M580

BMENUA0100 OPC UA Embedded Module

Installation and Configuration Guide

Original instructions

10/2019

www.schneider-electric.com

Schneider Electric

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

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

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

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

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

Table of Contents

Safety Information

Important Information

NOTICE

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

PLEASE NOTE

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

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

BEFORE YOU BEGIN

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

⚠ WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

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

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

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

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

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

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

START-UP AND TEST

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

⚠ WARNING

EQUIPMENT OPERATION HAZARD

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

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

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

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

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

Before energizing equipment:

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

OPERATION AND ADJUSTMENTS

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

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

About the Book

At a Glance

Document Scope

This manual describes the features and use of the M580 BMENUA0100 Ethernet communication module with embedded OPC UA server.

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

Validity Note

This document is valid for an M580 system when used with EcoStruxure™ Control Expert 14.1 or later.

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

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

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

Related Documents

Title of documentation	Reference number
Modicon M580 Standalone, System Planning Guide for Frequently Used Architectures	HRB62666 (English), HRB65318 (French), HRB65319 (German), HRB65320 (Italian), HRB65321 (Spanish), HRB65322 (Chinese)
Modicon M580 Standalone, System Planning Guide for Complex Topologies	NHA58892 (English), NHA58893 (French), NHA58894 (German), NHA58895 (Italian), NHA58896 (Spanish), NHA58897 (Chjnese)
Modicon M580 Hot Standby, System Planning Guide for Frequently Used Architectures	NHA58880 (English), NHA58881 (French), NHA58882 (German), NHA58883 (Italian), NHA58884 (Spanish), NHA58885 (Chinese)
Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	EIO0000002726 (English), EIO0000002727 (French), EIO0000002728 (German), EIO0000002730 (Italian), EIO0000002729 (Spanish), EIO0000002731 (Chinese)
M580 BMENOS0300, Network Option Switch, Installation and Configuration Guide	NHA89117 (English), NHA89119 (French), NHA89120 (German), NHA89121 (Italian), NHA89122 (Spanish), NHA89123 (Chinese)
Modicon M580, Hardware, Reference Manual	EIO0000001578 (English), EIO0000001579 (French), EIO0000001580 (German), EIO0000001582 (Italian), EIO0000001581 (Spanish), EIO0000001583 (Chinese)
Modicon M580, RIO Modules, Installation and Configuration Guide	EIO0000001584 (English), EIO0000001585 (French), EIO0000001586 (German), EIO0000001587 (Italian), EIO0000001588 (Spanish), EIO0000001589 (Chinese),
Modicon M580, Change Configuration on the Fly, User Guide	EIO0000001590 (English), EIO0000001591 (French), EIO0000001592 (German), EIO0000001594 (Italian), EIO0000001593 (Spanish), EIO0000001595 (Chinese)
Modicon X80, Discrete Input/Output Modules, User Manual	35012474 (English), 35012475 (German), 35012476 (French), 35012477 (Spanish), 35012478 (Italian), 35012479 (Chinese)
Modicon X80, BMXEHC0200 Counting Module, User Manual	35013355 (English), 35013356 (German), 35013357 (French), 35013358 (Spanish), 35013359 (Italian), 35013360 (Chinese)

Title of documentation	Reference number
Grounding and Electromagnetic Compatibility of PLC Systems, Basic Principles and Measures, User Manual	33002439 (English), 33002440 (French), 33002441 (German), 33003702 (Italian), 33002442 (Spanish), 33003703 (Chinese)
EcoStruxure™ Control Expert, Program Languages and Structure, Reference Manual	35006144 (English), 35006145 (French), 35006146 (German), 35013361 (Italian), 35006147 (Spanish), 35013362 (Chinese)
EcoStruxure™ Control Expert, System Bits and Words, Reference Manual	EIO0000002135 (English), EIO0000002136 (French), EIO0000002137 (German), EIO0000002138 (Italian), EIO0000002139 (Spanish), EIO0000002140 (Chinese)
EcoStruxure™ Control Expert, Operating Modes	33003101 (English), 33003102 (French), 33003103 (German), 33003104 (Spanish), 33003696 (Italian), 33003697 (Chinese)
EcoStruxure™ Control Expert, Installation Manual	35014792 (English), 35014793 (French), 35014794 (German), 35014795 (Spanish), 35014796 (Italian), 35012191 (Chinese)
Web Designer for FactoryCast User Manual	35016149 (English), 35016150 (French), 35016151 (German), 35016152 (Italian), 35016153 (Spanish), 35016154 (Chinese)
Modicon Controllers Platform Cyber Security, Reference Manual	EIO0000001999 (English), EIO0000002001 (French), EIO0000002000 (German), EIO0000002002 (Italian), EIO0000002003 (Spanish), EIO0000002004 (Chinese)

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

Chapter 1
BMENUA0100 Module Characteristics

Introduction

This chapter describes the BMENUA0100 Ethernet communications module with embedded OPC UA server.

What Is in This Chapter?

This chapter contains the following topics:

Module Features

Introduction

The Modicon BMENUA0100 OPC UA server module brings high performance OPC UA capabilities to Modicon M580 ePAC systems.

OPC UA is a modern, secure, open, reliable communications platform for industrial communications, designed to be flexible and scalable from resource constrained IoT sensors in the field through to enterprise grade servers hosted in the data center or the cloud. Beyond connecting and moving data around, OPC UA defines a comprehensive information model for publishing and managing meta-information and system context to simplify automation engineering and systems integration.

In realizing a communications standard for modern, connected industrial operations, OPC UA provides a common link between connected products in the field, automation and edge controllers, and enterprise applications and analytics. As such it is designed to be compatible with modern IT and security infrastructure such as firewalls, VPNs and proxies. OPC UA scales for both functional requirements and bandwidth.

Features

The BMENUA0100 module includes an OPC UA server and an embedded Ethernet switch. It is Included in the Control Expert **Hardware Catalog** in the **Communication** module group,

The BMENUA0100 brings the following features to the Modicon M580 platform:

General:

- Direct and optimized access to Control Expert data dictionary for simple mapping between Control Expert and OPC UA variables *(see page 45)*.
- Support for Hot Standby configurations via OPC UA Redundancy *(see page 49)*.
- Compatibility with M580 Safety systems as a type 1 non-interfering module as defined by TÜV Rheinland.
- Seamless Ethernet backplane communications.
- DHCP/FDR client for downloading stored (non-cybersecurity) configuration settings.
- NTP time server *(see page 104)* and client synchronization.
- Multiple diagnostic methods, including LEDs *(see page 112)*, DDT *(see page 115)*, OPC_UA variables and data items *(see page 124)*, Syslog *(see page 126)*, Modbus *(see page 129)*, SNMP *(see page 130)*, and secure web pages *(see page 131)* (see page 129).
- Firmware Upgrade via the EcoStruxure™ Maintenance Expert (see page 133) tool.
- Firmware integrity checking.
- Hardware secured storage.

Cybersecurity:

- Secure communications via HTTPS, OPC UA (optional), and IPSEC (optional).
- Module-level OPC UA security *(see page 90)* configurable via HTTPS.
- The ability to control inbound and outbound communication flow by enabling and disabling communication services *(see page 91)*.

- IPSEC *(see page 92)* based on a pre-shared key (PSK) for securing services such as SNMPv1, Modbus/TCP, Syslog, and NTPv4.
  NOTE: The BMENUA0100 supports main mode IPSEC, not aggressive mode. An IPSEC channel can be opened by either the BMENUA0100 server or a remote OPC UA client. On a PC client, IPSEC is supported and validated on Windows 7, 10 and Windows server 2016 systems.

