inpackets
Offset + 3	C01	C00	
Offset + 4	C03	C02	Snmp Outpackets
Offset + 5	C01	C00	
Offset + 6	C03	C02	Snmp InBad Versions
Offset + 7	C01	C00	
Offset + 8	C03	C02	Snmp V3 only: USM StatsUnknownUserNames
Offset + 9	C01	C00	
Offset + 10	C03	C02	Snmp V3 only: USM In BadCommunityUses
Offset + 11	C01	C00	
Offset + 12	C03	C02	Snmp V3 only: USM StatsWrongDigests
Offset + 13	C01	C00	
Offset + 14	C03	C02	Snmp V3 Only: USM UnknownSecurityModels
Offset + 15	C01	C00	

MODBUS Register Mapping of 8021x diagnostic

Address	MS Byte	LS Byte	Comments
Offset + 0	Port number: 0: front eth port #1 (up) 1: front eth port #1 (down) 2: backplane port	8021x service: 0: disable 1: enable	-
Offset + 1	MS Byte Reserved	8021x authentication state: 0: undefined 1: logoff 2: disconnected 3: connecting 4: acquired 5: authenticating 6: held 7: authenticated	-
Offset + 2	MAC [0]	MAC [1]	Supplicant MAC Address
Offset + 3	MAC [2]	MAC [3]	
Offset + 4	MAC [4]	MAC [5]	
Offset + 5	MAC [0]	MAC [1]	Authenticator MAC Address
Offset + 6	MAC [2]	MAC [3]	
Offset + 7	MAC [4]	MAC [5]	
Offset + 8	MSB- C00	C01	Authentication while timer
Offset + 9	MSB- C00	C01	Held while timer
Offset + 10	MSB- C00	C01	Start while timer
Offset + 11	MSB- C00	C01	Start count
Offset + 12	MSB- C00	C01	Rx EAPOL frames
Offset + 13	C02	LSB-C03	
Offset + 14	MSB- C00	C01	Tx EAPOL frames
Offset + 15	C02	LSB-C03	
Offset + 16	MSB- C00	C01	Tx EAPOL start frames
Offset + 17	C02	LSB-C03	
Offset + 18	MSB- C00	C01	Tx EAPOL logoff frames
Offset + 19	C02	LSB-C03	
Offset + 20	MSB- C00	C01	Tx EAPOL resp id frames
Offset + 21	C02	LSB-C03	
Offset + 22	MSB- C00	C01	Tx EAPOL resp frames
Offset + 23	C02	LSB-C03	
Offset + 24	MSB- C00	C01	Rx EAPOL req frames
Offset + 25	C02	LSB-C03	
Offset + 26	MSB- C00	C01	Rx EAPOL req id frames
Offset + 27	C02	LSB-C03	
Offset + 28	MSB- C00	C01	Rx EAPOL invalid frames
Offset + 29	C02	LSB-C03	

Address	MS Byte	LS Byte	Comments
Offset + 30	MSB- C00	C01	Rx EAPOL length error frames
Offset + 31	C02	LSB-C03	
Offset + 32	MAC [0]	MAC [1]	EAPOL last frame source MAC addr
Offset + 33	MAC [2]	MAC [3]	
Offset + 34	MAC [4]	MAC [5]	
Offset + 35	Outer EAP STATE: 0: unknown state 1: init 2: handshake 3: authenticated	Negotiated Outer EAP Type: 0: EAP UNDEFINED 4: EAP MD5 13: EAP TLS 21: EAP TTLS 25: EAP PEAP 26: EAP MSCHAPV2	-
Offset + 36	MS Byte	LS Byte	Reserved
Offset + 37	MS Byte	LS Byte	
Offset + 38	MS Byte	LS Byte	
Offset + 39	MS Byte	LS Byte	

