M580 IEC 61850

BMENOP0300 Module

Installation and Configuration Guide

Original instructions

QGH11908.08
05/2025

www.se.com

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

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.

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

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 M580 BMENOP0300 module. The main purpose of this module is to connect to intelligent electronic devices (IEDs) and supervision control software that utilize the IEC 61850 standard. The module enables PlantStruxure controllers to be easily integrated into an IEC 61850 environment.

NOTE: Any specific configuration settings contained in this guide are for instructional purposes only. The settings required for your specific application will differ from any examples presented in this guide.

This document is intended for users with knowledge of:

- IEC 61850 standards, content of services, data model, engineering process, etc.
- Control Expert configuration software, which is the engineering tool for the M580 platform and the BMENOP0300 module

Validity Note

This document has been updated for the release of EcoStruxure™ Control Expert 16.2.

The characteristics that are described in the present document, as well as those described in the documents included in the Related Documents section below, can be found online. To access the information online, go to the Schneider Electric home page www.se.com/ww/en/download/.

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.

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.

Information Related to Cyber Security

Information on cyber security is provided on the Schneider Electric website:
https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Document available for download on cyber security support section:

Title of Documentation	Reference Number
How can I ... Reduce Vulnerability to Cyber Attacks?	STN+v2
Cybersecurity Best Practices	7EN52-0390

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 (QGH11908)
- French (QGH11910)
- German (QGH11911)
- Italian (QGH11913)
- Spanish (QGH11914)
- Chinese (QGH11915)

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, M340, and X80 I/O Platforms, Standards and Certifications	EIO0000002726 (ENG) EIO0000002727 (FRE) EIO0000002728 (GER) EIO0000002730 (ITA) EIO0000002729 (SPA) EIO0000002731 (CHS)
Modicon M580, System Planning Guide for Complex Topologies	NHA58892 (ENG) NHA58893 (FRE) NHA58894 (GER) NHA58895 (ITA) NHA58896 (SPA) NHA58897 (CHS)
Modicon M580, RIO Modules, Installation and Configuration Guide	EIO0000001584 (ENG) EIO0000001585 (FRE) EIO0000001586 (GER) EIO0000001587 (ITA) EIO0000001588 (SPA) EIO0000001589 (CHS)
Modicon M580 BMENOC0301/11, Ethernet Communication Module, Installation and Configuration Guide	HRB62665 (ENG) HRB65311 (FRE) HRB65313 (GER) HRB65314 (ITA) HRB65315 (SPA) HRB65316 (CHS)
Modicon M580 BMENOC0321, Control Network Module, Installation and Configuration Guide	NVE24232 (ENG) NVE24233 (FRE) NVE24237 (GER) NVE24240 (ITA) NVE24239 (SPA) NVE24242 (CHS)
Modicon M580, Change Configuration on the Fly, User Guide	EIO0000001590 (ENG) EIO0000001591 (FRE) EIO0000001592 (GER) EIO0000001594 (ITA) EIO0000001593 (SPA) EIO0000001595 (CHS)
Modicon M580 Hot Standby, System Planning Guide for Frequently Used Architectures	NHA58880 (ENG) NHA58881 (FRE) NHA58882 (GER) NHA58883 (ITA) NHA58884 (SPA) NHA58885 (CHS)
Modicon X80, BMXNRP0200/0201 Fiber Converter Modules, User Guide	EIO0000001108 (ENG) EIO0000001109 (FRE) EIO0000001110 (GER) EIO0000001112 (ITA) EIO0000001111 (SPA) EIO0000001113 (CHS)
Modicon X80, Analog Input/Output Modules, User Manual	35011978 (ENG) 35011980 (FRE) 35011979 (GER) 35011982 (ITA) 35011981 (SPA) 35011983 (CHS)
Modicon X80, Discrete Input/Output Modules, User Manual	35012474 (ENG) 35012476 (FRE) 35012475 (GER) 35012478 (ITA) 35012477 (SPA) 35012479 (CHS)

Title of Documentation	Reference Number
Modicon X80, BMXEHC0200 Counting Module, User Manual	35013355 (ENG) 35013357 (FRE) 35013356 (GER) 35013359 (ITA) 35013358 (SPA) 35013360 (CHS)
EcoStruxure™ Control Expert, Program Languages and Structure, Reference Manual	35006144 (ENG) 35006145 (FRE) 35006146 (GER) 35013361 (ITA) 35006147 (SPA) 35013362 (CHS)
EcoStruxure™ Control Expert, Operating Modes	33003101 (ENG) 33003102 (FRE) 33003103 (GER) 33003696 (ITA) 33003104 (SPA) 33003697 (CHS)
Quantum using EcoStruxure™ Control Expert, Hardware Reference Manual	35010529 (ENG) 35010530 (FRE) 35010531 (GER) 35013975 (ITA) 35010532 (SPA) 5012184 (CHS)
EcoStruxure™ Control Expert, Installation Manual	35014792 (FRE) 35014793 (ENG) 35014794 (GER) 35014795 (SPA) 35014796 (ITA) 35012191 (CHS)

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.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in this manual, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2015	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2013	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements

Standard	Description
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2015	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2016	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term zone of operation may be used in conjunction with the description of specific hazards, and is defined as it is for a hazard zone or danger zone in the Machinery Directive (2006/42/EC) and ISO 12100:2010.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Characteristics of the BMENOP0300 Module

Introduction

This chapter describes the BMENOP0300 module linking IEC 61850 and Ethernet networks in an M580 system.

This chapter includes physical characteristics, port descriptions, and agency specifications for the BMENOP0300 module.

BMENOP0300 Module Description

Introduction

The BMENOP0300 module is installed on the local rack of an M580 system. The module provides interfaces for IEC 61850 communication.

Ruggedized Version

The BMENOP0300C (coated) equipment is the ruggedized version of the BMENOP0300 (standard) equipment. It can be used at standard temperatures and in harsh chemical environments.

For more information, refer to chapter *Installation in More Severe Environments*.

Altitude Operating Conditions

The characteristics apply to the modules BMENOP0300 and BMENOP0300C for use at altitude up to 2000 m (6560 ft). When the modules operate above 2000 m (6560 ft), apply additional derating.

For detailed information, refer to chapter *Operating and Storage Conditions*.

Functionality

The main purpose of the BMENOP0300 module is to provide connection with IEC 61850 IED devices as well as device management software that utilizes the IEC 61850 standard.

The BMENOP0300 module is mounted on the local rack and supports communication as:

- IEC 61850 server
- IEC 61850 client
- Generic Object-Oriented Substation Event (GOOSE) publisher
- GOOSE subscriber
- Modbus TCP server and client

The BMENOP0300 module also provides high network availability by supporting:

- RSTP protocol
- IP forwarding capability
- M580 redundant functionality
- SNTP, SNMP, and Syslog

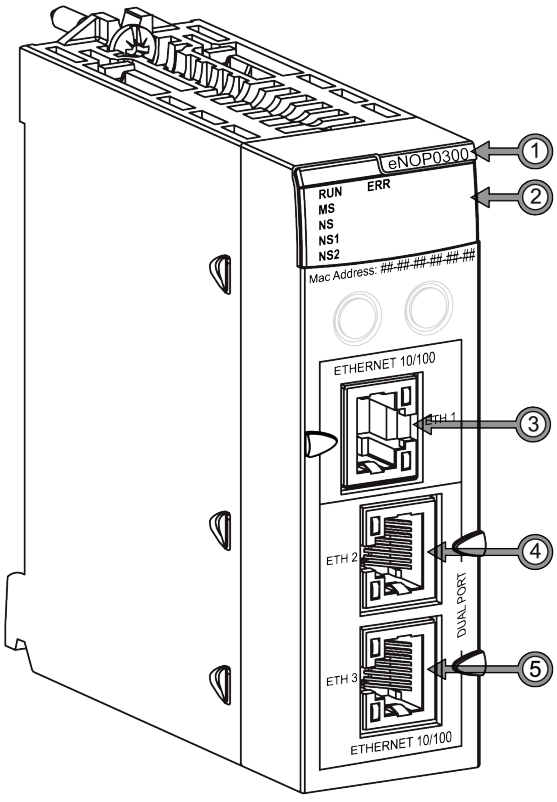
- Data modeling in IED configurator and DDDT representation in Control Expert
- Dual-bus backplane (X Bus and Ethernet)
- Cyber security

The maximum number of BMENOP0300 modules that can be mounted on a local rack is determined by your choice of controller. The maximum numbers of communication modules, including BMENOP0300 modules, supported by M580 controllers are as follows:

Controller	Maximum Number of Communication Modules
BMEP581020	2
BME•5820•0	2
BMEP5830•0	3
BME•5840•0	4
BMEP585040	4
BME•586040	4

External Features

BMENOP0300:



1 commercial reference (module name)

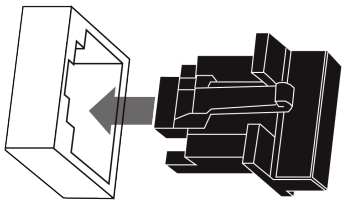
2 LED display

3 Ethernet port (ETH 1)

4 Ethernet port (ETH 2)

5 Ethernet port (ETH 3)

NOTE: To help prevent dust from entering the unused Ethernet ports on this module, cover the port with the stopper:



External Ports

The BMENOP0300 module has three external Ethernet ports, whose IP addresses can be configured in the **Communication Settings > IP Setting** tab.

Port	Description
ETH 1	The ETH 1 port allows the diagnosis of Ethernet ports and provides access to external tools and devices (Control Expert, ConneXium Network Manager, HMI, etc.). The port supports these modes: • port mirroring: In this mode, you can connect to a PC and use packet sniffing software to analyze the traffic traveling through one or more of the other module ports. • access port (default): In this mode, you can connect an Ethernet device (for example, HMI, PC with Control Expert installed, PC with ConneXium Network Manager tool) to communicate the PLC/CPU, the BMENOP0300 module, or other devices connected to the M580 network. • extended network: In this mode, you can connect the ETH 1 port to another existing DIO network that you wish to communicate with your M580 EIO network. **NOTE:** In port mirroring mode, the ETH 1 port acts like a read-only port. You cannot access devices (ping, connect to Control Expert, etc.) through the ETH_1 port. To configure this port, refer to the Configuring the Service/Extend Port topic, page 50.
Backplane	The Backplane port, located on the back of the module, allows you to connect to an Ethernet backplane The port supports this mode: • access port (default): In this mode, you can connect an Ethernet device (for example, HMI, PC with Control Expert installed, PC with ConneXium Network Manager tool) to communicate with the controller, the BMENOP0300 module, or other devices connected to the M580 network.
ETH 2 and ETH 3	These 2 copper ports provide: • connections for Ethernet services • star, loop, or mesh topology • support for RSTP **NOTE:** Only ETH 2 and ETH 3 ports support RSTP.

Communication Specifications

Introduction

The following specifications describe the capacities of the BMENOP0300 module.

Data In versus Data Out

The terms *data in* and *data out*, as used in this topic, refer to the flow of data from the point of view of the BMENOP0300 module, and vary depending on the role of the device as client or server.

- Data In: The BMENOP0300 module receives a data update from its connected devices, then synchronizes data with the controller:
  - As server: The BMENOP0300 module receives a command from a control object or GOOSE.
  - As client: The BMENOP0300 module receives a report/GOOSE response to a previous read request.
- Data Out: The BMENOP0300 module receives a data update from the controller, then propagates the data among its connected devices:
  - As server: The BMENOP0300 module sends a buffered report, unbuffered report, or GOOSE.
  - As client: The BMENOP0300 module issues a control object or polling command, a command for a buffered report, unbuffered report, or GOOSE.

IEC 61850 Messaging Specifications

The BMENOP0300 module presents the following IEC 61850 messaging features:

Feature	Client	Server
maximum number of concurrent IED connections	32	—
maximum number of words for data in flow variables	4,000[1,2,4]	4,000[1,2,4]
maximum number of words for data out flow variables	4,000[2,3]	4,000[2,3]
maximum number of simultaneous client connections	—	16
maximum number of data sets	—	68
maximum number of data attributes per data set	—	256
maximum number of virtual logical devices within an IED	—	16
maximum number of report control blocks within an IED	—	64 total buffered plus unbuffered report control block instances
maximum number of instances of a single buffered control block	—	8 (serving 8 clients)
maximum buffer size of each buffered control block	—	16k bytes **NOTE:** Refer to the description of the *Report Buffer* (after this table).
maximum number of control blocks for GOOSE publishing	—	4 control blocks

Feature	Client	Server
maximum number of GOOSE control block subscriptions	—	32 for both server/client
minimum interval of GOOSE publishing	—	20 ms
maximum number of inputs in a GOOSE data set	—	256
maximum size of GOOSE message	—	1520 bytes
time stamping resolution	—	1 ms

1. The maximum number of input words includes the sum of client and server input words.

2. The maximum number of variables depends on the data types included in the application, page 113 because the lengths of different data types varies.

3. The maximum number of output words includes the sum of client and server output words.

4. Module memory contains the most current (real-time) value for data in flow.

Report Buffer

The BMENOP0300 module reserves 16K bytes of memory in a single report buffer.

New reports are sometimes generated very quickly. At the same time, the sending of older reports may be delayed. In this case, some of the new reports overwrite (replace) the oldest reports in the buffer.

⚠WARNING

DATA OVERWRITE

Throughly test the response rates of your communications to and from the BMENOP0300 and/or BMENOP0300C module(s).

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

Configure your application to send events over a robust network in a timely manner. This helps reduce the likelihood that old, unsent events are replaced by new events in the buffer.

NOTE: Refer to the description of the buffered report control block, page 122.

Explicit Messaging Specifications

The BMENOP0300 module presents the following Modbus TCP explicit messaging features:

Feature		Capacity
Client		
	maximum number of simultaneous connections	16 connections
	maximum number of concurrent requests	16 requests
Server		
	maximum number of concurrent requests	12 requests
	maximum number of simultaneous connections	32 connections
Maximum Message Size		
	read	250 bytes (125 words) excluding header

Feature		Capacity
	write	240 bytes (120 words) excluding header

Comparing Standard Data Types: Control Expert and IEC 61850 Data Types

The following list presents IEC 61850 standard data types and the comparable data type used by Control Expert:

Control Expert Standard	Comparable IEC 61850 Standard		
Data Type	Data Type	Supported by	
		Server	Client
WORD	BITSTRING	√	√
BOOL[1]	BOOLEAN	√	√
WORD	CODED ENUM	√	√
WORD	Dbpos/Tcmd	√	√
WORD	ENUMERATED	√	√
REAL	FLOAT	√	√
INT	INT8	√	√
BYTE	INT8U	√	√
INT	INT16	√	√
UINT	INT16U	√	√
DINT	INT32	√	√
UDINT	INT32U	√	√
DINT	INT64	√	√
UDINT[2]	INT64U	√	√
Timestamp	TIME_850_FORMAT	√	√

1 In Control Expert, a BOOL occupies one BYTE.

2 UDINT is for low 32 bits and DINT for high 32 bits

BITSTRING

IEC 61850 supports trigger option, coded enum, and quality report elements in BITSTRING format. Control Expert maps BITSTRING to the WORD data type. In each of the following structures, Bit0 is the most significant bit.

Trigger option of report structure: The following bits indicate the stated trigger value when equal to 1:

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Reserved	Data-change	Quality-change	Data-update	Integrity	General-interroga-tion	0	0

Option field of report structure: The following bits indicate the stated option value when equal to 1:

MSB	Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7

	Re-served	Se-quence-number	Report-time-stamp	Reason for inclusion	Data-set-name	Data-refer-ence	Buffer-overflow	EntryID
LSB	Bit8	Bit9	Bit10	Bit11	Bit12	Bit13	Bit14	Bit15
	Conf-revision	Seg-menta-tion	–	–	–	–	–	–

Quality element structure: The following bits indicate the stated quality value when equal to 1:

MSB	Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
	Validity: 00 = good 01 = invalid 10 = reserved 11 = questionable		Overflow	Out-of-range	Bad-refer-ence	Oscillato-ry	Detec-ted failure	Old-data
LSB	Bit8	Bit9	Bit10	Bit11	Bit12	Bit13	Bit14	Bit15
	Incon-sistent	Inaccu-rate	Source: 0 = process 1 = substituted	Test	Opera-tor-blocked	–	–	–

CODED ENUM

Coded Enum definition from IEC 61850-8-1, only low byte is valid for DPS/DPC:

MSB	Reserved
LSB	0x00 = Intermediate state 0x40 = Off 0x80 = On 0xC0 = Bad-state

Coded Enum definition from IEC 61850-8-1, only low byte is valid for BSC/BAC:

MSB	Reserved
LSB	0x00 = Stop 0x40 = Lower 0x80 = Higher 0xC0 = Reserved

Dbpos/Tcmd

Dbpos (double position) definition from IEC 61850-8-1:

MSB	Reserved
LSB	0x00 = Intermediate state 0x40 = Off 0x80 = On 0xC0 = Bad-state

Tcmd definition from IEC 61850-8-1:

MSB	Reserved
LSB	0x00 = Stop 0x40 = Lower 0x80 = Higher 0xC0 = Reserved

Custom Data Types

The BMENOP0300 module also provides the following custom data types, which are used to support module DDTs, page 141:

- IED_ERT_BUF
- IED_ERT_BUF_MULTI_8(*)
- IED_ERT_BUF_MULTI_16(*)
- IED_EVT_M
- IED_EVT_Q
- IED_RPT
- IED_RPT_MULTI(*)
- TIME_850_FORMAT

(*) When multiple SOE event function is enabled.

Refer to the presentation of each custom data type elsewhere in this document for a description of its structure.

Performance Considerations

Introduction

This topic describes the factors that can influence the performance of an IEC 61850 communications module.

Response Times

A Modicon IEC 61850 module exchanges data with the controller in each controller cycle. A module that receives data from the controller/external IED stores that data in shared memory and executes the applicable configured function (report generation, GOOSE messaging and functions, etc.).

When the module is configured as an IEC 61850 server, the communication response time is a foremost consideration. The response time is the interval between the value change in the controller data and the BMENOP0300-generated event. This response time is dependent on many factors, including the answers to these questions:

- How many I/O mapping points changed during the configured cycle?
- Is the Modbus service enabled or disabled?
- How many data sets are there? Also, how many values and variables are in those data sets?
- How many buffered or unbuffered MMS report instances are required?
- Is the IEC 61850 client service enabled or disabled?

Load Guidelines

Complex applications can include thousands of configured IEC 61850 tags. This can be true even for customer applications that require stable response times and require fast execution speeds (e.g., a response time of less than 1 second).

In those cases, follow these guidelines to reduce the load on the module to optimize IEC 61850 performance:

- Set the deadband for the IEC 61850 analog points to reduce the quantity of changed data items for each controller cycle.
- When the IEC 61850 communications load is heavy, consider disabling any unused protocols (like Modbus) or reducing the number of points the protocol uses in a single module.
- You can assign the server and client functions to separate IEC 61850 communications modules to significantly increase performance. (IEC 61850 communications modules do not natively support the routing of events and commands.)
- Simplify your data model and reduce the quantity of report and GOOSE control blocks.
- Implement the general-interrogation service if the MMS report (data change or period method) does not conform to your configured response times.

  NOTE: During the system-design phase, confirm that the above factors are validated for your IEC 61850 application.

Standards and Certifications

Download

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

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

Installing the BMENOP0300 Module

Introduction

This chapter describes the installation process of the BMENOP0300 module within an M580 system.

Mounting an Ethernet Communications Module on the Modicon M580 Backplane

Introduction

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

NOTE: Fitting operations (installation, assembly, and disassembly) are described below.

Before Installing a Module

Before installing the Ethernet communications module, remove the protective cap from the module connector on the backplane.

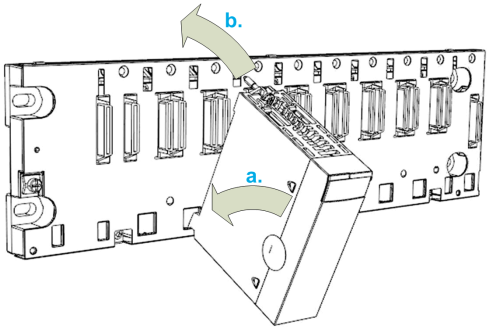
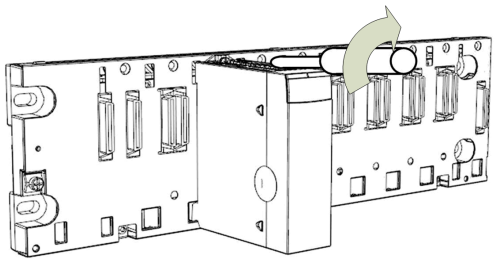
Selecting a Backplane

Install the Ethernet communications module in a single slot on a BMEXBP•••• Ethernet backplane.

Installing the Module on the Backplane

Mount the module in a single slot on the backplane:

Step	Action
1	Turn off the power supply to the system.
2	Remove the protective cover from the module interface on the backplane.

Step	Action
3	*a*: Insert the locating pins on the bottom of the module into the corresponding slots in the backplane.  *b*: Use the locating pins as a hinge and pivot the module until it is flush with the backplane. (The twin connector on the back of the module inserts into the connectors on the backplane.)
4	Tighten the retaining screw to hold the module in place on the backplane:  Tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).

Grounding Considerations

This section describes the wiring guidelines and best practices to be respected when installing and cabling the BMENOP0300 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 cables with the proper rating for your installation/ environment.

If you do not use proper, shielded 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 cables for all communication signals.
- Ground 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*.

Replacing a Module

Any Ethernet communications module on the backplane can be replaced 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.

BMENOP0300 Dual Network Redundancy

Introduction to Dual Networks

Introduction

The BMENOP0300 module supports dual network for redundancy required for high reliability communications. In this case, an interruption in communications for a port on the module is quickly addressed when another port assumes the communications functionality.

NOTE: The instructions in the following examples assume that you have already downloaded and installed the Modicon IEC61850 Configuration Tool.

Solutions

These dual-network solutions are supported through the installation and configuration of one or two network option modules:

- *one module:* The BMENOP0300 module supports multiple IP segments with unique physical interfaces, so you can use one module to support two IP segments. SCADA decides which IP segment to use as primary and secondary network. This solution does not require additional application programming because the two IP segments share one database and state machine.
- *two modules:* This solution, in which the two modules are configured within two different networks, requires additional application programming to confirm that the two modules synchronize with each other. The two modules use one dedicated elementary function block to simplify the programming process. Refer to the documentation for the IEC 61850 Configuration Tool for more information.

  NOTE: In this configuration, the module that controls communications at any given time is considered the *primary* module. This *primary* role is set by a dedicated DFB.

  Connecting more than one of the same module to both the backplane and an Ethernet network can cause a broadcast storm.

  ⚠ CAUTION

  ETHERNET BROADCAST STORM

  Do not connect more than one of the same module in a local rack to both the Ethernet backplane and an Ethernet network.

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

  You can connect one of each of the following modules to the Ethernet backplane and an Ethernet network:

  - a BME•58•0•0 controller module that manages an EIO main ring
  - a BMENOS0300 network option switch module
  - a BMENOC03•1 communication module
  - a BMENOP0300 IEC 61850 communication module

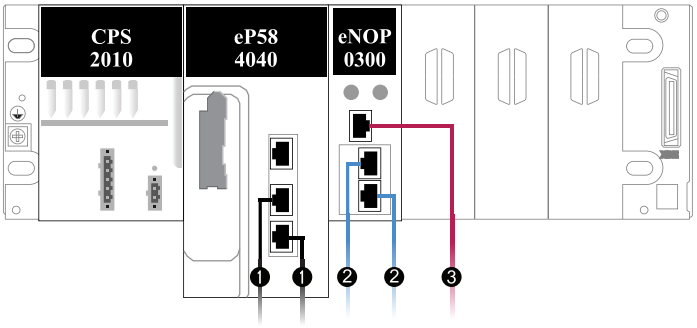
Dual Redundancy With a Single Module

Installation

Install a BMENOP0300 module on the Ethernet backplane according to the installation instructions.

Network Topology with a Single Module

This sample network uses a single BMENOP0300 module on an Ethernet backplane to achieve dual-network redundancy:



Legend:

1. The M580 PAC connects the local rack to network*1* (in this case, the main ring).
2. The ETH2 and ETH3 ports on the BMENOP0300 module connect to network segment*2*.
3. The ETH1 port on the BMENOP0300 module connects to network segment*3*.

NOTE: A more complete network that implements a single BMENOP0300 module appears in the description of the IP forwarding service.

Configuration with IP Forwarding

A single BMENOP0300 module achieves dual-network redundancy by implementing the IP forwarding service.

In this single-module configuration, enable the IP forwarding service to configure the two IP subnets that are connected to the ETH1 and ETH2 ports on the BMENOP0300 module.

In this case, a SCADA system assigns the primary and secondary roles for communications on the two network segments.

Additional application programming is not required because the two network segments share a single database and state machine.

NOTE: Refer to the detailed description of the IP forwarding service.

Dual Redundancy With Two Modules

Introduction

You can facilitate dual-network redundancy when you install and configure separate BMENOP0300 network option modules on two different IP segments. The two modules access the same IEC 61850 data model (server, client, and I/O mapping information) to support this functionality.

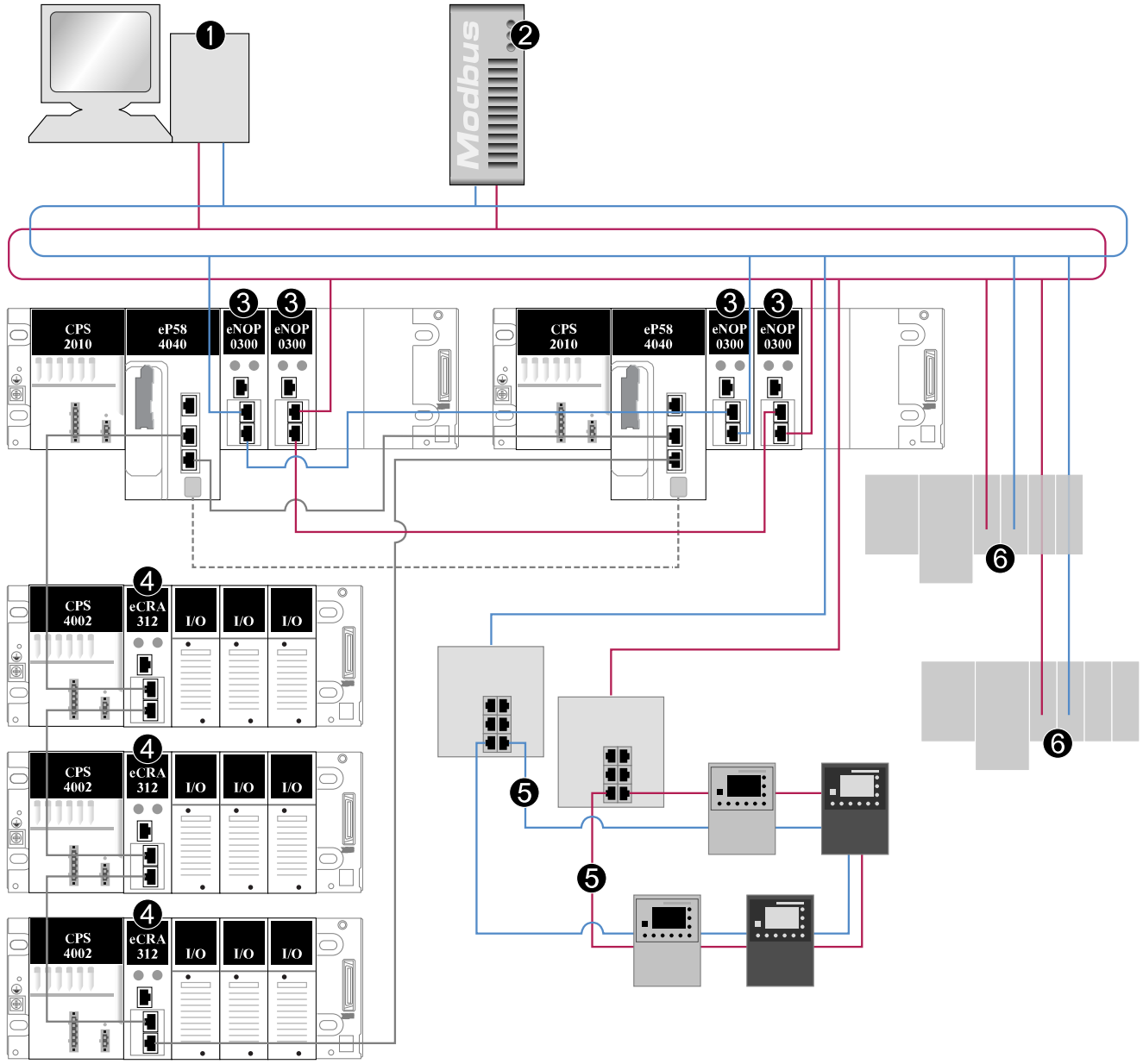
This configuration facilitates the synchronization of data between two BMENOP0300 ports or modules that perform the role of server. In this case, upstream clients or SCADA systems process only one set of data for the two servers.

NOTE:

- The configuration of *client* functionality for the BMENOP0300 is independent of the configuration for dual-network redundancy.
- The two BMENOP0300 modules synchronize with the report and control functions on the server side. They do not synchronize with GOOSE clients. Therefore do not implement this dual-network redundancy with GOOSE clients.

Sample Network

This sample network uses two BMENOP0300 modules on an Ethernet backplane to achieve redundancy for two networks (red and blue):



Legend:

1. An IEC 61850 client station (for example, SCADA) connects to both network segments.
2. A Modbus scanner scans both network segments.
3. Two BMENOP0300 modules connect to both network segments through their respective RSTP ports to facilitate link redundancy (optional).
4. BMXCRA312•0 modules connect remote I/O drops to the network.
5. IED rings connect to both network segments through network switches to facilitate communications and control by the upstream SCADA system.
6. Communications modules connect additional Ethernet backplanes to the two networks.

Configuration Process Overview

The Modicon IEC61850 Configuration Tool works in conjunction with the ST program to synchronize the data model values that are used by the two server modules. The upstream SCADA system or client, therefore, reads a single data set, not duplicate data sets.

You must understand this process to configure dual-network redundancy through a pair of BMENOP0300 modules:

1. Install two BMENOP0300 modules on a physical Ethernet backplane.
2. Add two BMENOP0300 modules (with the names *TestA* and *TestB* in this example) in Control Expert.
3. Complete the configuration for *TestA*.
4. Back up the *TestA* project file (.prj) with the IEC61850 Configuration Tool.
5. Use the IEC61850 Configuration Tool to export the dedicated DFB (two .xst files) for *TestA*.
6. Import the project file for *TestA* to *TestB*, and complete any additional configuration for *TestB* (if necessary).
7. Import the dedicated DFB (.xst) into Control Expert and define the primary and secondary roles for the two modules.
8. Rebuild the Control Expert project (**Build > Rebuild All Project**).

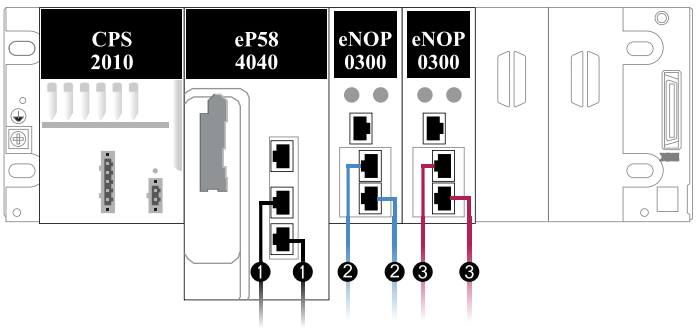
NOTE: These individual process steps are described in more detail below.

Module Assembly

Follow the directions to install two BMENOP0300 modules on an Ethernet backplane.

In the Control Expert application, add two BMENOP0300 modules to the Ethernet backplane.

For practical purposes, the examples in this document refer to the physical BMENOP0300 modules on the backplane in a left-to-right manner:



Legend:

1. The M580 PAC connects the local rack to network*1* (in this case, the main ring).
2. In the following examples, the left-hand BMENOP0300 module (**Module A**) will have the name *TestA* and is the primary communications module.
3. In the following examples, the right-hand BMENOP0300 module (**Module B**) will have the name *TestB* and is the standby communications module.

NOTE: You can easily see the correspondence between this left-to-right backplane installation and the alphabetical sequence (*TestA*, *TestB*). Schneider Electric, therefore, suggests retaining such a relationship between your real-world hardware setup and your application programming.

Module Name Mapping

Assign module names in the Control Expert application:

1. Double-click the left-hand BMENOP0300 module in the **PLC bus** (**Project > Configuration > PLC bus**).

   NOTE: This opens the **Configuration** screen for module *TestA*. Notice that the **IEC61850 Configuration** and **Update application** buttons are not active.

2. In the *Module name* field area, enter *TestA*.
3. Validate your Control Expert project.
4. Repeat these steps to assign the name *TestB* to the right-hand BMENOP0300 module in the **PLC bus**.

   NOTE: After you assign these names in the Control Expert and validate the application, the **IEC61850 Configuration** button is active on the **Configuration** screen for both modules.

IEC 61850 Configuration Mapping

IEC 61850 Mapping Overview

These individual process steps are described in more detail below. *TestA* and *TestB* are included in both your Control Expert application and your physical hardware configuration.

To prepare the system to implement dual-network redundancy, both modules require access the same IEC 61850 data model. These steps provide a conceptual view of the mapping of the IEC 61850 data model to both of these modules:

1. Create and export an IEC 61850 configuration for module *TestA*.
2. Export the IEC 61850 configuration for module *TestA* to a retrievable local folder.
3. Import the IEC 61850 configuration for module *TestA* to module *TestB*.

   NOTE: These individual process steps are described in more detail below.

Assign the Name to Module A

The left- and right-hand modules have the names *TestA* and *TestB* in the Control Expert application. Assign those same names to the modules in the IEC 61850 configuration:

1. In the Control Expert application, open the **Configuration** screen for the left-hand BMENOP0300 module in the **PLC bus** (**Project > Configuration > PLC bus**).
2. Click the **IEC61850 Configuration** button to launch the IEC61850 Configuration Tool and open the **Create Project** dialog box.
3. Click **Create New Project** and click **OK** to open the **IEC61850 Edition Selection** dialog box.
4. From the pull-down menu, select **Edition1** or **Edition2** and click **OK** to access the **General tab** for the module.

   NOTE: Both editions support dual-network redundancy.

5. In the **Server Function** area, select (click) the **Enable** checkbox to activate the **IEC61850 Server Settings** button.

6. Make a selection in the **Create IED Server** dialog box:
   - **Create an empty IED server**: In this case, click **OK** to confirm that *TestA* appears in the **IED Name** field, and click **OK** again to access the **IEC61850 Server** tab.
   - **Select an external ICD / CID file**: Drive (**...**) to find the file you want and click **OK**.
7. On the **IEC61850 Server** tab, configure the IEC 61850 server data model in accordance with your application requirements.
8. Perform these tasks in the **Export Dual Network DFB** area:
   - Confirm that *TestA* appears in the **ModuleA** field.
   - Enter *TestB* in the **ModuleB** field.

Select a Project Backup Folder

The DFB maps the names *TestA* and *TestB* to the BMENOP0300 modules in the Control Expert application after you set a destination folder for the IEC 61850 configuration files for module *TestA*. Later, you can import those files for *TestB* from the same location.

Set the project backup folder:

1. Click the **Start Page** icon in the upper-left corner of the IEC61850 Configuration Tool to open the **Application Preferences** dialog box.
2. Use the drive (**...**) button to select a destination folder with standard Windows commands, or accept the default location in the **Project Backup Folder** field.
3. In the **Global Settings** area, select (check) the **Export Excel / DFB** box to enable the export of the DFB and the ST sections.
4. Close the **Application Preferences** dialog box to return to the **IEC61850 Server** tab.

   NOTE: Modules *TestA* and *TestB* use the same data model (.prj file). This file is generated automatically and stored in the designated backup folder.

Export the IEC 61850 Configuration for Module TestA

Export the files:

1. Click the **Export DFB** button on the **IEC61850** tab to open the **Browse for Folder** dialog box.
2. Use standard Windows commands to locate and select the destination folder you identified above.
3. Click the **OK** button.
4. Save your IEC 61850 configuration and close the IEC61850 Configuration Tool.

   NOTE: Follow any prompts to save your configuration and continue.
5. Open the destination folder to confirm the creation of these new files:
   - `secondsection.xst`, `lastsection.xst`: These MAST logic sections appear almost immediately in the project backup folder when you click the **Export DFB** button.
   - TestA.prj: This file appears in the project backup folder only after you close the IEC61850 Configuration Tool.
   - **IEDCT_Backup > IEDCT_Backup > TestA_•••**: TestA.prj: The name of the folder that contains the TestA.prj file adds the module name (*TestA*) as a prefix and adds the current timestamp value as a suffix (using the YYYYMMDDHHMMSS format). For example, this is a potentially valid file name: TestA_20250225103022.

     NOTE: Using the timestamp value as a suffix to create files prevents duplicate names.

Import the IEC 61850 Configuration to TestB

You have just created an IEC 61850 data model for module *TestA*.

Now, import that data model to module *TestB*:

1. Double-click the right-hand BMENOP0300 module in the **PLC bus** (**Project > Configuration > PLC bus**) to open the **Configuration** screen for module *TestB*.
2. Click the **IEC61850 Configuration** button to launch the IEC61850 Configuration Tool and open the **Create Project** dialog box.
3. Click **Create New Project** and click **OK** to open the **IEC61850 Edition Selection** dialog box.
4. Click the **Open Project** radial button and drive (**...**) through the project backup folders until you see the IEC 61850 configuration file for *TestA* (TestA.prj).
5. Select the TestA.prj file and click the **Open** button to return to the **General** tab.
6. Close the IEC61850 Configuration Tool.

   NOTE: Follow any prompts to save your configuration and continue.
7. In the Control Expert application, click the **Update application** button on the **Configuration** screen for module *TestB*.
8. Rebuild and save your Control Expert project.

   NOTE: Every time you change the IEC 61850 protocol configuration for module *TestA*, you must re-export that information and re-import it for module *TestB*. Dual-network redundancy is maintained only when both modules share the same IEC 61850 data model.

Import the Logic Sections to Control Expert

Import the new logic sections to the Control Expert application:

1. In Control Expert, expand the MAST task logic (**Project Browser > Project > Programs > Tasks > MAST > Logic**).
2. Right-click the **Logic** folder and scroll to **Import** to open the **Import** dialog box.
3. Use standard Windows commands to drive to the location of the IEC 61850 protocol configuration files for *TestA*.
4. Select the file for the second logic section (`secondsection.xst`) and click the **Import** button to see the section appear in the **Logic** folder.
5. Repeat these steps to import the last logic section (`lastsection.xst`) file.