Authentication management:

- Role based access control (RBAC) and user authentication *(see page 96)* for HTTPS and OPC UA clients.
- Certificates *(see page 94)* for OPC UA client application entities.

M580 communication module features include:

- DHCP/FDR client for downloading stored non-cybersecurity configuration settings.
- Direct and optimized access to Control Expert data dictionary, for mapping Control Expert variables to OPC UA server variables *(see page 45)*.
- Ethernet backplane port for Ethernet communication over the local main Ethernet rack.
- X Bus backplane port for 24 Vdc power and rack addressing.
- NTP time server *(see page 104)* and client synchronization.
- Compatibility with Hot Standby configurations via OPC UA Redundancy *(see page 49)*.
- Safety configuration as a type 1 non-interfering module as defined by TÜV Rheinland.
- Multiple diagnostic methods, including LEDs *(see page 112)*, DDT *(see page 115)*, OPC_UA variables and data items *(see page 124)*, Syslog *(see page 126)*, Modbus *(see page 129)*, SNMP *(see page 107)*, and secured web pages *(see page 128)*.
- Firmware Upgrade via the EcoStruxure™ Maintenance Expert *(see page 137)* tool.
- Hardware secured storage.
- Integrity checking of firmware before updates.

Module Description

Introduction

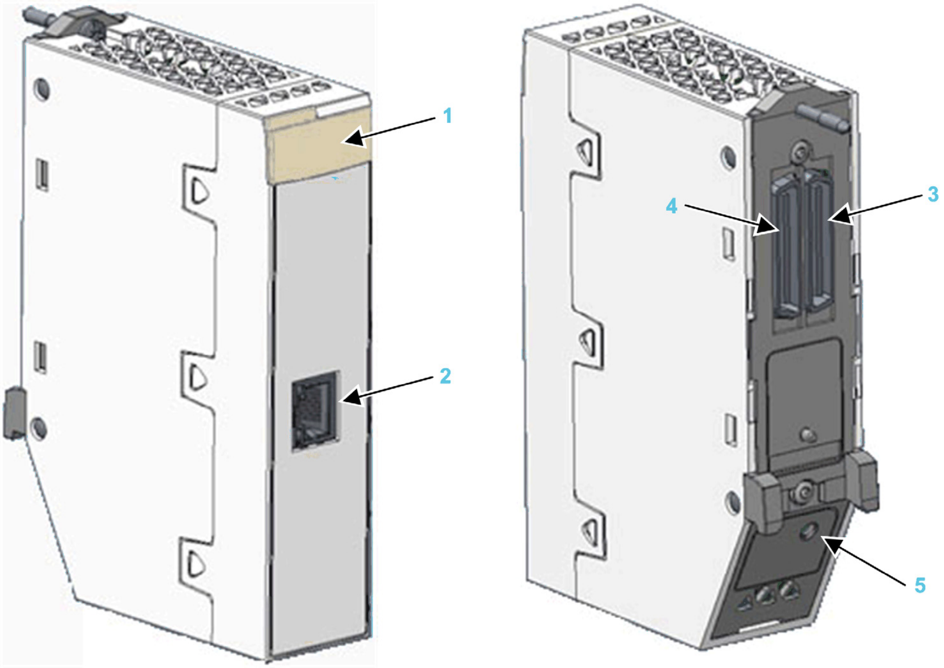
Schneider Electric offers two Ethernet communication modules with an embedded OPC UA server for communication with OPC UA clients, including SCADA:

- BMENUA0100 module for standard environments.
- BMENUA0100H module for harsh environments.

The module can be installed only in an Ethernet slot, on a main, local Ethernet rack. Refer to the topic *Supported BMENUA0100 Module Configurations (see page 58)* for a description of supported module placements, including the maximum number of BMENUA0100 modules that can be placed into a rack.

Physical Description

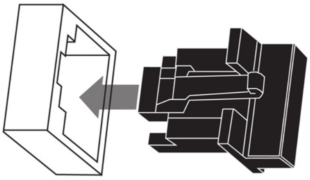
This figure shows the external features of the BMENUA0100 module:



1 LED array
2 Control port with Ethernet link and activity LEDs
3 Ethernet backplane port
4 X Bus backplane port
5 Cybersecurity operating mode rotary selector switch

Refer to the topic LED Diagnostics *(see page 112)* for information on reading module LEDs.

If the Ethernet control port is not enabled, use the stopper that ships with each module to help prevent debris from entering the control port:



External Ports

The BMENUA0100 module includes the following external ports:

Port	Description
Control port	The control port is the single port located on the front of the BMENUA0100 module. Its features include: ● When the control port is enabled, it is the exclusive interface for OPC UA communications. ● Operating speed up to 1 Gb/s. When operating at the speed of: ❍ 1 Gb/s, use only CAT6 copper shielded twisted four-pair cables. ❍ 10/100 Mb/s, use CAT5e or CAT6 copper shielded twisted four-pair cables. ● Dual IP stack that supports both IPv4 (32 bit) and IPv6 (128 bit) IP addressing: ❍ Both IPv4 and IPv6 are configured for the module. ❍ IPv6 configuration can be static or dynamic (via SLAAC). ❍ IPv4 default setting *(see page 101)* is auto-assigned based on the module MAC address, if an IP address is not configured. ● Secure access to the OPC UA server via both IPv4 and IPv6 protocols. ● HTTPS secure protocol (over IPv4) for firmware upgrade *(see page 137)* and cybersecurity configuration *(see page 82)*. ● NTPv4 secure protocol support. ● IPsec-provided security for non-secure services, including SNMPv1, Modbus TCP, and Syslog.

Port	Description
Ethernet backplane port	The BMENUA0100 Ethernet backplane port supports the IPv4 (32 bit) protocol. When the control port is disabled, the backplane port can support OPC UA communications. the backplane port includes the following features: ● Operating speed up to 100 Mb/s. ● Modbus TCP IPv4 Ethernet connectivity to the CPU: ❍ The Ethernet backplane port is the exclusive port for Modbus diagnostics. ● Exclusive port for non-cybersecurity configuration (IP, NTPv4, SNMPv1), by: ❍ Control Expert v14.1 and later ❍ FDR/DHCP server ● If the control port is disabled, the Ethernet backplane port provides secure access to the OPC UA server via the IPv4 protocol, and supports the following services: ❍ HTTPS secure protocol for firmware upgrade *(see page 137)* and cybersecurity configuration *(see page 82)*. ❍ NTPv4, SNMPv1 and Syslog.
X Bus backplane port	The BMENUA0100 module uses X Bus backplane communication to: ● Receive 24 Vdc power. ● Discover the rack and slot address of the BMENUA0100 module. **NOTE:** No other communication is performed via the X Bus backplane port of the BMENUA0100 module.

Rotary Switch

A three-position rotary switch is located on the back of the module. Use only the small, plastic screwdriver that ships with the module to change the switch position and configure a cybersecurity operating mode for the module.

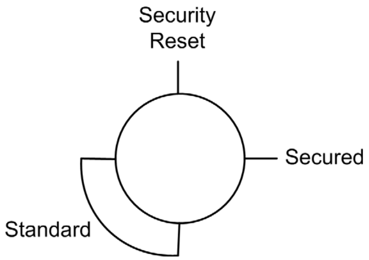
NOTICE

RISK OF UNINTENDED OPERATION

Use only the small, plastic screwdriver that ships with the module to change the rotary switch position. Using a metal screwdriver can damage the switch, rendering it inoperable.

Failure to follow these instructions can result in equipment damage.