MODBUS Register Mapping of E-Bus (SNAP) diagnostic

Address	MS Byte	LS Byte	Comments
Offset	Reserved	E-Bus Function: 0: disable 1: enable	-
Offset + 1	HDEP status of remote peer: 0: Initial 1: Established 2: Pre Sync 3: Sync 4: Out of Sync	HDEP status of this node: 0: Initial 1: Established 2: Pre Sync 3: Sync 4: Out of Sync	-
Offset + 2	Detected error code of remote peer: 0: None 1: bad decoding 2: sequence warning 3: sequence error 4: sequence bad 5: size error	Detected Error code of this node: 0: None 1: bad decoding 2: sequence warning 3: sequence error 4: sequence bad 5: size error	“2: sequence warning” is reserved “3: sequence error” indicates that implicit frame is missing “4: sequence bad” indicates excessive lost frames
Offset + 3	sq [0]	sq [1]	Tx sequence number
Offset + 4	sq [2]	sq [3]	
Offset + 5	sq [0]	sq [1]	Rx sequence number
Offset + 6	sq [2]	sq [3]	
Offset + 7	sq [0]	sq [1]	last Rx sequence number of remote peer
Offset + 8	sq [2]	sq [3]	
Offset + 9	Count [0]	Count [1]	Tx implicit frame count
Offset + 10	Count [2]	Count [3]	
Offset + 11	Count [0]	Count [1]	Tx HDEP frame count
Offset + 12	Count [2]	Count [3]	
Offset + 13	Count [0]	Count [1]	Tx error count
Offset + 14	Count [2]	Count [3]	
Offset + 15	Count [0]	Count [1]	Rx queue size
Offset + 16	Count [2]	Count [3]	
Offset + 17	Count [0]	Count [1]	Rx implicit frame count
Offset + 18	Count [2]	Count [3]	
Offset + 19	Count [0]	Count [1]	Rx HDEP frame count
Offset + 20	Count [2]	Count [3]	
Offset + 21	Count [0]	Count [1]	Processed Rx HDEP objects count
Offset + 22	Count [2]	Count [3]	
Offset + 23	Count [0]	Count [1]	Rx missed HDEP frame count
Offset + 24	Count [2]	Count [3]	
Offset + 25	Count [0]	Count [1]	Rx unrecoverable HDEP frame count
Offset + 26	Count [2]	Count [3]	

Address	MS Byte	LS Byte	Comments
Offset + 27	Count [0]	Count [1]	Rx error HDEP frame count
Offset + 28	Count [2]	Count [3]	
Offset + 29	Count [0]	Count [1]	Sync count
Offset + 30	Count [2]	Count [3]	
Offset + 31	Count [0]	Count [1]	Last sync time
Offset + 32	Count [2]	Count [3]	
Offset + 33	MS Byte Ebus or Xbus (1 is Ebus 0 is Xbus)	LS Byte	Ebus or Xbus
Offset + 34	MS Byte	LS Byte	Reserved
Offset + 35	MS Byte	LS Byte	
Offset + 36	MS Byte	LS Byte	
Offset + 37	MS Byte	LS Byte	
Offset + 38	MS Byte	LS Byte	
Offset + 39	MS Byte	LS Byte	

Detected Error Codes

Overview

This section contains a list of codes that describe the status of Ethernet communication module messages.

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.

Examine the first cycle after a cold or warm start, refer to *EcoStruxure™ Control Expert, System Bits and Words, Reference Manual* (Related Documents, page 11).

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
16#0F	Telegram service not configured
16#10	Network module missing
16#11	Request missing
16#12	Application server already active

Value	Communication report (least significant byte)
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:	
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

Detected Error Codes for RTU Communication

Introduction

The tables below describe the codes that correspond to detected errors for the DNP3 and IEC60870 communication standards.

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 problem
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 problem
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	TLS error

IEC60870 Communication 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	TLS error

Detected Error Codes for Open SSL/TLS

Introduction

This section describes the Open SSL/TLS error codes that can be detected in an M580 system with a BMENOR2200H module.