By default, an imported section goes to the end of the MAST logic. After you import both new ST sections, drag and drop the sections within the MAST task logic to conform to this sequence:

- `secondsection`: Place this section at the very beginning of the MAST logic.

  exception: In a Hot Standby configuration, the standby PAC executes the output values in the first logic section by default. In this case, put the *secondsection* after the Hot Standby section in the MAST logic.

  `lastsection`: Place this section at the very end of the MAST logic.

NOP_DUAL_COMM_MGR Derived Function Block

Introduction

The NOP_DUAL_COMM_MGR derived function block (DFB) is designed specifically to support dual-network redundancy in a configuration that implements two network option modules for communications.

Control Expert generates a value for the report status bits (`RPT_EN_A`, `RPT_EN_B`) in the DFB when you import the .prj file. The value of this bit identifies the primary communications module.

Server Functions

For server functionality, the primary role is managed by an upstream SCADA system. The report enable status (`RPT_EN_A`, `RPT_EN_B`) is set in the DFB or configured in the controller application.

When **Module A** and **Module B** have the same status (primary, none, reference is primary), the primary module is read from MOD_CTRL.

Client Functions

For clients, the primary role remains with the module that corresponds to the last known assignment. If that previous role assignment is not known, **Module A** executes the primary role.

Considerations

- In the dual-network redundancy configuration, **Module A** and **Module B** have their own DDT and MOD_INFO information, but they share a common IED DDT and MOD_CONTROL.
- The synchronization for the shared IED DDT is done in the controller application. It can be exported from the IEC61850 Configuration Tool.
- The DFB firmware checks the data model signature to confirm that both modules use the same IEC 61850 configuration information.
- The standby controller executes only the first section of MAST task logic to keep all data on the primary rack.

ST Section Syntax

When you export the IEC 61850 configuration files for a module, the call to the DFB appears at the beginning of this new section (`secondsection`) in the MAST logic:

Select the section in the **Logic** folder to view the content of the section:

```
(*second section with ST program*)
(*----------------------start for DFB calling----------------------*)
 NOP_DUAL_COMM_MGR_1 (ENABLE      := dual_nop_enable,
                      RPT_EN_A    := ,
                      RPT_EN_B    := ,
                      MOD_DIAG_A  := IED_A_MOD_CTRL.DualModDiag,
                      MOD_DIAG_B  := IED_B_MOD_CTRL.DualModDiag,
                      ERROR       => dual_nop_error,
                      STATUS      => dual_nop_status,
                      PRIMARY     => dual_nop_primary);
(*----------------------end for DFB calling------------------------*)

(*----------------------start for data in--------------------------*)
  IF dual_nop_primary = 1 THEN
     (*copy data out from module A to module B*)

  ELSIF dual_nop_primary = 2 THEN
     (*copy data out from module B to module A*)

  END_IF;
(*----------------------end for data in----------------------------*)
```

NOTE:

- The highlighted area at the top of the section shows the call to the NOP_DUAL_COMM_MGR_1 DFB.
- The DFB checks the health status for **Module A** and **Module B** and chooses one as a reference for time synchronization and an Entry ID.

Pin Assignment

Assign the appropriate values to the report enable pins (`RPT_EN_A`, `RPT_EN_B`):

Input	Value
`RPT_EN_A`	`TestA_MOD_INFO.SERVER_STATE.report_1.Status.0`
`RPT_EN_B`	`TestB_MOD_INFO.SERVER_STATE.report_1.Status.0`

DFB Inputs

This table describes the input parameters for the NOP_DUAL_COMM_MGR_1 derived function block:

Input	Type	Description
`ENABLE`	BOOL	*1:* The DFB is enabled for **Module A**. *0:* The DFB is disabled for **Module A**.
`RPT_EN_A`	BOOL	*1:* The report is enabled for **Module A**. *0:* The report is disabled for **Module A**.
`RPT_EN_B`	BOOL	*1:* The report is enabled for **Module B**. *0:* The report is disabled for **Module B**.
`MOD_DIAG_A`	ARRAY[0…8] OF UDINT	These inputs for **Module A** (`MOD_DIAG_A`) and **Module B** (`MOD_DIAG_B`) control the DDT instance that is generated by the IEC61850 Configuration Tool. (It was hidden in the DDT, but you can select it.)
`MOD_DIAG_B`	ARRAY[0…8] OF UDINT	

DFB Outputs

This table describes the output parameters for the NOP_DUAL_COMM_MGR_1 derived function block:

Input	Type	Description
ERROR	BOOL	*1:* The DFB detects an execution error. *0:* The DFB does not detect an execution error.
STATUS	UINT	*0:* OK (no detected errors) *1:* The IEC 61850 data model signature is mismatched. *2:* **Module A** or **Module B** is missing or not healthy. *3:* **Module A** is missing or not healthy. *4:* **Module B** is missing or not healthy. **NOTE:** When **Module A** or **Module B** is not healthy, the ERROR bit is not set.
PRIMARY	UINT	*0:* The primary role is not assigned. *1:* **Module A** is the primary communications module. *2:* **Module B** is the primary communications module.
MOD_DIAG_A	ARRAY[0…8] OF UDINT	These outputs for **Module A** (MOD_DIAG_A) and **Module B** (MOD_DIAG_B) control the DDT instances that are generated by the IEC61850 Configuration Tool.
MOD_DIAG_B	ARRAY[0…8] OF UDINT	

Configuring the BMENOP0300 Module

Introduction

This chapter shows you how to use Control Expert programming software, including the Modicon IEC 61850 Configuration Tool, to select and configure the BMENOP0300 module on the local rack.

You can download and install the IEC 61850 configuration tool package from the DVD provided or from www.se.com.

NOTE: The instructions presented in this chapter may include specific choices made for a sample project. Your Control Expert project may include different choices that are appropriate for your specific configuration.

NOTE: The device configuration procedure is valid when configuring a project by using Control Expert Classic. When you configure your device from a system project some commands are disabled in Control Expert editor. In this case you need to configure these parameters at system level by using the Topology Manager.

For more detailed information, refer to *EcoStruxure™ Control Expert, Topology Manager, User Manual*.

Creating a Project in Control Expert

Overview

This section shows you how to add modules, including the BMENOP0300 module, to your project, using Control Expert.

NOTE: For detailed information about how to use Control Expert, refer to the Control Expert online help.

Creating a Project in Control Expert

Introduction

You may have already created a project in Control Expert and installed a power supply. If so, jump to the instructions for Adding a BMENOP0300 Module, page 41. If not, the following pages show you how to create a new Control Expert project and add the following components:

- a controller
- a power supply
- a BMENOP0300 module

NOTE: Design your network so that IEC 61850 GOOSE transmissions and M580 EIO transmissions are not carried by the same media.

Creating and Saving a New Control Expert Project

The following steps describe the creation of a project in Control Expert:

Step	Action
1	Open Control Expert.
2	In the Control Expert main menu, select **File > New...**.

Step	Action
	Result: The **New Project** window opens, displaying a list of Schneider Electric controllers.
3	In the **New Project** dialog box, expand the Modicon M580 node and select both a controller, page 15 and a rack.
4	Click **OK**. **Result**: The **Project Browser** window opens.
5	To save the project, select **File > Save**. **Result**: The **Save As** dialog box opens.
6	In the **Save As** dialog box: 1. Enter a **File name** (the name of your Control Expert project). 2. Select the **.STU** or **.STA** extension in the **Save As** field. 3. Click **Save**.

Adding a Power Supply

Control Expert automatically adds a power supply to the PLC bus. If you want to replace the chosen supply:

- Click the power supply in your application and press **Delete** on your keyboard.

  — or—

- Right-click the power supply and select **Delete Module**.

Continue with the following steps to add a different power supply:

Step	Action
7	In the **Project Browser**, double-click **PLC Bus**. Control Expert displays the: • **PLC bus** dialog box with the selected controller in the second position • **Hardware Catalog** displaying the **PLC bus** tab
8	Expand the **Supply** node in the **Hardware Catalog**. Select the desired module (in this example, a 140 CPS 111 00) and drag it into the slot 1 position in the **PLC bus**.
9	Click **File > Save**. **NOTE:** Periodically save your changes as you make edits.

Adding a BMENOP0300 Module

Add a BMENOP0300 module to your project.

Step	Action
10	In Control Expert, expand the **Communication** node in the **Hardware catalog** and drag a BMENOP0300 module to any open slot in the **PLC bus**.
11	Click **File > Save**.

Configuring the Module Name

Overview

Use the **Configuration** tab of the BMENOP0300 module properties window to configure the module name.

The following steps present one example of how to configure the module name. Your own project configuration may differ.

Naming the Module

Follow these steps:

Step	Action
1	Double-click the BMENOP0300 module in the **PLC bus** window or right-click the module and select **Open Module**. **Result**: The BMENOP0300 configuration dialog opens.
2	Select the respective channel in the left pane and select the **Configuration** tab.
3	Enter a **Module name**: an ASCII string up to a maximum of 10 characters. **NOTE:** The beginning character cannot be an Arabic numeral.
4	Click the **Validate** icon in the Toolbar. **Result**: A message opens informing you that the module name cannot be edited after validation.
5	Click **OK** to close the message. **Result**: The **Module name** becomes read-only.

The maximum size of all BMENOP0300 module memory items is 8,000 words. The actual size is determined by the specific module configuration.

Refer to the topic Working with IEC 61850 Data Objects, page 111 for information about the data items automatically created by Control Expert when you click **Update application**.

Introducing the IEC 61850 Configuration Settings

Introduction

This section introduces the IEC 61850 configuration settings.

Selecting the IEC 61850 Edition

Overview

After configuring the module name and IP address settings for the module, create an IEC 61850 project, then select the IEC 61850 standard supported by your BMENOP0300 module.

Selecting the IEC 61850 Edition

To select the edition of IEC 61850 supported by your module, follow these steps:

Step	Action
1	In the **Configuration** tab, click the **IEC61850 Configuration** button. **Result**: The Modicon IEC 61850 Configuration Tool opens, displaying the **Create Project** dialog box. **NOTE:** Only one instance of the Modicon IEC 61850 Configuration Tool can be open at a time.
2	In the **Create Project** dialog box, select one of the following: • **Create New Project** • **Open Project** **NOTE:** A **Recover Project** selection appears when the Control Expert application is uploaded from the controller, but it does not have the IEC 61850 configuration. In this case, Control Expert sends the recovered project to the configuration tool, which asks you to locate a backup project to restore the module's settings. If you have not yet backed up your project, create a new project for the module.
3	If you selected **Open Project**: 1. Click the ellipsis button to display the **Open** dialog box. 2. Navigate to and select an existing project (.prj) file. 3. Click **Open**. **Result**: The selected project and path are displayed in the **Create Project** dialog box. 4. Click **OK**. **NOTE:** • Because the saved project file already contains an edition selection setting, the **IEC 61850 Edition Selection** dialog box (described below) does not appear. Instead, the **General** window opens. • If the previously saved IEC 61850 configuration cannot be found, the tool asks you to navigate to and select the IEC 61850 configuration file to open. If you do not select a saved configuration, you need to create and configure a new project.
4	If you selected **Create Project > OK**, the **IEC 61850 Edition Selection** dialog box opens.

Step	Action
5	Select the edition, or version, of the IEC 61850 protocol that applies to your module: • **Edition1** • **Edition2** **NOTE:** Use the BMENOP0300 module only in IEC 61850 networks where all devices support the same edition of the IEC 61850 protocol. The IEC 61850 configurator editions support the following schema versions: • Edition1: supports schema V1.6 • Edition2: supports schema V3.1
6	Click **OK**. **Result**: The **General** window opens.

NOTE: When Control Expert displays IEC 61850 configuration settings, it presents one of the following collections of module data:

- For a new IEC 61850 project, the **General** window displays default settings.
- For a project created using an existing IEC 61850 project file, the **General** window displays the saved configuration settings.

Using the Modicon IEC 61850 Configuration Tool

Introduction

The IEC 61850 configuration interface in Control Expert is the exclusive tool for configuring IEC 61850-based properties of the BMENOP0300 module.

Use the Modicon IEC 61850 Configuration Tool to perform the following tasks:

- Configure the BMENOP0300 module as an IEC 61850 server or client
- Configure the IP address settings for the module
- Configure Ethernet services for the module, including:
  - RSTP
  - SNTP
  - SNMP
  - Security
  - Switch settings (baud rates for the Ethernet ports)
  - Syslog

Workbench

The workbench is the parent window of the IEC 61850 interface. It presents:

- the toolbar
- one or more configuration windows, each on its own tab

Toolbar

The configuration toolbar has the following functions:

Icon / Name	Description
Save	Saves edits made to configuration settings. **NOTE:** If you have configured a project backup folder, a copy of the IEC 61850 configuration is saved to that location.
Validate	Performs a validation check of the configuration. **NOTE:** If one or more configuration errors are detected, a message opens describing one of the detected errors. Click this button after each configuration error is fixed, until the message indicates no detected errors.
Undo	Reverses the previous edit.
Redo	Repeats a text edit that was reversed via the **Undo** command.
Cut	Removes and saves selected text.
Copy	Copies selected text.
Paste	Inserts text that was cut or copied.
Full Screen	Toggles the size of the Modicon IEC 61850 Configuration Tool: normal size or full screen.

Saving and Backing Up your IEC 61850 Project

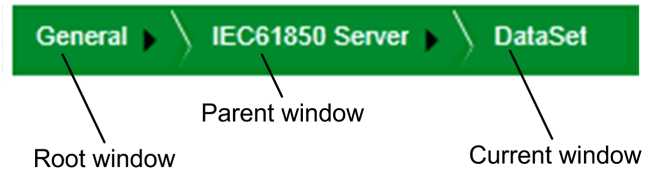
When you identify a project backup folder, a copy of the project file is saved to the specified location each time you click **Save**.

To specify a project folder, follow these steps:

Step	Action
1	In the upper left corner of the configuration tool, click the  icon. **Result**: The **Application Preferences** page opens.
2	In the **Global Settings** area, confirm the selection of **Save Project with Optimization**. This option removes unused data objects from all Logic Node Types and applies that memory to the module, thereby reducing the size of the configuration file that is sent to the module firmware but increasing the project-saving time.
3	Click the ellipsis button (...) to open **Browse For Folder** window.
4	Navigate to and select the folder where you want to store project backup files, then click **OK**.
3	Close the **Application Preferences** page.

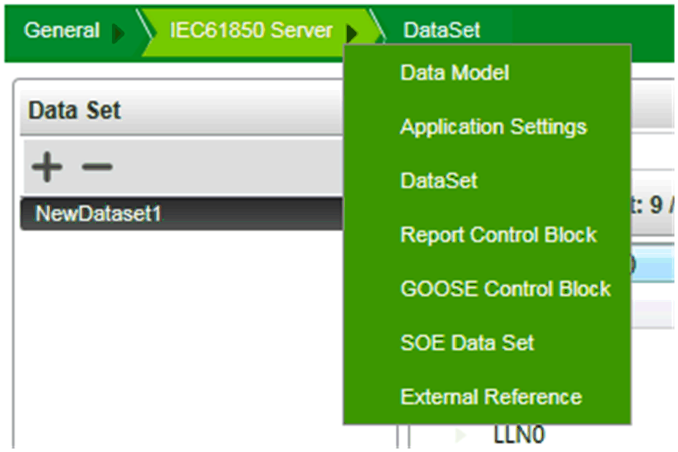
Breadcrumb Navigation

A *breadcrumb* navigation bar sits at the top of each tab, and describes the path to the displayed page, starting with the **General** window:



Click a *breadcrumb* item to move to that window.

You can also click a *breadcrumb* item to display a context menu containing the available child windows. For example, right-click on the black arrow in the **IEC 61850 Server** *breadcrumb* item to display the following menu:



Click the name of a child window to open it.

Exiting the Modicon IEC 61850 Configuration Tool

When you close the Modicon IEC 61850 Configuration Tool and Control Expert, it continues to run in the background on your PC.

To exit the Modicon IEC 61850 Configuration Tool, follow these steps:

Step	Action
1	Click the close button (with the red “x”) at the upper right corner of the Modicon IEC 61850 Configuration Tool.
2	In the **Confirm** dialog box, indicate if you want to save data before closing (Yes or No).

General Window

Introduction

After you select an IEC 61850 edition, the **General** window opens when you start up the Modicon IEC 61850 Configuration Tool.

Use the **General** window to:

- Edit module information.
- Select the Ethernet port used for GOOSE publication.
- Enable and disable the embedded IEC 61850 server.
- Enable and disable the embedded IEC 61850 client.
- Open the following windows where you can continue to configure BMENOP0300 module functions:
  - communication settings
  - server settings
  - client settings

Editing Module Information

Use the **Module Information** section to edit the name of the module, and to view settings that describe the module commercial reference and protocol edition.

The **Module Information** section presents the following settings and commands:

Setting	Description
Module Name	A read-only string of ASCII characters. This value is entered in the module **Configuration** tab when the module is added to the Control Expert project., page 41 **NOTE:** Control Expert uses this setting as the base string for naming module variables.
IEC 61850 Edition	A previously selected, page 43, read-only description of the edition of the IEC 61850 protocol supported by the BMENOP0300 module
Reference	The read-only commercial reference, or product name, for the BMENOP0300 module.
PDU Size	The size of the manufacturing message specification (MMS) protocol data unit (PDU), from 4K bytes to 64K bytes. Default = 16K bytes.
Communication Settings, page 50 button	Opens the **Communication Settings** window, which consists of the following tabs: • **IP Setting**, where you can assign roles and IP addresses to the four Ethernet ports of the module. • **RSTP**, where you can enter settings to configure the embedded Ethernet switch to be part of a redundant, loop-free logical Ethernet network. • **SNTP**, where you can configure the internal clock of the module to synchronize with a network time server. • **SNMP**, where you can configure the SNMP client service in the module that allows access to module diagnostic and management information. • **Security**, where you can restrict access to the module via TCP port 502. • **Switch**, where you can set baud rates for the four Ethernet ports. • **Syslog**, where you can log security events

Selecting GOOSE Publication Port

Use the **Goose Publish** area to specify the Ethernet port or ports used to transmit GOOSE control blocks.

The **Goose Publish** area presents the following settings:

Setting	Description
Ethernet Port	Select the port used for GOOSE publication: • ETH Port 1 • ETH Port 2&3 **NOTE:** GOOSE publication occurs if the Ethernet cable to the selected port is connected or disconnected. GOOSE diagnostic codes, page 169 are unaffected by the cable being connected or disconnected to the port.
Auto Enable	Indicate if a GOOSE transmission is sent on start-up or re-start: • Selected: A GOOSE transmission is enabled. • De-selected: A GOOSE transmission is not enabled.

Enabling and Disabling the IEC 61850 Server

Use the controls in the **Server Function** section to enable and disable the IEC 61850 server.

The **Server Function** section presents the following settings:

Setting	Description
Enable IEC 61850 Server	• Select the check box to enable the IEC 61850 server. • De-select the check box to disable the server (default). **NOTE:** • When this setting is selected, the **IEC 61850 Server Settings** button is enabled. • If you enable and configure the IEC 61850 server; and then disable the server, your server configuration settings are saved. The saved server settings are re-applied when you later select this setting and enable the server.
IEC 61850 Server Settings button	Opens the **Server Settings** window, where you can complete the configuration of server settings. **NOTE:** This button is enabled only when **Enable IEC 61850 Client** is selected.

NOTE: Enabling the server does not complete the server configuration. After enabling the server, click the **IEC 61850 Server Settings** button to open the **IEC 61850 Server** window where you can complete the server configuration.

Enabling and Disabling the IEC 61850 Client

Use the controls in the **Client Function** section to enable and disable the IEC 61850 client.

The **Client Function** section presents the following settings:

Setting	Description
Enable IEC 61850 Client	• Select the check box to enable the IEC 61850 client. • De-select the check box to disable the IEC 61850 client (default). **NOTE:** When this setting is: • Selected: The **IEC 61850 Client Settings** button is enabled. • De-selected: All previously configured client configuration settings for this module are permanently deleted.
IEC 61850 Client Settings button	Opens the **Client Settings** window, where you can complete the configuration of client settings. **NOTE:** This button is enabled only when **Enable IEC 61850 Client** is selected.

Configuring IP Addresses

Introduction

This section shows you how to assign an IP address to each Ethernet port on the BMENOP0300 module.

Assigning Roles and IP Addresses to Ethernet Ports

Introduction

Use the **Communication Settings > IP Setting** tab to assign roles and IP address settings to the three ports of the BMENOP0300 module.

After changing any IP address setting in this tab, click **Apply** to confirm and retain your edits before clicking another **Communication Settings** tab. Alternatively, you can click **Cancel** to delete your edits on the current tab and restore the previous setting.

Port Roles

The BMENOP0300 module includes three Ethernet ports and supports three different IP interfaces. These ports can be configured as the following port types:

Type	Description	Available		
		Port 1 (ETH 1)	Ports 2/ 3 (ETH 2/3)	Back-plane Port
Access Port	Diagnostic information is available via explicit messaging (Modbus) or via SNMP. **NOTE:** A port set to Access Port type uses the IP address of the network that is set for Ports 2/3.	√	√	√
Extended Network	You can extend the device network by adding another network to this port.	√	√	√
Port Mirroring	You can connect to this port via a PC and use packet sniffing software to analyze the traffic traveling through one or more of the other module ports.	√	–	–
Dedicated Network Ports	Ports 2 and 3 (ETH 2 and ETH 3) share a single IP address and are dedicated connections. **NOTE:** Ports 2 and 3 (ETH 2 and ETH 3) support RSTP, page 57.	–	√	–
√ The port type is available for this port. – The port type is not available for this port.				

The module includes an IP forwarding service that handles and forwards packets among the three IP interfaces.

Ethernet Frames

The BMENOP0300 module supports the Ethernet II frame type. The module supports the IEEE 802.3 frame type only for RSTP.

Assigning IP Address Settings

All IP addresses settings need to be manually assigned in this window as part of module configuration.

The **IP Setting** tab presents separate configuration areas for Port 1, Port 2/3, and the Ethernet Backplane Port. To configure each port, enter values for the following settings.

The BMENOP0300 module supports IP V4 only.

Setting	Description
Type	Select the role to assign to the port. Selections include: • Port 1: ◦ Access Port ◦ Port Mirroring ◦ Extended Network • Ports 2/3: Please configure IP settings of Ports 2/3 in Control Expert. • Backplane Port ◦ Access Port
IP	A 32-bit IP address assigned to the port, including both network and host components.
Sub-Network Mask	A 32-bit value used to mask the network portion of the IP address and reveal the host address.
Default Gateway	For ports 2/3, the IP address of the IP forwarding service that is the access point to a remote network. **NOTE:** 0.0.0.0 is a valid setting.

NOTE:

- If the IP address for a port is not configured, the BMENOP0300 modules automatically assign that port a MAC address-based IP address, page 52.
- If the IP address for a port is not valid (for example, a malformed or duplicate IP address), the module LEDs indicate the invalid IP address status.

Configuring Port Mirroring

You can configure **Port 1** (ETH 1) to serve as a mirroring port. A copy of Ethernet packets traveling through other selected ports is sent to **Port 1**, where you can use a packet sniffer to monitor and analyze network traffic.

When port mirroring is enabled, **Port 1** becomes a read-only port. There is no access to network devices via this port while port mirroring remains enabled.

To configure **Port 1** (ETH 1) for port mirroring, follow these steps:

Step	Action	
1	In the **Port 1** area, select **Port Mirroring** as the port **Type**. The check boxes at the bottom of the **Port 1** area are enabled.	
2	Select the ports whose traffic is mirrored and sent to **Port 1**:	
	Enable Internal Port	Select this to send a copy of traffic passing through the internal port (between the module's IP forwarding service and the CPU) to **Port 1**.
	Enable ETH 2	Select this to send a copy of traffic passing through **Port 2** (ETH 2) to **Port 1**.
	Enable ETH 3	Select this to send a copy of traffic passing through **Port 3** (ETH 3) to **Port 1**.
	Enable Backplane Port	Select this to send a copy of traffic passing through the backplane port to **Port 1**.

Step	Action
3	Click **Apply** to confirm your edits.
4	Click **Save** to save your edits.

Determining Port Default IP Addresses

If one or more Ethernet ports on the BMENOP0300 module are not manually assigned an IP address, the module automatically assigns default IP addresses that are based on the MAC address, as follows:

- When IP forwarding is disabled:
  - 10.10.xxx.yyy
- When IP forwarding is enabled:
  - 169.254.10.yyy for ETH_2 and ETH_3
  - 169.254.30.yyy for ETH_1

Where:

- 'xxx' represents the fifth octet of the module MAC address.
- 'yyy' represents the sixth octet of the module MAC address.

However, if the sixth octet of the module MAC address is 0xff or 0x00, 'yyy' is reset to 0xfe (254) to avoid the generation of an invalid IP address.

Configuring the IP Forwarding Service

Introduction

The BMENOP0300 module includes an IP forwarding service. The IP forwarding service provides transparency between networks in a PlantStruxure system and can route packets among a maximum of two subnetworks that each has its own distinct broadcast domain.

The IP forwarding service is supported by the following versions:

- BMENOP0300 as of firmware version 2.0
- Modicon IEC 61850 Configuration Tool as of version 3.0

NOTE: The maximum throughput for the BMENOP0300 module that uses the IP forwarding service is 1,350 packets per second.

NOTE: Only one of the following functions can be enabled at the same time: the IPsec protocol, page 62, the Ethernet backplane port, or the IP Forwarding service.

Use the configuration tool to configure the IP forwarding service by assigning unique IP address parameters (including the IP address and subnetwork mask) for the BMENOP0300 module.

You can also identify the default gateway for the BMENOP0300 module. (Refer to the description of the role of the default gateway, page 51.)

NOTE: The default gateway is the IP address of the control network router. Usually this router is a device that connects the control network to other networks higher up in the Ethernet infrastructure.

Displaying the IP Forwarding Service Parameters

To display the **IP Forwarding** page and access the parameters:

Step	Action
1	Click the **IP Setting** tab in the navigation tree in the left panel of the **Device Editor**. **Result**: The **Services** page opens.
2	In the **IP Setting** page, set the **IP Forwarding** field to **Enabled**. Then click **Apply**. **Result**: The **IP Forwarding** service appears in the navigation tree.
3	Click **IP Forwarding** in the navigation tree.
4	Enter IP addressing parameters for the **IP Forwarding** service.
5	Click **Apply** to save changes and leave the window open, or click **OK** to save changes and close the window.

Configuring the IP Forwarding Service

When configuring the IP forwarding service, how IPsec and the Ethernet backplane are defined affects the use of the IP forwarding service.

#	IPsec	Ethernet Backplane	IP Forwarding Service
1	enabled by user **NOTE**: A window displays in the configuration tool: When IPsec is enabled, the Ethernet backplane port and the IP Forwarding service are disabled automatically.	disabled (grayed, cannot be enabled)	disabled (grayed, cannot be enabled)
2	disabled by user	no change (not grayed, can be enabled)	no change (not grayed, can be enabled)
3	disabled (grayed, cannot be enabled)	disabled (grayed, cannot be enabled)	enabled by user **NOTE**: A window displays in the configuration tool: When the IP Forwarding service is enabled, the IPsec and Ethernet backplane port are disabled automatically.
4	no change (not grayed, can be enabled)	no change (not grayed, can be enabled)	disabled by user
5	no change (not grayed, can be enabled)	enabled by user	no change (not grayed, can be enabled)

Network Transparency via IP Forwarding Using One BMENOP0300 Module

Introduction to Transparency

You can segregate a network into multiple subnetworks to limit user access and increase performance. This usually means that devices in different subnetworks are not able to communicate directly.

You can, however, use the IP forwarding functionality, page 52 to enable Ethernet network transparency to facilitate seamless communications between devices in different subnetworks. This topic describes an example of IP forwarding supported by the BMENOP0300 module.

Before You Begin

Before you start this example, change your Control Expert configuration to facilitate the use of the IP forwarding service:

Step	Action
1	Enable the IP forwarding service, page 52.
2	Configure the service port (ETH1), page 50 as an extended network port.

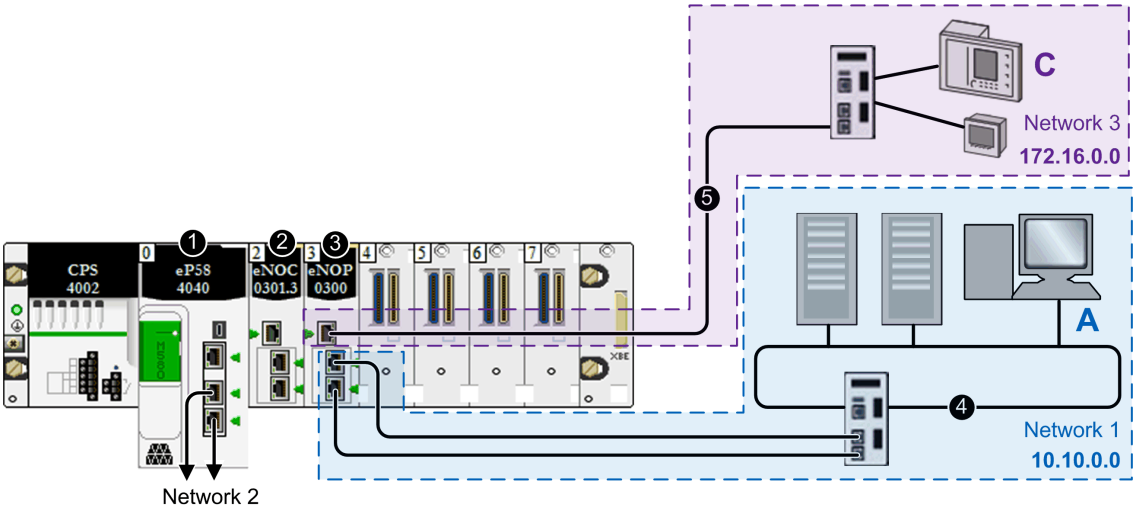
IP Forwarding Example

Suppose you want to provide transparency between two networks:

- On network 1, with the network address of 10.10.0.0, host A (a PC) uses the IP address 10.10.0.1.
- On network 3, with the network address 172.16.0.0, host C (an IED) uses the IP address 172.16.0.1.

To facilitate communications between hosts A and C, connect the networks 1 and 3 both physically and logically. The IP forwarding service in the BMENOP0300 module is the interface for these network connections.

In the following sample architecture, the IP forwarding service in the BMENOP0300 module provides transparency between these two networks. Host A in subnetwork 10.10.0.0 (blue) can communicate with host C in subnet 172.16.0.0 (purple) because the BMENOP0300 module is configured with an IP address in each of the two networks.



1 A BME•58•••• controller connects the local rack to the main ring.

2 A BMENOP0300 Ethernet communication module is connected to the controller over the Ethernet backplane (and is therefore on the same network at the controller).

3 The IP forwarding service of the BMENOP0300 Ethernet communication module has IP addresses in two subnetworks: network 1 (10.10.0.0) and network 3 (172.16.0.0).

4 Network 1, in subnetwork 10.10.0.0, includes a PC (host A).

5 Network 3, in subnetwork 172.16.0.0, includes IEDs.

In this example, the IP forwarding service of the BMENOP0300 module has two interfaces with different IP addresses in two subnetworks:

Network	IP Forwarding Service			
	IP Address	Sub-Network Mask	Network Address	Ethernet Interface
network 1	10.10.0.1	255.255.0.0	10.10.0.0	ETH 2, ETH 3
network 3	172.16.0.1	255.255.0.0	172.16.0.0	ETH 1

Now that you have established the IP forwarding service, add the IP address forwarding information to the PC (host A), the IEDs (host C), which allows the hosts to send packets beyond their own subnetworks by utilizing the IP forwarding service of the BMENOP0300 module.

- Configure the IEDs (host C) to forward all traffic that is destined for outside its subnetwork to the BMENOP0300 module. That is, confirm that all traffic for networks other than 172.16.0.0 is forwarded to the appropriate interface of the BMENOP0300 module.
- Also configure the PC (host A) in a similar way. However, in a PC environment, it is possible to configure distinct rules about communications. To facilitate communications between the example PC in the network 1 and the devices in network 3, set the IP address of the BMENOP0300 module in network 1 as the route for traffic that is destined for network 3.

  NOTE: The connections of network 1 and network 3 to the BMENOP0300 module, could be swapped, depending on which network requires the RSTP protocol.

Network Transparency via IP Forwarding Using Multiple BMENOP0300 Modules

IP Forwarding Example

You can enable IP forwarding in an M580 system with multiple BMENOP0300 modules.

- On network 1 (control network), with the network address of 192.168.1.0/24, the PC (SCADA) configures the following IP addresses in each of the three BMENOP0300 modules:.
  - NOP 1 (ETH1): 192.168.1.1
  - NOP 2 (ETH2): 192.168.1.2
  - NOP 3 (ETH3): 192.168.1.3

Set a Static Route

The PC (host A) resides in network 1, and can communicate with each of the BMENOP0300 modules in the local rack via the module's network 1 IP address. For the PC to communicate with devices in networks 2, 3, and 4, set the IP address of each respective BMENOP0300 module in each respective network (2, 3, and 4) as the route for traffic.

- For the PC (A) to communicate with intelligent electronic devices (IEDs) in network 2, add a static route to the PC:

  ```
  c:\route ADD 192.168.2.0 mask 255.255.255.0 192.168.1.1
  ```

  - 192.168.2.0 is network 2.
  - 192.168.1.1 is the IP address of the BMENOP0300 module in network 2.
- For the PC (A) to communicate with IEDs in network 3, add a static route to the PC:

  c:\route ADD 192.168.3.0 mask 255.255.255.0 192.168.1.2

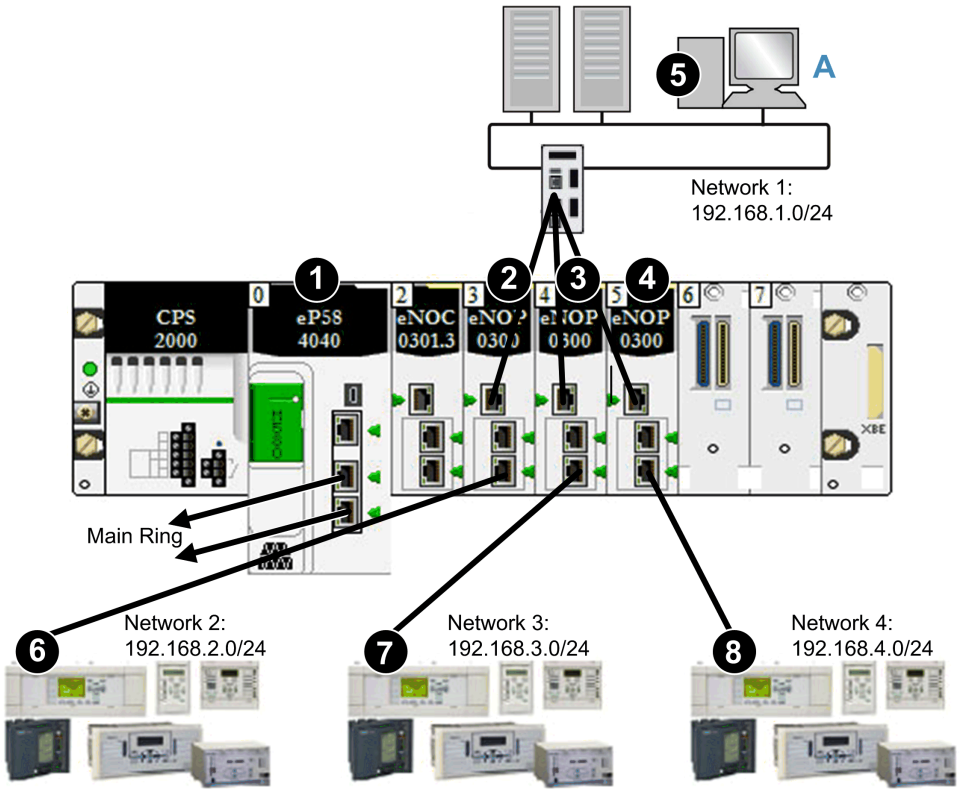
  - 192.168.3.0 is network 3.
  - 192.168.1.2 is the IP address of the BMENOP0300 module in network 3.
- For the PC (A) to communicate with IEDs in network 4, add a static route to the PC:

  c:\route ADD 192.168.4.0 mask 255.255.255.0 192.168.1.3

  - 192.168.4.0 is network 4.
  - 192.168.1.3 is the IP address of the BMENOP0300 module in network 4.

On each of networks 2, 3, and 4, each IED configures the direct connection to each BMENOP0300 module's IP address as its gateway.

Network	NOP IP Address (ETH2/3)	IED IP Address	IED Gateway IP Address
2	192.168.2.1/24	192.168.2.2/24 – 192.168.2.254/24	192.168.2.1
3	192.168.3.1/24	192.168.3.2/24 – 192.168.2.254/24	192.168.3.1
4	192.168.4.1/24	192.168.4.2/24 – 192.168.2.254/24	192.168.4.1



1 A BME•58•••• CPU connects the local rack to the main ring.

2 A BMENOP0300 module is connected to: **A)** the control network (network 1) via port ETH1 and **6)** network 2 via port ETH3.

3 A BMENOP0300 module is connected to: **A)** the control network (network 1) via port ETH1 and **7)** network 3 via port ETH3.

4 A BMENOP0300 module is connected to: **A)** the control network (network 1) via port ETH1 and **8)** network 4 via port ETH3.

5 On network 1 (control network), with the network address of 192.168.1.0, a PC uses the IP address 192.168.1.0/24.

6 network 2 with the address 192.168.2.0/24

7 network 3 with the address 192.168.3.0/24

8 network 4 with the address 192.168.4.0/24

Ethernet Services

Overview

This section describes the Ethernet services supported by the BMENOP0300 module.

Configuring the Rapid Spanning Tree Protocol

Introducing RSTP

Ethernet ports 2 and 3, located on the front of the BMENOP0300 module, support the *Rapid Spanning Tree Protocol* (RSTP). RSTP is an OSI layer 2 protocol defined by IEEE 802.1D 2004. RSTP performs two services:

- Creates a loop-free logical network path for Ethernet devices that are part of a topology that includes redundant physical paths.
- Automatically restores network communication, by activating redundant links, in the event the network experiences an interruption of service.

  NOTE: RSTP can take up to 50 ms to restore network communication in case of a service interruption. During this time, Ethernet packets may be dropped.

RSTP software, operating simultaneously in all network switches, obtains information from each switch, which enables the software to create a hierarchical logical network topology. RSTP is a flexible protocol that can be implemented on many physical topologies, including ring, mesh, or a combination of ring and mesh.

Use the **RSTP** tab of the **Communication Settings** window to configure RSTP for the embedded Ethernet switch in the BMENOP0300 module. After you make your selection, click **Apply** to preserve your edit.

NOTE: RSTP can be implemented only when all network switches are configured to support RSTP.