The positions on the rotary switch are:



The settings are:

- Secured mode
- Standard mode
- Security Reset

NOTE:

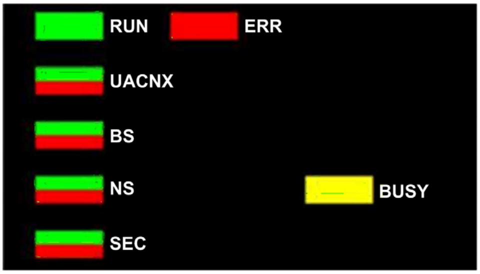
- The rotary switch is not accessible when the module is placed on the rack.
- In a Hot Standby system, verify that the BMENUA0100 module rotary switch positions – in both the primary and the standby local main racks – are the same. The system does not automatically perform this check for you.

Refer to the description of cybersecurity operating modes *(see page 26)* for information on each rotary switch position setting.

Module LEDs

LED Display

A 7-LED display panel is located on the front of the BMENUA0100 module:



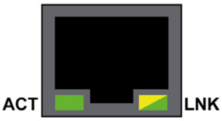
The LEDs display information about the module as follows:

LED	Describes the state of the module:
RUN	Operating condition.
ERR	Detected errors.
UACNX	OPC UA connections.
BS	Backplane port.
NS	Control port.
SEC	Cybersecurity condition.
BUSY	Data dictionary status

Refer to the LED Diagnostics topic *(see page 112)* for information on how to use these LEDs to diagnose the state of the BMENUA0100 module.

Control Port LEDs

The control port, on the front of the module, presents two LEDs describing the state of the Ethernet link over the port:



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

Refer to the LED Diagnostics topic *(see page 114)* for information on how to use the control port LEDs to diagnose the state of the BMENUA0100 module control port.

Chapter 2
Standards and Certifications

Overview

This chapter describes the standards and certifications that apply to the BMENUA0100 Ethernet communications module with embedded OPC UA server.

What Is in This Chapter?

This chapter contains the following topics:

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*

BMENUA0100 Module Standards

Agency Requirements

In addition to the standards and certifications *(see page 22)* that apply to Schneider Electric M580 modules, the BMENUA0100 OPC UA embedded Ethernet communication module conforms to the following agency standards:

Marking	Requirement
OPC Unified Architecture	OPC UA V1.03: OPC Unified Architecture machine to machine communication protocol.
CE	CE: Manufacturer’s declaration of conformity. The CE marking on the product and/or their packaging means that Schneider Electric holds the reference technical files available to European Union competent authorities according EN 61131-2.
CSA	CSA: Certificate of Compliance for Process Control Equipment (for Hazardous Locations) and Programmable Controller; CSA 22-2 N° 213 (Hazardous Location); CSA 22-2 N° 142 (Canadian Standards Association); ANSI/ISA 12.12.01, FM3611.
UL	UL: Underwriters Laboratories. UL 61010-2-201 (Certification for Industrial Control Equipment); UL 508.
✓	RCM ACE: Australian Communication Authority/Australia.
DNV	DNV: Norway Certification for Maritime Industry across vessel types and offshore structures.
Lloyd's Register	Lloyd’s Register: Marine and offshore application in Category ENV1, ENV2 as defined in LR Type Approval Systems Test Specification No 1 1996.
	RINA certification. Mutual Marine Insurance Association across vessel types and offshore structures.

Marking	Requirement
	Bureau Veritas Marine certification in accordance with the type described in this certificate and Bureau Veritas Rules for the Classification of Steel Ships.
ABS	Certificate of Design Assessment for products intended to be installed on an ABS classed vessel, MODU of the ABS rules or specifications.
	GL: German rules for classification of all types of vessels, our statutory interpretations, offshore standards.
РСТ	EAC Certification, certifies quality of supplied goods and their conformity with norms and standards Russia Federation.
Ex	IECEx Certificate of conformity. International Electromechanical Commission. IEC Certification Scheme for Explosive Atmospheres.
⚛	K3/C3 – K3/C2 nuclear certification; Cx certification validates overall quality level of the PAC system, application, and with respect to our processes (to provide traceability, development process and mastering, maturity in our overall quality management…); K3 deals with climatic or mechanical constraints, and consists of full environmental tests under specific mechanical constraints.

Chapter 3
BMENUA0100 Functional Description

Introduction

This chapter describes the supported functions of the BMENUA0100 Ethernet communications module with embedded OPC UA server.

What Is in This Chapter?

This chapter contains the following sections:

Section 3.1
Cybersecurity Operating Mode Settings

Cybersecurity Operating Modes

Introduction

The BMENUA0100 module can be configured to operate in either Secured or Standard mode. The 3-position rotary selector switch on the back of the module determines the operating mode.

The three rotary switch positions are:

- Secured mode
- Standard mode
- Security Reset

NOTE:

- The module’s default, out-of-the-box configuration, is the Secured mode.
- You can view the current position of the rotary switch in the Home page *(see page 87)* of the module web pages.

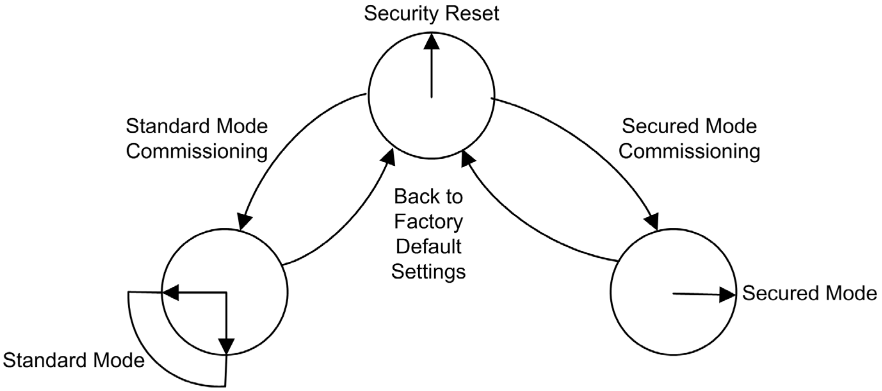
Because the rotary selector switch is not accessible while the module is on the rack, the switch position can be changed only when the module is powered off and removed from the rack. After a new switch position is selected, the module can be re-inserted into the rack and power applied.

NOTE: Use only the small, plastic screwdriver that ships with the module *(see page 18)* to change the switch position and configure a cybersecurity operating mode.

Changing Operating Mode

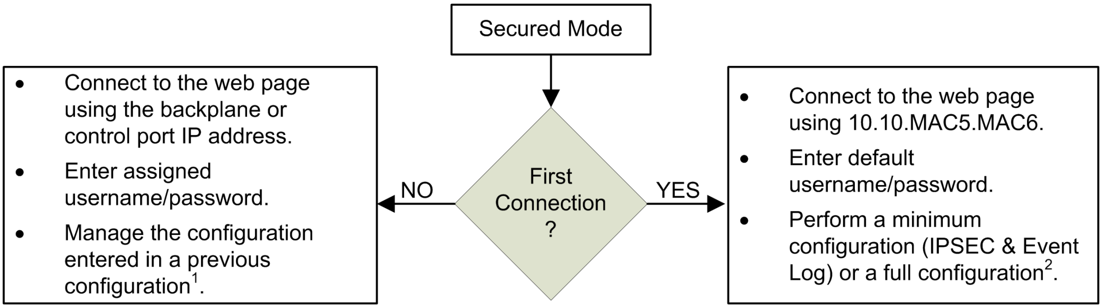
Each time you switch the cybersecurity operating mode from Secured mode to Standard mode, or from Standard mode to Secured mode, perform a Security Reset operation *(see page 78)* before configuring the new mode.

The position of the rotary switch determines the operating state of the module, as follows:


Security Reset
Standard Mode Commissioning
Secured Mode Commissioning
Back to Factory Default Settings
Secured Mode
Standard Mode

A new (out-of-the-box factory default) module, or a module for which a Security Reset has been performed, can be commissioned for either Standard mode *(see page 77)* or Secured mode *(see page 76)* operations.