Detected Error Codes for Open SSL/TLS

Detected Error Codes

Detected Error	Code
SSL_R_APP_DATA_IN_HANDSHAKE	100
SSL_R_ATTEMPT_TO_REUSE_SESSION_IN_DIFFERENT_CONTEXT	272
SSL_R_BAD_ALERT_RECORD	101
SSL_R_BAD_AUTHENTICATION_TYPE	102
SSL_R_BAD_CHANGE_CIPHER_SPEC	103
SSL_R_BAD_CHECKSUM	104
SSL_R_BAD_DATA	390
SSL_R_BAD_DATA_RETURNED_BY_CALLBACK	106
SSL_R_BAD_DECOMPRESSION	107
SSL_R_BAD_DH_G_LENGTH	108
SSL_R_BAD_DH_G_VALUE	375
SSL_R_BAD_DH_PUB_KEY_LENGTH	109
SSL_R_BAD_DH_PUB_KEY_VALUE	393
SSL_R_BAD_DH_P_LENGTH	110
SSL_R_BAD_DH_P_VALUE	395
SSL_R_BAD_DIGEST_LENGTH	111
SSL_R_BAD_DSA_SIGNATURE	112
SSL_R_BAD_ECC_CERT	304
SSL_R_BAD_ECDSA_SIGNATURE	305
SSL_R_BAD_ECPOINT	306
SSL_R_BAD_HANDSHAKE_LENGTH	332
SSL_R_BAD_HELLO_REQUEST	105
SSL_R_BAD_LENGTH	271
SSL_R_BAD_MAC_DECODE	113
SSL_R_BAD_MAC_LENGTH	333
SSL_R_BAD_MESSAGE_TYPE	114
SSL_R_BAD_PACKET_LENGTH	115
SSL_R_BAD_PROTOCOL_VERSION_NUMBER	116
SSL_R_BAD_PSK_IDENTITY_HINT_LENGTH	316
SSL_R_BAD_RESPONSE_ARGUMENT	117
SSL_R_BAD_RSA_DECRYPT	118
SSL_R_BAD_RSA_ENCRYPT	119

Detected Error	Code
SSL_R_BAD_RSA_E_LENGTH	120
SSL_R_BAD_RSA_MODULUS_LENGTH	121
SSL_R_BAD_RSA_SIGNATURE	122
SSL_R_BAD_SIGNATURE	123
SSL_R_BAD_SRP_A_LENGTH	347
SSL_R_BAD_SRP_B_LENGTH	348
SSL_R_BAD_SRP_G_LENGTH	349
SSL_R_BAD_SRP_N_LENGTH	350
SSL_R_BAD_SRP_PARAMETERS	371
SSL_R_BAD_SRP_S_LENGTH	351
SSL_R_BAD_SRTP_MKI_VALUE	352
SSL_R_BAD_SRTP_PROTECTION_PROFILE_LIST	353
SSL_R_BAD_SSL_FILETYPE	124
SSL_R_BAD_SSL_SESSION_ID_LENGTH	125
SSL_R_BAD_STATE	126
SSL_R_BAD_VALUE	384
SSL_R_BAD_WRITE_RETRY	127
SSL_R_BIO_NOT_SET	128
SSL_R_BLOCK_CIPHER_PAD_IS_WRONG	129
SSL_R_BN_LIB	130
SSL_R_CA_DN_TOO_LONG	132
SSL_R_CCS_RECEIVED_EARLY	133
SSL_R_CERTIFICATE_VERIFY_FAILED	134
SSL_R_CERT_LENGTH_MISMATCH	135
SSL_R_CHALLENGE_IS_DIFFERENT	136
SSL_R_CIPHER_CODE_WRONG_LENGTH	137
SSL_R_CIPHER_OR_HASH_UNAVAILABLE	138
SSL_R_CIPHER_TABLE_SRC_ERROR	139
SSL_R_CLIENTHELLO_TLSEXT	226
SSL_R_COMPRESSED_LENGTH_TOO_LONG	140
SSL_R_COMPRESSION_DISABLED	343
SSL_R_COMPRESSION_FAILURE	141
SSL_R_COMPRESSION_ID_NOT_WITHIN_PRIVATE_RANGE	307
SSL_R_COMPRESSION_LIBRARY_ERROR	142
SSL_R_CONNECTION_ID_IS_DIFFERENT	143
SSL_R_CONNECTION_TYPE_NOT_SET	144
SSL_R_COOKIE_MISMATCH	308
SSL_R_DATA_BETWEEN_CCS_AND_FINISHED	145
SSL_R_DATA_LENGTH_TOO_LONG	146
SSL_R_DECRYPTION_FAILED	147
SSL_R_DECRYPTION_FAILED_OR_BAD_RECORD_MAC	281
SSL_R_DH_KEY_TOO_SMALL	372