Configuring RSTP Settings

The following setting can be viewed and edited in the **Communication Settings > RSTP** tab:

Setting	Description
RSTP Operational State: Bridge Priority	Select one of the following RSTP roles for the module: • Root (0) • Backup Root (4096) • Participant (32768) (default) **NOTE:** Network switches running RSTP software periodically exchange information about themselves using special packets called Bridge Protocol Data Units (BPDUs), which act as a heartbeat. The Bridge Priority value is contained in the BPDU and establishes the relative position of the switch in the RSTP hierarchy.

Configuring Time Synchronization

Introduction

The simple network time protocol (SNTP) synchronizes the clock in the BMENOP0300 module to that of the network time server. Typical time service

configurations utilize redundant servers and diverse network paths to achieve high accuracy and reliability.

Use the time service for:

- recording events (sequence events)
- synchronizing events (trigger simultaneous events)

Time Synchronization Service Features

Features of the time synchronization service include:

- periodic time correction obtained from the reference-standard time server
- automatic switch-over to a backup time server if communication with the primary time server is interrupted
- availability of a function block for application programs that can read the accurate clock, and let project events or variables be time stamped
- configurable local time zone, including daylight savings time

  NOTE: Broadcast frames for clock synchronization are not supported.

Time Synchronization Process

The NTP client sends requests to the NTP server in the network to get the reference time for synchronizing the local time of the Ethernet communication module:

Stage	Description
1	Through an Ethernet network, an NTP client requests a time synchronization signal from an NTP server.
2	The NTP client calculates the correct time and stores the value.

On an Ethernet network, confirm that all controllers are synchronized with the same NTP server.

Power Up

To establish the accurate Ethernet system network time, the system performs the following at power-up:

- The BMENOP0300 module powers up.
- The BMENOP0300 module obtains the time from the NTP server.
- The service requires the requests to be sent periodically to obtain and maintain accurate time. Your **Polling Period** configuration partially determines the accuracy of the time.

After the accurate time is received, the service sets the status in the associated time service diagnostic.

The time service clock value starts at 0 until fully updated from the BMENOP0300 module.

Model	Starting date
Modicon M580 with Control Expert	January 1st 1970 00:00:00.00

Stop or Run the Controller

- Stop and run have no effect on the accuracy of the clock.
- Stop and run have no effect on the update of the clock.

- A transition from one operating mode to another has no effect on the accuracy of the Ethernet system network time.

Download Application

The status clock value associated with the time service register in the controller is re-initialized after an application is downloaded or after an SNTP server swap.

There will be two polling periods before the time is accurate.

Time Synchronization Configuration Settings

The **Communication Settings > SNTP** tab presents the following configuration settings:

Setting	Action
NTP Server Configuration:	
Primary NTP Server IP Address	Enter a valid IP address.
Secondary NTP Server IP Address	Enter a valid IP address.
Polling Period	The polling period is the time (in seconds) between updates from the SNTP server. To obtain optimal accuracy (and if your network allows), reduce the polling period to a small value. The default is 5 seconds. Valid values include: • minimum = 1 s • maximum = 120 s
Time Zone:	
Time Zone	Select the desired time zone from the drop-down list. The default value is your current system time zone (as found in Windows). You can also select **Custom Time Zone**.
Time Zone Offset	If you select **Custom Time Zone**, enter a value in the range of (24 hours * 60 minutes - 1) [1-minute step].
Daylight Saving:	
Automatically adjust clock for daylight saving change	• **De-select** (default): If you **do not** want the clock to automatically adjust for daylight saving, do not select the check box. In the **Start Daylight Saving** and **End Daylight Saving** fields, enter the month, day of week, and occurrence range from the respective drop-down lists. • **Select**: If you **do** want the BMENOP0300 module to automatically adjust for daylight saving, select the check box. The **Start Daylight Saving** and **End Daylight Saving** fields are disabled because their times are automatically changed in the spring and fall every year.
Start Daylight Saving	If you do not select the automatic daylight saving check box, select values for: • **Month**: January to December • **Day of Week**: Sunday to Saturday • **Occurrence**: 1 to 5 • **Hour**: 0 to 23
End Daylight Saving	If you do not select the automatic daylight saving check box, select values for: • **Month**: January to December • **Day of Week**: Sunday to Saturday • **Occurrence**: 1 to 5 • **Hour**: 0 to 23

Setting	Action
CPU Time Update:	
Update CPU time with this module	• **Select**: Update the controller clock with the time from the module. • **De-select**: Do not update the controller clock with the module time. **NOTE:** Use only one BMENOP0300 module to update the controller time.

When you finish editing time synchronization configuration settings, click **Apply** to save your edits.

NOTE: when SNTP is deactivated, the BMENOP module receives a time signal from the controller. Make sure you use the same time zone and daylight saving time settings as the controller.

Configuring the SNMP Agent

Description

The BMENOP0300 module includes an SNMP v1 agent. An SNMP agent is a software component running on the BMENOP0300 module that allows access to the module diagnostic and management information via the SNMP service. The SNMP tab is disabled by default in the Modicon IEC 61850 configuration tool.

SNMP browsers, network management software, and other tools typically use SNMP to access this data. In addition, the SNMP agent can be configured with a maximum of two IP addresses, typically from PCs running network management software, to be the target of event driven trap messages. These trap messages inform the management device of events such as cold start and unauthorized access.

Use the **Communication Settings > SNMP** tab to configure the SNMP agent in the BMENOP0300 module.

The SNMP agent can connect to and communicate with up to 2 SNMP managers as part of an SNMP service. The diagnostic information provided by the SNMP service is Standard SNMP MIB 2.

Viewing and Configuring SNMP Properties

The following settings can be viewed and edited in the **Communication Settings > SNMP** tab:

Setting	Description
IP Address Managers:	
IP Address Manager 1	The IP address of the first SNMP manager to which the SNMP agent sends notices of traps. Default IP address: 0.0.0.0
IP Address Manager 2	The IP address of the second SNMP manager to which the SNMP agent sends notices of traps. Default IP address: 0.0.0.0
Agent:	
Location	The device location (32 characters maximum)
Contact	Information describing the person to contact for device maintenance (32 characters maximum)
SNMP Manager	If this is: • **Selected**: the Location and Contact information **are not** editable • **De-selected**: Location and Contact settings **are** editable
Community Names:	

Setting	Description
Get	Password required by the SNMP agent before executing read commands from an SNMP manager (default = **public**).
Set	Password required by the SNMP agent before executing write commands from an SNMP manager (default = **private**).
Trap	Password that an SNMP manager requires from the SNMP agent before the manager accepts trap notices from the agent (default = **alert**).

When you finish editing SNMP property settings, click **Apply** to preserve your edits.

NOTE: The sysName SNMP parameter is not editable or visible in the Modicon IEC 61850 Configuration Tool. By default, sysName is set to BMENOP0300.

Security

Restricting Access to the BMENOP0300 Module

Using the Modicon IEC 61850 Configuration Tool, you can open **Communication Settings > Security** tab and restrict access to the module by:

- disabling the module FTP service
- disabling the module SNMP service
- disabling the module IPsec service
- specifying the Ethernet devices that may make TCP port 502 connections with the module

Enabling and Disabling the FTP, SNMP, and IPsec Services

The BMENOP0300 module uses the FTP service to support firmware upgrades, and uses the SNMP service to provide access to diagnostic information for the module.

You can enable and disable these services using the Modicon IEC 61850 Configuration Tool in the **Security** tab of the **Communication Settings** window:

- Select **Enable FTP** to enable the FTP service. De-select it to disable the service.
- Select **Enable SNMP** to enable the SNMP service. De-select it to disable the service.
- Select the **Enable IPsec** check box to enable the IPsec service. Then, enter a 16-ASCII-character string in the **Pre-Shared Key** field. De-select the Enable the **Enable IPsec** check box to disable the service.

When you finish editing the services, click **Apply** to preserve your edits.

Configuring Access Control

You can also use the **Security** tab of the **Communication Settings** window to specify the Ethernet devices that may make FTP, Port 502, and IEC 61850 connections with the module, in its role as server. When you select **Access Control**, add the IP addresses of the devices that may open a connection with the module.

When you enable access control, consider adding the following devices to the list of **Authorized Addresses and Subnet mask** so that they may communicate with the module:

- any client device that may send a request to the BMENOP0300 module, in its role as IEC 61850 Server

- your own maintenance PC so that you can communicate with the PLC via Control Expert to configure and diagnose your application
- any target device to which the BMENOP0300 module may be accessed

Adding and Removing Devices in the Authorized Address List

To add a device to the **Authorized Addresses** list:

Step	Description
1	In the **Access Control** area, select the **Access Control** check box.
2	In the **Access Control** editable table, select an empty field in the **IP Address** column and enter the appropriate IP address.
3	Enter the respective subnet mask address for each IP address in the **Subnet mask** column.
4	For each IP address you add, select **Yes** or **No** in the Subnet column.
5	For each of the IP addresses you entered: • **Select** the check box for each parameter to enable that functionality. • **De-select** the check box for each parameter to disable that functionality. Parameters: • FTP • Port 502 • IEC 61850 Server • SNMP
6	Repeat steps 2 through 5, for each additional device to which you want to grant access to the BMENOP0300 module. **NOTE:** Add an IP address only once. Duplicate IP addresses are not allowed.
7	When you finish making access control edits, click **Apply** to save your edits.

NOTE: You can authorize access control for a maximum of 128 devices.

Configuring IP Secure Communications

Introduction to IPsec

The Internet Engineering Task Force (IETF) developed and designed Internet Protocol Security (IPsec) as an open set of protocol standards that make IP communication sessions private and secure. The IPsec functionality of the BMENOP0300 module supports the data integrity and origin authentication of IP packets.

Follow the steps below to create a specific IPsec configuration on a Windows 7 PC. For more information about IPsec, refer to the Internet Engineering Task Force website (www.IETF.org).

Client-initiated communications are not supported from the BMENOP0300 module when IPsec is enabled. For example, peer-to-peer (BMENOP0300-to-BMENOP0300) communications are not supported when IPsec is enabled.

NOTE: You cannot enable the IPsec protocol and the IP Forwarding service at the same time. (You cannot build a Control Expert project when both are enabled. Refer to the table for using different services and protocols.)

Process Overview

Configure IPsec communications in these stages:

Stage	Name	Description
1	Policy	Create an IPsec policy, page 63.
2	Rule	**Tunnel Endpoint**: no tunnel (transport mode), page 64
		Connection type: network connections or local area network, page 64
		IP Filter List, page 64: • IP filter: ◦ *address*: IP address of the first BMENOP0300 module ◦ *protocol*: **Any** ◦ *description*: BMENOP0300 module 1 • IP filter 2: ◦ *address*: IP address of the second BMENOP0300 module ◦ *protocol*: **Any** ◦ *description*: BMENOP0300 module 2 **NOTE:** Repeat these steps for each BMENOP0300 module in your configuration.
		IP Filter Actions, page 65: • *action*: block, permit, negotiate • *method*: SHA-1 (no encryption) • *key expiration*: 86400
		Authentication Method, page 66: pre-shared key
3	General Properties, page 66	Security policy name and description
		Policy change timeout
		Key exchange settings: • PFS • authentication timeout (2879 min.) • Internet Key Exchange (IKE) security methods ◦ *key exchange encryption*: 3DES ◦ *Integrity*: SHA1 ◦ *Diffie-Hellman group*: 1024 - medium (2)
4	Enable/Disable	Enable or disable the IPsec policy, page 66.
5	Configuration Tool	Configure the pre-shared key, page 67.

Before You Begin

Configure IPsec manually for each PC that supports IPsec:

- These directions are for PCs that run Windows 7.
- Confirm that you have administrative privileges to configure IPsec.
- Harden the PC that hosts the IPsec client to decrease the attack surface and observe the defense-in-depth concept. Refer to *Schneider Electric's guidelines* to harden your PC to reduce the surface of vulnerability.

IP Security Policy

Create an IPsec policy to define the rules for secure communications within the IPsec protocol:

Step	Action
1	On a Windows 7 PC, open the **Administrative Tools** from the Control Panel. **NOTE:** Consult your Windows 7 documentation to access the **Administrative Tools**.
2	Double-click **Local Security Policy** to open the **Local Security Policy** window.

Step	Action
3	In the left pane, expand **Security Settings** and double-click **IP Security Policies on Local Computer**.
4	In the right pane, right-click and scroll to **Create IP Security Policy ...** to open the **Policy Wizard**.
5	In the **IP Security Policy Wizard**, select the **Next** button: a. Assign a name to a new **Security Policy** in the **Name** field. b Provide a description of the new policy in the **Description** field. (This step is optional).
6	Select the **Next** button to proceed to the **Requests for Secure Communication** window.
7	De-select the check box (**Activate the default ...**) and select **Next** to open the **Completing the IP Security Policy Wizard**.
8	De-select the **Edit properties** check box and select **Finish**.

NOTE: The new security policy appears in the right pane of the **IP Security Policies on Local Computer** window. You can double-click the security policy at any time to access its **Properties** window.

IP Security Rule

Configure an IPsec rule to enable an IPsec configuration to monitor traffic between the application layer and the network layer:

Step	Action
1	In Windows 7, double-click the policy to open the **Properties** window.
2	Select the **Rules** tab.
3	Select **Add...** to open the **Create IP Security Rule Wizard**.
4	Select **Next** to configure the **Tunnel Endpoint**.
5	Select **This rule does not specify a tunnel** to use the **Transport** mode within the IPsec protocol.
6	Select **Next** to configure the **Network Type**.
7	Select the **All network connections** option button to apply the policy to local and remote connections.
8	Select **Next** to access the **IP Filter List** configuration. **NOTE:** The **IP Filter List** identifies the traffic that is processed through the IPsec rule.

IP Filter List

IPsec uses packet filters to evaluate communication packets according to their connections to various services. Packet filters are located between the endpoints of a peer-to-peer connection to verify that the packets adhere to the established administrative rules for communications.

Every IP filter in a single IP filter list has the IP address of the same source of the communications packets. The IP addresses for the destinations of communications packets (BMENOP0300 modules) are different.

Create a filter list that contains the IP addresses for the BMENOP0300 modules that can communicate with the source (PC):

Step	Action
1	In Windows 7, in the **IP filter lists** table of the **Security Rule Wizard**, click **Add** to create a new **IP filter list**: a. Assign a name to a new **Filter List** in the **Name** field. b. Provide a description of the new **Filter List** in the **Description** field. (This step is optional.)
2	Select **Add** to open the **IP Filter Wizard** and select **Next**.
3	Provide an optional description of the new **IP Filter** in the **Description** field.
4	Select the **Mirrored** check box to communicate in both directions (source and destination).
5	Select **Next** to configure the **IP Traffic Source**.
6	Select **My IP Address** to designate the PC at one endpoint of the secure communications.
7	Select **Next** to configure the **IP Traffic Destination**.
8	Select **a specific IP Address or Subnet** and enter the IP address of the BMENOP0300 module in your configuration. (The BMENOP0300 module is the only destination for this traffic.)
9	Select **Next** to configure the **IP Protocol Type** and select **Any** to allow traffic from the trusted IP address.
10	Select **Next** to view the **Completing the IP Filter Wizard** window.
11	De-select the **Edit properties** check box, and select **Finish** to return to the **IP Filter List**.
12	Select **OK** to exit the **IP Filter List**.

IP Filter Actions

Configure filter actions:

Step	Action
1	In Windows 7, in the **Name** column of the **IP Filter List**, select the option button for the newly created IP filter list and click **Next** to configure the **Filter Action**.
2	Select the **Use Add Wizard** check box.
3	Select **Add** to open the **Filter Action Wizard**.
4	Select **Next** to configure the **Filter Action Name**: a. Enter a name for the **Filter Action** in the **Name** field. b. Provide an optional description of the new **Filter Action Name** in the **Description** field and Select **Next**.
5	Select **Negotiate security** and **Next**. **NOTE:** The source and destination addresses agree on a method for secure communication before packets are sent.
6	Select **Do not allow unsecure communication**, and select **Next**.
7	Select **Custom** in the **IP Traffic Security** window, and select **Settings** to customize the settings: a. Select **Data and Address integrity without encryption**, and select **SHA1** in the list to use secure hash algorithm 1. b. De-select the **Data integrity with encryption** check box to disable the Encapsulating Security Payload (ESP).. c. Select the **Generate a new key every** check box, and enter 86400 in the **seconds** field to specify that the IKE expires in 86400 seconds. d. Select **OK** to return to the **IP Traffic Security** configuration.

Step	Action
8	Select **Next**.
9	Select the **Edit properties** check box, and select **Finish**.
10	Do not select the **Use session key perfect forward secrecy (PFS)** check box.
11	Select **OK**.

Authentication Method

Source and destination devices can agree to use a secret text string before communications begin. In this case, the string is called a pre-shared key.

Configure the authentication method to use a pre-shared key:

Step	Action
1	In Windows 7, in the **Name** column of the **Filter Actions**, select the option button for the newly created IP filter list, and click **Next** to configure the **Authentication Method**.
2	Select the **Use this string to protect the key exchange (preshared key)** check box.
3	In the text field, use any 16 ASCII characters to create a case-sensitive name for the pre-shared key. **NOTE:** At the end of this process, you will configure an identical pre-shared key to create a connection between a specific IP address and the BMENOP0300 module.
4	Select **Next**.
5	De-select the **Edit properties** check box, and select **Finish**.

IP Security Policy General Properties

Configure the general properties:

Step	Action
1	In Windows 7, in the **Properties** window, select the **General** tab.
2	Click **Settings** to open the **Key Exchange Settings** window.
3	Do not select the **Master key perfect forward secrecy (PFS)** check box.
4	In the **minutes** field, enter 2879 to set the key lifetime to 2879 minutes (47 hours and 59 minutes).
5	Click **Methods...** to open the **Key Exchange Security Methods** window.
6	Click **Edit** to open the **IKE Security Algorithms** window.
7	In the three lists, make these selections: • **Integrity algorithm**: **SHA1** (Secure Hash Algorithm 1) • **Encryption algorithm**: **3DES** (Triple Data Encryption Algorithm) • **Diffie-Hellman group**: **Medium (2)** (Generate 1024 bits of master key material.)
8	Select **OK** to return to the **Key Exchange Security Methods** window.
9	Select **OK** to return to the **Key Exchange Settings** window.
10	Select **OK** to return to the **Properties** window.
11	Select **OK** to close the **Properties** window.

Enable and Disable the Policy

Assign or un-assign a local security policy to enable and disable secure communications:

Step	Action
1	In Windows 7, open **Local Security Policy** in **Administrative Tools**.
2	Right-click the name of the new local security policy in the **Name** column and make a selection: • **Assign**: Assign the local security policy to enable communications to the IPsec-enabled PC. • **Un-assign**: Un-assign the local security policy to disable communications to the PC.

The IPsec policy agent does not run if you see this message: **The service cannot be started**. In that case, configure the service to start automatically:

Step	Action
1	In Windows 7, expand (+) **Administrative Tools**.
2	Double-click **Services** to access the local services.
3	Double-click **IPsec Policy Agent** to open its properties.
4	Select the **General** tab.
5	In the **Startup type** list, select **Automatic**.
6	In the **Service status**, select **Start**. **NOTE:** When **Start** is grayed out, the service is already running.
7	Select **OK** to apply the changes and close the window.

NOTE: When you enable IPsec, the Ethernet backplane port of the BMENOP0300 module is disabled. This isolates the IPsec network (control room network) from the device network. (Refer to the table for using different services and protocols.)

Configure IPsec in the Configuration Tool

Enable IPsec and set the pre-shared key:

Step	Action
1	Open your Control Expert project.
2	In the configuration tool, double-click the name that you assigned to the BMENOP0300 module to open the configuration window. **NOTE:** You can also right-click the module and select **Open** to open the configuration window.
3	Select **Security** to view the configuration options.
4	In the **IPsec** menu, select **Enabled**.
5	In the **Pre-Shared Key** field, enter the 16-character name of the pre-shared key. **NOTE:** The ASCII characters in the case-sensitive pre-shared key match the 16-character pre-shared key that you defined earlier.
6	Select the **Apply** button to save the configuration.
7	Rebuild the project and download the application to apply these settings to the BMENOP0300 module.

Troubleshooting IPsec Communications

Use the standard Windows 7 IPsec diagnostic tools to troubleshoot IPsec communications. For example, these steps use the Microsoft Management Console (MMC) service for management applications:

Step	Action
1	In Windows 7, create a console that includes an IP Security Monitor.
2	Click a server name.
3	Double-click **Quick Mode**.
4	Double-click **Statistics** to see the number of authenticated bytes that are sent and received.

NOTE:

- You cannot reset the values. To refresh the count values, relaunch the Microsoft Management Console.
- Disable **IP Forwarding**, page 52 before you enable IPsec. IPsec applies to a single IP address.

Use a Wireshark network analyzer to confirm that IPsec communications have started for an established IKE session. IPsec packets have an authentication header instead of the normal protocol header. This table shows an example of a network trace of a successful IKE session that was established by a ping request between a Windows 7 PC (source) and BMENOP0300 module (destination):

Number	Time	Source	Destination	Protocol	Length	Information
1	0	192.168.20.2-01	192.168.20.1	ISAKMP	342	Identity Protection (Main Mode)
2	0.00477	192.168.20.1	192.168.20.2-01	ISAKMP	126	Identity Protection (Main Mode)
3	0.012426	192.168.20.2-01	192.168.20.1	ISAKMP	254	Identity Protection (Main Mode)
4	1.594495	192.168.20.1	192.168.20.2-01	ISAKMP	270	Identity Protection (Main Mode)
5	1.598533	192.168.20.2-01	192.168.20.1	ISAKMP	110	Identity Protection (Main Mode)
6	1.603296	192.168.20.1	192.168.20.2-01	ISAKMP	110	Identity Protection (Maine mode)
7	1.612634	192.168.20.2-01	192.168.20.1	ISAKMP	366	Quick Mode
8	3.202976	192.168.20.1	192.168.20.2-01	ISAKMP	374	Quick Mode
9	3.207794	192.168.20.2-01	192.168.20.1	ISAKMP	102	Quick Mode

Use these solutions to facilitate communications when IPsec is enabled:

Behavior	Explanation
There is no communication with the BMENOP0300 when IPsec is enabled on the Windows PC.	**Explanation:** The IPsec policy agent is not running. **Solution:** Configure IPsec to start automatically.
	Explanation: IPsec is not enabled on the BMENOP0300. **Solution:** Enable IPsec on the **Security** tab of the configuration tool.
	Explanation: IPsec is not configured properly in Windows. **Solution:** See **NOTE 1** (below).
Control Expert cannot connect to the BMENOP0300 via Ethernet.	**Explanation:** IPsec is not enabled on both the BMENOP0300 and the Windows PC. **Solution:** See **NOTE 2** (below).
	Explanation: IPsec is not configured properly in Windows. **Solution:** See **NOTE 1** (below).
	Explanation: The power to the BMENOP0300 module was recently cycled. **Solution:** See **NOTE 3** (below).
The firmware update tool is not able to connect to the BMENOP0300 via Ethernet.	**Explanation:** IPsec is not enabled on both the BMENOP0300 and the Windows PC. **Solution:** See **NOTE 2** (below).
	Explanation: IPsec is not configured properly in Windows. **Solution:** See **NOTE 1** (below).
	Explanation: The power to the BMENOP0300 was recently cycled. **Solution:** See **NOTE 3** (below).
	Explanation: The IKE and IPsec ports may be blocked by a firewall or another program associated with antivirus applications. **Solution:** See **NOTE 4** (below).
NOTE 1: Confirm that the parameters in the Windows configuration match those in the IPsec implementation: • Double-check the pre-shared key. • Double-check the IP address of the BMENOP0300 module in the configuration tool. • Disable **Perfect Forward Secrecy** for both communication endpoints in Windows.	
NOTE 2: Verify that the configuration and the **Local Security Policy** are enabled for IPsec.	
NOTE 3: Choose a solution: • Wait 5 minutes for the Windows security associations to timeout. • Unassign then reassign the local security policy in Windows to force the security associations to be reset.	
NOTE 4: Verify that the IKE port (UDP 500) and IPsec Authentication Header port (51) are open on any firewall between the PC application and the PAC, including the firewalls associated with antivirus applications (like McAfee or Symantec).	

Configuring Data Rates

Introduction

The embedded switch in the BMENOP0300 module includes four Ethernet ports. Use the **Communication Settings > Switch** tab to specify the data rate and duplex setting for each port, or you let each port auto-negotiate these settings with the connected device.

Configuring Baud Rate Settings

Select the **Enable** check box next to the respective port, and choose the desired setting in the **Baud Rate** drop-down list:

Port	Available settings
ETH1 ETH2 ETH3	Select one of the following settings: • 100 Mbits/sec Full duplex • 100 Mbits/sec Half duplex • 10 Mbits/sec Full duplex • 10 Mbits/sec Half duplex • Auto 10/100 Mbits/sec (default)
Backplane	100 Mbits/sec Full duplex

After you finish editing baud rate settings, click **Apply** to save your edits.

Configuring the Syslog Service

Introduction

The syslog service is used to log events regarding cyber security. The BMENOP0300 module acts as a syslog client to synchronize security events with a remote syslog server.

The syslog service is disabled by default by the BMENOP0300 module firmware.

NOTE: The service is not available when IPsec, page 62 is enabled.

Configure the syslog service in Control Expert. Select **Tools > Project Settings > General > PLC diagnostics**. Select the **Event Logging** check box to edit the following features:

Event Logging Type	Action
SYSLOG server address	Enter a valid IP address. Default: 0.0.0.0
SYSLOG server port number	Use the up/down arrows to select a value between 0 and 65535. Default: 601
SYSLOG server protocol	This field is disabled. Default: tcp

Click **Apply** to save your edits. Click **OK** to close the **Project Settings** window.

Syslog Service Operation

Cyber security events are logged to a minimum of 100 messages before the oldest events are over written by newer events. Cyber security events are logged even when the BMENOP0300 module is operating at maximum configuration.

The BMENOP0300 module detects the following security events:

- TCP lack of connection due to Access Control list (where IEC 61850 was implemented)
- Communication services were enabled/disabled via the ETH_PORT_CTRL elementary function. **NOTE**: If FTP is enabled in the Modicon IEC 61850 Configuration Tool, it can be disabled/enabled via ETH_PORT_CTRL.
- Ethernet port link up/down events
- RSTP topology change

- Configuration download of communication services
- Program operating mode change of communications (Run, Stop)
- FTP events
- Unsuccessful and successful FTP login (for firmware update)

These events are currently supported in Unity Pro 12.0:

Events Related to . . .	
Security/Authorization	**Changes in the System (Log Audit)**
Unsuccessful connection from the configuration tool or the BMENOP0300 module (unsuccessful connection due to ACL, unsuccessful login, unsuccessful TCP connection if not logged in)	Application or configuration download from the BMENOP0300 module Application or configuration upload to the BMENOP0300 module (including online changes)
Communication parameters run time change outside of the configuration (enable/disable of communication services: FTP)	Program operating mode change (Run, Stop, Init)
Baud rate changes: port link up and down	
Any topology change detected: RSTP (port role change, root change)	

NOTE:

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

Syslog Service Diagnostics

The BMENOP0300 module provides the following diagnostics for the syslog service:

- EVENT_LOG_STATUS bit in scanner DDDT
- EVENT_LOG_STATUS bit is set to 1 if the event log service is operational or disabled.
- EVENT_LOG_STATUS bit is set to 0 if the event log service is not operational.
- LOG_SERVER_NOT_REACHABLE bit in DDDT
- LOG_SERVER_NOT_REACHABLE bit is set to 1 if the syslog clients **does not** receive an acknowledgement of the TCP messages from the syslog server.
- LOG_SERVER_NOT_REACHABLE bit is set to 0 if the syslog client **does** receive an acknowledgement of the TCP messages from the syslog server.

Uploading and Downloading Configuration Settings

Overview

This section shows you how to transfer an application program between Control Expert and a BMENOP0300 module.

Uploading and Downloading Configuration Settings

Introduction

When you finish entering configuration settings for the BMENOP0300 module, perform the following tasks:

- Update the application.
- Build the project.
- Transfer the built project to the controller.

After the built application is transferred to the controller, the controller transfers configuration settings to the BMENOP0300 module.

NOTE: Configuration settings do not take effect until they are successfully downloaded from your PC to the controller and from the controller to the BMENOP0300 module.

Updating the Configuration

After you input configuration settings for the BMENOP0300 module, update the configuration as follows:

Step	Action
1	Close the Modicon IEC 61850 Configuration Tool. **Result**: The **Confirm** dialog box opens.
2	Click **Yes** to save your edits. **Result**: The **Confirm** dialog box closes. In the **Configuration** tab of the BMENOP0300 module **Properties** window, the **Update application** button is enabled.
3	Click the **Update application** button.

Clicking **Update application** button creates variables that display the following information and commands for your Control Expert project:

- the status of the IEC 61850 server and client
- the IEC 61850 data model mapped into the controller memory

Compiling the Project

To compile the updated project, in Control Expert select either **Build > Build Changes** or **Build > Rebuild All Project**. Check the **Output** window to confirm the process succeeded.

Downloading the Application Program

After the application has been compiled, connect Control Expert to the controller (**PLC > Connect**), then download the application to the controller (**PLC > Transfer Project to PLC**).

To transfer the compiled application program from Control Expert to the controller, follow these steps:

Step	Action
1	Connect Control Expert to the controller: Select **PLC > Connect**.
2	Stop controller operations if the controller is executing an earlier version of the application: Select **PLC > Stop**.
3	Download the application to the controller: Select (**PLC > Transfer Project to PLC**.

On next power-up, the BMENOP0300 module compares the configuration in the controller against the one stored in the module.

- If the configurations are different or if there is no configuration program in the module, the controller downloads the configuration to the BMENOP0300 module. The module stores the new configuration in its non-volatile memory and loads it on start-up.
- If the configurations are the same, the module loads the configuration stored in its non-volatile memory.

Uploading the Application Program

To transfer the current application program from the controller to Control Expert, follow these steps:

Step	Action
1	Connect Control Expert to the controller: Select **PLC > Connect**.
2	Stop controller operations if the controller is executing an earlier version of the application: Select **PLC > Stop**.
3	Upload the application to the controller: Select (**PLC > Transfer Project from PLC**.

NOTE: Uploading the application program does not also upload the IEC 61850 settings of the BMENOP0300 module. To apply IEC 61850 settings, confirm that you have saved these settings in a .prj file during a previous configuration. For instructions on how to apply saved IEC 61850 settings, refer to the topic Selecting the IEC 61850 Edition, page 43.

Archiving the Application Program

To archive the application in Control Expert, do one of the following:

- Select **File > Save As**, then save the file as an .STU file type.
- After building the project (**Build > Build Changes/Rebuild All Project**), select **File > Save Archive...** and save the file as an .STA file type.

  NOTE: Saving your application as an .STA or .STU file type saves the entire Control Expert project, including the IEC 61850 project file. If you export the application as a .ZEF file type, the IEC 61850 project file is not saved.

Configuring the IEC 61850 Server

Introduction

This chapter shows you how to configure the module as an IEC 61850 server.

Before configuring server properties, enable the IEC 61850 server function in the General window, page 47. After you enable the IEC 61850 server function, click the **IEC 61850 Server Settings** button to open the **Server Settings** window., page 74

NOTE: The IEC 61850 configurator editions support the following schema versions:

- Edition1: supports schema V1.6
- Edition2: supports schema V3.1

Working with Server Configurations

Introduction

Use the **IEC 61850 Server** window to perform the following functions for the BMENOP0300 module:

- View and edit server information, including:
  - IP address
- Create a new IEC 61850 server that is:
  - an empty IED server, then modeling
  - based on an external ICD or CID file
  - based on an external SCD file
- Delete an IEC 61850 server.
- Export an IEC 61850 server file to:
  - a CID/ICD file
  - an Excel spreadsheet file
- Open one of the following windows, where you can configure server functions:
  - Data Model, page 79
  - Application Settings, page 85
  - Data Set, page 87
  - Report Control, page 93
  - GOOSE Control, page 89
  - SOE Data Set, page 96
  - External Reference, page 98

Before configuring server properties, enable the IEC 61850 server function in the General, page 47 window. After you enable the IEC 61850 server function, click the **IEC 61850 Server Settings** button to open the **IEC 61850 Server** window.

Viewing Server Information

When a server is created, the **Server Information** area displays the following server settings:

Setting	Description
IED Name	The read-only server name. By default, it is the same as the **Module Name** in the **General** window, page 47.
Description	The configurable description of the server. By default, it displays the description provided by the ICD template.
IP	Select an IP address for the IEC 61850 server. IEC 61850 clients use this IP address to access the server. **NOTE:** The list can contain up to 3 IP addresses. IP addresses are added to the list in the **Communication Settings** window.

NOTE: Before you create a new IEC 61850 server, the **Server Information** settings are empty and disabled. After you create a new server instance, these settings display their default values.

Creating an Empty IED Server

To create a new empty IED server, follow these steps:

Step	Action
1	When the **IEC 61850 Server** window opens, the **Create IED Server** dialog box opens, presenting three selections: • Create an empty IED server. • Select an external Schneider Electric ICD / CID file. • Select an external Schneider Electric SCD file. **NOTE:** If you cancel the **Create IEC 61850 Server** window, click the **Create IEC 61850 Server** button  to re-open it.
2	Select **Create an empty IED server**. **Result**: The **OK** button is enabled.
3	Click **OK**. **Result**: The **Input IED Name** dialog box opens.
4	In the **Input IED Name** dialog box, accept the default name or enter a new name for this IED. **NOTE:** Use a maximum of 16 characters for the IED name.
5	Click **OK**. **Result**: The new server is created.
6	**Save** the new server. **NOTE:** A new empty IED server contains no predefined functions. Create all the functions your new IED server requires.

Creating a New Server from an External Schneider Electric ICD / CID File

You can create a new server instance from an ICD or CID file that was previously created and saved using the Modicon IEC 61850 Configuration Tool. To create a new server from an external ICD or CID file, follow these steps:

Step	Action
1	When the **IEC 61850 Server** window opens, the **Create IED Server** dialog box opens, presenting three selections: • Create an empty IED server. • Select an external Schneider Electric ICD / CID file. • Select an external Schneider Electric SCD file. **NOTE:** If you cancel the **Create IEC 61850 Server** window, click the **Create IEC 61850 Server** button  to re-open it.
2	In the **Create IED Server** dialog box, select **Select an external ICD / CID file**. **Result**: The file path field and browse button are enabled.
3	Click the browse button beneath your selection. **Result**: The **Open** dialog box opens.
4	In the files of type list, select the type of file you want to select: • ICD file (*.icd) • CID file (*.cid)
5	Navigate to and select an ICD or CID file, then click **Open**. **Result**: The dialog box closes, and the name of the selected file appears in the path box.
6	Click **OK**. **Result**: The **Input IED Name** dialog box opens.
7	In the **Input IED Name** dialog box, accept the default name or enter a new name for this IED.
8	Click **OK**. **Result**: The new server is created.
9	**Save** the new server.

Creating a New Server from an SCD File

The Modicon IEC 61850 Configuration Tool can create a new server from an IED file contained in an external SCD file. To create a new server from an external SCD file, follow these steps:

Step	Action
1	When the **IEC 61850 Server** window opens, the **Create IED Server** dialog box opens, presenting three selections: • Create an empty IED server. • Select an external Schneider Electric ICD / CID file. • Select an external Schneider Electric SCD file. **NOTE:** If you cancel the **Create IEC 61850 Server** window, click the **Create IEC 61850 Server** button  to re-open it.
2	In the **Create IED Server** dialog box, select **Select an external SCD file**. **Result**: The file path field and browse button are enabled.
3	Click the browse button beneath your selection. **Result**: The **Open** dialog box opens.
4	Confirm that in the files of type list, SCD file (*scd) is selected.
5	Navigate to and select the appropriate SCD file, then click **Open**. **Result**: The dialog box closes: • The name of the selected SCD file appears in the path box. • The **Select IED to Import** list is populated with IEDs associated with the selected SCD file.

Step	Action
6	In the **Select IED to Import** list, select the appropriate IED file, then click **OK**. **Result**: The **Input IED Name** dialog box opens.
7	In the **Input IED Name** dialog box, accept the default name for this IED. **NOTE:** Do not change the default IED name.
8	Click **OK**. **Result**: The new server is created.
9	**Save** the new server.

Deleting an Existing Server

You can delete the IEC 61850 server instance that is currently displayed in **IEC 61850 Server** window. To delete the server, follow these steps:

Step	Action
1	Open the server you want to display in the **IEC 61850 Server** window.
2	Click the **Delete this server configuration** button  . **Result**: The **Confirm** dialog box opens and asks if you are sure you want to delete the server.
3	In the **Confirm** dialog box, click **Yes**. **Result**: The server is deleted, and the **Create IEC 61850 Server** button  is enabled.
4	**Save** your edits.

Exporting the Server to a CID or ICD File

You can export the IEC 61850 server instance that is currently displayed in **IEC 61850 Server** window, as a CID or ICD file. To export a server, follow these steps:

Step	Action
1	Click the **Export** toolbar button  . **Result**: The **Save As** dialog box opens.
2	In the **Save As** dialog box: • Navigate to the location where you want to save the exported file. • Select a file type: CID or ICD (or IID for Edition 2.0). • Click **Save**.

Exporting the Server to an Excel Spreadsheet File

You can export the configured IEC 61850 server that is currently displayed in **IEC 61850 Server** window, as an Excel 97-2003 spreadsheet file. To export a server, follow these steps:

Step	Action
1	Click the **Export to Excel** button. **Result**: The **Save As** dialog box opens.
2	In the **Save As** dialog box: • Navigate to the location where you want to save the exported file. • Click **Save**.

The exported Excel spreadsheet file populates the following fields with configured server data:

- Reference: the path and name of the data item
- BasicType: the data type of the item
- FC: the functional constraint value of the data item
- DO/DA: the type of item: data object (DO) or data attribute (DA)
- Initial Value: The initialized value assigned to the data item

All other fields in the spreadsheet are not populated.

Opening Additional Server Property Windows

To continue configuring properties for the IEC 61850 server open in the **IEC 61850 Server** window, click one of the following:

- Data Model
- Application Settings
- Data Set
- Report Control
- GOOSE Control
- SOE Data Set
- External Reference

Data Model

Introduction

Use the **Data Model** window to view, add, remove, and edit the IEC 61850 data model for the BMENOP0300 module IED.

The **Data Model** window displays:

- a data model navigator (on the left), which you can use to move through the data model and select individual data items
- a data model editor, which you can use to view, add, remove, and edit the data items associated with the item selected in the data model navigator
- a file path display, which indicates the object path of the editing element

NOTE: The Modicon IEC 61850 Configuration Tool supports flexible data modeling. You can manage name space assignments in the application to meet your application needs. The Modicon IEC 61850 Configuration Tool does not manage name space designations by default.