The process for configuring the module for Secured mode operations varies, depending on whether you are connecting to the module configuration settings for the first time after performing a security reset:


Secured Mode
First Connection ?
NO
YES
• Connect to the web page using the backplane or control port IP address.
• Enter assigned username/password.
• Manage the configuration entered in a previous configuration[1].
• Connect to the web page using 10.10.MAC5.MAC6.
• Enter default username/password.
• Perform a minimum configuration (IPSEC & Event Log) or a full configuration[2].

1 For information about managing the configuration, refer to the configuration chapter. *(see page 81)*

2 For information on performing a configuration on first connection, refer to the topic Secured Mode Commissioning *(see page 76)*.

Secured Mode

When operating in Secured mode, the module will not engage in process communications – over either the control port or the backplane port – until valid cybersecurity settings have been configured. After Secured mode has been configured, you can configure cybersecurity settings using the module web pages *(see page 82)*, which can be accessed via the HTTPS protocol over either the backplane or control ports. In Secured mode, the module supports the level of cybersecurity that is specified in the cybersecurity configuration. Only after cybersecurity settings have been configured, can IP address, NTP client, and SNMP agent settings *(see page 100)* be configured using the Control Expert configuration software.

Standard Mode

When operating in Standard mode, module communications can begin immediately. Cybersecurity settings are not required and cannot be configured. Only the IP address and other settings available in Control Expert can be configured.

Security Reset

The **Security Reset** command restores the out-of-the-box factory default configuration settings. It deletes any existing cybersecurity configuration, white lists, certificates, and role based access control settings. While the process of restoring factory default settings is ongoing, the RUN LED continues blinking green. After completion of process, the RUN LED turns to solid green, and all services are disabled. To complete the security reset, either cycle power (off, then on) to the BMENUA0100 module, or physically remove the module from the rack (which turns off power) then re-insert the module into the rack (which turns power back on).

This setting can be made using either the rotary switch or the web pages (when operating in Secured mode):

- If set via rotary switch: the module ceases to be functional until the module is removed from the rack, the rotary switch is re-set to either the Secured or Standard position, and the module is again placed on the rack. The necessary configuration(s) will need to be applied.
- If set via the web pages: upon completion of the process cycle power (off / on) to – or hot swap – the module in Standard or in Secured mode. Both the cybersecurity and IP address settings need to be configured.

NOTE: After a Security Reset of the BMENUA0100 module, the following conditions apply to the module:

- No device certificates are preserved.
- All services are disabled except for HTTPS, which is used to create the cybersecurity configuration via the control port.
- Factory default settings are applied, including:
  - Username / Password default settings *(see page 29)*.
  - IP address default setting of 10.10.MAC5.MAC6 *(see page 101)*.

Default Username / Password Combination

The default username / password combination depends on the cybersecurity operating mode setting:

- Secured mode: admin / password
- Standard mode: installer / Inst@ller1

Functions Supported by Secured and Standard Operating Modes

The following functions are supported by the BMENUA0100 module in Secured and Standard modes:

Security Mode	Standard mode			Secured mode		
Control port	**Disable**	**Enable**		**Disable**	**Enable**	
Ethernet port	**Backplane**	**Backplane**	**Control port**	**Backplane**	**Backplane**	**Control port**
OPC UA Comm	Yes	No	Yes	Yes	No	Yes
Security Settings (3)	None	–	None	None, Sign, Sign&Encrypt (default value)	–	None, Sign, Sign&Encrypt (default value)
User authentication	No authentication (anonymous)	–	No authentication (anonymous)	Operator, Engineer, No authentication (anonymous)	–	Operator, Engineer, No authentication (anonymous)
SNMP V1	Yes (1)	Yes (1)	Yes (1)	Yes (1)	Yes (1)	Yes (1)
NTP V4	Client only (1)	Client (1), Server	Yes, Client only (1)	Client only (*)	Client (1), Server	Yes, Client only (1)
Event Log	No	No	No	Yes	Yes	Yes
IPSec	No	No	No	No	No	Yes for Modbus, SNMP V1, NTP V4 (2) and Syslog (IPSec enabled by default)
Web CS Config change (HTTPS)	No	No	No	Yes	Yes	Yes

1. Configurable with Control Expert.
2. NTP V4 can be configured to be transported outside IPSec tunnel.
3. For both Standard and Secured cybersecurity operating modes, if Security Settings is set to *None*, there is no user authentication (i.e. the **User Identifier token types** OPC UA setting *(see page 93)* is set to *Anonymous*.)
4. To provide Control Expert with online access to the CPU or Device Network, configure the PC (on which Control Expert is installed) with an IP address on the same subnet as the BMENUA0100 module control port, and use the BMENUA0100 module control port IP address as the PC gateway IP address. In this case, no IP address of the PC can be on the same subnet as the BMENUA0100 module backplane port.

Security Mode	Standard mode			Secured mode		
Control port	Disable	Enable		Disable	Enable	
Ethernet port	Backplane	Backplane	Control port	Backplane	Backplane	Control port
User authentication	–	–	–	Admin	Admin	Admin
Network Services Comm server Enable/Disable	If supported, always enabled (refer above)	If supported, always enabled (refer above)	If supported, always enabled (refer above)	All services are configurable (disabled by default)	All services are configurable (disabled by default)	All services are configurable (disabled by default)
Web Diagnostic (Home and Diagnostic pages only)	Yes	Yes	Yes	Yes	Yes	Yes
User authentication	Installer (default credentials)	Installer (default credentials)	Installer (default credentials)	Admin, Operator, Engineer, Installer	Admin, Operator, Engineer, Installer	Admin, Operator, Engineer, Installer
Firmware upgrade (HTTPS)	Yes	Yes	Yes	Yes	Yes	Yes, if HTTPS enabled
User authentication	Installer (default credentials)	Installer (default credentials)	Installer (default credentials)	Installer	Installer	Installer
Filtering: CPU to CPU Data Flows (Modbus)	–	–	Forward of Modbus data flow from CPU (always enabled)	–	–	Forward of Modbus data flow from CPU (disabled by default)

1. Configurable with Control Expert.
2. NTP V4 can be configured to be transported outside IPSec tunnel.
3. For both Standard and Secured cybersecurity operating modes, if Security Settings is set to *None*, there is no user authentication (i.e. the **User Identifier token types** OPC UA setting *(see page 93)* is set to *Anonymous*.)
4. To provide Control Expert with online access to the CPU or Device Network, configure the PC (on which Control Expert is installed) with an IP address on the same subnet as the BMENUA0100 module control port, and use the BMENUA0100 module control port IP address as the PC gateway IP address. In this case, no IP address of the PC can be on the same subnet as the BMENUA0100 module backplane port.

Security Mode	Standard mode			Secured mode		
Control port	**Disable**	**Enable**		**Disable**	**Enable**	
Ethernet port	**Backplane**	**Backplane**	**Control port**	**Backplane**	**Backplane**	**Control port**
Filtering: Control Expert Data Flows to CPU only (FTP, EIP, Explicit, Modbus, Ping)[4]	–	–	Forward of Control Expert data flows from Control Network to CPU only (always enabled)[4]	–	–	Forward of Control Expert data flows from Control Network to CPU only (disabled by default)[4]
Filtering: Control Expert Data Flows to Device Network (including CPU) (FTP, EIP, Explicit, Modbus, Ping)[4]	–	–	Forward of Control Expert data flows from Control Network to Device Network (always enabled)	–	–	Forward of Control Expert data flows from Control Network to Device Network (disabled by default)

1. Configurable with Control Expert.
2. NTP V4 can be configured to be transported outside IPSec tunnel.
3. For both Standard and Secured cybersecurity operating modes, if Security Settings is set to *None*, there is no user authentication (i.e. the **User Identifier token types** OPC UA setting *(see page 93)* is set to *Anonymous*.)
4. To provide Control Expert with online access to the CPU or Device Network, configure the PC (on which Control Expert is installed) with an IP address on the same subnet as the BMENUA0100 module control port, and use the BMENUA0100 module control port IP address as the PC gateway IP address. In this case, no IP address of the PC can be on the same subnet as the BMENUA0100 module backplane port.