Detected Error	Code
SSL_R_DH_PUBLIC_VALUE_LENGTH_IS_WRONG	148
SSL_R_DIGEST_CHECK_FAILED	149
SSL_R_DTLS_MESSAGE_TOO_BIG	334
SSL_R_DUPLICATE_COMPRESSION_ID	309
SSL_R_ECC_CERT_NOT_FOR_KEY_AGREEMENT	317
SSL_R_ECC_CERT_NOT_FOR_SIGNING	318
SSL_R_ECC_CERT_SHOULD_HAVE_RSA_SIGNATURE	322
SSL_R_ECC_CERT_SHOULD_HAVE_SHA1_SIGNATURE	323
SSL_R_ECDH_REQUIRED_FOR_SUITEB_MODE	374
SSL_R_ECGROUP_TOO_LARGE_FOR_CIPHER	310
SSL_R_EMPTY_SRTP_PROTECTION_PROFILE_LIST	354
SSL_R_ENCRYPTED_LENGTH_TOO_LONG	150
SSL_R_ERROR_GENERATING_TMP_RSA_KEY	282
SSL_R_ERROR_IN_RECEIVED_CIPHER_LIST	151
SSL_R_EXCESSIVE_MESSAGE_SIZE	152
SSL_R_EXTRA_DATA_IN_MESSAGE	153
SSL_R_GOT_A_FIN_BEFORE_A_CCS	154
SSL_R_GOT_NEXT_PROTO_BEFORE_A_CCS	355
SSL_R_GOT_NEXT_PROTO_WITHOUT_EXTENSION	356
SSL_R_HTTPS_PROXY_REQUEST	155
SSL_R_HTTPS_REQUEST	156
SSL_R_ILLEGAL_PADDING	283
SSL_R_ILLEGAL_SUITEB_DIGEST	380
SSL_R_INAPPROPRIATE_FALLBACK	373
SSL_R_INCONSISTENT_COMPRESSION	340
SSL_R_INVALID_CHALLENGE_LENGTH	158
SSL_R_INVALID_COMMAND	280
SSL_R_INVALID_COMPRESSION_ALGORITHM	341
SSL_R_INVALID_NULL_CMD_NAME	385
SSL_R_INVALID_PURPOSE	278
SSL_R_INVALID_SERVERINFO_DATA	388
SSL_R_INVALID_SRP_USERNAME	357
SSL_R_INVALID_STATUS_RESPONSE	328
SSL_R_INVALID_TICKET_KEYS_LENGTH	325
SSL_R_INVALID_TRUST	279
SSL_R_KEY_ARG_TOO_LONG	284
SSL_R_KRB5	285
SSL_R_KRB5_C_CC_PRINC	286
SSL_R_KRB5_C_GET_CRED	287
SSL_R_KRB5_C_INIT	288
SSL_R_KRB5_C_MK_REQ	289
SSL_R_KRB5_S_BAD_TICKET	290

Detected Error	Code
SSL_R_KRB5_S_INIT	291
SSL_R_KRB5_S_RD_REQ	292
SSL_R_KRB5_S_TKT_EXPIRED	293
SSL_R_KRB5_S_TKT_NYV	294
SSL_R_KRB5_S_TKT_SKEW	295
SSL_R_LENGTH_MISMATCH	159
SSL_R_LENGTH_TOO_LONG	404
SSL_R_LENGTH_TOO_SHORT	160
SSL_R_LIBRARY_BUG	274
SSL_R_LIBRARY_HAS_NO_CIPHERS	161
SSL_R_MESSAGE_TOO_LONG	296
SSL_R_MISSING_DH_DSA_CERT	162
SSL_R_MISSING_DH_KEY	163
SSL_R_MISSING_DH_RSA_CERT	164
SSL_R_MISSING_DSA_SIGNING_CERT	165
SSL_R_MISSING_ECDH_CERT	382
SSL_R_MISSING_ECDSA_SIGNING_CERT	382
SSL_R_MISSING_EXPORT_TMP_DH_KEY	166
SSL_R_MISSING_EXPORT_TMP_RSA_KEY	167
SSL_R_MISSING_RSA_CERTIFICATE	168
SSL_R_MISSING_RSA_ENCRYPTIG_CERT	169
SSL_R_MISSING_RSA_SIGNING_CERT	170
SSL_R_MISSING_SRP_PARAM	358
SSL_R_MISSING_TMP_DH_KEY	171
SSL_R_MISSING_TMP_ECDH_KEY	311
SSL_R_MISSING_TMP_RSA_KEY	172
SSL_R_MISSING_TMP_RSA_PKEY	173
SSL_R_MISSING_VERIFY_MESSAGE	174
SSL_R_MULTIPLE_SGC_RESTARTS	346
SSL_R_NON_SSLV2_INITIAL_PACKET	175
SSL_R_NO_CERTIFICATES_RETURNED	176
SSL_R_NO_CERTIFICATE_ASSIGNED	177
SSL_R_NO_CERTIFICATE_RETURNED	178
SSL_R_NO_CERTIFICATE_SET	179
SSL_R_NO_CERTIFICATE_SPECIFIED	180
SSL_R_NO_CIPHERS_AVAILABLE	181
SSL_R_NO_CIPHERS_PASSED	182
SSL_R_NO_CIPHERS_SPECIFIED	183
SSL_R_NO_CIPHER_LIST	184
SSL_R_NO_CIPHER_MATCH	185
SSL_R_NO_CLIENT_CERT_METHOD	331
SSL_R_NO_CLIENT_CERT_RECEIVED	186