The data model editor presents a different interface, depending on the item selected in the data model navigator. In the data model editor, you can add and remove optional data items. Mandatory data items are automatically added by default, and cannot be removed.

Expand the navigation tree control and select a data item to display its related data items in the data editor:

In the data model navigator, select a...	...to display the following items in the data model editor...
Module IED	Logical devices
Logical device	Logical nodes
Logical node	Data objects
Data object	Sub data objects and data attributes

Working with Logical Devices

A module IED can include up to 16 logical devices. The **System** logical devices node is mandatory. It is included by default and cannot be removed.

Each logical device includes the following parameters:

- **Instance**:

  the name of the logical device, up to 16 characters long
- **Description**:

  the editable description for a logical device

To add a logical device, follow these steps

Step	Action
1	In the data model navigator, select the module IED. **Result**: The data model editor displays a list of logical devices.
2	Click **Add**. **Result**: The **Input Logical Device Instance Name** dialog box opens.
3	Enter a logical device name of up to 16 ASCII characters.
4	Click **OK**. **Result**: The dialog box closes, and the new logical device is added to the data model editor.

Step	Action
5	(Optional) In the data model editor, type in a **Description** for the new logical device, then click **Enter**.
6	**Save** your edits.

To add a new extension logical node, follow these steps:

Step	Action
1	In the data model navigator, select a logical device. **Result**: The data model editor displays a logical node table, a logical node group selector, and a logical node class list.
2	In the logical node group selector, select a logical node alphabetical group. **Result**: The logical node class list displays items for the selected group.
3	Click the **Add Extension Logical Node** button to add a new node. **Result**: The **Add Logical Node** dialog box opens.
4	In the **Add Logical Node** dialog box, • Edit your customized **Class** name. **NOTE:** Choose a **Class** name that contains four uppercase letters. The name cannot be the same as any existing pre-defined class names, or it will not be applied. • Accept the default Prefix (SE), or enter a value. **NOTE:** If you enter a different prefix value, it is added to the **Name** string. However, the **Type** value is the concatenation of the SE prefix and the LnClass value. • Enter a **Type** value. Instance value is automatically generated.
5	Click **OK**. **Result**: The new logical node is added to the table.
6	**Save** your edits.

To remove an optional logical device, select it in the data model editor, then right-click and select **Delete**. When the item disappears from the list, click **Save**.

Working with Logical Nodes

The logical node table displays a list of logical nodes for the selected logical device. **LLN0** is mandatory for each logical device; **LPHD** is mandatory for each system logical device. They are included by default and cannot be removed. Refer to the appendix for a list of logical nodes, page 184 supported by the BMENOP0300 module IED.

Each logical node includes the following parameters:

- **Name**:

  the read-only name of the logical node
- **Prefix**:

  an optional prefix to the logical node, for ASCII “x” characters long, editable only when a new logical node is instantiated (Thereafter it is read-only.)
- **LnClass**:

  the read-only name of the logical node class
- **Instance**:

  a read-only sequential number automatically assigned to a new logical node, “y” characters long, which, when more than one instance of a logical node class is added, this value increments by a value of 1

  NOTE: The combined length of the **Prefix** plus **Instance** (x + y) cannot exceed 12 characters.

- **Type**:

  the name (an editable value of up to 64 ASCII characters) of the logical node template, which is composed of several data objects. You can create several instances of logical node with the same type (logical node template).

  For example, a logical node type of class ARIS begins with “SE_ARIS_”.

  - If you input text that matches this naming convention, (for example, "SE_ARIS_12345") the Modicon IEC 61850 Configuration Tool uses the input text as the Type setting.
  - If you input text that does not match this naming convention, the Modicon IEC 61850 Configuration Tool adds the expected prefix to your input text. (for example, if you input the text "V001”, the value is edited to "SE_ARIS_V001".

- **Description**:

  an editable text field you can use to describe the logical node

To add a logical node, follow these steps:

Step	Action
1	In the data model navigator, select a logical device. **Result**: The data model editor displays a logical node table, a logical node group selector, and a logical node class list.
2	In the logical node group selector, select a logical node alphabetical group. **Result**: The logical node class list displays items for the selected group.
3	Drag an item from the logical node class list to the logical node table. **Result**: The **Add Logical Node** dialog box opens.
4	In the **Add Logical Node** dialog box, accept the default **Prefix** setting, or enter a new value. In the **Add Logical Node** dialog box: • Accept the default **Prefix** (SE), or enter a value. **NOTE:** if you enter a different prefix value, it will be added to the **Name** string. However the **Type** value will be the concatenation of the prefix “SE” and the **LnClass** value. • Enter a **Type** value. **LnClass** and **Instance** values are automatically generated.
5	Click **OK**. **Result**: The new logical node is added to the table.
6	**Save** your edits.

To remove an optional logical node, select it in the logical node table, then right-click and select **Delete**. When the item disappears from the list, click **Save**.

Working with Data Objects

The data object table displays a list of data objects for the selected logical node. The collection of available data objects for each logical node is pre-defined by the IEC 61850 protocol. Mandatory data objects are included by default and cannot be individually removed.

NOTE: Mandatory data objects for an optional logical node can be removed only by removing the optional logical node.

Each data object includes the following parameters:

- **Name**:

  the name of the data object:

  - read-only for default data objects
  - editable for extended data objects

    NOTE: For data objects that can be added to a logical node more than once, the name includes a numerical instance suffix. For example, *Ind1* represents the first instance of the *Ind* data object of the *GGIO* logical node.

- **Common Data Class (CDC)**:

  the read-only IEC 61850 protocol-specified group to which the data object belongs

  NOTE: Refer to the appendix for a list of CDCs, page 190 supported by the BMENOP0300 module IED.

- **Mandatory**:

  a read-only indicator that, when selected, indicates the data object is required for the logical node and cannot be removed

- **Type Name**:

  an editable value that defines data objects inside a logical node, whose type is derived from and extends a common data class

  For example, a type name of the common data class SPS begins with “SE_ SPS_”.

  - If you input text that matches this naming convention, (for example, "SE_ SPS_12345") the Modicon IEC 61850 Configuration Tool uses the input text as the Type Name setting.
  - If you input text that does not match this naming convention, the Modicon IEC 61850 Configuration Tool adds the expected prefix to your input text. (for example, if you input the text "V001”, the value is edited to "SE_SPIS_ V001".

There are two ways to add a data object:

- Add an optional data object.
- Extend a data object for the editing logical node.

  NOTE: When you add a data object to a logical node, the data object is added not only to the logical node instance, but to the underlying structure of the logical node object itself. Therefore, if a logical node can be added to a logical device more than once (for example, **LDevice > GGIO**) every instance of that logical node contains the newly added data object.

To add a new data object, follow these steps

Step	Action
1	In the data model navigator, select a logical node. **Result**: The data model editor displays a data object table and a data object list.
2	Drag an item from the data object list to the data object table. **Result**: The **Edit Data Object** dialog box opens.
3	In the **Edit Data Object** dialog box, enter or select a **Type**. The text you enter or select is concatenated with the prefix “SE” and the **CDC** value to form the **Type Name**.
4	Clock **OK** to close the dialog box. The new data object appears in the data object table. **NOTE:** If the data object can be added to the table: • Only once, it is removed from the data object list. • More than once, the data object remains in the list and a numerical instance suffix is added to the data object name in the table.
5	**Save** your edits.

To add a new extension object, follow these steps

Step	Action
1	In the data model navigator, select a logical node. **Result**: The data model editor displays a data object table and a data object list.
2	Click **Add Extension Object**. **Result**: The **Edit Data Object** dialog box opens.
3	In the **Edit Data Object** dialog box: • Enter a **Name** of the new data object, up to ten ASCII characters. **NOTE:** Verify that the first character of the value is a capital letter. • Select a **Common Data Class** value. • Enter or select a **Type**. The text you enter or select is concatenated with the prefix "SE" and the **CDC** value to form the **Type Name**.
4	Clock **OK** to close the dialog box. The new data object appears in the data object table.
5	**Save** your edits.

To remove an optional data object, select it in the data object table, then right-click and select **Delete**. When the item disappears from the list, click **Save**.

Working with Data Attributes

The data attribute table displays a list of data attributes for the selected data object. The collection of available data attributes for each data object is pre-defined by the IEC 61850 protocol. Mandatory data attributes are included by default and cannot be individually removed.

NOTE: A logical device can support up to 10000 data attributes.

Each data attribute includes the following parameters:

- **Name**:

  the read-only name of the data attribute
- **BasicType**:

  the read-only IEC 61850 protocol-specified data type for the data attribute
- **Mandatory**:

  a read-only indicator that, when selected, indicates the data attribute is required for the data object and cannot be removed
- **FC**: the functional constraint group of the data attribute
- **Type**: a text string describing the data attribute with the following **BasicType** values:
  - a pre-determined, non-editable value = The **Type** setting is not displayed.
  - a variable type, specified at the time of creation = The value is displayed.

  NOTE: When you add a data attribute to a data object, the data attribute is added not only to the data object instance, but also to the underlying structure of the data object. Therefore, if a data object can be added to a logical node more than once (for example, **LDevice > GGIO > Beh > stVal)**) every instance of that data object contains the newly added data attribute.

To add a data attribute, follow these steps

Step	Action
1	In the data model navigator, select a data object. **Result**: The data model editor displays a data attribute table and a data attribute list.
2	Drag an item from the data attribute list to the data attribute table. **Result**: The data attribute is added to the table. **NOTE:** If the data object can be added to the table: • Only once, it is removed from the data object list.

Step	Action
	• More than once, the data object remains in the list and a numerical instance suffix is added to the data object name in the table.
3	For some data attributes the **Select Type of Data Attribute** dialog box opens: • For some attributes of the *Struct* **BasicType**, specify the attribute type. • For some attributes of the *Enum* **BasicType**, select from a list of existing **Type** values. For example: **LDevice > SEMSTA1 > Beh > stVal)**. In these cases, select a **Type** value, and click **OK**.
4	After the new data attribute appears in the data attribute table, **Save** your edits.

To remove an optional data attribute, select it in the data attribute table, then right-click and select **Delete**. When the item disappears from the list, click **Save**.

Working with a Data Object that includes Sub Data Objects

The structure of some data objects includes sub data objects (for example, **LDevice > MHAI > HPhV**). When you add a data object that includes sub data objects, the data model editor displays both a data object editor and a data attribute editor. You can use these editors to add and remove optional data sub objects and data attributes for this kind of data object.

Both the data object editor, page 81 and the data attribute editor, page 83 work in the same manner as described above.

Instantiating Data Objects and Data Attributes

Introduction

Use the **Application Settings** window to:

- Display IEC 61850 server data objects and data attributes.
- Instantiate data attributes and data objects by assigning an initial value to data attributes.

Before you can use the **Application Settings** window, first enable the IEC 61850 server, page 47 resident in the BMENOP0300 module; then create a new server instance, page 74 for the module.

NOTE:

- Assigning an initial value to a data attribute instantiates both that attribute and the associated data object. An instantiated data attribute is indicated by the DAI object designation; an instantiated data object is indicated by the DOI object designation (or SDI for sub data objects).
- Attributes with a value set to an empty string are not instantiated by the application. If values for all data attributes of a data object are set to an empty string, the application does not instantiate the data object.
- For data attributes of the functional constraint CF, the initial value remains constant after the configuration is instantiated. For data attributes of other function constraint items, the initialized value is the default value if not included in I/O mapping; otherwise, the functional constraint item is not instantiated.
- For data out flow variables, an assigned initial value takes effect only if a variable is not mapped to controller memory. If a variable is mapped to controller memory, its value comes from controller memory.

Adding Data Objects and Data Attributes

The **Application Settings** window presents a **Data Object Filter** and a data table. Use the **Data Object Filter** to select data objects and data attributes of the IEC 61850 server, then drag them onto the data table. The data table displays the data objects and data attributes you add to it in the following nested order:

LDevice > LNode > Data Object > Data Attribute

To add data objects and data attributes to the data table, follow these steps:

Step	Action
1	In the **Data Object Filter**, select a logical device in the **LDevice** list. **Result**: The contents of the **LNode** filter presents logical nodes of the selected logical device.
2	In the **LNode** list, select a logical node. **Result**: The contents of the **FC** list presents functional constraint items of for the selected logical node.
3	In the **FC** list, select a functional constraint item. **Result**: The **Data Object Filter** displays the data objects and nested data attributes associated with the selected functional constraint item.
4	Do one of the following: • Drag a data object or data attribute in the **Data Object Filter** and drop it onto the data table to add it to the list. • Click the **Add All** button to add all of the displayed data objects and data attributes to the list.
5	(Optional) Type in a text **Description** for each data object added to the list.
6	Repeat steps 1...5 for each data object or data attribute you want to add to the data table.
7	**Save** your edits to preserve the structure of the data table you created.

Instantiating Data Attributes and Data Objects

Assigning an initial value to a data attribute instantiates both that attribute and the associated data object. To edit the initial value of a data attribute, follow these steps:

Step	Action
1	In the data table, expand the **LDevice**, **LNode**, and data object rows until the associated **Data Attribute Instance** items are visible.
2	In the **Initial Value** column, enter or select a value for the data attribute.
3	Repeat steps 1 and 2 for each data attribute you want to instantiate.
4	**Save** your edits.

Removing Data Attributes and Data Objects from the Data Table

To remove a data attribute from the data table, select the data attribute, then do one of the following:

- Click the right mouse button and select **Delete**.
- Click the **Delete** key.

If you delete all attributes of a data object, that data object is removed from the data table.

Working with Data Sets

Introduction

A data set is a collection of data attributes and data objects that can originate with many different logical devices and logical nodes. Data sets can provide an efficient method of viewing and transferring data. The IEC 61850 server can include up to 68 data sets and up to 256 basic type data attributes. Furthermore, I/O events that are produced by an ERT module, to which the ERT data set is dedicated, can be mapped to an IEC 61850 report directly.

Use the **Data Set** window to:

- Create a new data set.
- View the list of existing data sets.
- Edit the contents of a new or existing data set by adding data attributes to, or removing data attributes from the data set collection.
- Remove a data set from the IEC 61850 server.

Before you can use the **Data Set** window, first enable the IEC 61850 server, page 48 resident in the BMENOP0300 module; then create a new server instance, page 74 for the module.

After you create a data set, you can add it to GOOSE control blocks, page 93 and also to Report control blocks, page 89.

NOTE:

- When you add a *stVal* or *cVal* attribute, also add its companion *q* (quality) data attribute. The *q* attribute contains valuable data information for your application.
- Do not add a *t* attribute to a GOOSE data set.

Creating a Data Set

To create a new data set, follow these steps:

Step	Action
1	In the **General** > **IEC 61850 Server** > **Data Model** window, create the data model for your module.
2	In the **General** > **IEC 61850 Server** > **Data Set** window, in the **Data Set** list, click the **+** button. **Result**: A new data set appears in the data set list, with the default name 'NewDatasetn' (where n represents the sequential number of the data set).
3	Do one of the following: • Accept the default data set name. • Double-click the default name, then type a new name and press **Enter**.
4	In the **Description** area, do one of the following: • Accept the default data set description, which is the reference path to the data set. • Type in a different description.
5	In the **Data Object Filter**, use the filtering lists to navigate to the data attribute you want to add to the data set. Make filtering selections for: • **LDevice**: Select an IEC 61850 server logical device. • **LNode**: Select a logical node associated with the selected logical device. • **FC**: Select a functional constraint. **Result**: The data attribute list, located below the filtering lists, presents the data attributes that satisfy the selected filtering criteria.

Step	Action
6	Add data attributes to the data set in one of the following ways: • Drag a data object node from the data attribute list and drop it on the **FCDA** table. **NOTE:** When you add a data object, all of its data attributes are also added, even though they are not visible in the list. • Drag a single data attribute from the data attribute list and drop it on the **FCDA** table. Only the selected data attribute is added to the data set. **Result**: The **FCDA** table displays the data set in nested groups, as follows: **LDevice > LNode > Data Object > Data Attribute**
7	Repeat steps 3 and 4, above, until all data attributes are added to the data set.
8	**Save** your edits.

Editing an Existing Data Set

To edit an existing data set, follow these steps:

Step	Action
1	In the **Data Set** list, select an existing data set. **Result**: The data attributes of the selected data set appear in the data set list.
2	To add data attributes, follow steps 3 to 5 in Creating a Data Set, page 87 (above).
3	To remove data attributes, select one or more data attributes in the **FCDA** table, right click, then select **Delete** from the context menu.
4	**Save** your edits.

Viewing Data Set Contents

To display the data attributes assigned to a data set, select the data set in the **Data Set** list. The data attributes appear in the **FCDA/FDC** table.

Removing a Data Set from the IEC 61850 Server

To remove a data set from the IEC 61850 Server, follow these steps:

Step	Action
1	In the **Data Set** list, select an existing data set. **Result**: The data attributes of the selected data set appear in the data set list.
2	Click the **–** button. **Result**: The data set is removed from the list.
3	**Save** your edits.

Configuring Report Control Blocks

Introduction

Use report control blocks to transmit the information contained in data sets. Configure each report control block to specify how the IEC 61850 server that resides in the BMENOP0300 module transmits event data to IEC 61850 clients.

There are two kinds of report control blocks:

- Buffered (BRCB): Internal events (triggered by data-change and quality-change) cause one of the following:
  - the immediate transmission of a report
  - the buffering of a report (within practical limitations) for later transmission

  A report is buffered so that data object values are not lost due to transport flow control constraints or a connection interruption. A buffered report control block provides sequence-of-events (SOE) functionality.The buffer size of a buffered report control block is fixed at 16k bytes for each report control block instance.
- Unbuffered (URCB): Internal events (triggered by data-change and quality-change) cause the immediate transmission of a report on a "best effort" basis. If no association exists, or if the transport data flow is not fast enough to support the transmission, report data may be lost.

The IEC 61850 server in the BMENOP0300 module supports:

- up to 64 buffered or unbuffered report control block instances within a single IED
- up to 8 instances of a single buffered control block, which can be transmitted to 8 clients, upon the occurrence of possibly different triggering conditions

Before you can use the **Report Control Block** window, confirm that you have done the following:

- Enable the IEC 61850 server, page 48 resident in the BMENOP0300 module.
- Create a new server instance, page 74 for the module.
- Create a data set incorporating data attributes from this BMENOP0300 module, page 15.

  NOTE:

  - The BMENOP0300 module stores report control blocks in the LDevice System, at the LNode LLN0.
  - Although the BMENOP0300 module cyclically scans the data status in the M580 controller, the module's scan cycle is not synchronize with PAC scan cycle. If the amount of data scanned by the BMENOP0300 module is large, and if the PAC scan cycle is short, some changes to data values may not be detected by the BMENOP0300 module.
  - Minor changes in the value of an analog input can cause the generation of unnecessary reports. The BMENOP0300 module supports the creation of a deadband value range for analog data attributes (DA). Use the deadband feature to limit unwanted report generation. If the analog input change is less than the deadband magnitude, no report is generated.

Report Control Settings

Every report control block presents the following configuration settings:

Setting	Description
Identification area:	
Buffered	Do one of the following: • Select this check box to enable buffering for this report control block. • De-select this check box to disable buffering. This check box is de-selected by default.
ReportCB Name	Enter a 10-character maximum report control name.
Description	The editable description of the report control block, from 0...50 characters long.
Data Set	Select the data set to include in the report control block.
Report ID	A string value, 0...129 characters long, used as the source identifier in report control block transmissions.
Conf Rev	The read-only revision number for the report control block. The initial value is 10000. **NOTE:** This setting is increased in increments of 10000 each time one of the following changes occurs: • The identity of the data set associated with this control block changes. • Content of the associated data set changes.
Parameters area:	
Buffer Time (ms)	The time interval in milliseconds for the buffering of internal notifications caused by data-change (dchg) or quality-change (qchg) by the BRCB for inclusion into a single report.
Integrity Period	Enter a value, in milliseconds, to periodically force the transmission of all values in the data set. Using this setting synchronizes data values in all clients that receive the transmission.
Indexed	Do one of the following: • Select this check box to enable indexing of this report control block. • De-select this check box to disable indexing. This check box is selected by default. **NOTE:** The module supports up to 8 instances of indexed report control blocks.
Index Number	Select an index number for the report control block.
Trigger Conditions area:	
Data Change	Select this check box to transmit a report upon a change in value for an item in the data set.
Quality Change	Select this check box to transmit a report upon a change in quality for any item in the data set.
Period	Select this check box to transmit a report of all data set values upon expiration of the **Integrity Period**. **NOTE:** The integrity report is not available in a standby BMENOP0300 module in a redundant M580 network.
General Interrogation	Select this check box to transmit a report, in response to a request from a client, containing values for all data items in the data set. **NOTE:** • All buffered events are transmitted before the general-interrogation report is transmitted. • If the IEC 61850 server receives a request for a general interrogation report while executing a previous general interrogation request, execution of the current request stops. The server instead begins to execute the new general interrogation request.

Setting	Description
Report Content area:	
Sequence Number	Select this check box to include an auto-generated transmission sequence number to the report control block transmission. This lets the client determine if all transmissions have been received.
Report Timestamp	Select this check box to include a time stamp in the report control block transmission.
Reason for inclusion	The reason for sending this report, for example: • data change • quality change • general interrogation • periodic transmission
Data Set Name	Select this check box to include the configured data set name in the report control block transmission.
Data Reference	The name of the data set referenced in the report.
Buffer Overflow	Select this check box to include the buffer overflow in the report content. This check box is de-selected by default.
Entry Id	Select this check box to include the entry ID in the report content. This check box is de-selected by default.
Configuration Revision	Select this check box to include the **Configuration Revision** setting of the report control block in the transmission.

Creating a New Report Control Block

To create a new report control block, follow these steps:

Step	Action
1	In the **Report Control** list, click the **+** button. **Result**: A new report control block appears in list, with the default name *report_n* (where n represents the sequential number of the control block).
2	Enter values for the **Identification**, **Parameters**, **Trigger Conditions** and **Report Content** settings. Refer to the description of Report Control Settings (above). **NOTE:** To enter a setting value, click **Enter** or move your cursor and click outside the setting input field.
3	**Save** your edits.

Editing an Existing Report Control Block

To edit an existing report control block, follow these steps:

Step	Action
1	In the **Report Control** list, select an existing control block. **Result**: The settings for the selected report control block appear in the **Identification**, **Parameters**, **Trigger Conditions** and **Report Content** areas.
2	Enter values for the **Identification**, **Parameters**, **Trigger Conditions** and **Report Content** settings. Refer to the section Report Control Settings (above). **NOTE:** To enter a setting value, click **Enter** or move your cursor and click outside the setting input field.
3	**Save** your edits.

Removing a Report Control Block

To remove a report control block from the IEC 61850 Server, follow these steps:

Step	Action
1	In the **Report Control** list, select an existing control block. **Result**: The settings for the selected report control block appear in the **Identification**, **Parameters**, **Trigger Conditions** and **Report Content** areas.
2	Click the **–** button. **Result**: The control block is removed from the list.
3	**Save** your edits.

Publishing GOOSE Control Blocks

Introduction

The BMENOP0300 module can publish module event data via GOOSE control blocks. Each control block references a data set with data attributes that can describe module status and value information. The module sends GOOSE control blocks in the form of multicast transmissions over a VLAN. Other devices that subscribe to the VLAN receive the transmitted data.

Use the **GOOSE Control Block** window to:

- Create a new GOOSE control block.
- View the list of existing GOOSE control blocks.
- Edit the contents of a new or existing GOOSE control block.
- Remove a GOOSE control block from the IEC 61850 server.

Before you can use the **GOOSE Control Block** window, confirm that you have done the following:

- Enable the IEC 61850 server, page 48 in the BMENOP0300 module.
- Create a new server instance, page 74 for the module.
- Create the data set, page 87 you want to add to, and be published by, a GOOSE control block.

  NOTE: The BMENOP0300 module stores GOOSE control blocks in the LDevice System, at the LNode LLN0.

GOOSE Control Settings

NOTE: When publishing GOOSE transmissions:

- You can use the GooseSimulation element of the MODULE_STATE DDT to publish either normal (0) or simulated (1) GOOSE transmissions.
- The relative diagnostic information of each GOOSE transmission is collected in a dedicated DDT instance.

Every GOOSE control block includes the following settings:

Setting	Description
Parameters area:	
Configuration Revision	The read-only revision number for the GOOSE control block. The initial value is 10000. **NOTE:** This setting is increased in increments of 10000 each time one of the following changes occurs: • The identity of the data set associated with this control block changes. • Content of the associated data set changes.
Description	The editable description of the GOOSE control block, up to 50 characters long.
GOOSE ID	An editable string value, from 1...128 characters long, used as the source identifier in GOOSE message transmissions. The default value is the reference path of this GOOSE control block, in the form of: IED name / logical device name / logical node name.GoID
Data Set	Select the data set, page 87 to include in the GOOSE control block. **NOTE:** Data set size cannot exceed 1500 bytes. If the size of the data set is exceeding the limitation an error message box prompts you, when clicking **Validate All** button.
Publishing area:	
MAC Address[1]	Enter the multicast address for GOOSE filtering. Valid values include: 01-0C-CD-01-00-01 ... 01-0C-CD-01-01-FF

Setting	Description
VLAN ID[1]	Enter the VLAN ID for the GOOSE control block. A 3-character value that can include 0...9, and A...F. GOOSE subscribers use this to filter received messages based on VLAN identity. Default = 000. **NOTE:** A setting of 000 indicates no VLAN ID is required. Switching equipment drops the VLAN tag when VLAN ID is set to 000.
APP ID[1]	Enter the APP ID for the GOOSE control block. A 4-character value that can include 0...9, and A...F. GOOSE subscribers use this to filter received messages based on the application configuration. Default = 0.
VLAN Priority[1]	Select the priority, 0...7, to be applied to VLAN transmissions of the GOOSE control block. Ethernet switches that manage the VLAN use this value to prioritize messages in their packet transmission queues.
Min. Time (ms)[1]	Enter the minimum time, from 20...1000 ms, between VLAN transmissions containing this GOOSE control block. Confirm that the minimum time is less than the maximum time.
Max. Time (ms)[1]	Enter the maximum time, from 20...1000 ms, between VLAN transmissions containing this GOOSE control block. Confirm that the maximum time is greater than the minimum time.
1 This setting is enabled only if **GOOSE Publishing** is selected. Otherwise, it is disabled and contains no value.	

Creating a New GOOSE Control Block

To create a new GOOSE control block, follow these steps:

Step	Action
1	In the **GOOSE Control** list, click the **+** button. **Result**: A new GOOSE control block appears in list, with the default name *goosectrln* (where n represents the sequential number of the control block).
2	Enter values for the **Parameters** and **Publishing** settings. Refer to the section GOOSE Control Settings, page 93 (above). **NOTE:** To enter a setting value, click **Enter** or move your cursor and click outside the setting input field.
3	**Save** the new GOOSE control block.

Editing an Existing GOOSE Control Block

To edit an existing GOOSE control block, follow these steps:

Step	Action
1	In the **GOOSE Control** list, select an existing control block. **Result**: The settings for the selected GOOSE control block appear in the **Parameters** and **Publishing** areas.
2	Enter values for the **Parameters** and **Publishing** settings. Refer to the section GOOSE Control Settings, page 93 (above). **NOTE:** To enter a setting value, click **Enter** or move your cursor and click outside the setting input field.
3	**Save** your edits.

Removing a GOOSE Control Block

To remove a GOOSE control block from the IEC 61850 Server follow these steps:

Step	Action
1	In the **GOOSE Control** list, select an existing control block. **Result**: The settings for the selected GOOSE control block appear in the **Parameters** and **Publishing** areas.
2	Click the **–** button. **Result**: The control block is removed from the list.
3	**Save** your edits.

Working with SOE Data Sets

Introduction

You can use the Modicon IEC 61850 Configuration Tool to create a data set in the IEC 61850 server of the BMENOP0300 module that links to data produced by an SOE module. After the SOE data set is created, you can use it to populate the data fields of a report control block.

Use the **SOE Data Set** window to:

- View the list of existing SOE data sets.
- Create a new SOE data set.
- Edit the contents of a new or existing SOE data set by:
  - adding data attributes to, or removing data attributes from the data set collection
  - assigning an **Event ID** value to each data attribute in the collection
- Remove an SOE data set from the IEC 61850 server.

Before you can use the **SOE Data Set** window, confirm that you have done the following:

- Enable the IEC 61850 server, page 48 in the BMENOP0300 module.
- Create a new server instance, page 74 for the module.

Creating an SOE Data Set

To create a new SOE data set, follow these steps:

Step	Action
1	In the **SOE Data Set** list, click the **+** button. **Result**: A new data set appears in the data set list with the default name 'SOEDataSet*n*' (where *n* represents the sequential number of the SOE data set).
2	Do one of the following: • Accept the default data set name. • Double-click the default name, type a new name, and select **Enter**.
3	In the **Description** area, do one of the following: • Accept the default data set description, which is the reference path to the data set. • Type in a different description.
4	The multiple SOE event transfer functionality requires: • IEC61850 configuration Tool version 3.3 or any subsequent supporting version(s) • Control Expert 15.3 or any subsequent supporting version(s) • BMENOP0300 module firmware SV2.60 or any subsequent supporting version(s). To configure the SOE data set allowing transfer of multiple SOE events in each controller cycle, select **Enable** in the **Max Concurrent SOE Events No.** area. Then select in the drop list the maximum concurrent SOE events you want to transfer in each controller cycle. **NOTE:** You can configure SOE data sets with different maximum concurrent SOE events.
5	In the **Data Object Filter**, use the filtering lists to navigate to the data attribute you want to add to the data set. Make filtering selections for: • **IED**: Select the IED name of the IEC 61850 server. • **LDevice**: Select an IEC 61850 server logical device. • **LNode**: Select a logical node associated with the selected logical device. • **FC**: Select a functional constraint. • **DA**: Select a data object with the same functional constraint in the selected logic node. **Result**: data attribute list, located below the filtering lists, presents the data attributes that fulfill the selected filtering criteria.

Step	Action
6	To add data attributes to the data set, drag a data object node from the data attribute list and drop it in the **FCDA** table. **Result**: The **FCDA** table displays the data set in nested groups, as follows: **LDevice > LNode > Data Object > Data Attribute**
7	Input an Event ID for the data attribute you added to the data set. **NOTE:** • For a Quantum ERT, Event Id is the channel number (1...32). • For Mx80 SOE, the Event Id is the channel number (0...15). • For an Mx80 CRA, the Event ID is generated by Control Expert.
8	Repeat the steps 5, 6 and 7 until all data attributes are added to the data set.
9	**Save** your edits.

Editing an Existing SOE Data Set

To edit an existing SOE data set, follow these steps:

Step	Action
1	In the **Data Set** list, select an existing SOE data set. **Result**: The data references of the selected data set appear in the **FCDA** table.
2	To add data references, follow steps 5 to 7 in the procedure “Creating an SOE Data Set” above.
3	To remove data references, select one or more data reference items in the **FCDA** table and right click **Delete**.
4	**Save** your edits.

Viewing Data Set Contents

To display the data references assigned to an SOE data set, select the SOE data set in the **Data Set** list. The data attributes appear in the **FCDA** table.

Removing a Data Set from the IEC 61850 Server

To remove a data set from the IEC 61850 Server, follow these steps:

Step	Action
1	Confirm that the data set you want to remove has not been added to the data model, page 79.
2	In the **Data Set** list, select an existing SOE data set. **Result**: The data references of the selected data set appear in the **FCDA** table.
3	Click the **–** button. **Result**: The SOE data set is removed from the list.
4	**Save** your edits.

Subscribing to GOOSE Control Blocks from External References

Introduction

You can configure the IEC 61850 server in the BMENOP0300 module to subscribe to GOOSE published by external IEDs.

The method of subscribing to remote GOOSE data is different for the IEC 61850 client and server:

- For the IEC 61850 server, use the **External Reference** window to map the data attributes of a remote IED to the data attributes of the local IED. The data attributes of the local IED are updated with changes when the server receives the GOOSE published by remote IED.
- For the IEC 61850 client, use the **Control Block** tab of the **I/O Mapping** window to subscribe to GOOSE data configured in a remote IED. Map the related data attributes in I/O mapping so that you can locate the data attributes that are updated after receiving data.

In the **External Reference** window, the BMENOP0300 module adds the data attributes (DAs) subscribed from the external IED to the controller memory, then updates the values of the subscribed DAs as they change. The BMENOP0300 module performs this update when operating in either normal or simulation mode.

For GOOSE subscriptions in simulation mode, it is possible to control LPHD.sim.stVal to receive or reject GOOSE data attribute for the server. Note that the client does not support simulation mode and will ignore all GOOSE that are marked as simulation.

When the BMENOP0300 module receives a GOOSE update, the relative diagnostic information is collected with dedicated DDT instances of IED_GOOSE.

LGOS is not supported automatically when subscribing to GOOSE, but it is possible to manage LGOS in your controller application using GOOSE diagnostic information.

Use the **External Reference** window to:

- Create mapping items that associate data attributes of the local BMENOP0300 module to data attributes contained in GOOSE messages published by an external module.
- Edit mapping items you previously created.
- Remove mapping items you previously created.

Before you can use the **External Reference** window, confirm that you have done the following:

- Enable the IEC 61850 server, page 48 resident in the BMENOP0300 module.
- Create a new server instance, page 74 for the module.

Mapping Internal Data Attributes to GOOSE External References

Follow these steps to map the internal data attributes (that you want to receive and store external data) to the external data attributes in a GOOSE transmission:

Step	Action
1	In the **External** panel, click the **Import SCD / CID** button. **Result**: The **Importing external IED** dialog box appears.
2	In the **Importing external IED** dialog box, click the ellipsis button. **Result**: The **Open** dialog box displays.
3	In the **Open** dialog box, navigate to and select an SCD or CID file; then click **Open**.

Step	Action
4	In the **Select IED to Import** list, select the **IED** that publishes the data you want to import, and click **OK**. **NOTE:** Because all imported IEDs are managed in the same space, confirm that each imported IED has a unique name. The software will not import IEDs with same name as previously imported IED.
5	In the **GOOSE** list, select the control block that contains the data you want to import. **Result**: The external reference list, located below the **External** filtering selections, presents the external references that satisfy the selected filtering criteria.
6	In the **External** panel, select a data attribute from the external references list, then drag it to the area marked **Drag external information here to create mapping**. A row is added to the **Mapping** table, and the data attribute you added appears on the left side of the newly added mapping item. **Result**: Select the right box of the data item in the **Mapping** table to which you want the external reference mapped. Repeat this step as many times as there are mapping items to populate.
7	In the **Internal** data panel, use the filtering lists to select the data attribute you want to add to the controller memory. Filtering items include: • **IED**: the read-only name of the module • **LDevice**: Select an IEC 61850 server logical device. • **LNode**: Select a logical node associated with the selected logical device. • **FC**: Select a functional constraint. **Result**: The data attribute list, located below the filtering selections, presents the data attributes that satisfy the selected filtering criteria.
8	Use your cursor to select a data attribute in the **Internal Data Objects** data attribute list, and drag it to the right box of the data item in the **Mapping** table to which you want the internal data item mapped. **NOTE:** When you select an internal data attribute, confirm that it is the same data type as the data item to which it is mapped. If you attempt to map data items of different types, a message box opens indicating the attempted mapping is not permitted. Repeat this step as many times as there are mapping items to populate.
9	When you finish adding mapping items, **Save** your edits.

Editing Mapping Items

After a mapping item is created, by adding both an internal data attribute and an external reference, you can edit the item by replacing the internal data attribute.

To edit the internal data attribute, follow these steps:

Step	Action
1	In the **Internal Data Objects** filter, navigate to the data attribute you want to add.
2	Select the replacement internal data item, and drag it to the right box of a mapping item. The new internal data item overwrites the old one.

Deleting a Mapping Item

To delete an item from the mapping list, select the item in **Mapping** panel, then right click and select **Delete**.

Configuring the IEC 61850 Client

Introduction

This chapter shows you how to configure the module as an IEC 61850 client.

Before configuring client properties, enable the IEC 61850 client function in the General, page 47 window. After you enable the IEC 61850 client function, click the **IEC 61850 Client Settings** button to open the Client Settings window, page 100.

Configuration

Overview

Use the **IEC 61850 Client** window to import IEDs into, and delete IEDs from, your project. After you add an IED to your project, you can:

- View basic information (including the IP address) and the data structure describing the IED.
- Use the **I/O Mapping** window to map data objects and data attributes from the IED server to PAC memory addresses.
  - Use the **Parameter** tab to map data object and data attributes from the IED model to a PAC memory address. The mapping data could be updated via report, GOOSE, or polling. The report has the highest performance.
  - Use the **Control Block** tab to map a report control block, GOOSE control block or Dons/ SBOns/Does/SBOes control block from the IED model to PAC memory address. The related DDT, page 120 will be generated.
  - Write PAC program to control the Report, GOOSE, polling and Dons/ SBOns/Does/SBOes control block to trigger the BMENOP0300 to communicate with the remote IED.

To use the **IEC 61850 Client** window, enable the IEC 61850 client, page 48 resident in the BMENOP0300 module.

Importing an IED

To import an IED into your project, follow these steps:

Step	Action
1	In the **IEC 61850 Client** window, click the **Import IEDs** button  . **Result**: The **Import IED** dialog box opens.
2	In the **Select CID/SCD file** area, do the following: 1. Click the browse button. An **Open** dialog box opens. 2. Navigate to and select the CID or SCD file that contains the IEDs you want to add. 3. Click **OK** to close the dialog box. **Result**: The **Select IED to Import** list populates.
3	Select one or more IEDs from the **Select IED to Import** list.
4	Click **OK** to close the **Import IED** dialog box. **Result**: Each selected IED is displayed in its own tile in the **IEC 61850 Client** window, with the IED name appearing in the tile header.
5	**Save** your edits.