NOTE: In addition to the functions listed above, both the backplane port and the control port (if enabled) support the following features in both Standard mode and Secured mode:

- Firmware signing
- Firmware encryption
- Secure Boot
- Secure Storage

Section 3.2
OPC UA Services

Introduction

This section describes the services supported by the OPC UA server embedded in the BMENUA0100 module.

What Is in This Section?

This section contains the following topics:

OPC UA Server

Introduction

The primary purpose of the BMENUA0100 Ethernet communication module is to provide an OPC UA communication channel over Ethernet between M580 CPUs and OPC UA clients. The data of the M580 CPU is mapped to variables in the BMENUA0100 module, and made available to OPC UA clients via a high performance OPC UA server communication stack embedded in the BMENUA0100 module. OPC UA clients connect to the embedded OPC UA server stack using IP address of the BMENUA0100 module's control port or backplane port, thereby establishing a client server connection. The BMENUA0100 module is able to handle a maximum of three (3) simultaneous OPC UA client connections.

NOTE: The terms of each connection between an OPC UA client and the OPC UA server embedded in the BMENUA0100 module are determined by the client, which sets the attributes of the connection between the client and server.

The OPC UA server stack embedded in the BMENUA0100 module consists of functionalities defined by the following terms:

- Profile: a full-featured definition of functionality that comprises other profiles, facets, conformance groups, and conformance units.
- Facet: defines a partial functionality.
- Conformance Group: a collection of conformance units.
- Conformance Unit: a specific service, for example, read, write, and so forth.

BMENUA0100 Supported Profile

The BMENUA0100 module supports the **Embedded 2017 UA Server Profile**. As stated in the OPC Foundation web site, this profile: *is a FullFeatured Profile that is intended for devices with more than 50 MBs of memory and a more powerful processor. This Profile builds upon the Micro Embedded Device Server Profile. The most important additions are: support for security via the Security Policies and support for the Standard DataChange Subscription Server Facet. This Profile also requires that Servers expose all OPC-UA types that are used by the Server including their components and their super-types.*" For more information, refer tot he OPC Foundation website at: *http://opcfoundation.org/UA-Profile/Server/EmbeddedUA2017.*

BMENUA0100 Supported Facets

The BMENUA0100 module supports the following Facets:

- **Server Category → Facets → Core Characteristics**:
  - **Core 2017 Server Facet** (*http://opcfoundation.org/UA-Profile/Server/Core2017Facet*)
- **Server Category → Facets → Data Access**:
  - **ComplexType 2017 Server Facet** (*http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017*)
  - **Data Access Server Facet** (*http://opcfoundation.org/UA-Profile/Server/DataAccess*)
  - **Embedded DataChange Subscription Server Facet** (*http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription*)

- Server Category → Facets → Generic Features:
  - Method Server Facet (*http://opcfoundation.org/UA-Profile/Server/Methods*)
- Security Category → Facets → Security Policy:
  - Basic128RSA15 (*http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15*)
  - Basic256 (*http://opcfoundation.org/UA/SecurityPolicy#Basic256*)
  - Basic256Sha256 (*http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256*)
- Transport Category → Facets → Client-Server:
  - UA-TCP- UA-SC UA-Binary (*http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary*)

The following topics discuss the services, related to the above-referenced facets, that are supported by the BMENUA0100 module.

BMENUA0100 OPC UA Server Stack Services

Supported OPC UA Services

The BMENUA0100 module OPC UA server stack supports the following service sets and services:

Service Set	Services
Attribute	● Read ● Write
Discovery	● FindServers ● GetEndpoints
Method	● Call
MonitoredItem	● CreateMonitoredItems ● ModifyMonitoredItems ● DeleteMonitoredItems ● SetMonitoringMode
SecureChannel	● OpenSecureChannel ● CloseSecurechannel
Session	● CreateSession ● ActivateSession ● CloseSession
Subscription	● CreateSubscription ● ModifySubscription ● DeleteSubscription ● SetPublishingMode ● SetMonitoringMode ● Publish ● Republish
View	● Browse ● BrowseNext ● TranslateBrowsePathToNodeIds ● RegisterNodes ● UnregisterNodes

NOTE: For a description of these service sets and services, refer to the document *OPC Unified Architecture Specification Part 4: Services (Release 1.04)*.

BMENUA0100 OPC UA Server Stack Data Access Services

Supported Data Access Services

Data access by the BMENUA0100 module embedded OPC UA server stack is enabled by its support of the following facets and related services:

- Data Access Server Facet
- ComplexType 2017 Server Facet
- Core 2017 Server Facet

NOTE: In the following facet descriptions, italicized text indicates a direct quote of the OPC Foundation source material. Click on the links below and use the *OPC Foundation Unified Architecture Profile Reporting Visualization Tool* to access a description of each facet.

Core 2017 Server Facet

The Core 2017 Server Facet *defines the core functionality required for any UA Server implementation. The core functionality includes the ability to discover endpoints, establish secure communication channels, create Sessions, browse the AddressSpace and read and/or write to Attributes of Nodes. The key requirements are: support for a single Session, support for the Server and Server Capabilities Object, all mandatory Attributes for Nodes in the AddressSpace, and authentication with UserName and Password. For broad applicability, it is recommended that Servers support multiple transport and security Profiles*. For a full description of this facet, refer to *http://opcfoundation.org/UA-Profile/Server/Core2017Facet*.

The BMENUA0100 module embedded OPC UA server stack supports the following conformance units in the Core 2017 Server Facet:

- View Service Set, includes the following groups and services:
  - View Basic: includes the Browse and the BrowseNext services.
  - View TranslateBrowsePath: includes the TranslateBrowsePathsToNodeIds service.
  - View Register Nodes: includes the RegisterNodes and UnregisterNodes services as a way to optimize access to repeatedly used Nodes in the Server's OPC UA AddressSpace.
- Attribute Service Set, includes the following groups and services:
  - Attribute read: includes the Read service, which supports reading one or more attributes of one or more Nodes, including support of the IndexRange parameter to read a single element or a range of elements when the Attribute value is an array.
  - Attribute Write values: includes the Write Value service, which supports writing one or more values to one or more Attributes of one or more Nodes.
  - Attribute Write Index: includes the Write Index service, which supports the IndexRange for writing to a single element or a range of elements when the Attribute value is an array and partial updates is allowed for this array.

Data Access Server Facet

The Data Access Server Facet *specifies the support for an Information Model used to provide industrial automation data. This model defines standard structures for analog and discrete data items and their quality of service. This Facet extends the Core Server Facet which includes support of the basic AddressSpace behaviour*. For a full description of this facet, refer to *http://opcfoundation.org/UA-Profile/Server/DataAccess*.

ComplexType 2017 Server Facet

The ComplexType 2017 Server Facet *extends the Core Server Facet to include Variables with structured data, i.e. data that are composed of multiple elements such as a structure and where the individual elements are exposed as component variables. Support of this Facet requires the implementation of structured DataTypes and Variables that make use of these DataTypes. The Read, Write and Subscriptions service set shall support the encoding and decoding of these structured DataTypes. As an option the Server can also support alternate encodings, such as an XML encoding when the binary protocol is currently used and vice-versa*. For a full description of this facet, refer to *http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017*.