Detected Error	Code
SSL_R_NO_COMPRESSION_SPECIFIED	187
SSL_R_NO_GOST_CERTIFICATE_SENT_BY_PEER	330
SSL_R_NO_METHOD_SPECIFIED	188
SSL_R_NO_PEM_EXTENSIONS	389
SSL_R_NO_PRIVATEKEY	189
SSL_R_NO_PRIVATE_KEY_ASSIGNED	190
SSL_R_NO_PROTOCOLS_AVAILABLE	191
SSL_R_NO_PUBLICKEY	192
SSL_R_NO_RENEGOTIATION	339
SSL_R_NO_REQUIRED_DIGEST	324
SSL_R_NO_SHARED_CIPHER	193
SSL_R_NO_SHARED_SIGNATURE_ALGORITHMS	376
SSL_R_NO_SRTP_PROFILES	359
SSL_R_NO_VERIFY_CALLBACK	194
SSL_R_NULL_SSL_CTX	195
SSL_R_NULL_SSL_METHOD_PASSED	196
SSL_R_OLD_SESSION_CIPHER_NOT_RETURNED	197
SSL_R_OLD_SESSION_COMPRESSION_ALGORITHM_NOT_ RETURNED	344
SSL_R_ONLY_DTLS_1_2_ALLOWED_IN_SUITEB_MODE	387
SSL_R_ONLY_TLS_1_2_ALLOWED_IN_FIPS_MODE	297
SSL_R_OPAQUE_PRF_INPUT_TOO_LONG	327
SSL_R_PACKET_LENGTH_TOO_LONG	198
SSL_R_PARSE_TLSEXT	227
SSL_R_PATH_TOO_LONG	270
SSL_R_PEER_DID_NOT_RETURN_A_CERTIFICATE	199
SSL_R_PEER_ERROR	200
SSL_R_PEER_ERROR_CERTIFICATE	201
SSL_R_PEER_ERROR_NO_CERTIFICATE	202
SSL_R_PEER_ERROR_NO_CIPHER	203
SSL_R_PEER_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	204
SSL_R_PEM_NAME_BAD_PREFIX	391
SSL_R_PEM_NAME_TOO_SHORT	392
SSL_R_PRE_MAC_LENGTH_TOO_LONG	205
SSL_R_PROBLEMS_MAPPING_CIPHER_FUNCTIONS	206
SSL_R_PROTOCOL_IS_SHUTDOWN	207
SSL_R_PSK_IDENTITY_NOT_FOUND	223
SSL_R_PSK_NO_CLIENT_CB	224
SSL_R_PSK_NO_SERVER_CB	225
SSL_R_PUBLIC_KEY_ENCRYPT_ERROR	208
SSL_R_PUBLIC_KEY_IS_NOT_RSA	209
SSL_R_PUBLIC_KEY_NOT_RSA	210
SSL_R_READ_BIO_NOT_SET	211