Displaying IED Information

After importing an IED, you can use the IEC 61850 client window to view basic information and the data structure of the IED. Basic information for the imported IED server includes the following read-only settings:

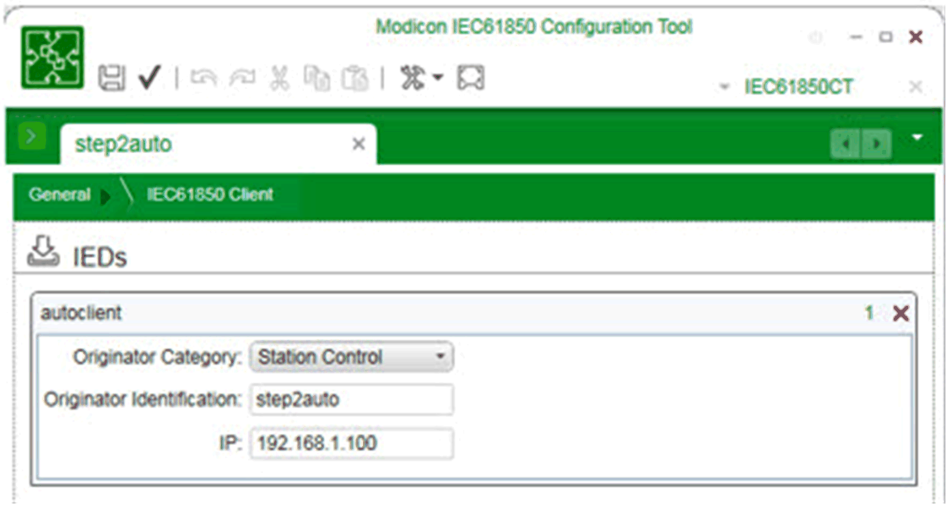
Setting	Description
Originator Category	The basis for changing values and IEC 61850 control services: • Bay Control: control operation issued from an operator using a client located at bay level • Station Control: control operation issued from an operator using a client located at station level • Remote Control: control operation from a remote operator outside the substation (for example: network control center) • Automatic Bay: control operation issued from an automatic function at bay level • Automatic Station: control operation issued from an automatic function at station level • Automatic Remote: control operation issued from an automatic function outside of the substation • Maintenance: control operation issued from a maintenance/ service tool • Process: status change occurred without control action (for example: external trip of a circuit breaker or detected error inside the breaker)
Originator Identification	The configurable address of the originator that caused a change of a controllable value. If NULL, the originator of a particular action is not known or not reported.
IP	an editable 32-bit IP address assigned to the server in the imported IED, including both network and host components **NOTE:** Examine the IP parameters in this field to confirm that the imported IP address matches your client file (.icd). If the IP addresses do not match, manually enter the appropriate address here.

Configuring the IEC 61850 Client

Configuring the IEC 61850 client includes the following tasks:

A . View Basic IED Information

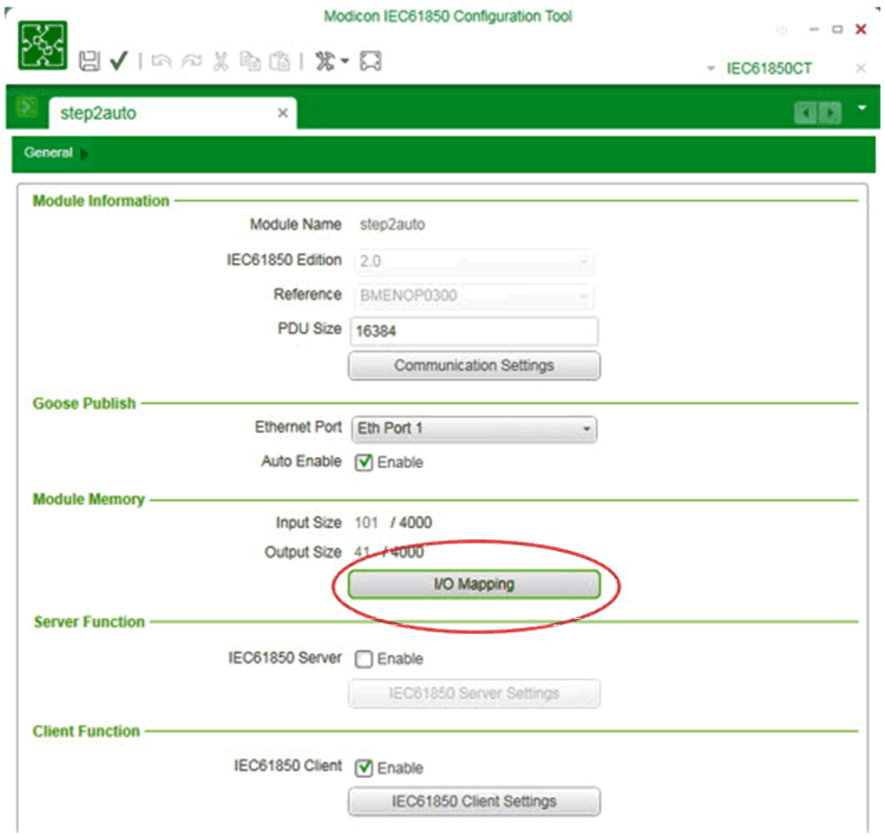
Use the IEC 61850 client window to display basic IED information, page 101. This information is used in the control operation and can be edited:



B. Use I/O Mapping

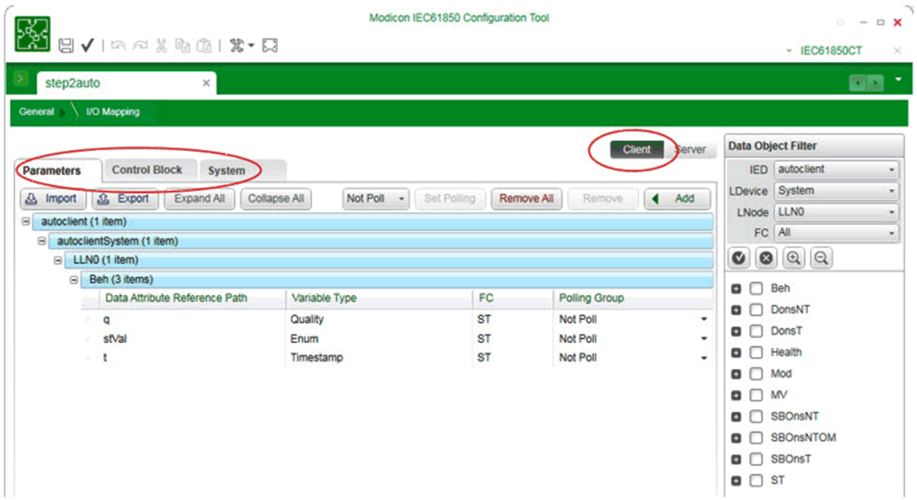
Use the I/O Mapping window to map data objects and associated data attributes from the IED server to the PAC DDT. Achieve this through the following steps:

1. In the **General** window, click the **I/O Mapping** button:

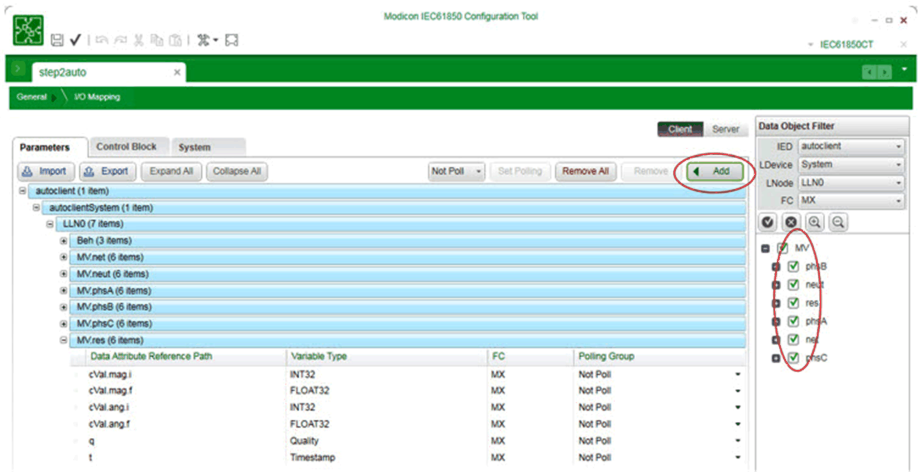


   The **I/O Mapping** window, in step 2. below, opens.

2. In the **I/O Mapping** window, click the **Client** button to display the client I/O mapping interface (because the default interface is for server mapping). The client I/O mapping interface displays 3 tabs: **Parameters**, **Control Block**, and **System**:



3. Configure the parameters and control block settings. Click the **Parameters** and **Control Block** tabs to toggle between these frames. When configuring parameters, you can drag parameters from the **Data Object Filter** to the **Parameters** frame. If you want to configure a series of parameters, you can select these parameters in the **Data Object Filter**, then click the **Add** button in the **Parameters** frame, and all the selected parameters will be mapped:



In the control block frame, you can configure the Control and Report control block. The FC drop-down menu presents four items. If you select:

- CO, you can see the Control control blocks under the current LNode.
- GO, you can see the GOOSE control block under the LNode.
- BR, you can see the BRCB block under the LNode.
- UR, you can see the URCB block under the LNode.

To configure the **Polling Group** control block, in the I/O Mapping frame select the parameters you want to poll, and in the Polling Group column select the group you want to set. The default is Not Poll.

C. Using the Control Block

The block will not work until you change the Cmd of the block. To send out a request or command to a server, first enter values for the block's other attributes, and only then change the value of the Cmd. For example, if you want to enable a report, follow these steps:

1. Set the Index value of the Report Block. Before setting the value, you need know if the Report Block is indexed. If not, accept the default Index value of 0. Otherwise set this to a value between 1 and the maximum value (which can be found in the server's model file).
2. Set the Attribute value. If you want to enable the Report, set the value to 1. Otherwise set the value to 0.
3. Change the Cmd value.

D. Enable/Disable Report Backfill

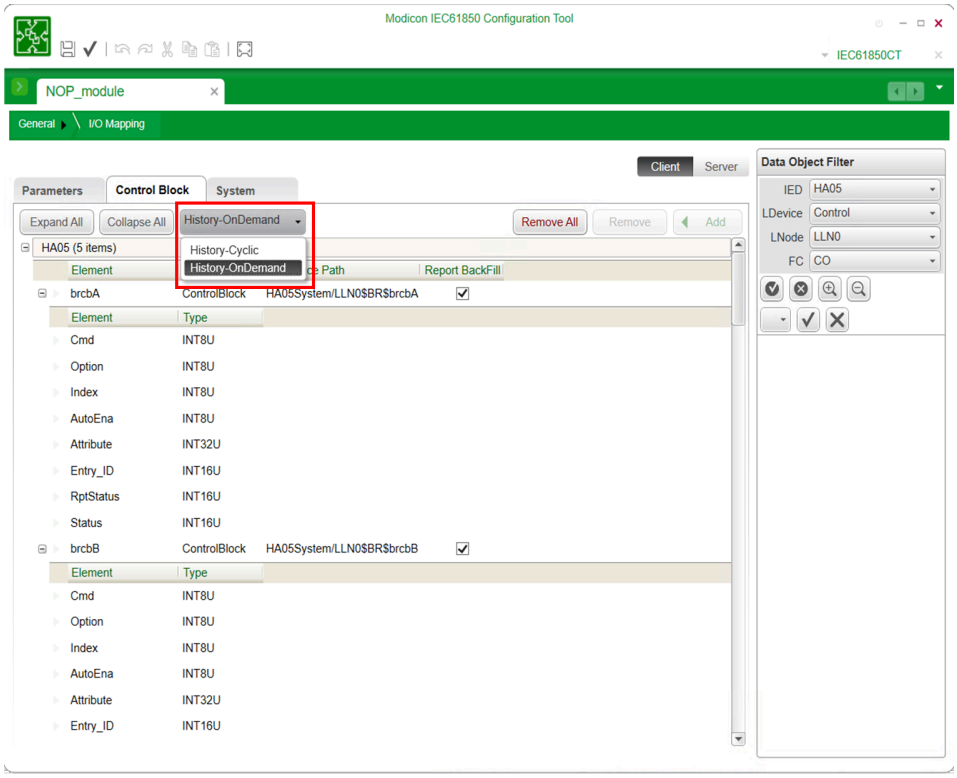
When click the **Control Block** panel, tool allows you to enable or disable report backfill feature and backfill mechanism: Cyclic or OnDemand.

- **Report Backfill**: it will generate specific Device DDT which receives buffered MMS report when connection recovery from remote IED and BRCB is enabled.
- **Cyclic mode**: to set refresh rate to publish buffered data.
- **On-demand mode**: manually publish buffered data.

NOTE:

The minimum firmware version for this feature is SV2.71.

The minimum IEDCT version for this feature is V3.41.



Deleting IEDs

To delete an IED that has previously been imported into the IEC 61850 client, follow these steps:

Step	Action
1	Click the **Delete IED** button ✕ located in the upper right corner of each IED tile, **Result**: The **Confirm** dialog box opens asking you if you are sure you want to delete the IED.
2	Click **Yes**. **Result**: The IED is removed from the collection.
3	**Save** your edits.

Working with IEC 61850 Data Objects

Overview

This chapter shows you how to map data attributes to controller memory using the **I/O Mapping** window; then shows you how to use the new data objects in your program logic.

Mapping Data Attributes to Controller Memory

Introduction

You can use the **I/O Mapping** window to link IEC 61850 client and IEC 61850 server data items to memory locations in the controller. You can access data items by navigating through the IEC 61850 protocol data structure:

IED > LDevice > LNode > Functional Constraint (FC)

The **I/O Mapping** window supports the following functional constraints:

FC	Server	Client	Description
BR	–	√	Buffered report control block
CF	–	–	Configuration value
CO	√	√	Process control service command or status
DC	–	–	Description attribute
GO	–	√	GOOSE report control block
MX	√	√	Process measurement value
RP	–	√	Unbuffered report control block
ST	√	√	Process status value
√ The FC is supported. – The FC is not supported.			

There are three groups of data items:

- *System* items contain the operating status of a module. System data items, for both the client and server, are automatically mapped to the controller. You cannot add items to, or delete items from, the system data table is fixed.
- *Parameter* items can originate with either the client or the server. No parameters are mapped to the controller by default. You can add both client and server data objects and data attributes to the mapping table.
- *Control block* items contain data provided by the following control blocks and services:
  - unbuffered report control blocks (RP)
  - buffered report control blocks (BR)
  - GOOSE control blocks (GO)
  - process control service command (CO)
  - polling group service

  NOTE: Polling group service data items are not displayed by the Modicon IEC 61850 Configuration Tool. Instead, they are included in the data structure created by Control Expert when you click the **Update application** button in the **Configuration** tab of the BMENOP0300 module **Properties** window.

Viewing System Data Items

To view *system* data items, follow these steps:

Step	Action
1	In the **I/O Mapping** window, select one of the following: • **Server** to display data items for the IEC 61850 server • **Client** to display data items for the IEC 61850 client
2	Click the **System** tab. The mapping table displays system data items for the module in its role as server or client.

Adding Parameter Data Items

To add *parameter* data items, follow these steps:

Step	Action
1	In the **I/O Mapping** window, select one of the following: • **Server** to display data items for the IEC 61850 server • **Client** to display data items for the IEC 61850 client
2	Click the **Parameters** tab. The **Data Object Filter** presents data objects associated with the selected tab.
3	In the **Data Object Filter**, make the following selections: 1. In the **IED** list, select an IED. **NOTE:** If you selected **Server** in step 1, the server IED is pre-selected. 2. In the **LDevice** list, select a device. 3. In the **LNode** list, select the logical node object that contains the data object (attributes) you want to map to an address in the controller. 4. In the **FC** list, select the functional constraint for the data attributes you want to map to an address in the controller. 5. Expand the **Beh**, **Health**, and **Mod** menus and click the appropriate *t* (timestamp) or *q* (quality) attributes to select them. The **Data Object Filter** displays the associated data objects and data attributes.
4	Select a data object or data attribute in the **Data Object Filter**, and then drag it to the mapping table in the **Parameters** tab. If you selected a: • Data object: The data object and all its associated data attributes are added to the table. • Data attribute: Only the selected data attribute is added to the table. **NOTE:** The data object order of data mapping depends on the structure defined in the data model, page 79.
5	If you selected **Client** in step 1, expand the mapping table to display each data attribute, then edit the **Polling Group** setting for the attribute. Settings include: • Not Poll: Indicates client can update data via control block (default) • Group-1 • Group-2 • Group-3 • Group-4 • Group-5
6	Repeat steps 2...5 for each data object or data attribute you want to add to map to a located memory address in the controller.
7	**Save** your edits.

When you finish configuring the BMENOP0300 module, close the Modicon IEC 61850 Configuration Tool, then click **Update application** in the **Configuration** tab of the module **Properties** window. Control Expert creates DDT variables for each

data attribute, page 111 and displays each new DDT variable in the Control Expert **Data Editor**.

Adding Control Block and Service Data Items

To add data attributes from remote IEDs to the BMENOP0300 module in its role as IEC 61850 client, follow these steps:

Step	Action
1	In the **I/O Mapping** window, click **Client**. **Result**: The **Data Object Filter** presents the IEDs associated with the module in its role as IEC 61850 client.
2	In the **I/O Mapping** window, click **Control Block**. **Result**: The **Data Object Filter** presents data objects associated with the selected tab.
3	In the **Data Object Filter**, drill down to the data attributes you want to add, by making the following selections: 1. Select an **IED**. 2. Select an **LDevice** object. 3. Select an **LNode** object. 4. Select an **FC** object. Depending on the specific IED content, you can select: • BR: buffered report control block • RP: unbuffered report control block • CO: process control value service • GO: GOOSE control block **Result**: The **Data Object Filter** displays the associated data objects and data attributes.
4	Select a item in the **Data Object Filter**, and then drag it to the mapping table in the selected tab.
5	Repeat steps 2...4 for each data item you want to add to map to a located memory address in the controller.
6	**Save** your edits.

Each block you add displays the following columns:

- **Element**:

  the name of the control block, up to thirteen ASCII character (If the original name exceeds the maximum length, a dialog box asks you to edit and shorten this value.)
- **Variable**:

  the concatenation of the **Element** value and the device DDT
- **Type**:

  the type of mapping item: a control block or elementary variable
- **Device DDT**:

  the device DDT of the mapped item in the PAC
- **IED**:

  the name of the IED to which the mapped item belongs
- **Reference Path**:

  the IEC 61850 protocol reference path to the control block or data object
- **Array**:

  a check mark indicating this element is an array
- **Length**:

  for array elements, the number of items in the array

When you finish configuring the BMENOP0300 module, close the Modicon IEC 61850 Configuration Tool, then click **Update application** in the **Configuration** tab of the module **Properties** window. Control Expert creates DDT variables for each

data attribute, page 111 and displays each new DDT variable in the Control Expert **Data Editor**.

Removing Data Attributes from the Mapping Table

To remove one or more data attributes from a mapping table, follow these steps:

Step	Action
1	In the mapping table, select an item you want to delete.
2	Click the right mouse button to open a context menu.
3	Click **Delete** to remove the selected data items from the mapping table.
4	Repeat steps 1...3 for each item you want to delete.
5	**Save** your edits.

Export I/O Mapping File for Server IED

To export an I/O mapping file for the server IED, follow these steps:

Step	Action
1	In the **I/O Mapping** window, select **Server**.
2	Confirm that the mapping table of the server is not empty.
3	Click **Export**.
4	In the **Save As** dialog box: • Navigate to the location where you wish to save the mapping file. • (Optionally) Change the file name. • Click **Save**. The file, with a .map extension, is saved to the target location.

Import I/O Mapping File for Server IED

To import an I/O mapping file for the server IED, follow these steps:

Step	Action
1	In the **I/O Mapping** window, select **Server**.
2	Confirm that the mapping table of the server is not empty.
3	Click **Import**.
4	In the **Open** dialog box: • Navigate to and select the mapping file to be imported. **NOTE:** Confirm that the name of the selected mapping file is the same as the name of the server IED name. • Click **Open**.
5	The **Confirm** dialog box opens and asks if you want to import the selected mapping file. Click **Yes**.
6	If you selected a mapping file with a name different than the server IED name, an **Error** message displays asking you to confirm the mapping file name. Click **OK** and return to step 4, above.
7	If you selected a mapping file with the correct name and format, all the pre-existing mapping items in the server IED are removed, and the items in the mapping file are imported.

Export I/O Mapping File for Client IED

To export an I/O mapping file for the client IED, follow these steps:

Step	Action
1	In the **I/O Mapping** window, select **Client**.
2	In the **Data Object Filter**, select the name of the IED to be exported, and confirm that the mapping table of the client is not empty.
3	Click **Export** to generate a mapping file for the selected client IED.
4	In the **Save As** dialog box: • Navigate to the location where you wish to save the mapping file. • (Optionally) Change the file name. • Click **Save**. The file, with a .map extension, is saved to the target location.

Import I/O Mapping File for Client IED

To import an I/O mapping file for the client IED, follow these steps:

Step	Action
1	Confirm that the target client IED file to be imported exists.
2	In the **I/O Mapping** window, select **Client**.
3	Click **Import**.
4	In the **Open** dialog box: • Navigate to and select the mapping file to be imported. **NOTE:** Confirm that the name of the selected IED name exists in the current project. • Click **Open**.
5	The **Confirm** dialog box opens and asks if you want to import the selected mapping file. Click **Yes**.
6	If you selected an IED name that does not exist in the current project, an **Error** message displays asking you to confirm the IED name. Click **OK** and return to step 4, above.
7	If you selected an IED with the correct name and format, all the pre-existing items in the client IED are removed, and the mapping file is imported for the target client IED.

Understanding the Relationship Between the PAC Scan Time and the Quantity of I/O Data

The BMENOP0300 module cyclically exchanges data with the PAC controller. The data included in this cyclical exchange depends on the PAC scan time and the amount of data to be exchanged. You will want to apply a PAC scan time that is sufficiently long to permit the exchange of all data between the module and the controller. The following formula applies:

PAC scan time > Max[10 ms, (DataSum/150) ms]

In this formula, DataSum is the amount of input data, in bytes, that is available in the module memory of the IEC 61850 configurator.

The following examples apply the above formula to determine a minimum suggested PAC scan time:

Example	DataSum (input data to be exchanged, in bytes)	Minimum Suggested PAC Scan Time
1	300	10 ms
2	3000	20 ms

Working with IEC 61850 Data Objects

Introduction

After you select data items in the **I/O Mapping** window, click **Update application**. Control Expert creates the following data objects for each BMENOP0300 module in your project:

- a **DDT** located variable structure, including:
  - {Module_name}_MOD_INFO
  - {Module_name}_MOD_CONTROL
  - {Module_name}_{IED name}
- a **Device DDT** unlocated variable structure that follows the IEC 61850 data model:

  Module > IED > DataModel > LD > LN > DO > <SDO> > DA

You can access the data stored in variables using the dot addressing notation of the IEC 61850 data model, for example: “Module.IED.DataModel.LDevice.LNode.DO.DA”.

Working with Device DDT Variables

In the **Variables** tab of the **Data Editor** window, the **Type** column displays values as follows:

- The top-most node displays the module name.
- Leaf (or end) nodes are of the data type, and point to the located variable identified in the **Value** column.

Working with Located Variables

Control Expert creates unlocated variables for each data attribute mapped in the **I/O Mapping** window. Click the **Variables** tab of the **Data Editor** to view the located address of each variable.

The IEC 61850 data model and Control Expert support different collections of data types, page 20. When Control Expert creates new located variables from IEC 61850 data attributes, it assigns each new variable a data type supported by Control Expert.

Controller State Management

IEC 61850 Server

The BMENOP0300 module stops detecting events (report/GOOSE) when the controller is stopped. However, any report could be triggered by an animation table. In this case, the GOOSE publishing continues with the last information. Integrity reports continue. The BMENOP0300 does not update its value of GOOSE subscription into the controller.

All the quality of the data object (DO) are invalid in the response to a read request from SCADA when the controller stops. In addition, the BMENOP0300 module supports the management of the PhyHealth data object (DO) in the LPHD node of each logic device. When the controller stops, the PhyHealth stVal is set to "warning" and returns to "OK" when the controller again begins to run. When the controller is stopped, the BMENOP0300 module denies all control operations.

IEC 61850 Client

When the controller stops, the BMENOP0300 module does **not** update its value of GOOSE subscription into the controller; it disconnects with the remote IEDs.

IEC 61850 Roles and Functions

Depending on the state of the controller, the following functions are supported:

IEC 61850 Role/Function	**Controller State**	
	Run	**Stop**
Server:		
• buffered and unbuffered reporting	X	X
• GOOSE	X	X
• control commands	X	–
Client:		
• buffered and unbuffered reporting	X	–
• GOOSE	X	–
• control commands	X	–
X: supported –: not supported		

DDT Data Structures

Introduction

If you enable the IEC 61850 server, enable the client, and create one or more report and GOOSE control blocks, Control Expert adds the following DDT data structures to your project:

- module information
- module control
- module diagnostic
- module state
- server state
- client state
- GOOSE control block
- control objects
- buffered report control block
- unbuffered report control block
- polling control block
- history report for client side

Module Information

The `{Module_name}_MOD_INFO` DDT presents information for the module, IED server, and IED client states, as well as the module control status, the names of which are the prefix of the DDT:

Element	Type	Description
MODULE_STATE	{Module}_STATE	global status of the BMENOP0300 modules
SERVER_STATE	{Module}_SERVER_ STATE	server diagnostic information
CLIENT_STATE	{Module}_CLIENT_STATE	client diagnostic information

Module Control

The `{Module_name}_MOD_CONTROL` DDT presents information for module control for networks redundancy, the name of which is the prefix of the DDT:

Element	Type	Description
DualModuleDiag[1]	ARRAY [0...8] of UDINT	module diagnostic. Its content is reserved for system usage and is not displayed by default in Control Expert. Its contents is a copy of `{Module_name}_MOD_DIAG`.
ModDiag[1]	MOD_DIAG	module diagnostic
ModuleControl[2]	WORD	module mode control, one bit per functions
SimulateMode[2]	BOOL	Bit 0: Effect on GOOSE publish • 0: normal mode • 1: simulation mode
ClearDiag[2]	BOOL	Bit 1: Clear diagnostic information of IEC 61850 • 1: clear, take effect on raise edge
[1] read only [2] read write		

Module Diagnostics

The `{Module_name}_MOD_DIAG` DDT presents read-only information for module diagnostics, the name of which is the prefix of the DDT. This data is updated by the IEC 61850 server:

Element	Type	Description
HeartBeat	UDINT	the counter of heart beat, increment per PAC cycle
ScanCount	UDINT	the counter of I/O data scan
CurEntryID	ARRAY [0...3] of WORD	entry ID
TimeStamp	TIME_850_FORMAT	time entry
ScanState	WORD	scan status • 0: idle • 1: on-going
ModelSig	UDINT	module signature

Module State

The `{Module_name}_MODULE_STATE` DDT presents diagnostic information for the IEC 61850 module, the name of which is the prefix of the DDT (read only):

Element		Type	Bit	Description
EthStatus		WORD	–	Ethernet status
	Port1Link	BOOL	0	link up/down for Ethernet port 1
	Port2Link	BOOL	1	link up/down for Ethernet port 2
	Port3Link	BOOL	2	link up/down for Ethernet port 3
	EthBkpPortLink	BOOL	3	link up/down for Ethernet backplane port
	NetworkStatus	BOOL	6	0: Traffic overload detected (example: broadcast storm). Check your network topology and configuration. 1: No traffic overload detected.
	GlobalStatus	BOOL	7	0: One or more services not operating normally. 1: Operational services.

Element		Type	Bit	Description
ServiceStatus		WORD	–	one bit for each user-observable feature
	RstpService	BOOL	0	0: Service not operating normally. 1: Service operating normally or disabled.
	Port502Service	BOOL	1	0: Service not operating normally. 1: Service operating normally or disabled.
	SnmpService	BOOL	2	0: Service not operating normally. 1: Service operating normally or disabled.
	MainIpAddressStatus	BOOL	3	main IP address status (0 in the case of duplicate IP or no IP assigned)
	IedServer	BOOL	6	0: Service not operating normally. 1: Service operating normally or disabled.
	IedClient	BOOL	7	0: Service not operating normally. 1: Service operating normally or disabled.
	SntpClient	BOOL	8	0: Service not operating normally. 1: Service operating normally or disabled.
	FirmwareUpgrade	BOOL	9	0: Service not operating normally. 1: Service operating normally or disabled.
	FtpServer	BOOL	10	0: Service not operating normally. 1: Service operating normally or disabled.
	LldpService	BOOL	11	LLDP service status
	EventLogStatus	BOOL	12	0: Event log service not operating normally. 1: Event log service operating normally or disabled.
	LogServerNotReachable	BOOL	13	0: Acknowledgment received from the syslog server. 1: No acknowledgment received from the syslog server.
	SNtpServerNotReachable	BOOL	15	0: Service not operating normally. 1: Service operating normally or disabled.
EthPort1Port2Status		BYTE	–	Ethernet port 1 and 2 status
	Port 1 function	–	0...-1	0: disabled 1: access port 2: mirror port 3: network port
	(Reserved)	–	2...-3	–
	Port 2 function	–	4...-5	0: disabled 1: access port 2: mirror port 3: network port
	RSTP Role	–	6...-7	0: alternate 1: backup 2: designated 3: root

Element		Type	Bit	Description
EthPort3BkpStatus		BYTE	–	Ethernet port 3 and backplane port status
	Port 3 function	–	0...-1	0: disabled 1: access port 2: mirror port 3: network port
	RSTP Role	–	2...-3	0: alternate 1: backup 2: designated 3: root
	Eth Bkp Port function	–	4...-5	0: disabled 1: access port 2: mirror port 3: network port
	(Reserved)	–	6...-7	–
FirmwareVersion		WORD	–	MSB: major revision LSB: minor revision
ServiceStatus2		WORD	–	One bit for each user-observable feature
	IPForwardingService	BOOL	0	0: Service not operating normally. 1: Service operating normally or disabled.
	Network3MainIpAddressStatus	BOOL	2	Network 3IP Address Status (0 if duplicate IP address or no IP address assigned)
FreeMemory		WORD	–	free dynamic memory space of module (KB) **NOTE:** Only for module with firmware version SV2.60 or any subsequent supporting version (s). For earlier firmware versions, the free memory value = 0.
InPackets		UINT	–	number of packets received
InErrors		UINT	–	number of inbound packets that contain detected errors
OutPackets		UINT	–	number of packets sent
OutErrors		UINT	–	number of outbound packets that contain detected errors
ConfSig		UDINT	–	Signature of configuration file

Server State

The `{Module_name}_SERVER_STATE` DDT presents diagnostic information for the IEC 61850 server in the module, the name of which is the prefix of the DDT:

Element	Type	Description
Active	`BOOL`	server status: • 0 = disabled • 1 = enabled
Health	`BOOL`	server health: • 0 = not operational • 1 = operational

Element	Type	Description
ProtoEd	BYTE	IEC 61850 protocol edition: • 0x10 = 1.0 • 0x20 = 2.0
ActiveConn	BYTE	number of established server connections
VariableRd	UDINT	count of read variable requests received by the server
VariableRdErr	UDINT	count of rejected MMS read variable requests
VariableWrt	UDINT	count of write variable requests received by the server
VariableWrtErr	UDINT	count of rejected MMS write variable requests
ReportsTx	UDINT	count of information report messages sent by the server
GooseTx	UDINT	count of GOOSE messages transmitted by the server
GooseRx	UDINT	count of GOOSE messages received by the server
GooseErr	UDINT	count of invalid GOOSE messages received by the server
ErrorCode (low word)	WORD	
InvalidConf	BOOL	low word: • 0x0001: invalid configuration • 0x0002: stack init error detected • 0x0004: config init error detected • 0x0010...0x00F0: BP comm error detected • 0x0100: DB binding error detected
StackInitErr	BOOL	
ConfInitErr	BOOL	
BpCommErr	BOOL	
DbBindErr	BOOL	
ErrorCode (high word)	WORD	
ClockNotSyn	BOOL	high word: • 0x1000: clock not synchronized • 0x2000: default IP • 0x4000: IP not available
DefaultIp	BOOL	
IPNotAvailable	BOOL	
RptEntity	IED_RPT[x], page 139	report diagnostic information
GooseEntity	IED_GOOSE[x], page 98	report diagnostic information

Client State

The {Module_name}_CLIENT_STATE DDT presents diagnostic information for the IEC 61850 client in the module, the name of which is the prefix of the DDT:

Element	Type	Description
Active	BOOL	client status: • 0 = disabled • 1 = enabled
Health	BOOL	client health: • 0 = not operational • 1 = operational
ProtoEd	BYTE	IEC 61850 protocol edition: • 0x10 = 1.0 • 0x20 = 2.0
ActiveConn	BYTE	number of established server connections: 0...16

Element	Type	Description
IEDHealth1	WORD	IED connection status: • 0 = disconnected • 1 = connected **NOTE:** Each bit represents one IED in the same order as the sequence of IEDs in the SCL file.
{IED_HEALTH}	BOOL	Bit-0
{IED_HEALTH}	BOOL	Bit-1
...	BOOL	...
{IED_HEALTH}	BOOL	Bit-15
IEDHealth2	WORD	IED connection status: • 0 = disconnected • 1 = connected **NOTE:** Each bit represents one IED in the same order as the sequence of IEDs in the SCL file.
{IED_HEALTH}	BOOL	Bit-0
{IED_HEALTH}	BOOL	Bit-1
...	BOOL	...
{IED_HEALTH}	BOOL	Bit-15
VariableRd	UDINT	count of read variable requests received by the server
VariableRdErr	UDINT	count of rejected MMS read variable requests
VariableWrt	UDINT	count of write variable requests received by the server
VariableWrtErr	UDINT	count of rejected MMS read variable requests
ReportsRx	UDINT	count of information report messages received by the client
GooseRx	UDINT	count of GOOSE messages received by the client
GooseErr	UDINT	count of invalid GOOSE messages received by the client
ErrorCode (low word)	WORD	
InvalidConf	BOOL	low word: • 0x0001: invalid configuration • 0x0002: stack init error detected • 0x0004: config init error detected • 0x0010: BP communication detected error • 0x0020: data dictionary disabled • 0x0100: DB binding error detected • 0x1000: Report ID mismatch detected
StackInitErr	BOOL	
ConfInitErr	BOOL	
BpCommErr	BOOL	
DdtRdErr	BOOL	
DbBindErr	BOOL	
RptidMismatch	BOOL	
Error Code (high word)	WORD	
ClockNotSyn	BOOL	High word: • 0x0001...0x00FF: configuration inconsistent (index of IED in SCL) • 0x1000: clock not synchronized • 0x2000: default IP address • 0x4000: IP not available
DefaultIp	BOOL	
IPNotAvailable	BOOL	
GooseEntity	IED_GOOSE [x]	report diagnostic information

GOOSE Diagnostics

The `{Module_name}_IED_GOOSE` DDT presents GOOSE control block diagnostic information for the IEC 61850 module, the name of which is the prefix of the DDT:

Element	Type	Description
Service	`BYTE`	• 0 = publish • 1 = GOOSE subscribe for server • 2 = GOOSE subscribe for client
Status	`BOOL`	• TRUE = active • FALSE = not active
NdsCom	`BOOL`	The Need Commission attribute has a value of TRUE if the GoCB requires further configuration when: • The attribute DataSet has a value of NULL. • The number or size of values being conveyed by the elements in the DatSet referenced data-set exceeds constraint determined by the SCSM or the implementation.
Simulation	`BOOL`	A value of TRUE indicates Sim messages are received and accepted.
LastStNum	`UDINT`	the last state number
LastSqNum	`UDINT`	the last sequence number
LastError	`UINT`	the last detected error: • 1: MAC not consistent with configuration. • 2: AppID not consistent with configuration. • 3: GOOSE data set not consistent with configuration. • 4: initAddr is missing. • 5: GOOSE not received after Time to Alive expired. • 6: stNum is out of order. • 7: sqNum out of order. • 8: GOOSE ConfRev not consistent with configuration. • 9: Decoding GOOSE data error detected. • 10: Other unknown detected errors. • 11: NdsCom = TRUE. • 12: Go Ref is incorrect.
Reserve	`UINT`	<reserved>

DDT Overview for Server

The `{Module}_{IED name}` DDT overview for the IEC 61850 server data structure is as follows:

Element	Type	Trigger	Definition
Freshness	BOOL	-	0: data is not fresh 1: data is fresh When there is no IEC 61850 connection or backplane communication, this element is set to 0 (FALSE).
-DataModel			

Element	Type	Trigger	Definition
-{LD}	{LD_Type} -{LN_Type} -{DO_Type} -{DA_Type} {LD_Type} -{LN_Type} -{DO_Type} -{DA_Type}	-	This definition can be viewed in the IEC 61850 Configuration Tool by navigating to **IEC61850 Server > Data Model**.
-{LD}	{LD_Type} -{LN_Type} -{DO_Type} -{DA_Type} {LD_Type} -{LN_Type} -{DO_Type} -{DA_Type}	-	This definition can be viewed in the IEC 61850 Configuration Tool by navigating to **IEC61850 Server > Data Model**.
... ...			
-DatasetSOE -{SOE DS name} -{SOE DS name}	{ERT_BUF}	-	It is used to transfer external events to the BMENOP0300 module.

DDT Overview for Client

The `{Module}_{IED name}` DDT overview for the IEC 61850 client data structure is as follows

Element	Type	Trigger	Definition
Freshness	BOOL	-	0: data is not fresh 1: data is fresh When there is no IEC 61850 connection or backplane communication, this element is set to 0 (FALSE).
ConenctCtrl	BOOL	-	0: Auto connect 1: disconnect
-Data Model			
-{LD}	{LD_Type} -{LN_Type} -{DO_Type} -{DA_Type} {LD_Type} -{LN_Type} -{DO_Type} -{DA_Type}	-	This definition can be viewed in the IEC 61850 Configuration Tool by navigating to **IEC61850 Server > Data Model**.

Element	Type	Trigger	Definition
-{LD}	{LD_Type} -{LN_Type} -{DO_Type} -{DA_Type} {LD_Type} -{LN_Type} -{DO_Type} -{DA_Type}	-	This definition can be viewed in the IEC 61850 Configuration Tool by navigating to **IEC61850 Server > Data Model**.
-PollBlock			Polling control for each IED
POLL_GRPx X= 1...5	{Module}_POLLING_ CTRL	-	
-ControlBlock			General control
-{LD}	{LD_Type} -{LN_Type} -{DO_Type} -{CB_Type} {LD_Type} -{LN_Type} -{DO_Type} -{CB_Type}	-	
-ReportBlock			Report control
{report cb name}	{LD_Type} -{LN_Type} - {{Module}_Report_BRCB} - {{Module}_Report_ URCB} ..... {LD_Type} -{LN_Type} - {{Module}_Report_BRCB} - {{Module}_Report_ URCB}	-	

Element	Type	Trigger	Definition
-gooseDiagnostic			Goose control block
{ModuleGoose-Diag}	{IED_1} {LD_1} {GooseName} {a} {b} {IED_2} {LD_1} {GooseName} {a} {b}	-	IEDName LD_Name GooseDiag BOOL BOOL IEDName LD_Name GooseDiag BOOL BOOL

Buffered Report Control Block

The data structure of the buffered report `{Report_name}_REPORT_BRCB` of the client function:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Option	BYTE	-	option: operation selection, whose values include: • 1: set RptEna • 2: set BufTms • 3: set IntgPd • 4: set ResvTms • 5: set TrgOps • 6: set OptFlds • 8: set EntryID • 9: set RptID **NOTE:** Execute option value 9 once before enabling the report control block in the server to receive report information. • 10: set DataSet **NOTE:** For set RptID and set DataSet commands, the source is the SCL file and cannot be set dynamically in controller memory. • 11: set GI • 12: set Purge buffer • 101: get RptEna • 102: get BufTms • 103: get IntgPd • 104: get ResvTms • 105: get TrgOps • 106: get OptFlds • 108: get EntryID • 120: get ConfRev • 121: get SgNum
Index	`BYTE`	-	buffer index number: 1...99 **NOTE:** If the Index element is set to 0 (FALSE), indexing is not used for this report. In this case, leave the element value at 0.