BMENUA0100 OPC UA Server Stack Discovery and Security Services

Introduction

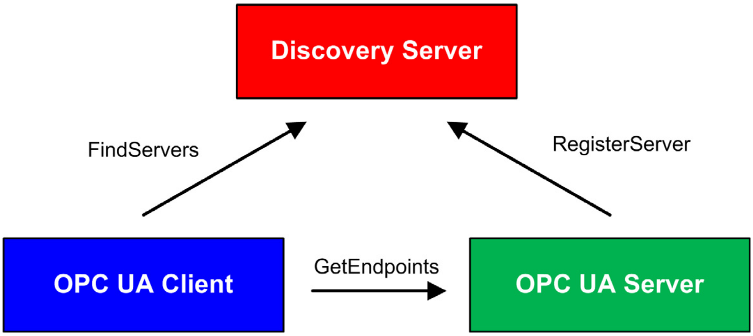
The BMENUA0100 module embedded OPC UA server stack supports both discovery and security services.

To connect to the OPC UA server in the BMENUA0100 module, an OPC UA client requires information describing the server, including its network address, protocol, and security settings. OPC UA defines a set of discovery features a client can use to obtain this information.

The information needed to establish a connection between an OPC UA client and an OPC UA server is stored in an endpoint. An OPC UA server can possess several endpoints, each containing:

- Endpoint URL (network address and protocol), for example:
  - For IPv4: opc.tcp://172.21.2.30:4840, where:
    - opc.tcp = protocols
    - 172.21.2.30 = IPv4 address
    - 4840 = opcua-tcp port number configured in Control Expert
  - For IPv6: opc.tcp://[2a01:cb05:431:f00:200:aff:fe02:a0a]:50000, where:
    - opc.tcp = protocols
    - [2a01:cb05:431:f00:200:aff:fe02:a0a] = IPv6 address
    - 50000 = opcua-tcp port number configured in Control Expert
- Security Policy (including a set of security algorithms and key length)
- Message Security Mode (security level for exchanged messages)
- User Token Type (server supported types of user authentication)

One or more OPC UA servers can exist. In the case of multiple servers, a discovery server can be used to provide information regarding each server. Individual servers can register with the discovery server. Clients can request a list of some or all of the available servers from the discovery server and use the GetEndpoints service to acquire connection information from an individual server.



The BMENUA0100 module supports several discovery and security services, including:

- Discovery Service Set
- SecureChannel Service Set
- Session Service Set

The decision to enable or disable services depends on the cybersecurity policy you decide to implement for the server.

Discovery Service Set

The BMENUA0100 OPC UA server stack supports the Discovery Service Set, which is incorporated in the Core 2017 Server Facet *(see page 36)*. As implemented in the BMENUA0100 module, the supported services include:

- FindServers: As implemented in the BMENUA0100 module OPC UA server stack, this service finds all servers only on the local OPC UA server.
- GetEndpoints: Returns the Endpoints supported by a server and all of the configuration information required to establish a SecureChannel and a Session. Can provide a filtered Endpoints return list, based on profiles.

SecureChannel Service Set

The BMENUA0100 OPC UA server stack supports the SecureChannel Service Set, which includes the following services:

- OpenSecureChannel: Opens or renews a SecureChannel that provides confidentiality and integrity for the exchange of messages during a session. This Service requires the OPC UA server stack to apply the various security algorithms to the messages as they are sent and received.
- CloseSecureChannel: Terminates a SecureChannel.

Session Service Set

The BMENUA0100 OPC UA server stack supports the Session Service Set, which is incorporated in the Core 2017 Server Facet *(see page 36)*. As implemented in the BMENUA0100 module, the supported services include:

- CreateSession: After creating a SecureChannel with the OpenSecureChannel service, a client uses this service to create a session. The server returns two values which uniquely identify the session:
  - A sessionId, which is used to identify the session in the audit logs and in the server's AddressSpace.
  - An authenticationToken, which is used to associate an incoming request with a session.
- ActivateSession: Used by the client to specify the identity of the user associated with the session. It cannot be used to change the session user.
- CloseSession: Terminates a session.

NOTE: For the CreateSession and ActivateSession services, if the SecurityMode = None then:

1. The Application Certificate and Nonce are optional.
2. The signatures are null/empty.

BMENUA0100 OPC UA Server Stack Publish and Subscribe Services

Subscriptions

Instead of permanently reading information by polling, the OPC UA protocol includes the Subscription function. This function enables the OPC UA high performance stack embedded in the BMENUA0100 module to provide publish/subscribe services, which are used when the module connects to remote devices.

An OPC UA client can subscribe to one or more selected nodes and let the server monitor these items. Upon the occurrence of a change event, for example a change in value, the server notifies the client of the change. This mechanism significantly reduces the quantity of data that is transferred. This reduces bandwidth consumption and is the recommended mechanism for reading information from an OPC UA server.

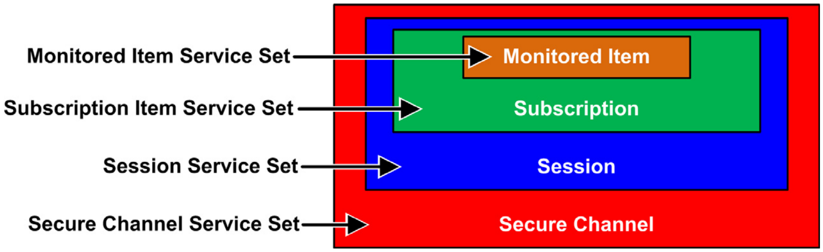
An OPC UA client can subscribe to the multiple types of information that an OPC UA server provides. The subscription groups together these varying types of data, called Monitored Items, to form a single collection of data called a Notification.

A subscription must:

- Consist of at least one Monitored Item.
- Be created within the context of a Session, which is created within the context of a Secure Channel.

NOTE: The subscription can be transferred to another session.

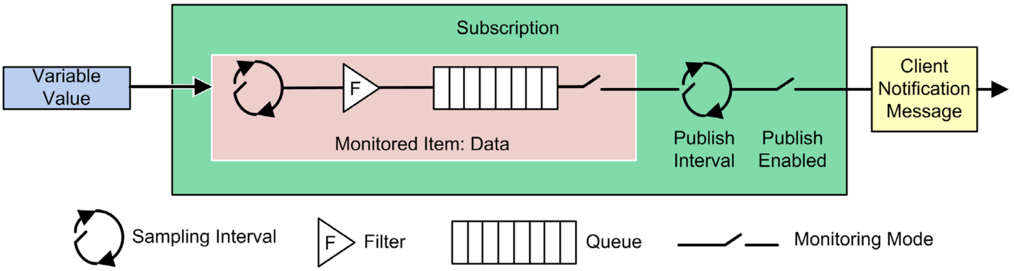
The service sets involved in a client subscription are described below:


Monitored Item Service Set
Subscription Item Service Set
Session Service Set
Secure Channel Service Set
Monitored Item
Subscription
Session
Secure Channel

Change Events

A client can subscribe to a data change event, which is triggered by a change to the value attribute of a variable, as a Monitored Item.

The configurable subscription settings, their sequence and roles, are described below:



The following three settings determine how Monitored Items are added to a subscription:

- Sampling Interval: the sampling time interval set for each Monitored Item in the subscription. This is the frequency by which the server checks the data source for changes. For a single Variable item, the Sampling Interval can be smaller (i.e. faster) than the period between notifications to the client. In this case, the OPC UA Server may queue the samples and publish the complete queue. In extreme cases, the server will revise (i.e. slow) the Sampling Interval so that the data source will not experience excessive queuing load that may be caused by the sampling itself.
  NOTE: If OPC UA queuing of data samples is supported, the queue size (i.e., the maximum number of values which can be queued) can be configured for each monitored item. When the data is delivered (published) to the client, the queue is emptied. In case of a queue overflow, the oldest data is discarded and replaced by new data.
- Filter: a collection of several criteria used to identify which data changes or events are reported, and which should are blocked.
- Monitoring Mode: used to enable or disable data sampling and reporting.