Detected Error	Code
SSL_R_READ_TIMEOUT_EXPIRED	312
SSL_R_READ_WRONG_PACKET_TYPE	212
SSL_R_RECORD_LENGTH_MISMATCH	213
SSL_R_RECORD_TOO_LARGE	214
SSL_R_RECORD_TOO_SMALL	298
SSL_R_RENEGOTIATE_EXT_TOO_LONG	335
SSL_R_RENEGOTIATION_ENCODING_ERR	336
SSL_R_RENEGOTIATION_MISMATCH	337
SSL_R_REQUIRED_CIPHER_MISSING	215
SSL_R_REQUIRED_COMPRESSION_ALGORITHM_MISSING	342
SSL_R_REUSE_CERT_LENGTH_NOT_ZERO	216
SSL_R_REUSE_CERT_TYPE_NOT_ZERO	217
SSL_R_REUSE_CIPHER_LIST_NOT_ZERO	218
SSL_R_SCSV_RECEIVED_WHEN_RENEGOTIATING	345
SSL_R_SERVERHELLO_TLSEXT	275
SSL_R_SESSION_ID_CONTEXT_UNINITIALIZED	277
SSL_R_SHORT_READ	219
SSL_R_SHUTDOWN_WHILE_IN_INIT	407
SSL_R_SIGNATURE_ALGORITHMS_ERROR	360
SSL_R_SIGNATURE_FOR_NON_SIGNING_CERTIFICATE	220
SSL_R_SRP_A_CALC	361
SSL_R_SRTP_COULD_NOT_ALLOCATE_PROFILES	362
SSL_R_SRTP_PROTECTION_PROFILE_LIST_TOO_LONG	363
SSL_R_SRTP_UNKNOWN_PROTECTION_PROFILE	364
SSL_R_DOING_SESSION_ID_REUSE	221
SSL_R_CONNECTION_ID_TOO_LONG	299
SSL_R_SSL3_EXT_INVALID_ECPOINTFORMAT	321
SSL_R_SSL3_EXT_INVALID_SERVERNAME	319
SSL_R_SSL3_EXT_INVALID_SERVERNAME_TYPE	320
SSL_R_SSL3_SESSION_ID_TOO_LONG	300
SSL_R_SSL3_SESSION_ID_TOO_SHORT	222
SSL_R_SSLV3_ALERT_BAD_CERTIFICATE	1042
SSL_R_SSLV3_ALERT_BAD_RECORD_MAC	1020
SSL_R_SSLV3_ALERT_CERTIFICATE_EXPIRED	1045
SSL_R_SSLV3_ALERT_CERTIFICATE_REVOKED	1044
SSL_R_SSLV3_ALERT_CERTIFICATE_UNKNOWN	1046
SSL_R_SSLV3_ALERT_DECOMPRESSION_FAILURE	1030
SSL_R_SSLV3_ALERT_HANDSHAKE_FAILURE	1040
SSL_R_SSLV3_ALERT_ILLEGAL_PARAMETER	1047
SSL_R_SSLV3_ALERT_NO_CERTIFICATE	1041
SSL_R_SSLV3_ALERT_UNEXPECTED_MESSAGE	1010
SSL_R_SSLV3_ALERT_UNSUPPORTED_CERTIFICATE	1043