Element	Type	Trigger	Definition
AutoEna	BYTE	-	How is report enabled? • 0 = enable on demand • 1 = auto enable **NOTE:** Use Auto-enable so that the report is enabled in case of redundant switchover.
Attribute	DWORD	-	common area for read/write of attribute, depending on the selected option: • BufTms DWORD • IntgPd DWORD • ResvTms DWORD • ConfRev DWORD • TrgOps low WORD of attribute Refer to the BITSTRING topic, page 20 for the bit detail of trigger option. • OptFlds low WORD of attribute Refer to the BITSTRING topic, page 20 for the bit detail of option field. • SgNum low WORD of attribute • RptEna low WORD (bit 0) of attribute • GI low WORD (bit 0) of attribute • PurgeBuf low WORD (bit 0) of attribute
Entry_ID	UINT [4]	-	entry ID reported in the last response **NOTE:** Supported only by buffered report control blocks (BRCB).
RptStatus	WORD	-	• low byte: index of report control block (1...99) • high byte: ◦ bit 0 = ConfRev change ◦ bit 1 = buffer overflow
Status	WORD	-	Status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6..7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

AddCause Detected Error Codes

The following is a list of report and control object detected AddCause error codes:

Code	Short Description	Explanation of IEC 61850-7-2
1	Not-supported	Not supported.
2	Blocked-by-switching-hierarchy	Not successful, because one of the downstream Loc switches like in CSWI has the value TRUE.
3	Select-failed	Canceled due to an unsuccessful selection (select service).
4	Invalid-position	Control action is aborted due to invalid switch position (Pos in XCBR or XSWI).
5	Position-reached	Switch is already in the intended position (Pos in XCBR or XSWI).
6	Parameter-change-in-execution	Control action is blocked due to running parameter change.
7	Step-limit	Control action is blocked because tap changer has reached the limit EndPosR or EndPosL in YLTC).

Code	Short Description	Explanation of IEC 61850-7-2
8	Blocked-by-Mode	Control action is blocked because the LN (CSWI or XCBR/XSWI)is in a mode (Mod) which does not allow any switching.
9	Blocked-by-process	Control action is blocked due to some external event at process level that prevents a successful operation for example blocking indication (EEHealth in XCBR or XSWI).
10	Blocked-by-interlocking	Control action is blocked due to interlocking of switching devices (in CILO attribute EnaOpn.stVal= FALSE or EnaCls.stVal= FALSE).
11	Blocked-by-synchrocheck	Control action with synchrocheck is aborted due to exceed of time limit and missing synchronism condition.
12	Command-already-in-execution	Control select or cancel service is rejected because control action is already running.
13	Blocked-by-health	Control action is blocked due to some internal event that prevents a successful operation (Health).
14	1-of-n-control	Control action is blocked because another control action in a domain (for example substation) is already running (in any XCBR or XSWI of that domain the DPC.stSeld= TRUE).
15	Abortion-by-cancel	Control action is aborted due to cancel service.
16	Time-limit-over	Control action is terminated due to exceed of some time limit.
17	Abortion-by-trip	Control action is aborted due to a trip (PTRC with ACT. general = TRUE).
18	Object-not-selected	Control action is rejected because control object was not selected.
19	Object-already-selected	Select action is not executed because the addressed object is already selected.
20	No-access-authority	Control action is blocked due to lack of access authority.
21	Ended-with-overshoot	Control action executed but the end position has overshoot.
22	Abortion-due-to-deviation	Control action is aborted due to deviation between the command value and the measured value.
23	Abortion-by-communication-loss	Control action is aborted due to the loss of connection with the client that issued the control.
24	Blocked-by-command	Control action is blocked due to the data attribute CmdBlk.stVal is TRUE.
25	None	Command not successful due to Unknown causes.
26	Inconsistent-parameters	The parameters between successive control services are not consistent for example the ctlNum of Select and Operate service are different.
27	Locked-by-other-client	Another client has already reserved the object.

Detected Error Codes

The following is a list of detected error codes for operations (polling, report control, GOOSE control and general control):

Function	Code	Short Description	Explanation of IEC 61850-7-2
Control point	1...27	AddCause	Refer to AddCause, page 123 detected errors.
	61	Disconnected	Offline with remote IED
	63	Input parameter error detected	Input parameter in data block is incorrect. For example, a CtlVal is out of range.
Polling	61	Disconnected	Offline with remote IED
	62	Polling did not succeed	One or more DOs or DAs are missing in remote IED. Polling will continue if this error is detected.
	63	Input parameter error detected	Input parameter in data block is incorrect.
Report Control	60	Auto-enable did not succeed	A report was not enabled after going online. Check the AutoEna element setting of the control block.
	61	Disconnected	Offline with remote IED
	63	Input parameter error detected	Input parameter in data block is incorrect.
GOOSE Control	0	GOOSE disabled	GOOSE control block is disabled
	1	GOOSE enabled	GOOSE control block is enabled
	61	Disconnected	Offline with remote IED

Unbuffered Report Control Block

The data structure of the unbuffered report `{Report_name}_REPORT_URCB` of the client function:

Element	Type	Trigger	Definition
Cmd	`BYTE`	Dchg	trigger: effective on change
Option	`BYTE`	-	option: operation selection, whose values include: • 1: set RptEna • 2: set BufTms • 3: set IntgPd • 5: set TrgOps • 6: set OptFlds • 7: set ResvUrcb • 9: set RptID • 10: set DataSet **NOTE:** For set RptID and set DataSet commands, the source is the SCL file and cannot be set dynamically in controller memory. • 11: set GI • 101: get RptEna • 102: get BufTms • 103: get IntgPd • 105: get TrgOps • 106: get OptFlds • 107: get ResvUrcb • 111: get GI • 120: get ConfRev • 121: get SgNum
Index	`BYTE`	-	buffer index number: 1...99 **NOTE:** If the Index element is set to 0 (FALSE), indexing is not used for this report. In this case, leave the element value at 0.

Element	Type	Trigger	Definition
AutoEna	BYTE	-	How is report enabled? • 0 = enable on demand • 1 = auto enable **NOTE:** Use Auto-enable so that the report is enabled in case of redundant switchover.
Attribute	DWORD	-	common area for read/write of attribute, depending on the selected option: • BufTms DWORD • IntgPd DWORD • ConfRev DWORD • GI low WORD of attribute • TrgOps low WORD of attribute Refer to the BITSTRING topic, page 20 for the bit detail of trigger option. • OptFlds low WORD of attribute Refer to the BITSTRING topic, page 20 for the bit detail of option field. • SgNum low WORD of attribute • RptEna low WORD (bit 0) of attribute • UrcbResv low WORD (bit 0) of attribute
RptStatus	UINT	-	• low byte: index of report control block (1...99) • high byte: bit 0 = ConfRev change
Status	STATUS	-	Status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6..7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

GOOSE Control Block

The data structure of the {Module_name}_GOOSE_CB DDT:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Option	BYTE	-	option: operation selection: • 0 = GOOSE disable • 1 = GOOSE enable • 2 = Get GoCB
Status	WORD	-	status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6..7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

Polling Control Block

The data structure of the {Module_name}_POLLING_CTRL DDT:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Option	BYTE	-	Not displayed.
Status	WORD	-	status of command execution: • Busy: command is executing • OK: command is successful • Unsuccessful: one of the following events occurred: ◦ the client received a negative response. ◦ a timeout occurred before the client received a response.

NOTE: If a polling command detects an error for a DO, the Status element for that DO displays a detected error code, page 124, and the polling process continues for the next DO.

History Report for Client Side

The data structure of the {Module_name}_CLIENT_HISTORY_MODULENAME DDDT:

There are two modes: Cyclic and On-demand.

DDDT table for Cyclic mode:

Element	Type	Description
HISTORY_SERVICE_HEARTBEAT	UINT	Heartbeat to check if history service is active
CLEAR_HISTORY_DATA	BOOL	If value is from 0 to 1, clear the history data
HISTORY_BUFFER_FULL	BOOL	History event counts are greater than or equal to 100000 items
MEMORY_LOW	BOOL	Module free memory is less than 10% of NOP physical memory
TOTAL_HISTORY_REPORT_COUNT	UDINT	Total history report counts
PLAY_CYCLIC_HISTORY	BOOL	Start/Stop display history value: • 1: start • 0: stop
BACKFILL_REFRESH_RATE	UDINT	Backfill refresh rate (MS)
EVENT_COUNT	UDINT	Total history event counts
IED1_NAME		IED1_NAME is an example
IED1_NAME.REPORT_COUNT_THIS_IED	UDINT	Report counts of this IED
IED1_NAME.DataModel	-	DDT to display the history value, the data structure is completely same as the real time DDDT
IED1_NAME.ReportBlock	-	Report information of history
IED1_NAME.ReportBlock.ReportName.EntryID	ARRAY[0..3] OF UINT	Display EntryID of history report
IED1_NAME.ReportBlock.ReportName.Index	BYTE	-
IED1_NAME.ReportBlock.ReportName.EntryTime_1970	TIME_850_FORMAT	Display EntryTime of history report in TIME_850_FORMAT
IED1_NAME.ReportBlock.ReportName.EntryTime	Entry_Time_Format	Display EntryTime of history report in Entry_Time_Format

NOTE: The table above only displays one IED. If multiple IEDs exist, they continue to be displayed.

DDDT table for On-demand mode:

Element	Type	Definition
HISTORY_SERVICE_ HEARTBEAT	UINT	Heartbeat to check if history service is active
CLEAR_HISTORY_DATA	BOOL	If value is from 0 to 1, clear the history data
HISTORY_BUFFER_FULL	BOOL	History event counts are greater than or equal to 100000 items
MEMORY_LOW	BOOL	Module free memory is less then 10% of NOP physical memory
TOTAL_HISTORY_ REPORT_COUNT	UDINT	Total history reports counts
ONDEMAND_FLAG	BOOL	Flag for controlling on-demand process
EVENT_COUNT	UDINT	Total history event counts
IED1_NAME	-	IED1_NAME is an example
IED1_NAME.REPORT_ COUNT_THIS_IED	UDINT	Report counts of this IED
IED1_NAME.DataModel	-	DDDT to display the history value, the data structure is completely same as the real time DDDT.
IED1_NAME.ReportBlock	-	Report information of history
IED1_NAME.ReportBlock. ReportName.EntryID	ARRAY[0..3] OF UINT	Display EntryID of history report
IED1_NAME.ReportBlock. ReportName.Index	BYTE	-
IED1_NAME.ReportBlock. ReportName.EntryTime_ 1970	TIME_850_ FORMAT	Display EntryTime of history report in TIME_850_ FORMAT
IED1_NAME.ReportBlock. ReportName.EntryTime	Entry_Time_ Format	Display EntryTime of history report in Entry_Time_ Format

NOTE: The table above only displays one IED. If multiple IEDs exist, they continue to be displayed.

OPER Control Objects

The OPER control object presents alternative structures, depending on the data type: BOOLEAN, INT8, INT32, ENUM, or ANA. An example of each DDT structure follows for the OPER control object:

The data structure of the `{Module_name}_CO_OPER_BOOL` control object DDT:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Check	BYTE	-	• bit 0...1: operation type: ◦ 0 = operate ◦ 1 = select ◦ 2 = cancel ◦ 3 = auto (select & operate) • bit 2...4 = reserved • bit 5: synchrocheck: whether to perform synchrocheck • Bit 6: synchrocheck: whether to check for interlocking condition • Bit 7: test
CtVal	BYTE	-	bit 0: ctlVal; value to control

Element	Type	Trigger	Definition
Resv	BYTE	-	reserved for alignment
Status	WORD	-	Status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6..7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

The data structure of the {Module_name}_CO_OPER_INT8 control object DDT:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Check	BYTE	-	• bit 0...1: operation type: ◦ 0 = operate ◦ 1 = select ◦ 2 = cancel ◦ 3 = auto (select & operate) • bit 2...4 = reserved • bit 5: synchrocheck: whether to perform synchrocheck • Bit 6: synchrocheck: whether to check for interlocking condition • Bit 7: test
CtVal	INT	-	value to control
Resv	BYTE	-	reserved for alignment
Status	WORD	-	status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6...7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

The data structure of the {Module_name}_CO_OPER_INT32 control object DDT:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Check	BYTE	-	• bit 0...1: operation type: ◦ 0 = operate ◦ 1 = select ◦ 2 = cancel ◦ 3 = auto (select & operate) • bit 2...4 = reserved • bit 5: synchrocheck: whether to perform synchrocheck • Bit 6: synchrocheck: whether to check for interlocking condition • Bit 7: test
CtVal	DINT	-	value to control
Status	WORD	-	status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6...7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

The data structure of the {Module_name}_CO_OPER_FLOAT and {Module_name}_CO_OPER_FLOAT control object DDTs:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Check	BYTE	–	• bit 0...1: operation type: ◦ 0 = operate ◦ 1 = select ◦ 2 = cancel ◦ 3 = auto (select & operate) • bit 2...4 = reserved • bit 5: synchrocheck: whether to perform synchrocheck • Bit 6: synchrocheck: whether to check for interlocking condition • Bit 7: test
CtlVal_i	UDINT	–	value to control int32 point
CtlVal_f	REAL	–	value to control float point
Status	STATUS	–	status of command execution

The data structure of the `{Module_name}_CO_OPER_ENUM` control object DDT:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Check	BYTE	-	• bit 0...1: operation type: ◦ 0 = operate ◦ 1 = select ◦ 2 = cancel ◦ 3 = auto (select & operate) • bit 2...4 = reserved • bit 5: synchrocheck: whether to perform synchrocheck • Bit 6: synchrocheck: whether to check for interlocking condition • Bit 7: test
CtVal	DINT	-	value to control
Status	WORD	-	status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6...7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

The data structure of the `{Module_name}_CO_OPER_ANA` control object DDT:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	trigger: effective on change
Check	BYTE	-	• bit 0...1: operation type: ◦ 0 = operate ◦ 1 = select ◦ 2 = cancel ◦ 3 = auto (select & operate) • bit 2...4 = reserved • bit 5: synchrocheck: whether to perform synchrocheck • Bit 6: synchrocheck: whether to check for interlocking condition • Bit 7: test
CtVal_i	DINT	-	value to control

Element	Type	Trigger	Definition
CtVal_f	REAL	-	value to control
Status	WORD	-	status of command execution: • low byte: same as command trigger • high byte: ◦ bits 6...7: 1 = OK; 2 = error detected ◦ bits 0...5: detected error code

NOTE: The internal protocol stack of BMENOP0300 checks the paired member of ctlVal.i and ctlVal.f during one control operation, so you should add both of them into I/O mapping table. If some client tools do not support to write ctlVal.i and ctlVal.f in one operation, you should find a way to guarantee ctlVal.i and ctlVal.f be written together. For example, in IEDScout using “Write all value” checkbox.

Working with the BMENOP0300 in a PAC Application

Introduction

This topic describes the following operations for the BMENOP0300:

- control operation as server
- control operation as client
- connection operation as client

Control Operation as Server

The BMENOP0300 module supports four kinds of control models:

- Direct Operate normal security mode (Dons)
- Select before Operate normal security mode (SBOns)
- Direct Operate enhanced security mode (Does)
- Select before Operate enhanced security mode (SBOes)

NOTE: If the control model of the control object is Does or SBOes, it is mandatory to add the “stVal” and “t” data attributes of the upper layer data object into I/O mapping.

According to IEC 61850 standard, the control operations present dependencies that call for some programming in the PAC application.

Task 1 / PAC state: control operation is allowed only when the PAC is in RUN state.

Item	Status	Behavior	How to configure?
PAC state	STOP	The Oper is rejected.	Use Control Expert to manage the PAC state.
PAC state	RUN	The Oper is operational.	

Task 2 / Control model: control operation is not allowed when control model is status only:

Item	Status	Behavior	How to configure?
Control Model	Status only	The Oper is rejected.	Set it in “Application setting”.
Control Model	Direct-with-normal-security / Sbo-with-normal-security / Direct-with-enhance-security / Sbo-with-enhance-security	The Oper is operational.	

Task 3 / LN/Beh.stVal: Logic node’s beh status determines if this control operation is allowed. This can be managed in the PAC as needed:

Item	Status	Behavior	How to configure?
LN/Beh.stVal	OFF (5)	The Oper is rejected.	Set it in “Application setting” if it is not mapped in I/O mapping, or manage it in PAC application if it is mapped in I/O mapping.
LN/Beh.stVal	ON (1)	The Oper is operational.	

Task 4 / Does/SBOes mode is a more secured control operation compared to the normal mode. The BMENOP0300 module verifies the DO status from the PAC when the operation is executed. Because each CDC has a different definition for control command and status, follow the programming logic as described below in your PAC application to manage the DO status:

- The BMENOP0300 module verifies the status updating of data objects during the operation and sends one negative response if the DO status is not expected.
- The BMENOP0300 module determines whether the DO status is updating according to the time stamp of DO status. Therefore, the time stamp attribute is needed for the enhanced control model. Consequently, you will need to manage both status and time stamp in the PAC application to provide the control status for enhanced mode.
- In a PAC application, you could identify the control operation by means of the control number, which needs to be managed in the PAC application. When the control number is incremented, it indicates a new operation has begun. Add program logic to your application to manage DO status as described in the following table. Your program logic will include two actions:
  - Update the DO status according to the control value.
  - Update the DO time stamp, which is configured in UTC format.
- Note that each CDC presents different behavior, according to its specifications, as described in the following table.

CDC	Status of DO	Expected status
SPC	stVal	stVal should be equal to ctlVal.
	t	Time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation.
DPC	stVal	stVal is ON when ctlVal is TRUE. stVal is OFF when ctlVal is FALSE.
	t	Time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation.
INC	stVal	stVal should be equal to ctlVal and within range.
	t	time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation.
ENC	stVal	stVal should be equal to ctlVal and within range.
	t	Time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation
ISC	valWTr.posVal	valWTr.posVal should be equal to ctlVal and within range
	t	Time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation.
BSC	valWTr.posVal	When ctlVal is STOP: valWTr.posVal should have no change. When ctlVal is HIGHER: valWTr.posVal should become bigger. When ctlVal is LOWER: valWTr.posVal should become smaller.
	t	Time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation.
APC	mxVal.i / mxVal.f	mxVal.i or mxVal.f should be equal to ctlVal and within range.
	t	Time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation.
BAC	mxVal.i / mxVal.f	When ctlVal is STOP: mxVal.i and mxVal.f should have no change. When ctlVal is HIGHER:

CDC	Status of DO	Expected status
		mxVal.i or mxVal.f should become bigger. When ctlVal is LOWER: mxVal.i or mxVal.f should become smaller.
	t	Time stamp should update accordingly.
	Oper.ctlNum	Control number should increase after each operation.

NOTE: The BMENOP0300 module supports the operation of one point set to the same value for many successive iterations. Use the control number in PAC logic to determine if control operation is executing.

Control Operation as Client

The BMENOP0300 module supports one dedicated data block that can trigger a request for a report block, GOOSE block, control block, or a polling operation. Create a manually enabled report after module start up to confirm the report functions as intended.

The data block for each command is composed of three elements: command trigger options, and status. The option type and content depends on the type of command, but the trigger and status are same type with different content:

- Command: Triggers the sending of a request. (The detailed operation information is contained in the Option element.)
- Option: Indicates the kind of command requested.
- Status: Contains the Command trigger value, the status of the command, and any detected error code.

The data structure for all commands is the `DATA_BLOCK_TEMPLATE` data structure, set forth below:

Element	Type	Trigger	Definition
Cmd	BYTE	Dchg	Command trigger: The BMENOP0300 module sends one command if this value has changed.
Option	BYTE	-	Request option
Option	Type depends on control block	-	Request option
Status	WORD	-	Low byte: Same as trigger command.
			High byte: Bit6~bit7: 0: Busy 1: OK 2: Error detected Bit0~Bit5: Detected error code. Refer to error code for the specific function type.

Status detected error codes

Function	Code	Meaning	Possible reason
Control point	1~27	AddCause	Refer to the AddCause, page 123 detected error descriptions, defined by the IEC 61850 standard.
	61	Disconnected	Offline with remote IED.

Function	Code	Meaning	Possible reason
	63	Input parameter error detected	Input parameter in data block is incorrect. Such as input CtlVal is out of range.
Polling	61	Disconnected	Offline with remote IED.
	62	Polling is not operational	Some DOs or DAs is missing in remote IED. Polling will contnue if this error is detected.
	63	Input parameter error	Input parameter in data block is incorrect.
Report Control	60	AutoEna is not operational	The report was not enabled after going online. This error code depends on the AutoEn setting in the Report Control block.
	61	Disconnected	Offline with remote IED.
	63	Input parameter error detected	Input parameter in data block is incorrect. For example, index is out of range.
GOOSE Control	0	GOOSE disabled	GOOSE control block is disabled.
	1	GOOSE enabled	GOOSE control block is enabled.
	61	Disconnected	Offline with remote IED.

Example 1: `REPORT_URCB` displaying a normal structure:

Element	Current Value	Next Value	Remark
Cmd	0	-> 1	The change of value triggers the operation of a single request.
Option	0	1	Sets the report enable attribute.
Index	0	3	Indicates the 3rd instance of this report.
AutoEna	0	0	-
Attribute	0	1	1 indicates the report is enabled.
RptStatus	-	3	Report instance number.
Status	-	0x4001	This operation is executed successfully.
Italics and bold text indicates elements to be completed by the application.			

Example 2: `REPORT_URCB` displaying an abnormal structure:

Element	Current Value	Next Value	Remark
Cmd	0	-> 5	The change of value triggers the operation of a single request.
Option	0	1	Sets the report enable attribute.
Index	0	3	Indicates the 3rd instance of this report.
AutoEna	0	0	-
Attribute	0	1	1 indicates the report is enabled.
RptStatus	-	3	Report instance number.

Status	-	0xBF05=
		{
		0x8000 +
		0x3F00 +
		0x0005
		}
			This operation is not executed successfully.
			0x8000: error
			0x3F00: error code 63, incorrect input parameter (e.g., index could be out of range).
			0x0005: command trigger

Italics and bold text indicates elements to be completed by the application.			

Example 3: `{Module}_CO_BOOL` displaying a normal structure:

Element	Current Value	Next Value	Remark
Cmd	0	-> 2	The change of value triggers the operation of a single request.
Check	0	0	Operate directly.
CtlVal	0	1	Set point as TRUE.
Status	0	0x4002	This operation is executed successfully.
Italics and bold text indicates elements to be completed by the application.			

Example 4: `{Module}_CO_BOOL` displaying an abnormal structure:

Element	Current Value	Next Value	Remark
Cmd	0	-> 3	The change of value triggers the operation of a single request.
Check	0	0	Operate directly.
CtlVal	0	1	Set point as TRUE.

Status	0	0xBD03=
		{
		0x8000 +
		0x3D00 +
		0x0003
		}
			This operation is not executed successfully.
			0x8000: error
			0x3D00: error code 61, remote IED is not connected.
			0x0003: command trigger

Italics and bold text indicates elements to be completed by the application.			

Connection Operation as Client

The BMENOP0300 client DDT supports connection control to the remote IED with ConnectCtrl. The module attempts to connect with the remote IED by default after start up. The status of the connection can be checked via the health status in client state, or by the Freshness element of the client DDT, as shown below for a `{Module}_{IED name` client:

Element	Type	Definition
Freshness	BOOL	0: Data is not fresh 1: Data is fresh When there is no IEC 61850 connection or backplane communication, set it as FALSE.
ConenctCtrl	BOOL	0: Auto connect 1: Disconnect
Data Model	–	–
PollBlock	–	Polling control for each IED
ControlBlock	–	General control
ReportBlock	–	Report control
GooseBlock	–	GOOSE control

Working With Sequence of Event (SOE) Timestamped Data Sets

Overview

The BMENOP0300 module supports the transfer of data objects from external devices – including the BMXERT1604, BMXCRA31210, and the 140ERT854x0 – via report control block to management tools such as SCADA. Each data object presents the data value, quality, and a timestamp. The report control block provides a consistent sequence of events (SOE) time stamped at the source.

This chapter describes how to:

- Configure timestamped SOE data sets and report control blocks.
- Program the operations of elementary functions (EFs) and elementary function blocks (EFBs) to support the configuration, including:
  - NOP850_EVTS
  - NOP850_EVTS_MULTI_8
  - NOP850_EVTS_MULTI_16
  - T850_TO_T870
  - T870_TO_T850

Configuring SOE events in the IEC 61850 Configuration Tool

Introduction

The BMENOP0300 module supports the transfer of external events originated by ERT and CRA modules to SCADA via a buffered report control block. The BMENOP0300 module cyclically detects data objects in controller memory and includes them in a report control block with each data object status value, quality and timestamp data.

For BMENOP0300 with firmware SV2.50 or earlier, only one event can be transferred in each controller cycle.

Transferring multiple events (up to 16) in each controller cycle requires:

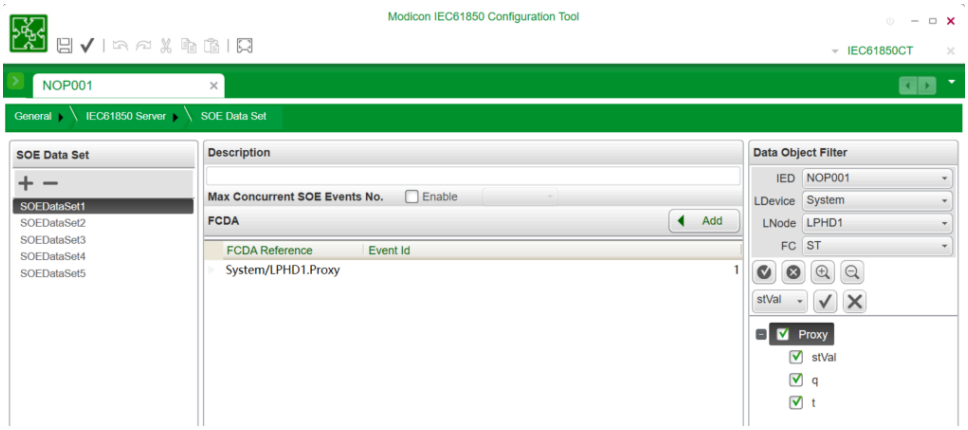
- IEC61850 configuration Tool version 3.3 or any subsequent supporting version (s).
- Control Expert 15.1 or any subsequent supporting version(s).
- BMENOP0300 module firmware SV2.60 or any subsequent supporting version (s).

Configuring SOE Events

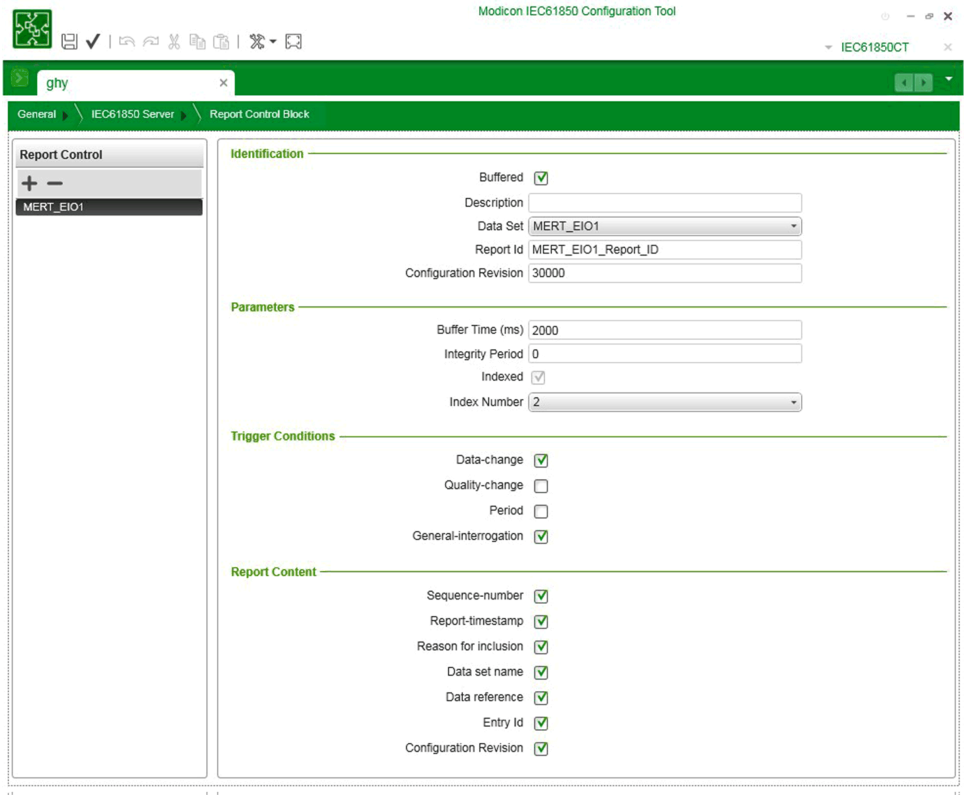
To preserve memory mapping and retain the SOE timestamping that originated with the source ERT or CRA module, the BMENOP0300 module provides a single dedicated channel for the transfer of external events.

The BMENOP0300 module supports the creation and use of a single dedicated data set that can contain data objects of the single point setting (SPS) class and data object (DO) functional constraint. Each DO instance represents a single ERT/CRA channel, and includes the status value (stVal), quality (q), and timestamp (t) data attributes.

When configuring the data set, you need to include all DOs. The DO instances included in the report can originate from any kind of logical node (LN). When adding a DO instance to the data set, you need to specify the link with the channel (Event ID), as shown below:



Next, you need to associate a single buffered report control block (BRCB) with this data set, as shown below:



After mapping the DO into PAC variables, two DDT instances are automatically created and added to the application:

- IED_RPT or IED_RPT_MULTI is the DDT that contains report diagnostic information.

  NOTE: IED_RPT_MULTI is created instead of IED_RPT when enabling concurrent SOE events.

- IED_EVT is the event data transferred via the selected channel from PAC, which presents two different structures, depending on the source platform:
  - IED_EVT_M for Mx80 devices
  - IED_EVT_Q for Quantum devices

NOTE: The BMENOP0300 module can add these events into a buffered report control block, according to the configuration. Because the Quantum ERT uses local time, whereas the Mx80 ERT uses UTC time, the BMENOP0300 module can manage the Quantum ERT time conversion from 60870 local time to 61850 UTC time. No such time conversion is required for Mx80 ERT/CRA.

Data Type Structure: IED_RPT and IED_RPT_MULTI

Element	Type	Description
Status	WORD	Report status: • bits 0...7: Report enabled/disabled. Each bit represents one report instance: ◦ 0 = disabled ◦ 1 = enabled • bits 8...15: buffer overflow: ◦ 0 = no buffer overflow ◦ 1 = overflow
DaChgCnt	WORD	A counter value that increments each time a report is generated.

Data Type Structure: IED_EVT_M

This structure describes the format of events used by Mx80 devices using the IEC 61850 format:

<table>
<tr><th>Element</th><th>Type</th><th colspan="4">Description</th></tr>
<tr><td>Reserv</td><td>BYTE</td><td colspan="4"><reserved></td></tr>
<tr><td>Value</td><td>BYTE</td><td colspan="4">Input value</td></tr>
<tr><td>EventID</td><td>WORD</td><td colspan="4">An event identifier, which can be one of the following:
• the channel number
• a user-defined value</td></tr>
<tr><td>SecondSince Epoch</td><td>DWORD</td><td colspan="4">The interval, in seconds, from 1970-01-01 00:00:00 UTC to the present.</td></tr>
<tr><td>FracOfSec_L</td><td>WORD</td><td colspan="4" rowspan="2">The fraction of the second when the value element, above, has been determined. The fraction of second is calculated as:
(SUM from i = 0 to 23 of bi*2**–(i+1) s).</td></tr>
<tr><td>FracOfSec_H</td><td>BYTE</td></tr>
<tr><td>TimeQuality</td><td>BYTE</td><td colspan="4">TimeQuality provides information regarding the sending IED, and consists of the following attributes:</td></tr>
<tr><td></td><td></td><td>Bits</td><td>Attribute</td><td>Type</td><td>Description</td></tr>
<tr><td></td><td></td><td>0...4</td><td>TimeAccuracy</td><td>CODED ENUM</td><td>The accuracy class of the time source. Only the value of 10 = 1 ms is supported.</td></tr>
<tr><td></td><td></td><td>5</td><td>ClockNotSynchron-ized</td><td>BOOL</td><td>When set to 1, this indicates the time source of the sending IED is not synchronized with external UTC time.</td></tr>
<tr><td></td><td></td><td>6</td><td>ClockFailure</td><td>BOOL</td><td>When set to 1, this indicates the time source of the sending IED is unreliable.</td></tr>
<tr><td></td><td></td><td>7</td><td>LeapSeconds-Known</td><td>BOOL</td><td>When set to 1, this indicates that SecondSinceEpoch value includes all leap year seconds. When set to 0, this indicates leap seconds are not included and seconds are calculated from the present date assuming a constant day length of 86400 s.</td></tr>
</table>

Data Type Structure: IED_EVT_Q

This structure describes the format of events used by Quantum devices using the IEC 61850 format:

Element	Type	Description
Reserv	BYTE	<reserved>
Value	BYTE	Input value
Event ID	WORD	An event identifier, which can be one of the following: • the channel number • a user-defined value
Reserved	BYTE	<reserved>
Month	BYTE	Month
Year	BYTE	Year
Ms_Lsb	BYTE	Time in milliseconds (least significant byte)
Ms_Msb	BYTE	Time in milliseconds (most significant byte)
Min	BYTE	Invalid time/minutes
Hour	BYTE	Summer time/hours
Day	BYTE	Weekday/day of the month

Data Type Structure: IED_ERT_BUF

Element	Type	Description
NewTS	BYTE	Time stamp of the new event
EvtSrc	BYTE	Event source: • 0 = Quantum • 1 = Mx80
EventEnti-ty	WORD [6]	Event entity, which can be one of the following: • `IED_EVT_Q` • `IED_EVT_M`

Data Type Structure: IED_ERT_BUF_MULTI_8 and IED_ERT_BUF_MULTI_16

Element	Type	Description
NewTS	BYTE	Time stamp of the new event
EvtSrc	BYTE	Event source: 1 = Mx80
Nb_EVT	INT	Number of events transferred
Evt_Buf	One of the following: • ARRAY_IED_ERT_EVT_8 • ARRAY_IED_ERT_EVT_16	Contains the event to be transferred. Each event is structured in a DDT of type `IED_ERT_EVT` containing the EventEntity elements (WORD[6]).

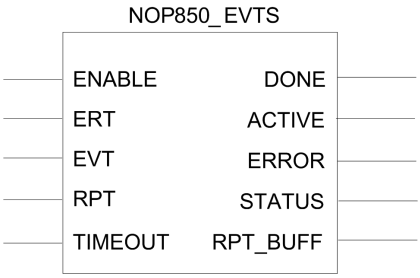
NOP850_EVTS Elementary Function Block Operations for the BMENOP0300

Introduction

Use the NOP085_EVTS elementary function block (EFB) to:

- Manage and synchronize the transfer of external events from an ERT or CRA into the memory of the BMENOP0300 module.
- Manage the transfer external events between a PLC and the BMENOP0300 module.

Representation in FBD



NOTE:

- When the timestamped event originates at a Quantum platform, the time stamp is local time (UTC+TimeZone). The BMENOP0300 firmware converts this local time into UTC and includes it in the outgoing report control block. The time zone depends on the BMENOP0300 SNTP configuration in Modicon IEC61850 Configuration Tool.
- When the timestamped event originates at an M80 platform, the time stamp is UTC time and BMENOP0300 firmware includes it in the outgoing report control block without conversion.

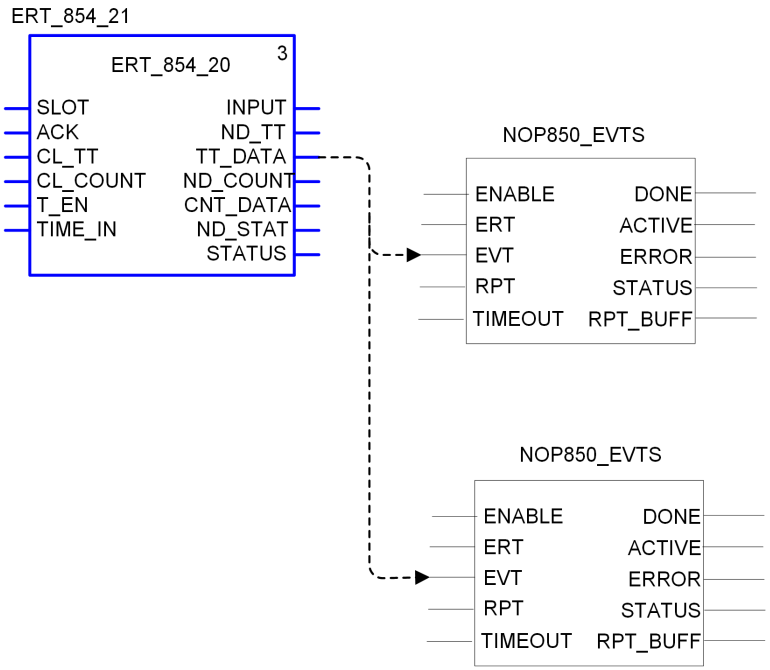
Input Parameters

Input parameter	Type	Description
ENABLE	BOOL	Start transferring
ERT	BYTE	ERT type: • 0 = Quantum ERT • 1 = Mx80 ERT
EVT	One of the following: • IED_EVT_Q, page 140 • IED_EVT_M, page 139	Event description, including value, quality, time stamp, ID, DDT, and IED_EVT_x
RPT	IED RPT, page 139	Report information. DDT IED_RPT
TIMEOUT	INT	Time threshold in 100 ms increments for triggering an event (a value greater than 0)

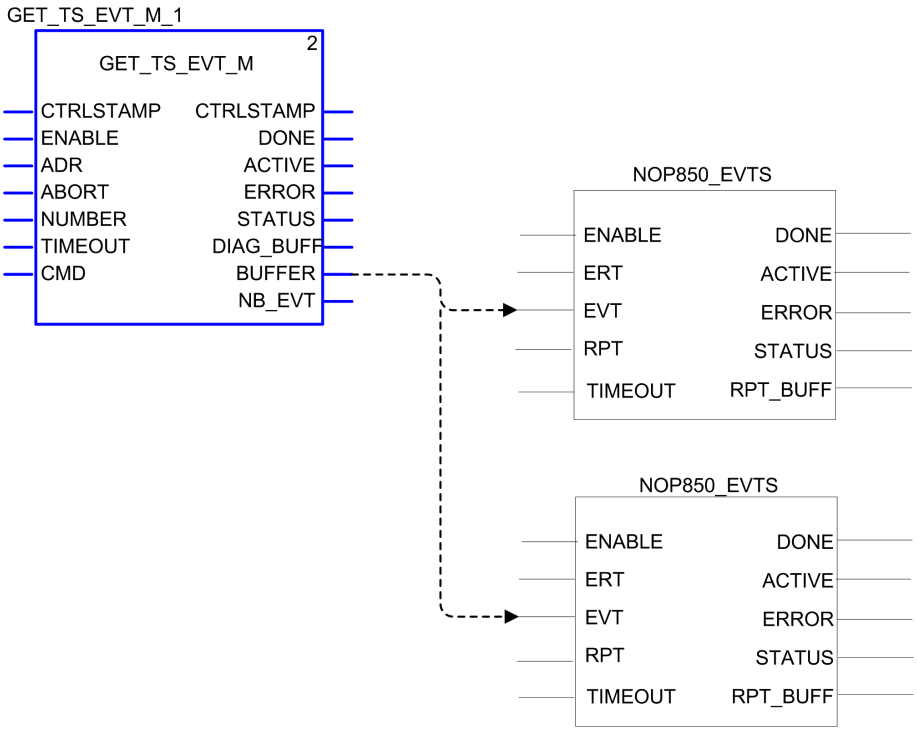
Output Parameters

Output parameter	Type	Description
DONE	BOOL	A value of 1 (true) indicates the function block completed successfully.
ACTIVE	BOOL	A value of 1 (true) indicates execution of the function block is in progress.
ERROR	BOOL	A value of 1 (true) indicates the function block detects an execution error.
STATUS	INT	Identifies the detected error: • 1 = Input parameter is not valid. • 2 = <Reserved> • 3 = Time format is not valid. **NOTE:** Only dates after January 01, 2000 are valid. • 4 = time out occurrence (default 10 s) • 5 = parameter change during runtime • 6 = Data change counter of report is abnormal **NOTE:** This EFB restarts if a time out (4) or abnormal data change counter event (6) occurs.
RPT_BUFF	IED ERT BUF, page 140	Raw buffer containing event time stamp entities.