The following two settings apply to the Subscription itself:

- Publishing Interval: The period after which notifications collected in the queues are delivered to the client in a Notification Message (Publish Response). The OPC UA Client must confirm that the OPC UA server has received enough Publish Tokens (Publish Requests), so that whenever the Publish Interval elapsed and a notification is ready to send, the server uses such a token and sends the data within a Publish Response. In case that there is nothing to report (e.g. no values have changed) the server will send a KeepAlive notification to the Client, which is an empty Publish, to indicate that the server is still alive.
- Publish Enabled: Enables and disables the sending of the Notification Message.

Embedded DataChange Subscription Server Facet

The Embedded DataChange Subscription Server Facet *specifies the minimum level of support for data change notifications within subscriptions. It includes limits which minimize memory and processing overhead required to implement the Facet. This Facet includes functionality to create, modify and delete Subscriptions and to add, modify and remove Monitored Items. As a minimum for each Session, Servers shall support one Subscription with up to two items. In addition, support for two parallel Publish requests is required. This Facet is geared for a platform such as the one provided by the Micro Embedded Device Server Profile in which memory is limited and needs to be managed.* For a full description of this facet, refer to *http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription*.

This facet supports the following services:

- Monitored Item Service Set
- Subscription Service Set

Monitored Item Service Set

The Monitored Item Service Set supports the following services:

- CreateMonitoredItems: An asynchronous call used to create and add one or more MonitoredItems to a subscription.
- ModifyMonitoredItems: an asynchronous call to modify monitored items. This service is used to modify MonitoredItems of a subscription. Changes to the MonitoredItem settings shall be applied immediately by the server. They take effect as soon as practical.
- DeleteMonitoredItems: an asynchronous call to delete monitored items. This service is used to remove one or more MonitoredItems of a subscription. When a MonitoredItem is deleted, its triggered item links are also deleted.
- SetMonitoringMode: an asynchronous call to set the monitoring mode for a list of MonitoredItems. This service is used to set the monitoring mode for one or more MonitoredItems of a subscription. Setting the mode to DISABLED causes all queued notifications to be deleted.

Subscription Service Set

The Subscription Service Set supports the following services:

- CreateSubscription: an asynchronous call to create a subscription.
- ModifySubscription: an asynchronous call to modify a subscription. The server immediately applies changes to the subscription, and changes take effect as soon as practical.
- DeleteSubscription: an asynchronous call to delete one or more subscriptions belonging to the client session. Successful completion of this service deletes all Monitored Items associated with the subscription.
- Publish: This Service is used for two purposes: to acknowledge the receipt of NotificationMessages for one or more subscriptions, and to request the server to return a NotificationMessage or a keep-alive message.
- Republish: an asynchronous republish call to get lost notifications. This service requests the subscription to republish a NotificationMessage from its retransmission queue. If the server does not have the requested message in its retransmission queue, it returns an error response.
- SetPublishingMode: an asynchronous call to enable sending of Notifications on one or more subscriptions.

BMENUA0100 OPC UA Server Stack Transport Services

Support for the UA-TCP UA-SC UA-Binary Facet

The BMENUA0100 module supports the UA-TCP UA-SC UA-Binary transport facet. (For additional information, refer to the online description at *http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary*.)

This transport facet defines a combination of network protocols, security protocols, and message encoding that is optimized for low resource consumption and high performance. It combines the simple TCP-based network protocol UA-TCP 1.0 with the binary security protocol UA-SecureConversation 1.0 and the binary message encoding UA-Binary 1.0.

Data that passes between an OPC UA client and the BMENUA0100 module embedded OPC UA server uses the TCP protocol, and is binary coded in accordance with the OPC UA Binary File Format.

NOTE: The OPC UA Binary File Format replaces the XML UA-Nodeset Schema from the OPC Foundation. It improves performance and memory consumption. It does not require an XML parser.

Section 3.3
Discovering PAC Variables

Mapping Control Expert PAC Variables to OPC UA Data Logic Variables

Introduction

The OPC UA embedded server in the BMENUA0100 module uses Unified Messaging Application Services (UMAS) data dictionary requests to browse and discover M580 PAC application variables. You will need to activate the data dictionary in the Control Expert project settings.

NOTE: The BMENUA0100 module can support a maximum data dictionary size of greater than 100000 variables.

All collected variables are translated from the Control Expert data logic model view to the OPC UA data logic model view using the appropriate OPC UA stack services. An OPC UA client connected to the BMENUA0100 module–over its control port, or over its backplane port via the CPU or a BMENOC0301/11 communication module–can retrieve this collection of data using the services of the Data Access Server Facet *(see page 37)* supported by the Embedded 2017 UA Server Profile *(see page 33)*.

Preloading the Data Dictionary to Avoid Communication Interruptions

An online application change made with Control Expert temporarily breaks OPC UA server/client communication while the server acquires an updated data dictionary. This interruption is caused by inconsistent CPU data mapping while the data dictionary is updated. During the period of communication loss, the status of the monitored nodes goes to BAD. To avoid this disruption of operations, a synchronization mechanism can be set up between the BMENUA0100 module and the Control Expert configuration software, based on a preload of the updated data dictionary.

This feature is enabled in Control Expert in the **Tools → Project Settings...** window, in the **General → PLC embedded data** area, using the **Preload on build changes** and **Effective Build changes time-out** settings *(see EcoStruxure™ Control Expert, Operating Modes)*. Refer to the Control Expert online help for these topics for information on how to configure this feature.

Activating the Data Dictionary

To activate the data dictionary in Control Expert:

Step	Action
1	In Control Expert, with the project open, select **Tools → Project Settings**.
2	In the **Project Settings** window, navigate to **General → PLC embedded data**, then select **Data dictionary**. **NOTE:** If the EcoStruxure™ Control Expert project includes a BMENUA0100 module and this setting is not selected, a detected error is generated during the application build.

Variable Data Type Conversion

The BMENUA0100 module can discover and convert to OPC UA data types the following basic variable types supported by the Control Expert data logic model:

Control Expert Elementary Data Type	OPC UA Data Type
BOOL	Boolean
EBOOL	Boolean
INT	Int16
DINT	Int32
UINT	UInt16
UDINT	UInt32
REAL	Float
BYTE	Byte
WORD	UInt16
DWORD	UInt32
DATE*	UInt32
TIME*	UInt32
TOD*	UInt32
DT*	Double
STRING	Byte array
* Refer to following table describing date-related data type conversion.	

For Control Expert data of types DATE, TIME, TOD, DT, the corresponding OPC UA data types are as follows:

Control Expert Elementary Data Type	Example value displayed in Control Expert	OPC UA Data Type	Corresponding value in OPC UA type
DATE	D#2017-05-17	UInt32	0x20170517
TIME	T#07h44m01s100ms	UInt32	27841100
TOD	TOD#07:44:01	UInt32	0x07440100
DT	DT#2017-05-17-07:44:01	Double	4.29E-154

Discoverable Variables

For all variables, the OPC UA client does not directly access a discovered PAC data logic variable. Instead, the client accesses the discovered PAC variable through an OPC UA data logic variable, which exists in the BMENUA0100 module and is mapped to the underlying PAC variable. Because of the pass-through nature of data variable access, the acquisition request process is not optimized, and data dictionary acquisition performance is not representative of PAC performance.