Detected Error	Code
SSL_R_SSL_CTX_HAS_NO_DEFAULT_SSL_VERSION	228
SSL_R_SSL_HANDSHAKE_FAILURE	229
SSL_R_SSL_LIBRARY_HAS_NO_CIPHERS	230
SSL_R_SSL_SESSION_ID_CALLBACK_FAILED	301
SSL_R_SSL_SESSION_ID_CONFLICT	302
SSL_R_SSL_SESSION_ID_CONTEXT_TOO_LONG	273
SSL_R_SSL_SESSION_ID_HAS_BAD_LENGTH	303
SSL_R_SSL_SESSION_ID_IS_DIFFERENT	231
SSL_R_TLSV1_ALERT_ACCESS_DENIED	1049
SSL_R_TLSV1_ALERT_DECODE_ERROR	1050
SSL_R_TLSV1_ALERT_DECRYPTION_FAILED	1021
SSL_R_TLSV1_ALERT_DECRYPT_ERROR	1051
SSL_R_TLSV1_ALERT_EXPORT_RESTRICTION	1060
SSL_R_TLSV1_ALERT_INAPPROPRIATE_FALLBACK	1086
SSL_R_TLSV1_ALERT_INSUFFICIENT_SECURITY	1071
SSL_R_TLSV1_ALERT_INTERNAL_ERROR	1080
SSL_R_TLSV1_ALERT_NO_RENEGOTIATION	1100
SSL_R_TLSV1_ALERT_PROTOCOL_VERSION	1070
SSL_R_TLSV1_ALERT_RECORD_OVERFLOW	1022
SSL_R_TLSV1_ALERT_UNKNOWN_CA	1048
SSL_R_TLSV1_ALERT_USER_CANCELLED	1090
SSL_R_TLSV1_BAD_CERTIFICATE_HASH_VALUE	1114
SSL_R_TLSV1_BAD_CERTIFICATE_STATUS_RESPONSE	1113
SSL_R_TLSV1_CERTIFICATE_UNOBTAINABLE	1111
SSL_R_TLSV1_UNRECOGNIZED_NAME	1112
SSL_R_TLSV1_UNSUPPORTED_EXTENSION	1110
SSL_R_TLS_CLIENT_CERT_REQ_WITH_ANON_CIPHER	232
SSL_R_TLS_HEARTBEAT_PEER_DOESNT_ACCEPT	365
SSL_R_TLS_HEARTBEAT_PENDING	366
SSL_R_TLS_ILLEGAL_EXPORTER_LABEL	367
SSL_R_TLS_INVALID_ECPOINTFORMAT_LIST	157
SSL_R_TLS_PEER_DID_NOT_RESPOND_WITH_CERTIFICATE_LIST	233
SSL_R_TLS_RSA_ENCRYPTED_VALUE_LENGTH_IS_WRONG	234
SSL_R_TOO_MANY_WARN_ALERTS	409
SSL_R_TRIED_TO_USE_UNSUPPORTED_CIPHER	235
SSL_R_UNABLE_TO_DECODE_DH_CERTS	236
SSL_R_UNABLE_TO_DECODE_ECDH_CERTS	313
SSL_R_UNABLE_TO_EXTRACT_PUBLIC_KEY	237
SSL_R_UNABLE_TO_FIND_DH_PARAMETERS	238
SSL_R_UNABLE_TO_FIND_ECDH_PARAMETERS	314
SSL_R_UNABLE_TO_FIND_PUBLIC_KEY_PARAMETERS	239
SSL_R_UNABLE_TO_FIND_SSL_METHOD	240

Detected Error	Code
SSL_R_UNABLE_TO_LOAD_SSL2_MD5_ROUTINES	241
SSL_R_UNABLE_TO_LOAD_SSL3_MD5_ROUTINES	242
SSL_R_UNABLE_TO_LOAD_SSL3_SHA1_ROUTINES	243
SSL_R_UNEXPECTED_MESSAGE	244
SSL_R_UNEXPECTED_RECORD	245
SSL_R_UNINITIALIZED	276
SSL_R_UNKNOWN_ALERT_TYPE	246
SSL_R_UNKNOWN_CERTIFICATE_TYPE	247
SSL_R_UNKNOWN_CIPHER_RETURNED	248
SSL_R_UNKNOWN_CIPHER_TYPE	249
SSL_R_UNKNOWN_CMD_NAME	386
SSL_R_UNKNOWN_DIGEST	368
SSL_R_UNKNOWN_KEY_EXCHANGE_TYPE	250
SSL_R_UNKNOWN_PKEY_TYPE	251
SSL_R_UNKNOWN_PROTOCOL	252
SSL_R_UNKNOWN_REMOTE_ERROR_TYPE	253
SSL_R_UNKNOWN_SSL_VERSION	254
SSL_R_UNKNOWN_STATE	255
SSL_R_UNSAFE_LEGACY_RENEGOTIATION_DISABLED	338
SSL_R_UNSUPPORTED_CPHER	256
SSL_R_UNSUPPORTED_COMPRESSION_ALGORITHM	257
SSL_R_UNSUPPORTED_DIGEST_TYPE	326
SSL_R_UNSUPPORTED_ELLIPTIC_CURVE	315
SSL_R_UNSUPPORTED_PROTOCOL	258
SSL_R_UNSUPPORTED_SSL_VERSION	259
SSL_R_UNSUPPORTED_STATUS_TYPE	329
SSL_R_USE_SRTP_NOT_NEGOTIATED	369
SSL_R_WRITE_BIO_NOT_SET	260
SSL_R_WRONG_CERTIFICATE_TYPE	383
SSL_R_WRONG_CIPHER_RETURNED	261
SSL_R_WRONG_CURVE	378
SSL_R_WRONG_MESSAGE_TYPE	262
SSL_R_WRONG_NUMBER_OF_KEY_BITS	263
SSL_R_WRONG_SIGNATURE_LENGTH	264
SSL_R_WRONG_SIGNATURE_SIZE	265
SSL_R_WRONG_SIGNATURE_TYPE	370
SSL_R_WRONG_SSL_VERSION	266
SSL_R_WRONG_VERSION_NUMBER	267
SSL_R_X509_LIB	268
SSL_R_X509_VERIFICATION_SETUP_PROBLEMS	269