Quantum ERT FBD Example



Mx80 ERT FBD Example



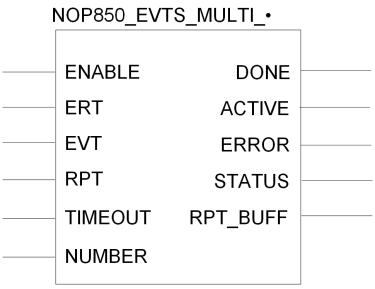
NOP850_EVTS_MULTI_8 and NOP850_EVTS_MULTI_16 Elementary Function Block Operations for the BMENOP0300

Introduction

Use the NOP850_EVTS_MULTI_8 and NOP850_EVTS_MULTI_16 elementary function blocks (EFB) to:

- Manage and synchronize the transfer of multiple external events from an ERT or CRA into the memory of the BMENOP0300 module.
- Manage the transfer of multiple external events between a controller and the BMENOP0300 module.

Representation in FBD



NOTE: Only timestamped event originating at an M580 platform are supported.

Input Parameters

Input parameter	Type	Description
ENABLE	BOOL	Start transferring
ERT	BYTE	ERT type = 1 (for x80 ERT)
EVT	One of the following: • ARRAY_IED_EVT_M_8 • ARRAY_IED_EVT_M_16	Array of event description, including status value, quality, time stamp, ID. The DDT ARRAY_IED_EVT_M_8 and ARRAY_IED_EVT_M_16 are arrays containing respectively 8 and 16 DDT IED_EVT_M, page 139.
RPT	IED_RPT_MULTI, page 139	Report information.
TIMEOUT	INT	Time threshold in 100 ms increments for triggering an event (a value greater than 0)
NUMBER	INT	Number of events transferred to the report.

Output Parameters

Output parameter	Type	Description
DONE	BOOL	A value of 1 (TRUE) indicates the function block completed successfully.
ACTIVE	BOOL	A value of 1 (TRUE) indicates execution of the function block is in progress.

Output parameter	Type	Description
ERROR	BOOL	A value of 1 (TRUE) indicates the function block detects an execution error.
STATUS	INT	Identifies the detected error: • 1 = Input parameter is not valid. • 2 = <Reserved> • 3 = Time format is not valid. **NOTE:** Only dates after January 01, 2000 are valid. • 4 = time out detected (default 10 s) • 5 = parameter change during runtime • 6 = Data change counter of report is detected in error **NOTE:** This EFB restarts if a time out is detected (4) or if a data change counter event is detected as in error (6).
RPT_BUFF	One of the following: • IED_ERT_BUF_MULTI_8, page 140 • IED_ERT_BUF_MULTI_16, page 140	Raw buffer containing event time stamp entities.

Programming Example

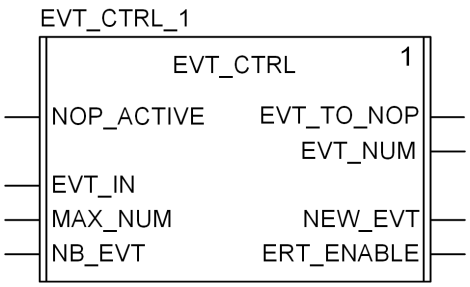
The following points have to be taken into account when programming the transfer of multiple events in parallel using the EFBs NOP850_EVTS_MULTI_8, NOP850_EVTS_MULTI_16 and GET_TS_EVTS_M:

- The output parameter NB_EVT of the EFB GET_TS_EVTS_M represents the cumulative value of events buffered (up to defined maximum number). It cannot be directly connected to the input parameter NUMBER of the EFB NOP850_EVTS_MULTI_8 or NOP850_EVTS_MULTI_16 which represents the number of multiple events to transfer into the memory of the BMENOP0300 module at a time.
- When multiple events are transferred in parallel, the buffer size of the EFB GET_TS_EVTS_M is set to a value greater than 1 and the output parameter DONE cannot be triggered until the number of events equals to the buffer size. If the number of events is smaller than the buffer size, you can not use directly the output parameter DONE of the EFB GET_TS_EVTS_M for enabling the EFB NOP850_EVTS_MULTI_8 or NOP850_EVTS_MULTI_16.

To transfer multiple events in parallel using the EFBs NOP850_EVTS_MULTI_8, NOP850_EVTS_MULTI_16 and GET_TS_EVTS_M, you need to create a DFB to:

- temporarily store the events read by the EFB GET_TS_EVTS_M.
- send events and the number of events to the EFB NOP850_EVTS_MULTI_8 or NOP850_EVTS_MULTI_16.
- send a signal for enabling the EFB NOP850_EVTS_MULTI_8 or NOP850_EVTS_MULTI_16 and disabling the EFB GET_TS_EVTS_M.

The elements (parameters, variables, and code) for implementing this DFB is given below in details.



DFB inputs parameters:

Parameter	Type
NOP_ACTIVE	BOOL
EVT_IN	ARRAY[1..102] OF INT
MAX_NUM	INT
NB_EVT	INT

DFB output parameters:

Parameter	Type
EVT_TO_NOP	ARRAY[1..96] OF INT
EVT_NUM	INT
NEW_EVT	BOOL
ERT_ENABLE	BOOL

DFB public variables:

Parameter	Type
SEND_ST_INDEX	INT
SEND_END_INDEX	INT
BUFF2	ARRAY[1..96] OF INT

DFB private variables:

Parameter	Type
BUFF1	ARRAY[1..96] OF INT
NEXT_SEND_NUMBER	INT
A	INT
TRIGGER_0	TRIGGER
read_P	BOOL
DUMMY	BOOL
EVT_NUMBER_SAVE	INT
BUFF_DUMMY	ARRAY[1..96] OF INT
SEND_FREE	BOOL
DUMMY96	ARRAY[1..96] OF INT
pp2	DINT
pp1	DINT
M	INT

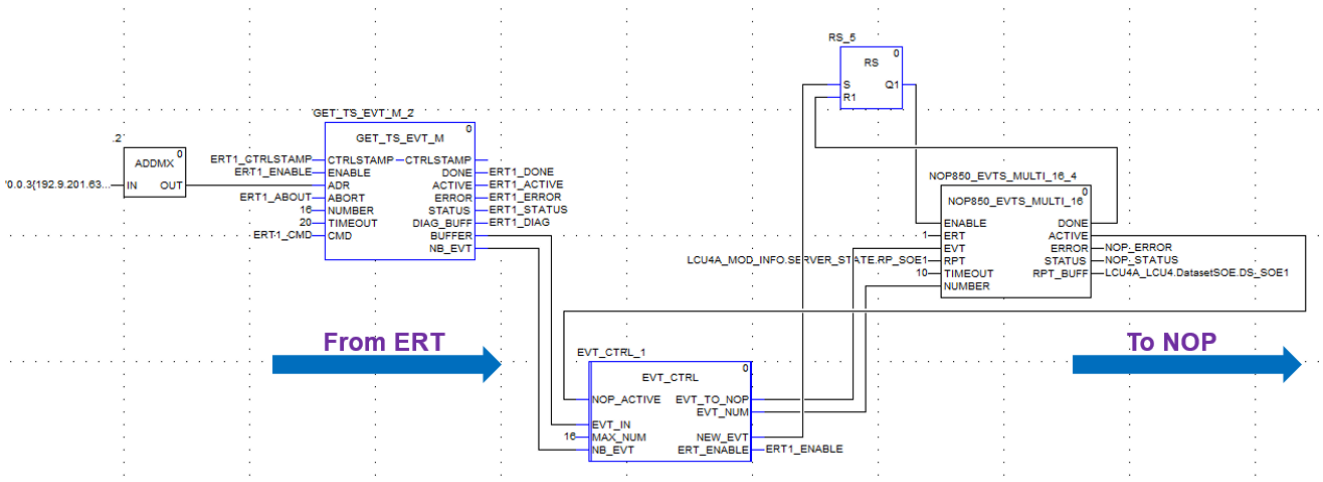
DFB code in ST language:

```
ERT_ENABLE:=NB_EVT<MAX_NUM;

IF NOT NOP_ACTIVE AND NOT NEW_EVT THEN
SEND_ST_INDEX:=SEND_END_INDEX;
SEND_END_INDEX:=NB_EVT;

EVT_TO_NOP:=DUMMY96;M:=1;
FOR A:=(SEND_ST_INDEX)*6+1 TO SEND_END_INDEX*6 DO

EVT_TO_NOP[M]:=(EVT_IN[A]);
M:=M+1;
```

```
END_FOR;
EVT_NUM:=SEND_END_INDEX-SEND_ST_INDEX;

IF EVT_NUM >0 THEN
NEW_EVT:=1;
END_IF;
END_IF;

(*CLEAR NEW EVT FLAG*)
IF NOP_ACTIVE AND NEW_EVT THEN
NEW_EVT:=0;

IF SEND_END_INDEX=MAX_NUM THEN
SEND_END_INDEX:=0;
SEND_ST_INDEX:=0;
ERT_ENABLE:=1;
END_IF;
END_IF;
```

Example

Here is an example of DFB instance used in an application program task in Functional Block Diagram (FBD) language:



Configure the maximum number of events to read (input parameter `NUMBER` of the EFB `GET_TS_EVT_M`) lower or equal to the number of event transferred concurrently (16 in this example).

T850_TO_T870 and T870_TO_T850 Elementary Functions for the BMENOP0300

Introduction

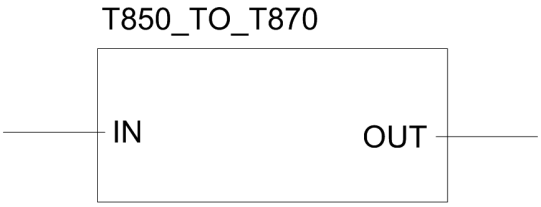
The BMENOP0300 module is a device that sends and receives data timestamped according to the IEC 61850 protocol. Some Mx80 ERT devices send and receive data timestamped according to the IEC 60870 protocol.

To enable data transfer between devices that support different timestamp structures, you can use the following elementary functions in your program logic:

- `T870_TO_T850`: This EF takes IEC 60870 timestamped data (for example, data generated by the BMXNOR0200 module) and converts it to the IEC 61850 format.
- `T850_TO_T870`: This EF takes IEC 61850 timestamped data generated by the BMENOP0300 module and converts it to the IEC 60870 format where it can be used by other Mx80 ERT devices.

T850_TO_T870 Representation in FBD

The following graphic depicts the T850_TO_870 function:

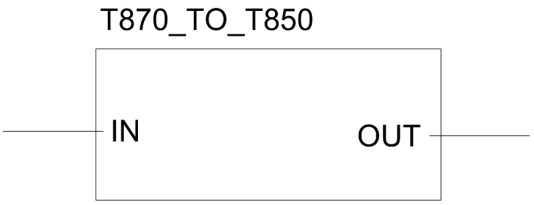


T850_TO_T870 Parameters

Parameter	Type	Description
Input parameters:		
`IN`	`TIME_850_FORMAT`	the IEC 61850 timestamp format
Output parameters:		
`OUT`	`TIME_870_FORMAT`	the IEC 60870 timestamp format

T870_TO_T850 Representation in FBD

The following graphic depicts the `T870_TO_T850` function:



T870_TO_T850 Parameters

Parameter	Type	Description
Input parameters:		
IN	TIME_870_FORMAT	the IEC 60870 timestamp format
Output parameters:		
OUT	TIME_850_FORMAT	the IEC 61850 timestamp format

Data Type Structure: TIME_850_FORMAT

Element	Type	Description
Seconds	DWORD	seconds since 01-01-1970 **NOTE:** Only dates after January 01, 2000 are valid.
Ms_Quality	DWORD	milliseconds in IEC 61850 format in low three bytes (Highest byte manages quality.)

Data Type Structure: TIME_870_FORMAT

Element	Type	Description
ms	WORD	from 0...59999 ms
min	BYTE	Numerical minute reference: 0...59. The highest bit indicates time validity: • 0 = valid time • 1 = invalid time
hour	BYTE	numerical hour reference: 0...23 **NOTE:** SU (summertime) is not supported.
day	BYTE	numerical day reference: 1...31. **NOTE:** Day of week is not supported.
mon	BYTE	numerical month reference: 1...12
year	BYTE	numerical year reference: 0...99
reserved	BYTE	<reserved>

Explicit Messaging

Introduction to Explicit Messaging

About Explicit Messaging

Overview

The BMENOP0300 module supports explicit messaging through the Modbus TCP protocol. *Modbus TCP*: Use the DATA_EXCH function block or WRITE_VAR and READ_VAR function blocks in application logic to create a Modbus TCP explicit message.

NOTE: A single Control Expert application can contain more than 16 explicit messaging blocks, but only 16 explicit messaging blocks can be active at the same time.

This chapter describes how to configure Modbus TCP explicit messages through these mechanisms:

- DATA_EXCH function block (in application logic)
- Control Expert interface

Explicit Messaging Using the DATA_EXCH Block

Overview

Use this overview of the DATA_EXCH function block to configure Modbus TCP explicit messages.

These instructions describe the configuration of the DATA_EXCH function block's management parameter, which is common to both Modbus TCP explicit messaging.

In a redundant system, the primary BMENOP0300 module sends the explicit message. Even when a switchover occurs and the primary becomes the standby, the module can run the active sections.

Configuring Explicit Messaging Using DATA_EXCH

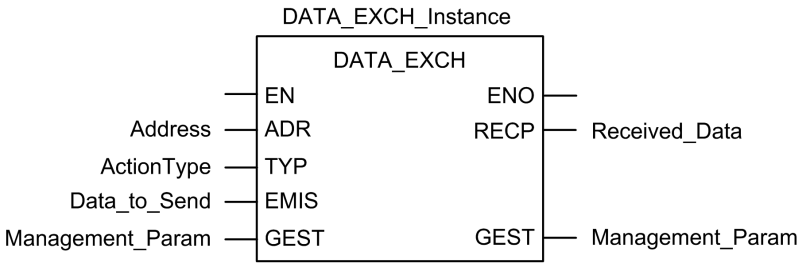
Overview

Use the DATA_EXCH function block to configure Modbus TCP explicit messages.

The Management_Param, the Data_to_Send, and the Received_Data parameters define the operation.

EN and ENO can be configured as additional parameters.

FBD Representation



Input Parameters

Parameter	Data type	Description
EN	BOOL	This parameter is optional. When this input is set to one, the block is activated and can solve the function blocks algorithm. When this input is set to zero, the block is deactivated and won't solve the function block algorithm.
Address	Array [0...7] of INT	The path to the destination device, the content of which can vary depending on the message protocol. Use the Address function as an is input to the block parameter ADR.. Refer to a description of the Address parameter
ActionType	INT	The type of action to perform. For Modbus TCP protocols, this setting = 1 (transmission followed by await reception).
Data_to_ Send	Array [n...m] of INT	The content of this parameter is specific to the protocol. Refer to Control Expert online help.

Input/Output Parameters

The Management_Param array is local:

Parameter	Data type	Description
Management_Param	Array [0...3] of INT	The management parameter, consisting of four words

Do not copy this array during a switchover from a primary to a standby CPU in a redundant system. De-select the **Exchange On STBY** check bocx in Control Expert when you configure a redundant system.

NOTE: Refer to the description of redundant system data management and the T_M_ECPU_HSBY DDT in the *M580 Hot Standby System Planning Guide*.

Output Parameters

Parameter	Data type	Description
ENO	BOOL	This parameter is optional. When you select this output you also get the EN input. ENO output is activated upon successful execution of the function block.
Received_Data	Array [n...m] of INT	the Modbus TCP response, of which the structure and content depends upon the specific protocol

Configuring the DATA_EXCH Management Parameter

Introduction

The structure and content of the management parameter of the `DATA_EXCH` block is common to Modbus TCP explicit messaging.

Configuring the Management Parameter

The management parameter consists of four contiguous words:

Data source	Register	Description	
		High Byte (MSB)	**Low Byte (LSB)**
Data managed by the system	`Management_Param[0]`	Exchange number	Two read-only bits: • Bit 0 = Activity bit • Bit 1 = Cancel bit
	`Management_Param[1]`	Operation report, page 181	Communication report, page 180
Data managed by the user	`Management_Param[2]`	Block timeout. Values include: • 0 = infinite wait • other values = timeout x 100 ms, for example: ◦ 1 = 100 ms ◦ 2 = 200 ms	
	`Management_Param[3]`	Length of data sent or received: • Input (before sending the request): length of data in the `Data_to_Send` parameter, in bytes • Output (after response): length of data in the `Received_Data` parameter, in bytes	

Activity Bit

The activity bit is the first bit of the first element in the table. The value of this bit indicates the execution status of the communication function:

- **1**: The bit is set to 1 when the function launches.
- **0**: The bit returns to 0 upon the completion of the execution. (The transition from 1 to 0 increments the exchange number. If an error is detected during the execution, search for the corresponding code in the operation and communication report, page 180.)

For example, you can make this declaration in the management table:

```
Management_Param[0] ARRAY [0..3] OF INT
```

For that declaration, the activity bit corresponds to this notation:

```
Management_Param[0].0
```

NOTE: The notation previously used requires configuration of the project properties in such a way as to authorize the extraction of bits on integer types. If this is not the case, `Management_Param[0].0` cannot be accessed in this manner.

Modbus TCP Explicit Messaging Using DATA_EXCH

Overview

This section shows you how to configure DATA_EXCH function block parameters for Modbus TCP explicit messages.

Modbus TCP Explicit Messaging Function Codes

Overview

You can execute Modbus TCP explicit messages using either a Control Expert DATA_EXCH function block or the Modbus Explicit Message Window.

NOTE: Configuration edits made to an Ethernet module are not saved to the operating parameters stored in the CPU and, therefore, are not sent by the CPU to the module on startup.

Function Codes

The function codes supported by the Control Expert graphical user interface include the following standard explicit messaging functions:

Function Code (dec)	Description
1	Read bits (%M)
2	Read input bits (%I)
3	Read words (%MW)
4	Read input words (%IW)
15	Write bits (%M)
16	Write words (%MW)

NOTE: You can use the DATA_EXCH function block to execute any Modbus function, via program logic. Because the available function codes are too numerous to list here, refer instead to the Modbus IDA website for more information about these Modbus functions, at http://www.Modbus.org.

Configuring Modbus TCP Explicit Messaging Using DATA_EXCH

Introduction

When you use the DATA_EXCH block to create an explicit message for a Modbus TCP device, configure this block the same way you would configure it for any other Modbus communication. Refer to the Control Expert online help for instructions on how to configure the DATA_EXCH block.

Configuring ADDM Block Unit ID Settings

When you configure the DATA_EXCH block, use the ADDM block to set the DATA_EXCH block's Address parameter. The ADDM block presents the configuration format ADDM('rack.slot.channel[ip_address]UnitID.message_type.protocol') where:

Parameter	Description
rack	the number assigned to the rack containing the communication module
slot	the position of the communication module in the rack
channel	the communication channel (set to a value of 0)
ip_address	the IP address of the remote device (for example, 192.168.1.7)
Unit ID	the destination node address, also known as the Modbus Plus on Ethernet Transporter (MET) mapping index value
message_type	the three-character string **TCP**
protocol	the three-character string **MBS**

The Unit ID value in a Modbus message indicates the destination of the message.

Refer to the Modbus diagnostic codes, page 159.

Contents of the Received_Data Parameter

The `Received_Data` parameter contains the Modbus response. The length of the response varies, and is reported by `Management_Param[3]` after the response is received. The format of the Modbus response is described, below:

Offset (words)	Length (bytes)	Description
0	2	First word of the Modbus response: • High byte (MSB): ◦ if successful: Modbus Function Code ◦ if not: Modbus function code + 16#80 • Low byte (LSB): ◦ if successful: depends on the request ◦ if not: Modbus exception code
1	Length of the `Received_Data` parameter – 2	Remainder of the Modbus response: depends on the specific Modbus request)

NOTE:

- Structure the response in little endian order.
- In some cases of detected errors, Received_Data is also used to judge the type of detected error along with Management_Param.

Modbus TCP Explicit Message Example: Read Register Request

Introduction

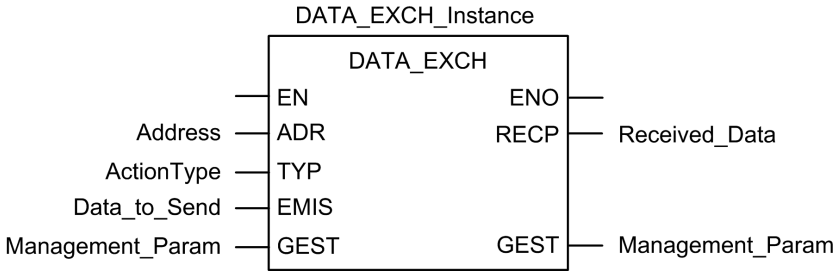
Use the `DATA_EXCH` function block to send a Modbus TCP explicit message to a remote device at a specific IP address to read a single word located in the remote device.

The `Management_Param`, the `Data_to_Send`, and the `Received_Data` parameters define the operation.

`EN` and `ENO` can be configured as additional parameters.

Implementing the DATA_EXCH Function Block

To implement the DATA_EXCH function block, create and assign variables for the for following:



Configuring the Address Variable

The Address variable identifies the explicit message originating device and the target device. Note that the Address variable does not include the Xway address elements {Network.Station} because you are not bridging through another PAC station. Use the ADDM function to convert the following character string to an address:

ADDM('0.1.0{192.168.1.7}TCP.MBS'), where:

- rack = 0
- module (slot number) = 1
- channel = 0
- remote device IP address = 192.168.1.7
- message type = TCP
- protocol = Modbus

Configuring the ActionType Variable

The ActionType variable identifies the function type for the DATA_EXCH function block:

Variable	Description	Value (hex)
ActionType	Transmission followed by wait for response	16#01

Configuring the DataToSend Variable

The DataToSend variable contains the target register address and the number of registers to read:

Variable	Description	Value (hex)
DataToSend [0]	• High byte = Most significant byte (MSB) of register address 16#15 (21 decimal) • Low byte = function code: 16#03 (03 decimal)	16#1503
DataToSend [1]	• High byte = Most significant byte (MSB) of the number of registers to read: 16#00 (0 decimal) • Low byte = Least significant byte (LSB) of register address: 16#0F (15 decimal)	16#000F
DataToSend [2]	CIP request instance information: • High byte = not used: 16#00 (0 decimal) • Low byte = Least significant byte (LSB) of the number of registers to read: 16#01 (1 decimal)	16#0001

NOTE: For detailed information about M580 network topologies, refer to the *Modicon M580 Standalone System Planning Guide for Frequently Used Architectures* and *Modicon M580 System Planning Guide for Complex Topologies*.

Viewing the Response

Use a Control Expert Animation table to display the ReceivedData variable array. Note that the ReceivedData variable array consists of the entire data buffer.

To display the Modbus TCP response, follow these steps:

Step	Action	
1	In Control Expert, select **Tools** > **Project Browser**.	
2	In the Project Browser, select the **Animation Tables** folder, and click the right mouse button. **Result**: A pop-up menu appears.	
3	Select **New Animation Table** in the pop-up menu. **Result**: A new animation table and its properties dialog open.	
4	In the Properties dialog, edit the following values:	
	Name	Type in a table name. For this example: **ReceivedData**.
	Functional module	Accept the default **<None>**.
	Comment	(Optional) Type your comment here.
	Number of animated characters	Type in **100**, representing the size of the data buffer in words.
5	Click **OK** to close the dialog.	
6	In the animation table's **Name** column, type in the name of the variable assigned to the databuffer: **ReceivedData** and press **Enter**. **Result**: The animation table displays the ReceivedData variable.	
7	Expand the ReceivedData variable to display its word array, where you can view the CIP response contained in the ReceivedData variable. **NOTE:** Each array entry presents 2 bytes of data in little endian format. For example, '03' in word[0] is the low byte, and '02' is the high byte.	

Diagnostics

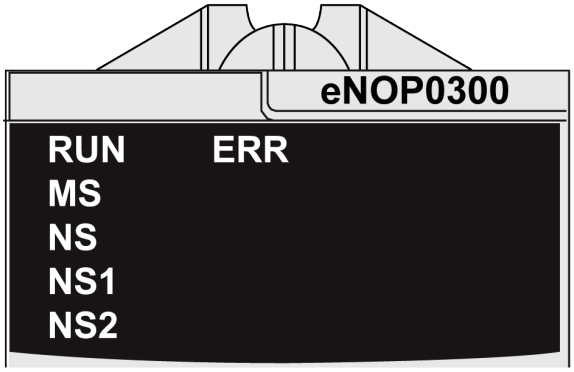
Overview

This chapter describes the diagnostics for the BMENOP0300 module.

LED Indicators on the BMENOP0300 Module

Display

These LEDs are on the front of the BMENOP0300 module:



LED Display Panel Indicators

Use the LEDs on the front panel to diagnose module conditions, as follows:

LED	RUN	ERR	MS (module status)	NS, NS1, NS2[1] (network status)
Condition	**Green**	**Red**	**Green/Red**	**Green/Red**
power OFF	OFF	OFF	OFF	OFF
during power up	LED indicator test 1. All indicators OFF 2. RUN ON for 0.25 seconds, then OFF 3. ERR ON for 0.25 seconds, then OFF 4. MS green ON for 0.25 seconds, then red ON for 0.25 seconds, then green ON 5. NS green ON for 0.25 seconds, then red ON for 0.25 seconds, then OFF 6. All indicators OFF			

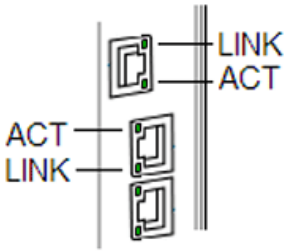
LED	RUN	ERR	MS (module status)	NS, NS1, NS2[1] (network status)
Condition	**Green**	**Red**	**Green/Red**	**Green/Red**
not configured or in default configuration	OFF	flashing	flashing green	**OFF**: If no IP address has been assigned to the module **flashing green**: Module has an IP address, but no 61850 connections are established. **steady green**: At least one 61850 connection is established. **steady red**: Its IP address is already in use (duplicate IP).
configured and in normal operational state with no error detected	steady ON (regardless of controller in RUN/STOP or module in error)	OFF if no error detected	steady green if module is operating correctly	
configured and in normal operational state with an error detected		**flashing**: If there is an X Bus promptness error detected. **steady ON**: If there is another error detected (non-X Bus promptness error).	**flashing red**: If there is a recoverable minor error detected. (Duplicate IP is a recoverable minor error.) **steady red**: If there is a non-recoverable major error detected (example: firmware detected error, self-test detected error, checksum detected error, or RAM test detected error at power up).	
OS update	flashing	OFF	steady red	steady red

1 The NS, NS1, and NS2 LEDs indicate the network status of their respective subnets.

NOTE:

- NS1 is reserved and is always OFF.
- NS2 indicates Network 3 status when IP forwarding is enabled.

Ethernet Port LED Indicators



Use the Ethernet port LEDs to diagnose the status of the respective Ethernet port:

Name	Color	Status	Description
LINK (link/speed)	green	ON	100 Mbits link detected
	yellow	ON	10/100 Mbits link detected
	—	OFF	no detected link
ACT	green	blinking	active link (transmit or receive detected)
		ON	detected but inactive link
		OFF	no detected link

Modbus Diagnostic Codes

Introduction

BMENOP0300 IEC 61850 modules in M580 systems support the diagnostic codes in the following tables.

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 Diagnostics Data (Internal port)	39	103
Ethernet Port Diagnostics Data (**ETH 1**)	142	103
Ethernet Port Diagnostics Data (**ETH 2**)	245	103
Ethernet Port Diagnostics Data (**ETH 3**)	348	103
Ethernet Port Diagnostics Data (backplane)	451	103
Modbus TCP/Port 502 Diagnostic Data	554	114
Modbus TCP/Port 502 Connection Table Data	668	515
SNTP Diagnostics	1218	57
QoS Diagnostics	1275	11
IEC 61850 Server Diagnostic	2025	20
IEC 61850 Client Diagnostics	2047	20

IEC 61850 Server Diagnostics

Address	MS Byte	LS Byte	Modbus Type	Comments
Offset	Active	Health	WORD	Active: 1 = configured Health: 1 = Service is operational.
Offset + 1	ProtoEd	Active-Conn	WORD	ProtoEd: IEC 61850 Edition version ActiveConn: Number of connections established with this server
Offset + 2	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the server receives a read variable request
	LSW - MSB	LSW - LSB		
Offset + 4	MSW - MSB	MSW - LSB	UDINT	the number of rejected MMS read variable requests
	LSW - MSB	LSW - LSB		
Offset + 6	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the server receives a write variable request
	LSW - MSB	LSW - LSB		
Offset + 8	MSW - MSB	MSW - LSB	UDINT	the number of rejected MMS write variable requests

Address	MS Byte	LS Byte	Modbus Type	Comments
	LSW - MSB	LSW - LSB		
Offset + 10	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the server sends an information report message
	LSW - MSB	LSW - LSB		
Offset + 12	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the server sends a goose
	LSW - MSB	LSW - LSB		
Offset + 14	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the server receives a goose
	LSW - MSB	LSW - LSB		
Offset + 16	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the server receives an invalid goose
	LSW - MSB	LSW - LSB		
Offset + 18	MSW - MSB	MSW - LSB	DWORD	detected error code
	LSW - MSB	LSW - LSB		
Offset + 20	MSW - MSB	MSW - LSB	DWORD	internalErr
	LSW - MSB	LSW - LSB		

IEC 61850 Client Diagnostics

Address	MS Byte	LS Byte	Modbus Type	Comments
Offset	Active	Health	WORD	Active: 1 = configured Health: 1 = Service is operational.
Offset + 1	ProtoEd	ActiveConn	WORD	ProtoEd: IEC 61850 Edition version ActiveConn: Number of connections established with this server
Offset + 2	MSW - MSB	MSW - LSB	UDINT	IED connection status
	LSW - MSB	LSW - LSB		
Offset + 4	MSW - MSB	MSW - LSB	UDINT	reserved
	LSW - MSB	LSW - LSB		
Offset + 6	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the client receives a read variable request
	LSW - MSB	LSW - LSB		
Offset + 8	MSW - MSB	MSW - LSB	UDINT	the number of rejected MMS read variable requests
	LSW - MSB	LSW - LSB		
Offset + 10	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the client sends a write variable request
	LSW - MSB	LSW - LSB		
Offset + 12	MSW - MSB	MSW - LSB	UDINT	the number of rejected MMS write variable requests
	LSW - MSB	LSW - LSB		
Offset + 14	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the client sends an information report message
	LSW - MSB	LSW - LSB		
Offset + 16	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the client receives a goose
	LSW - MSB	LSW - LSB		
Offset + 18	MSW - MSB	MSW - LSB	UDINT	a counter that increments each time the client receives an invalid goose
	LSW - MSB	LSW - LSB		

Address	MS Byte	LS Byte	Modbus Type	Comments
Offset + 20	MSW - MSB	MSW - LSB	DWORD	detected error code
	LSW - MSB	LSW - LSB		
Offset + 22	MSW - MSB	MSW - LSB	DWORD	internalErr
	LSW - MSB	LSW - LSB		

Modbus Register Mapping of NTP Diagnostics Data

Address	MS Byte	LS Byte	Modbus Type	Comments
Offset + 0	MSW - MSB	MSW - LSB	Uint32	primary NTP server IP address
Offset + 1	LSW - MSB	LSW - LSB		
Offset + 2	MSW - MSB	MSW - LSB	Uint32	secondary NTP server IP address
Offset + 3	LSW - MSB	LSW - LSB		
Offset + 4	MSW - MSB	BYTE	Uint8	polling period (in seconds)
Offset + 5	MSW - MSB	BYTE	Uint8	update controller with module time
Offset + 6	MSW - MSB	MSW - LSB	Uint32	time zone
Offset + 7	LSW - MSB	LSW - LSB		
Offset + 8	MSB	LSB	Int16	time zone offset (in minutes
Offset + 9	Unused	BYTE	Uint8	daylight saving time bias (in minutes)
Offset + 10	Unused	LSB	Uint8	daylight saving start date - month
Offset + 11	Unused	LSB	Uint8	daylight saving start date - week #, day of week MS 4-bits: occurrence # (1 = first occurrence, 2 = second occurrence, ..., 5 = fifth or last occurrence) LS 4-bits: day of the week (0 = Sunday, ..., 6 = Saturday)
Offset + 12	MSW - MSB	MSW - LSB	Uint32	daylight saving start time (seconds elapsed from midnight)
Offset + 13	LSW - MSB	LSW - LSB		
Offset + 14	Unused	LSB	Uint8	daylight saving end date - month
Offset + 15	Unused	LSB	Uint8	daylight saving end date - week #, day of week
Offset + 16	MSW - MSB	MSW - LSB	Uint32	daylight saving end time (seconds elapsed from midnight)
Offset + 17	LSW - MSB	LSW - LSB		
Offset + 18	Unused	BYTE	Uint8	SNTP mode
Offset + 19	Unused	BYTE	Uint8	reserved
...	–	–	–	–
Offset + 32	Unused	BYTE	Uint8	reserved
Offset + 33	MSW - MSB	MSW - LSB	UDINT	network time service status
Offset + 34	LSW - MSB	LSW - LSB		
Offset + 35	MSW - MSB	MSW - LSB	UDINT	link to NTP server status
Offset + 36	LSW - MSB	LSW - LSB		
Offset + 37	MSW - MSB	MSW - LSB	UDINT	current NTP server IP address
Offset + 38	LSW - MSB	LSW - LSB		
Offset + 39	MSW - MSB	MSW - LSB	UDINT	NTP server type
Offset + 40	LSW - MSB	LSW - LSB		

Address	MS Byte	LS Byte	Modbus Type	Comments
Offset + 41	MSW - MSB	MSW - LSB	UDINT	NTP server time quality
Offset + 42	LSW - MSB	LSW - LSB		
Offset + 43	MSW - MSB	MSW - LSB	UDINT	number of NTP requests sent
Offset + 44	LSW - MSB	LSW - LSB		
Offset + 45	MSW - MSB	MSW - LSB	UDINT	number of communication errors
Offset + 46	LSW - MSB	LSW - LSB		
Offset + 47	MSW - MSB	MSW - LSB	UDINT	number of NTP responses received
Offset + 48	LSW - MSB	LSW - LSB		
Offset + 49	MSW - MSB	MSW - LSB	UINT	last error
Offset + 50	MSW - MSB	MSW - LSB	UDINT	current time
Offset + 51	LSW - MSB	LSW - LSB		
Offset + 52	MSW - MSB	MSW - LSB	UINT	current date
Offset + 53	MSW - MSB	MSW - LSB	UDINT	daylight saving status
Offset + 54	LSW - MSB	LSW - LSB		
Offset + 55	MSW - MSB	MSW - LSB	DINT	time since last update
Offset + 56	LSW - MSB	LSW - LSB		

Modbus Register Mapping of QoS Diagnostic Data

Address	MS Byte	LS Byte	Modbus Type	Comments
Offset	MS Byte	LS Byte	UINT	802.1Q tag enable/disable
Offset + 01	MS Byte	LS Byte	UINT	reserved for DSCP PTP event
Offset + 02	MS Byte	LS Byte	UINT	reserved for DSCP PTP general
Offset + 03	MS Byte	LS Byte	UINT	reserved for DSCP EIP urgent
Offset + 04	MS Byte	LS Byte	UINT	reserved for DSCP EIP scheduled
Offset + 05	MS Byte	LS Byte	UINT	reserved for DSCP EIP high
Offset + 06	MS Byte	LS Byte	UINT	reserved for DSCP EIP low
Offset + 07	MS Byte	LS Byte	UINT	reserved for DSCP EIP explicit
Offset + 08	MS Byte	LS Byte	UINT	reserved for DSCP Modbus IO scanner (same as DSCP EIP high)
Offset + 09	MS Byte	LS Byte	UINT	DSCP Modbus client/server (same as EIP explicit)
Offset + 10	MS Byte	LS Byte	UINT	DSCP SNTP
Offset + 11	MS Byte	LS Byte	UINT	DSCP IEC 61850 client

Get Status Summary: Request

Modbus function code 8 / sub-function code 21: request

Field	Length (bytes)	Value (hex)
function code	1	08
sub-function code hi	1	00
sub-function code low	1	15

Field	Length (bytes)	Value (hex)
operation code hi	1	00
operation code low	1	76

Get Status Summary: Response

Modbus function code 8 / sub-function code 21: response

Field	Length (bytes)	Value (hex)
function code	1	08
sub-function code hi	1	00
sub-function code low	1	15
operation code hi	1	00
operation code low	1	76
byte count	1	depends on product
number of LEDs	2	depends on product
each LED color [1]	2	0 = off 1 = on green 2 = on red
each LED status [1]	2	LED status number (see LED Status table)
name string [1]	N	LED name (null terminated)
. . .	–	–
number of services	2	depends on product
each service color [1]	2	0 = off or N/A 1 = green 2 = red
each service status [1]	2	service status number (see Services Status table)
name string [1]	N	service name
. . .	–	–