Firmware Version Compatibility

Introduction

This section describes the history of firmware versions for the BMENOR2200H module and their compatibility with Control Expert.

Firmware Version Compatibility

Backward Compatibility

The BMENOR2200H module supports backward compatibility. That is, new firmware versions can execute old applications, but new applications cannot download the old firmware versions on the module:

Firmware version	EcoStruxure Control Expert version					
	14.0	15.0	15.1	15.3	16.0	16.4
1.0	OK	Legacy	Legacy	Legacy	Legacy	Legacy
2.01	OK	OK	Legacy	Legacy	Legacy	Legacy
3.01	OK	OK	OK	Legacy	Legacy	Legacy
4.01	OK	OK	OK	OK	Legacy	Legacy
4.10	OK	OK	OK	OK	OK	Legacy
4.20	OK	OK	OK	OK	OK	OK

OK: All firmware versions are compatible with the corresponding software version number.

Legacy: Legacy features are compatible with the corresponding software version number. (Downloading new functions to this software version on the module causes application errors.)

Application Update from BMENOR2200.2

For BMENOR2200H module, it is available to apply new hardware and firmware on an existing configuration. When it is needed to enable control port from an old configuration, a BMENOR2200H.3 module must be configured to replace the BMENOR2200H.2 module.

M580 Application Update Tool provides a method to easily upgrade bulk application for BMENOR2200H.2 modules (without control port) to BMENOR2200H.3 modules (with control port).

NOTE:

1. New module with control port can directly replace the old module without control port in a running system. New hardware can run on the old configuration but the control port is automatically disabled. In HSBY cases, firmware of the two BMENOR modules should be upgraded to the same version even the hardware is of different type.
2. The minimum firmware version for module with control port is version 4.01.
3. Configuration with new features cannot be downloaded to an old firmware. It will cause new feature non-working (application failure). Select the correct firmware version in DTM before configuration.

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, SFC 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 communication 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 latest implemented value is equal to the preselection value.

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.

Ethernet:

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

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.

A gateway device interconnects two different networks, sometimes through different network protocols. When it connects networks based on different protocols, a gateway converts a datagram from one protocol stack into the other. When used to connect two IP-based networks, a gateway (also called a router) has two separate IP addresses, one on each network.

H

harsh environment:

Resistance to hydrocarbons, industrial oils, detergents and solder chips. Relative humidity up to 100%, saline atmosphere, significant temperature variations, operating temperature between -10°C and + 70°C, or in mobile installations. For hardened (H) devices, the relative humidity is up to 95% and the operating temperature is between -25°C and + 70°C.

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 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.

HTTPS server:

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

I

IP address:

The 32-bit identifier, consisting of both a network address and a host address assigned to a device connected to a TCP/IP network.

L

local rack:

An M580 rack containing the controller 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 three 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 through a 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 agent:

The SNMP application that runs on a network device.

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.

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 mask:

The subnet mask is a 32 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.

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.

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

trap:

A trap is an event directed by an SNMP agent that indicates one of these events:

- A change has occurred in the status of an agent.
- An unauthorized SNMP manager device has attempted to get data from (or change data on) an SNMP agent.

Schneider Electric
1884 Boulevard de la Défense
92000 Nanterre
France

se.com

© 2026 Schneider Electric. All rights reserved.

PHA90072.06