LED Status

Modbus function code 8 / sub-function code 21: LED status

LED Status Number (hex)	Description
1	ready for operation
2	not ready for operation
3	error detected
4	no error detected
5	in operation
6	duplicate IP address
7	waiting for address server response
8	default IP address in use
9	IP address configuration conflict detected

LED Status Number (hex)	Description
A	not configured
B	recoverable error detected
C	connections established
D	–
E	connections error detected
F	running
10	detected error present
11	Ethernet link established
12	no Ethernet link established
13	connected to 100 Mbps link
14	not connected to 100 Mbps link
15	connected to full duplex link
16	note connected to full duplex link
17	configuration error detected

Services Status

Modbus function code 8 / sub-function code 21: services status

Service Status Number	Description
1	enabled
2	working properly
3	disabled
4	not configured
5	at least one connection not working
6	enabled on
7	enabled off

BMENOP0300 Module Response

Modbus function code 8 / sub-function code 21: module response

Field	Length (bytes)	Value (hex)	
function code	1	08	
sub-function code hi	1	00	
sub-function code low	1	15	
operation code hi	1	00	
operation code low	1	76	
byte count	1	D6	
number of LEDs	2	6	
LED 1 color	2	byte 0 = LED color	0 (black) = LED off 1 (green) = green LED on
		byte 1 = blinking	0 (not blinking) 1 (blinking) = green LED blinking

Field	Length (bytes)	Value (hex)	
LED 1 status	2	0	
LED 1 name string	4	RUN	
LED 2 color	2	byte 0 = LED color	0 (black) = LED off 2 (red) = red LED on
		byte 1 = blinking	0 (not blinking) 1 (blinking) = red LED blinking
LED 2 status	2	0	
LED 2 name string	4	ERR	
LED 3 color	2	byte 0 = LED color	0 (black) = LED off 2 (red) = red LED on
		byte 1 = blinking	0 (not blinking) 1 (blinking) = red LED blinking
LED 3 status	2	0	
LED 3 name string	11	mod status	
LED 4 color	2	byte 0 = LED color	0 (black) = LED off 1 (green) = green LED on 2 (red) = LED on 3 (yellow) = red and green LEDs on 4 (blink first green, then yellow) = green on, red blinking 5 (blink first red, then yellow) = red and green blinking
		byte 1 = blinking	0 (not blinking) 1 (blinking) = LED in byte 0 blinking
LED 4 status	2	0	
LED 4 name string	15	network status	
LED 5 color	2	byte 0 = LED color	0 (black) = LED color 1 (green) = green LED on 2 (red) = LED on 3 (yellow) = red and green LEDs on 4 (blink first green, then yellow) = green on, red blinking 5 (blink first red, then yellow) = red and green blinking
		byte 1 = blinking	0 (not blinking) 1 (blinking) = LED in byte 0 blinking
LED 5 status	2	0	
LED 5 name string	17	network status 1	
LED 6 color	2	byte 0 = LED color	0 (black) = LED off 1 (green) = green LED on 2 (red) = LED on 3 (yellow) = red and green LEDs on 4 (blink first green, then yellow) = green on, red blinking 5 (blink first red, then yellow) = red and green blinking

Field	Length (bytes)	Value (hex)	
		byte 1 = blinking	0 (not blinking 1 (blinking) = LED in byte 0 blinking
LED 6 status	2	0	
LED 6 name string	17	network status 2	
number of services	2	5	
service 1 color	2	0 = off <default> 1 = green	
service 1 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) <default>	
service 1 name string	15	access control	
service 2 color	2	0 = off <default> 1 = on green 2 = on red	
service 2 status	2	4 (corresponds to LED color 0) <default> 2 (corresponds to LED color 1) 5 (corresponds to LED color 2) – link to server down	
service 2 name string	21	network time service	
service 3 color	2	0 = off <default> 1 = green	
service 3 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) <default>	
service 3 name string	18	IED server service	
service 4 color	2	0 = off <default> 1 = green	
service 4 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) <default>	
service 4 name string	18	IED client service	
service 5 color	2	0 = off <default> 1 = green	
service 5 status	2	1 (corresponds to LED color 1) 3 (corresponds to LED color 0) <default>	
service 5 name string	23	IP forwarding service	

Modbus Diagnostic Codes

Modbus NTP Diagnostic Codes

The BMENOP0300 module supports the following NTP diagnostic codes, which begin at 41219 (decimal):

Address	MS Byte	LS Byte	Modbus Type	Comments
41219	MSW - MSB	MSW - LSB	UDINT	Enabled/disabled
Offset + 01	LSW - MSB	LSW - LSB		
Offset + 02	MSW - MSB	MSW - LSB	UDINT	Primary NTP Server IP Address
Offset + 03	LSW - MSB	LSW - LSB		
Offset + 04	MSW - MSB	MSW - LSB	UDINT	Secondary NTP Server IP Address
Offset + 05	LSW - MSB	LSW - LSB		
Offset + 06	Unused	LS Byte	USINT	Polling Period
Offset + 07	Unused	LS Byte	USINT	Daylight Saving Auto Adjustment
Offset + 08	Unused	LS Byte	USINT	Update CPU with Module Time
Offset + 09	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 NTP Requests Sent
Offset + 30	LSW - MSB	LSW - LSB		
Offset + 31	MSW - MSB	MSW - LSB	UDINT	Number of Communication Errors
Offset + 32	LSW - MSB	LSW - LSB		
Offset + 33	MSW - MSB	MSW - LSB	UDINT	Number of NTP Reponses Received
Offset + 34	LSW - MSB	LSW - LSB		

Address	MS Byte	LS Byte	Modbus Type	Comments
Offset + 35	MS Byte	LS Byte	UINT	Last Error
Offset + 36	MSW - MSB	MSW - LSB	UDINT	Current Time
Offset + 37	LSW - MSB	LSW - LSB		
Offset + 38	MS Byte	LS Byte	UINT	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		

Modbus QoS Diagnostic Codes

The BMENOP0300 module supports the following QoS diagnostic codes, which begin at 41261 (decimal):

Address	MS Byte	LS Byte	CIP Type	Comments
41261	MS Byte	LS Byte	UINT	802.1Q Tag enable / disable
Offset + 01	MS Byte	LS Byte	UINT	Reserved for DSCP PTP Event
Offset + 02	MS Byte	LS Byte	UINT	Reserved for DSCP PTP General
Offset + 03	MS Byte	LS Byte	UINT	Reserved for DSCP EIP Urgent
Offset + 04	MS Byte	LS Byte	UINT	Reserved for DSCP EIP Scheduled
Offset + 05	MS Byte	LS Byte	UINT	Reserved for DSCP EIP High
Offset + 06	MS Byte	LS Byte	UINT	Reserved for DSCP EIP Low
Offset + 07	MS Byte	LS Byte	UINT	Reserved for DSCP EIP Explicit
Offset + 08	MS Byte	LS Byte	UINT	Reserved for DSCP Modbus IO Scanner (same as DSCP EIP High)
Offset + 09	MS Byte	LS Byte	UINT	DSCP Modbus Client/Server (same EIP Explicit)
Offset + 10	MS Byte	LS Byte	UINT	DSCP NTP
Offset + 11	MS Byte	LS Byte	UINT	DSCP IEC 61850_Client

IEC 61850 Diagnostic Codes

Introduction

The BMENOP0300 module supports IEC 61850 server, server report, and client diagnostic codes.

Server Diagnostic Codes

Address	MS Byte	LS Byte	Mod-bus Type	Comments
42201	Active	Health	WORD	• Active: 1 indicates configured • Health: 1 indicates service is operational
42201+ 1	ProtoEd	ActiveConn	WORD	• ProtoEd :IEC 61850 Edition version • ActiveConn:Number of connection established with this server
42201+ 2	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the server receives a read variable request.
	LSW - MSB	LSW - LSB		
42201+ 4	MSW - MSB	MSW - LSB	UDINT	Number of rejected MMS read variable requests
	LSW - MSB	LSW - LSB		
42201+ 6	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the server receives a write variable request.
	LSW - MSB	LSW - LSB		
42201+ 8	MSW - MSB	MSW - LSB	UDINT	Number of rejected MMS write variable requests
	LSW - MSB	LSW - LSB		
42201+ 10	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the server sends an information report message.
	LSW - MSB	LSW - LSB		
42201+ 12	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the server sends a GOOSE.
	LSW - MSB	LSW - LSB		
42201+ 14	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the server receives a GOOSE.
	LSW - MSB	LSW - LSB		
42201+ 16	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the server receives an invalid GOOSE.
	LSW - MSB	LSW - LSB		
42201+ 18	MSW - MSB	MSW - LSB	DWOR-D	Detected error code
	LSW - MSB	LSW - LSB		

Server Report Diagnostic Codes

Address	MS Byte	LS Byte	Mod-bus Type	Comments
42221	Enabled	Overflow	WORD	• Enabled: 1 indicates configured • Overflow: 1 indicates service is operational
42221+ 1	MSB	LSB	WORD	Counter for data exchange for one report-1
...	...	...	...	...
...	...	...	...	...

Address	MS Byte	LS Byte	Modbus Type	Comments
42221	Enabled	Overflow	WORD	• Enabled: 1 indicates configured • Overflow: 1 indicates service is operational
42221+ 63	MSB	LSB	WORD	Counter for data exchange for one report – 64

Client Diagnostic Codes

Address	MS Byte	LS Byte	Modbus Type	Comments
42349	Active	Health	WORD	• Active: 1 indicates configured • Health: 1 means service is operational
42349+ 1	ProtoEd	ActiveConn	WORD	• ProtoEd :IEC 61850 Edition version • ActiveConn:Number of connections established with this server
42349+ 2	MSW - MSB	MSW - LSB	UDINT	IED connection status
	LSW - MSB	LSW - LSB		
42349+ 4	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the client receives a read variable.
	LSW - MSB	LSW - LSB		
42349+ 6	MSW - MSB	MSW - LSB	UDINT	Number of rejected MMS read variable requests
	LSW - MSB	LSW - LSB		
42349+ 8	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the client sends a write variable request
	LSW - MSB	LSW - LSB		
42349+ 10	MSW - MSB	MSW - LSB	UDINT	Number of rejected MMS write variable requests
	LSW - MSB	LSW - LSB		
42349+ 12	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the client receives an information report message.
	LSW - MSB	LSW - LSB		
42349+ 14	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the client receives a goose.
	LSW - MSB	LSW - LSB		
42349+ 16	MSW - MSB	MSW - LSB	UDINT	A counter that increments each time the client receives an invalid goose.
	LSW - MSB	LSW - LSB		
42349+ 18	MSW - MSB	MSW - LSB	DWORD	Detected error code
	LSW - MSB	LSW - LSB		

Redundant System Switchover

Overview

The BMENOP0300 module supports the M580 redundancy function. In an M580 redundancy system, the primary and standby PACs continuously exchange data including the state RAM of the two BMENOP0300 modules.

Use the IP address xx.xx.0.xx to validate a redundant configuration, then rebuild your Control Expert project.

NOTE:

- Because the primary M580 controller automatically synchronizes I/O data between the primary and standby controllers, it is not necessary to execute any operations on the BMENOP0300 module in the standby PAC.
- Configure the standby PAC to execute only the first section of program logic, and place all code for BMENOP0300 module operations into code sections that follow the first section.

IEC 61850 Server Functions in an M580 Redundancy System

SCADA:

In an M580 redundancy system, the primary PAC performs SCADA functions in the same manner as a standalone PAC. The standby PAC does not communicate with SCADA, but does monitor PAC memory each scan and generates reports.

On switchover, the primary PAC closes the connection with SCADA; the standby PAC starts to listen for and accept new connection requests from SCADA. The former standby PAC, now the primary, first applies the data values received from the former primary to its local database, and then begins to perform SCADA functions after a SCADA connection is established.

Report Functions:

On every PAC cycle, the two BMENOP0300 modules synchronize the buffered report **Entry ID** value. After switchover, confirm that SCADA explicitly sets the **Entry ID** to the BMENOP0300 module in the new primary PAC so that the module can continue to send buffered reports. If the **Entry ID** is not synchronized, or if synchronization is not successful, the oldest reports are re-sent during switchover buffer time. In this case, SCADA can detect if it has received a duplicated event report by comparing the report time tags.

The **Integrity Period** setting can be used in a redundant system to generate buffered and unbuffered reports on both primary and standby BMENOP0300 modules. Note that buffered report data can be overwritten by new integrated period report data very quickly depending on the setting. If a period is very short, it may cause unsent report data to be lost in the new primary controller after the controller switchover.

⚠WARNING

LOSS OF DATA

Do not use this feature in case of fast integrated period value in a redundant system.

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

GOOSE:

Only the BMENOP0300 module in the primary PAC can publish GOOSE transmissions.

The BMENOP0300 modules in both the primary and standby PACs receive GOOSE data from the remote IED. However, the data received by the standby PAC is not added to memory, but is only added to the local database.

On switchover, the BMENOP0300 module in the standby PAC takes over the task of sending GOOSE. However, the *stNum* and *sqNum* fields are not synchronized.

IEC 61850 Client Functions in an M580 Redundant System

Connection with Remote IED:

Only the BMENOP0300 module in the primary PAC communicates with the remote IED; the BMENOP0300 module in the standby PAC does not establish a connection with remote IED.

The BMENOP0300 modules in both the primary and standby PACs synchronize data out values from PAC memory to the local database. However, because the standby PAC does not send output data to the remote IED, the remote IED receives output data only from the BMENOP0300 module in the primary PAC.

GOOSE:

The BMENOP0300 modules in both the primary and standby PACs receive GOOSE data from the remote IED. However, the data received by the standby PAC is not added to memory, but is only added to the local database.

Report Functions:

Automatically enable the report function for buffered and unbuffered report control blocks by setting the `AutoEna` field to 1 (auto enable). After switchover, the BMENOP0300 module sets the **Entry ID** to the remote IED and automatically enables the report when establishing a connection with the remote IED.

Switchover:

On switchover, the BMENOP0300 module in the primary PAC closes the connection with remote IED; the BMENOP0300 module in the former standby PAC, now the primary, begins to communicate with remote IED.

If the execution of a report control block/GOOSE command, polling command, or control operation is interrupted by a switchover, the high byte of the `Status` element for that object returns a detected error bit. Add an error handling procedure to your program logic that will manage this detected error by re-sending the command.

BMENOP0300 IP Address Recovery Time

Use the following formula to determine the BMENOP0300 module IP address recovery time in a M580 redundancy system:

500 ms (IP address swapping) + connection establishment time (3 s)

NOTE: The maximum swap time may increase if the end device does not respond in a timely manner.

NOTE: During the swap, there may be disruption in communication between the BMENOP0300 module and the end device. Confirm that the application can tolerate this communication disruption.

Firmware Upgrade

Introduction

This chapter shows you how to upgrade the firmware for the BMENOP0300 module.

Firmware Update with Automation Device Maintenance

Overview

The EcoStruxure™ Automation Device Maintenance is a standalone tool that allows and simplifies the firmware update of devices in a plant (single or multiple).

The tool supports the following features:

- Automatic device discovery
- Manual device identification
- Certificate management
- Firmware update for multiple devices simultaneously

  NOTE: For a description of the download procedure, refer to the *EcoStruxure™ Automation Device Maintenance, User Guide*.

Firmware Upgrade with Unity Loader

Introduction

These instructions assume that:

- You are familiar with Control Expert.
- You put the M580 controller in Stop mode.
- You confirmed that you enabled the **FTP** setting in the **Security** tab of your Control Expert application.
- You installed Unity Loader on your PC during the Control Expert installation.

  Refer to the Unity Loader, User Manual for a description of the download procedure.

Firmware Compatibility

Modules are upward compatible. You can upgrade the firmware of a module to the latest available version.

NOTE: Do not downgrade the firmware of a module.

Due to new hardware in the module, firmware SV2.50 or earlier is not allowed to download to a module with PV04 or any subsequent comparable version(s). In this case, you can not complete the firmware downgrade and Unity Loader displays an error message.

NOTICE
FIRMWARE UPGRADE COMPATIBILITY MISMATCH Do not downgrade a BMENOP0300 or BMENOP0300C module PV04 or any subsequent hardware version(s) with a firmware SV2.50 or earlier. **Failure to follow these instructions can result in equipment damage.**

The following table shows the firmware compatibility among product versions:

Product Version (**PV**)	Fimware Version (**SV**)	
	SV2.40 or earlier	SV2.50 or any subsequent supporting version(s)
PV01, PV02, PV03	Yes	Yes
≥PV04	No	Yes

Upgrading the Firmware

Follow these steps to upgrade the module firmware:

Step	Action
1	On your PC, install the Unity Loader software provided with Control Expert.
2	Connect the PC that is running Unity Loader to one of the module ports.
3	Launch the Unity Loader software.
4	Select the **Firmware** tab.
5	In the PC list box, select the .ldx file that contains the firmware file.
6	Check that the transfer sign is green to allow the transfer from the PC to the module.
7	Select **Transfer**.
8	Select **Close** after the transfer is complete.
9	Confirm that the installation of the firmware did not create an application mismatch condition.

Protocol Conformance

Statement of Protocol Conformance

Conformance

The BMENOP0300 module complies with Edition 1.0 or 2.0 of the IEC 61850 communication protocol. Use the module only in a network in which all devices support the same edition of the protocol.

The BMENOP0300 module was tested against and conforms to the following standards,:

- PICS: Protocol Implementation Conformance Statement
- PIXIT: Protocol Implementation Conformance Extra Information for Testing
- MICS: Model Implementation Conformance Statement
- TICS: Technical Issue Conformance Statement

These documents are available in the IEC 61850 Configuration Tool.

Appendices

What's in This Part

Detected Error Codes

What's in This Chapter

Overview

This chapter contains a list of codes that describe the status of Ethernet communication module messages.

Modbus TCP Explicit Messaging Detected Error Codes

Introduction

If a `DATA_EXCH` function block does not execute a Modbus TCP explicit message, Control Expert returns a hexadecimal detected error code.

Modbus TCP Detected Error Codes

Modbus TCP hexadecimal detected error codes include:

Detected Error Code	Description
16#800D	Timeout on the explicit message request
16#8012	Bad device
16#8015	Either: • Nor resources to handle the message, or • Internal detected error: no buffer available, no link available, impossible to send to the TCP task
16#8018	Either: • Another explicit message for this device is in progress, or • TCP connection or encapsulation session in progress
16#8030	Timeout on the Forward_Open request
Note: The following 16#81xx detected errors are Forward_Open response detected errors that originate at the remote target and are received via the CIP connection.	
16#8100	Connection in use or duplicate Forward_Open
16#8103	Transport class and trigger combination not supported
16#8106	Ownership conflict
16#8107	Target connection not found
16#8108	Invalid network connection parameter
16#8109	Invalid connection size
16#8110	Target for connection not configured
16#8111	RPI not supported
16#8113	Out of connections
16#8114	Vendor ID or product code mismatch
16#8115	Product type mismatch

Detected Error Code	Description
16#8116	Revision mismatch
16#8117	Invalid produced or consumed application path
16#8118	Invalid or inconsistent configuration application path
16#8119	Non-Listen Only connection not opened
16#811A	Target object out of connections
16#811B	RPI is smaller than the production inhibit time
16#8123	Connection timed out
16#8124	Unconnected request timed out
16#8125	Parameter detected error in unconnected request and service
16#8126	Message too large for unconnected_send service
16#8127	Unconnected acknowledge without reply
16#8131	No buffer memory available
16#8132	Network bandwidth not available for data
16#8133	No consumed connection ID filter available
16#8134	Not configured to send scheduled priority data
16#8135	Schedule signature mismatch
16#8136	Schedule signature validation not possible
16#8141	Port not available
16#8142	Link address not valid
16#8145	Invalid segment in connection path
16#8146	Detected error in Forward_Close service connection path
16#8147	Scheduling not specified
16#8148	Link address to self invalid
16#8149	Secondary resources unavailable
16#814A	Rack connection already established
16#814B	Module connection already established
16#814C	Miscellaneous
16#814D	Redundant connection mismatch
16#814E	No more user-configurable link consumer resources: the configured number of resources for a producing application has reached the limit
16#814F	No more user-configurable link consumer resources: there are no consumers configured for a producing application to use
16#8160	Vendor specific
16#8170	No target application data available
16#8171	No originator application data available
16#8173	Not configured for off-subnet multicast
16#81A0	Detected error in data assignment
16#81B0	Optional object state detected error
16#81C0	Optional device state detected error
Note: All 16#82xx detected errors are register session response detected errors.	
16#8200	Target device does not have sufficient resources
16#8208	Target device does not recognize message encapsulation header
16#820F	Reserved or unknown detected error from target

Explicit Messaging: Communication and Operation Reports

Overview

Communication and operation reports are part of the management parameters.

NOTE: Test communication function reports at the end of their execution and before the next activation. On cold start-up, confirm that all communication function management parameters are tested and reset to 0.

It may be helpful to use the%S21 to examine the first cycle after a cold or warm start.

Communication Report

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

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

Value	Communication report (least significant byte)
16#00	Correct exchange
16#01	Exchange stop on timeout
16#02	Exchange stop on user request (CANCEL)
16#03	Incorrect address format
16#04	Incorrect destination address
16#05	Incorrect management parameter format
16#06	Incorrect specific parameters
16#07	Error detected in sending to the destination
16#08	Reserved
16#09	Insufficient receive buffer size
16#0A	Insufficient send buffer size
16#0B	No system resources: the number of simultaneous communication EFs exceeds the maximum that can be managed by the processor
16#0C	Incorrect exchange number
16#0D	No telegram received
16#0E	Incorrect length
16#0F	Telegram service not configured
16#10	Network module missing
16#11	Request missing
16#12	Application server already active
16#13	UNI-TE V2 transaction number incorrect
16#FF	Message refused

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

Operation Report

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

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

Modbus TCP Explicit Messaging Detected Error Codes

Introduction

If an `MBP_MSTR` function block does not execute an explicit message, Control Expert displays a hexidecimal detected error code.

Refer to the TCP/IP Ethernet detected error codes topic for a description of those codes.

Modbus TCP Detected Error Codes

Modbus TCP hexadecimal detected error codes include:

Code (hexadecimal)	Description
16#800D	Timeout on the explicit message request
16#8015	Either: • Nor resources to handle the message, or • Internal event: no buffer available, no link available, impossible to send to the TCP task
16#8018	Either: • Another explicit message for this device is in progress, or • TCP connection or encapsulation session in progress
16#8030	Timeout on the Forward_Open request
Note: The following 16#81xx events are Forward_Open response detected error codes that originate at the remote target and are received via the CIP connection.	
16#8100	Connection in use or duplicate Forward_Open
16#8103	Transport class and trigger combination not supported
16#8106	Ownership conflict
16#8107	Target connection not found
16#8108	Invalid network connection parameter
16#8109	Invalid connection size
16#8110	Target for connection not configured
16#8111	RPI not supported
16#8113	Out of connections
16#8114	Vendor ID or product code mismatch
16#8115	Product type mismatch
16#8116	Revision mismatch
16#8117	Invalid produced or consumed application path
16#8118	Invalid or inconsistent configuration application path
16#8119	Non-Listen Only connection not opened
16#811A	Target object out of connections
16#811B	RPI is smaller than the production inhibit time
16#8123	Connection timed out
16#8124	Unconnected request timed out
16#8125	Parameter event in unconnected request and service
16#8126	Message too large for unconnected_send service
16#8127	Unconnected acknowledge without reply
16#8131	No buffer memory available
16#8132	Network bandwidth not available for data
16#8133	No consumed connection ID filter available
16#8134	Not configured to send scheduled priority data
16#8135	Schedule signature mismatch
16#8136	Schedule signature validation not possible

Code (hexadecimal)	Description
16#8141	Port not available
16#8142	Link address not valid
16#8145	Invalid segment in connection path
16#8146	Event in Forward_Close service connection path
16#8147	Scheduling not specified
16#8148	Link address to self invalid
16#8149	Secondary resources unavailable
16#814A	Rack connection already established
16#814B	Module connection already established
16#814C	Miscellaneous
16#814D	Redundant connection mismatch
16#814E	No more user-configurable link consumer resources: the configured number of resources for a producing application has reached the limit
16#814F	No more user-configurable link consumer resources: there are no consumers configured for a producing application to use
16#8160	Vendor specific
16#8170	No target application data available
16#8171	No originator application data available
16#8173	Not configured for off-subnet multicast
16#81A0	Event in data assignment
16#81B0	Optional object state event
16#81C0	Optional device state event
Note: All 16#82xx events are register session response detected error codes.	
16#8200	Target device does not have sufficient resources
16#8208	Target device does not recognize message encapsulation header
16#820F	Reserved or unknown event from target

Supported Data Model Items

What's in This Chapter

Overview

This chapter describes the items supported by the data model of the BMENOP0300 module.

Logical Nodes

Overview

The BMENOP0300 module supports the logical nodes (LNs) appearing in the following groups.

Group L: System Logical Nodes

Name	Description
LLN0	Logical node zero
LPHD	Physical device information
LCCH	Physical communication channel supervision
LGOS	GOOSE subscription
LTIM	Time management
LTMS	Time master supervision

Group A: Automatic Control Logical Nodes

Name	Description
ACTM	Control mode selection
AJCL	Joint control
ANCR	Neutral current regulator
APSF	PSS 4B filter function
APSS	PSS control, common information
APST	PSS 2A/B filter function
ARCO	Reactive power control
ARIS	Resistor control
ATCC	Automatic tap changer
AVCO	Voltage control

Group C: Control Logical Nodes

Name	Description
CALH	Alarm handling
CCGR	Cooling group
CPOW	Point-on-wave switching
CSWI	Switch controller
CSYN	Synchronizer controller

Group F: Functional Block Logical Nodes

Name	Description
FCNT	Counter
FCSD	Curve shape description
FFIL	Generic filter
FHBT	Functional heartbeat
FLIM	Control function output
FPID	PID regulator
FRMP	Ramp function
FSCH	Scheduler
FSPT	Set-point control
FXOT	Action at over threshold
FXPS	Functional priority status
FXUT	Action at under threshold

Group G: Generic Reference Logical Nodes

Name	Description
GAPC	Generic automatic process control
GGIO	Generic process I/O
GSAL	Generic security application

Group H: Hydropower Specific Logical Nodes

Name	Description
HBRG	Turbine – generator shaft bearing
HCOM	Combinator
HDAM	Hydropower dam
HDFL	Deflector control
HDLS	Dam leakage supervision
HEBR	Electrical brake
HGOV	Governor control mode
HGPI	Gate position indicator

Name	Description
HGTE	Dam gate
HITG	Intake gate
HJCL	Joint control
HLKG	Leakage supervision
HLVL	Water level indicator
HMBR	Mechanical brake
HNDL	Needle control
HNHD	Water net head data
HOTP	Dam over-topping protection
HRES	Hydropower / water reservoir
HSEQ	Hydropower unit sequencer
HSPD	Speed monitoring
HSST	Surge shaft
HTGV	Guide vanes (wicket gate)
HTRB	Runner blades
HTRK	Trash rack
HTUR	Turbine
HUNT	Hydropower unit
HVLV	Valve (butterfly valve, ball valve)
HWCL	Water control

Group I: Interfacing and Archiving Logical Nodes

Name	Description
IARC	Archiving
IFIR	Fire detection and alarm
IHMI	Human machine interface
IHND	Hand interface
ISAF	Safety alarm function
ITCI	Telecontrol interface
ITMI	Telemonitoring interface
ITPC	Teleprotection communication

Group K: Mechanical and Non-Electric Primary Equipment Logical Nodes

Name	Description
KFAN	Fan
KFIL	Filter
KPMP	Pump
KTNK	Tank
KVLV	Valve control
KHTR	Heater, cubicle heater

Group M: Metering and Measurement Logical Nodes

Name	Description
MENV	Environmental information
MFLK	Flicker measurement name
MHAI	Harmonics or interharmonics
MHAN	Non-phase-related harmonics or interharmonics
MHYD	Hydrological information
MMDC	DC measurement
MMET	Meteorological information
MMTN	Metering single phase
MMTR	Metering 3 phase
MMXN	Non-phase-related measurement
MMXU	Measurement
MSQI	Sequence and imbalance
MSTA	Metering statistics

Group P: Protection Function Logical Nodes

Name	Description
PDIF	Differential
PDIR	Direction comparison
PDIS	Distance
PDOP	Directional overpower
PDUP	Directional underpower
PFRC	Rate of change of frequency
PHAR	Harmonic restraint
PHIZ	Ground detector
PIOC	Instantaneous overcurrent
PMRI	Motor restart inhibition
PMSS	Motor starting time supervision
POPF	Over power factor
PPAM	Phase angle measuring
PRTR	Rotor protection
PSCH	Protection scheme
PSDE	Sensitive directional earthfault
PTEF	Transient earth fault
PTHF	Thyristor protection
PTOC	Time overcurrent
PTOF	Overfrequency
PTOV	Overvoltage
PTRC	Protection trip conditioning
PTTR	Thermal overload
PTUC	Undercurrent

Name	Description
PTUF	Underfrequency
PTUV	Undervoltage
PUPF	Underpower factor
PVOC	Voltage controlled time
PVPH	Volts per Hz
PZSU	Zero speed or underspeed

Group Q: Power Quality Logical Nodes

Name	Description
QFVR	Frequency variation
QITR	Current transient
QIUB	Current unbalance variation
QVTR	Voltage transient
QVUB	Voltage unbalance variation
QVVR	Voltage variation

Group R: Protection Related function Logical Nodes

Name	Description
RBRF	Breaker failure
RDIR	Directional element
RFBC	Field breaker configuration
RFLO	Fault locator
RMXU	Differential measurements
RPSB	Power swing detection/blocking
RREC	Autoreclosing
RSYN	Synchronism-check

Group S: Supervision and Monitoring Logical Nodes

Name	Description
SARC	Monitoring and diagnostics for arcs
SCBR	Circuit breaker supervision
SFLW	Supervision of media flow
SIMG	Insulation medium supervision (gas)
SIML	Insulation medium supervision (liquid)
SLTC	Tap changer supervision
SLVL	Supervision of media level
SOPM	Supervision of operating mechanism
SPDC	Monitoring and diagnostics for partial discharges

Name	Description
SPOS	Supervision of the position of a device
SPRS	Supervision media pressure
SPTR	Power transformer supervision
SSWI	Circuit switch supervision
STMP	Temperature supervision
SVBR	Vibration supervision

Group T: Instrument Transformer and Sensor Logical Nodes

Name	Description
TANG	Angle
TAXD	Axial displacement
TCTR	Current transformer
TDST	Distance
TFLW	Liquid flow
TFRQ	Frequency
TGSN	Generic sensor
THUM	Humidity
TLVL	Media level
TMGF	Magnetic field
TMVM	Movement sensor
TPOS	Position indicator
TPRS	Pressure sensor
TRTN	Rotation transmitter
TSND	Sound pressure sensor
TTMP	Temperature sensor
TTNS	Mechanical tension / stress
TVBR	Vibration sensor
TVTR	Voltage transformer
TWPH	Water acidity

Group X: Switchgear Logical Nodes

Name	Description
XCBR	Circuit breaker
XFFL	Switching control for field flashing
XSWI	Circuit switch

Group Y: Power Transformers Logical Nodes

Name	Description
YEFN	Earth fault neutralizer (Petersen coil)
YLTC	Tap changer
YPSH	Power shunt
YPTR	Power transformer

Group Z: Further Power System Equipment Logical Nodes

Name	Description
ZAXN	Auxiliary network
ZBAT	Battery
ZBSH	Bushing
ZCAB	Power cable
ZCAP	Capacitor bank
ZCON	Converter
ZGEN	Generator
ZGIL	Gas insulated line
ZLIN	Power overhead line
ZMOT	Motor
ZREA	Reactor
ZRES	Resistor
ZRRC	Rotating reactive component
ZSAR	Surge arrestor
ZSCR	Semi-conductor controlled rectifier
ZSMC	Synchronous machine
ZTCF	Thyristor controlled frequency converter
ZTCR	Thyristor controlled reactive component

Common Data Classes

CDCs

The BMENOP0300 module supports the following common data classes (CDCs):

CDC	Description	Information Type
ACD	Directional protection activation information	Status information
ACT	Protection activation information	Status information
APC	Controllable analogue process value	Controls information
ASG	Analog setting	Analog settings
BAC	Binary controlled analog process value	Controls information
BCR	Binary counter reading	Status information
BSC	Binary controlled step position information	Controls information

CDC	Description	Information Type
CMV	Complex measured value	Measurment information
CSD	Curve shape description	Descriptive information
CSG	Curve shape setting	Analog settings
CURVE	Setting curve	Analog settings
DEL	Phase to phase related measured values of a three-phase system	Measurement information
DPC	Controllable double point	Controls information
DPL	Device name plate	Descriptive information
DPS	Double point status	Status information
ENC	Controllable enumerated status	Controls information
ENG	Enumerated status setting	Status settings
ENS	Enumerated status	Status information
HDEL	Harmonic value for DEL	Measurment information
HMV	Harmonic value	Measurment information
HST	Histogram	Status information
HWYE	Harmonic value for WYE	Measurment information
INC	Controllable integer status	Controls information
ING	Integer status setting	Status settings
INS	Integer status	Status information
ISC	Integer controlled step position information	Controls information
LPL	Logical node name plate	Descriptive information
MV	Measured value	Measurment information
ORG	Object reference setting	Status settings
RST	Operational restriction	Hydro-specific information
SAV	Sampled value	Measurment information
SEC	Security violation counting	Status information
SEQ	Sequence	Measurment information
SPC	Controllable single point	Controls information
SPG	Single point setting	Status settings
SPS	Single point status	Status information
TAG	Maintenance and operational tag	Hydro-specific information
TSG	Time setting group	Status settings
VSG	Visible string setting	Status settings
WYE	Phase to ground/neutral related measured values of a three-phase system	Measurment information

Glossary

C

CID:

configured IED description: The SCL file that describes the communication-related part of an instantiated IED within a project. The communication section contains the address of the IED. The substation section related to this IED may be present and, if so, contains project-specific assigned name values.

D

DAI:

instantiated data attribute: A single data attribute that has been assigned an initial value by the Modicon IEC 61850 Configuration Tool, thereby instantiating both the data attribute and its parent data object (DO).

data set:

A collection of data attributes and data objects that can be viewed and transmitted together. Although data sets are related to logical nodes, the member data attributes can originate in different logical nodes and logical devices. Data sets are used to define data collections that form the basis for reporting and logging using buffered report control blocks, unbuffered report control blocks, and GOOSE control blocks.

DDT:

derived data type: A derived data type is a set of elements with the same type (ARRAY) or with different types (structure).

DOI:

instantiated data object: A single data object with one or more data attributes (DAs) that have been assigned an initial value by the Modicon IEC 61850 Configuration Tool.

DRS:

(*dual-ring switch*) A ConneXium extended managed switch that has been configured to operate on an Ethernet network. Predefined configuration files are provided by Schneider Electric to downloaded to a DRS to support the special features of the main ring / sub-ring architecture.

E

EF:

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

A function does not have any information on the internal state. Several calls to the same function using the same input parameters will return the same output values. You will find information on the graphic form of the function call in the [*functional block (instance)*]. Unlike a call to a function block, function calls include only an output which is not named and whose name is identical to that of the function. In FBD, each call is indicated by a unique [number] via the graphic block. This number is managed automatically and cannot be modified.

Position and configure these functions in your program to execute your application.

You can also develop other functions using the SDKC development kit.

ERT:

encoder, receiver, transmitter: ERT is a wireless protocol used to automatically read and transmit data from utility meters over a short range so utility personnel need not physically enter a premises and manually take readings from each meter.

Ethernet:

A 10 Mb/s, 100 Mb/s, or 1 Gb/s, CSMA/CD, frame-based LAN that can run over copper twisted pair or fiber optic cable, or wireless. The IEEE standard 802.3 defines the rules for configuring a wired Ethernet network; the IEEE standard 802.11 defines the rules for configuring a wireless Ethernet network. Common forms include 10BASE-T, 100BASE-TX, and 1000BASE-T, which can utilize category 5e copper twisted pair cables and RJ45 modular connectors.

explicit messaging:

TCP/IP-based messaging for Modbus TCP . It is used for point-to-point, client/server messages that include both data (typically unscheduled information between a client and a server) and routing information.

F

FTP:

(*file transfer protocol*) A protocol that copies a file from one host to another over a TCP/IP-based network, such as the internet. FTP uses a client-server architecture as well as separate control and data connections between the client and server.

G

GOOSE:

generic object-oriented substation event: A control model defined by the IEC 61850 protocol that provides a mechanism for the transfer of event data relating to module status and value settings. GOOSE is a sub-set of the GSE model. As implemented in the Ethernet communication module, GOOSE is used to publish and subscribe to event data in the form of VLAN transmissions.

I

ICD:

IED capability description: A mandatory SCL file used to exchange data from the IED configurator to the system configurator. This file describes the functional and engineering capabilities of an IED type. It contains exactly one IED section for the IED type whose capabilities are described. The IED name shall be TEMPLATE.

IED:

intelligent electronic device: An IEC 61850 protocol compliant, microprocessor based industrial device incorporating one or more processors with the capability of receiving or sending data/controls from or to an external source (for example, electronic multifunction meters, digital relays, controllers).

IID:

instantiated IED description: An SCL file that contains the configuration data for a single IED in an application. This file must contain the instantiated device description, communication settings, and data type templates. The file may optionally contain a description of LNs bound to the substation object.

IPsec:

(*internet protocol security*) An open set of protocol standards that make IP communication sessions private and secure for traffic between modules using IPsec, developed by the internet engineering task force (IETF). The IPsec authentication and encryption algorithms require user-defined cryptographic keys that process each communications packet in an IPsec session.

L

LD:

logical device: A collection of a group of functions. Each function is defined as a logical node. A physical device can include one or more LDs. The IEC 61850 server includes a root LD named *System*.

LN:

logical node: A specific function of a logical device (LD), defined by a collection of data objects (DOs).

M

MB/TCP:

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

R

RSTP:

(*rapid spanning tree protocol*) A protocol that allows a network design to include spare (redundant) links to provide automatic backup paths if an active link stops working, without the need for loops or manual enabling/disabling of backup links.

S

SCD:

substation configuration description file: An SCL file containing a detailed description of an entire substation design. It must include sections describing the substation, communication, IED, and data type template. A single SCD file comprises multiple SSD and ICD files.

SCL:

system configuration description language: An XML based language that allows a formal description of power utility automation systems, the devices and the relation between them, and the IED configuration.

SNMP:

(*simple network management protocol*) Protocol used in network management systems to monitor network-attached devices for events. 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*.

Index

G

H

I

L

M

N

P

Q

R

S

T

U

V

W

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

QGH11908.08