NOTE: References, of the REF_TO type, to application variables in the OPC UA server are not accessible by the OPC UA client.

Examples of Control Expert PAC variables discoverable by the OPC UA server in the BMENUA0100 module include:

- Structured variables with sub-fields: DDT and array variables.
- Program Unit variables are discoverable as follows:
  - Input/Output variables are accessible by the OPC UA client only for the BOOL type.
  - Input variables and Output variables are accessible by the OPC UA client, except for the types REF_TO, ARRAY, String, and Structure.

In addition, the following variables are discoverable by the OPC UA server by mapping them to application varables, then discovering the mapped application variables:

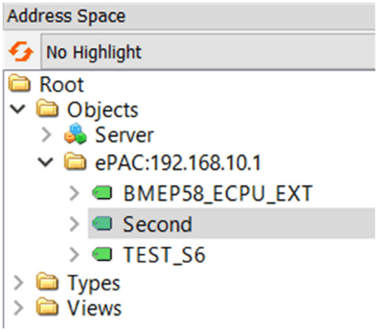
- Topological I/O variables:
  - Inputs: %I, %IW, %ID, %IF.
  - Outputs: %Q, %QW, %QD, %QF.
- Located variables: %M, %MW, %MD, %MF.
- System variables: %S, %SW, %SD.

NOTE: Variable discovery includes a variable (or symbol) for an extracted bit (for example, MyBoolVar located on %MW100.1).

Presentation of Discovered Variables in the OPC UA Client

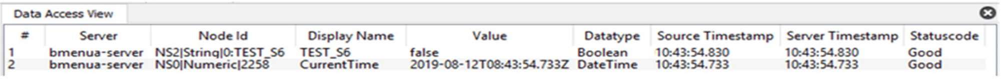
The OPC UA server in the BMENUA0100 module can organize and graphically display discovered PAC variables. An OPC UA client tool can connect to the BMENUA0100 module and view a node tree presentation of OPC UA server variables.

In the following example, an OPC UA client (in this example, the Unified Automation UaExpert client tool) connected to the BMENUA0100 module can view PAC variables in its **Address Space** windows. The M580 PAC IP address is represented by the node ePAC:192.168.10.1. Its child nodes represent Control Expert application variables:



In the example above, the first sub-node, BMEP58_ECPU_EXT, represents the device DDT for the M580 CPU, which is automatically instantiated when the CPU was added to the Control Expert application. The subsequent nodes represent other objects added to the application.

Using the OPC UA client tool, the node TEST_S6 was dragged and dropped into the tool's **Data Access View** window, where the details of the variable are displayed:



#	Server	Node Id	Display Name	Value	Datatype	Source Timestamp	Server Timestamp	Statuscode
1	bmenua-server	NS2|String|0:TEST_S6	TEST_S6	false	Boolean	10:43:54.830	10:43:54.830	Good
2	bmenua-server	NS0|Numeric|2258	CurrentTime	2019-08-12T08:43:54.733Z	DateTime	10:43:54.733	10:43:54.733	Good

In this case, the variable OPC UA data type is *Boolean* (indicating the underlying PAC data type is BOOL) and its value is *false*.

NOTE: The **Server Timestamp** attribute of the OPC UA nodes is received from the BMENUA0100 OPC UA server in UTC (Universal Time Coordinated). It is displayed to the user in local time. The data are not timestamped at their respective sources, but are timestamped by the OPC UA server. To avoid compatibility conflicts with some OPC UA clients, both source timestamp and server timestamp values are setup with the same server timestamp value.

Reading and Writing Discovered Variables in the OPC UA Client

An OPC UA tag in an OPC UA client (for example a SCADA) that refers to an array variable allows the client to read or write all elements of the array. For example the tag ‘MyArray’ declared as ARRAY[0...31] OF INT.

However, for the client to be able to read or write only a single element of an array, it is necessary to declare a specific tag that references the targeted single array element. For example ‘MyInt’ declared as INT referring to MyArray[2].

Section 3.4
Hot Standby and Redundancy

OPC UA Server Redundancy

Introduction

In a Hot Standby configuration, a BMENUA0100 module is installed in each Hot Standby main local rack. Each BMENUA0100 module is configured with a unique, static IP address. The two BMENUA0100 modules will retain their IP addresses, and will not exchange IP addresses on a Hot Standby switchover or swap.

NOTE: In a Hot Standby system, verify that the BMENUA0100 modules in the primary and the standby PACs:

- Are configured with identical cybersecurity settings *(see page 82)*, and
- Have their rotary selector switches *(see page 18)* (located on the back of the module) set to the same position.
- Are installed in the same slot number *(see page 58)* in their respective local main racks.

The system will not automatically perform these checks for you.

The BMENUA0100 module DDT includes the SERVICE_LEVEL *(see page 124)* variable, which provides information to an OPC UA client regarding the health of the OPC UA server in the BMENUA0100 module.

NOTE: In a Hot Standby system, it is recommended that you include the READ_DDT elementary function, for the purpose of updating the DDT of the BMENUA0100 module. Add the READ_DDT to a code section that executes when the CPU is in standby mode. This design returns BMENUA0100 diagnostic information that can be exchanged between the primary and standby CPUs. The application can use this information to perform a consistency check of the supported services and the cybersecurity configurations for the BMENUA0100 modules in the primary and standby CPUs.

If the Hot Standby CPU T_M_ECPU_HSBY DDT *(see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)* and its CMD_SWAP element are made available as HMI variables in a SCADA system, the SCADA application can trigger a swap by writing to the appropriate mapped OPC UA variable in the BMENUA0100.

In a Hot Standby system, the BMENUA0100 module that manages OPC UA communications with the SCADA may be the one located in the standby local rack. For this reason, you need to select the **Exchange on STBY** attribute for all scanned application variables to provide consistency of variable values between the primary and standby PACs.

In additon, to maintain consistency, the applications in the two Hot Standby PACs need to be synchronized.

In rare cases (primarily when the ECPU_HSBY_1.PLCX_ONLINE bit is set to false either manually or programmatically), one of the PACs in a Hot Standby system may be in Wait mode. In this mode, this PAC (the standby) is not synchronized with the primary PAC and variables read from this PAC are inaccurate. The state of a responding PAC may be monitored via the following T_M_ECPU_HSBY DDT fields:

- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.WAIT
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_PRIMARY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_STANDBY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.STOP

Also, the Hot Standby system permits the two PACs to operate while running different applications. To provide for the consistency of variables between the primary and standby PACs, the data layout of the 2 PACs needs to be consistent, as shown by the T_M_ECPU_HSBY DDT field: .

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = false

Non-Transparent Server Redundancy in Warm Mode

The OPC UA server in the BMENUA0100 supports non-transparent server redundancy in warm failover mode. To communicate with the two BMENUA0100 modules in a Hot Standby system, an OPC UA client will:

- Support OPC UA redundancy.
- Create connections to both BMENUA0100 modules in a Hot Standby configuration: one in the primary PAC, one in the Standby PAC.
- Activate only the connection to the BMENUA0100 in the rack of the primary Hot Standby CPU.
- Verify that both BMENUA0100 modules share the same configuration (except for IP address) – including the cybersecurity configuration – before activating the connection to the BMENUA0100 module in the new primary (former standby) PAC.

NOTE: When OPC UA redundancy is configured in a standalone system (with two BMENUA0100 modules in the local rack), it is recommended that you programmatically check the module DDTs to confirm that the supported services and the cybersecurity configurations for the BMENUA0100 modules are consistent.

NOTE: In the following parts of this topic, content is borrowed from the document: *OPC Unified Architecture Specification Part 4: Services, Release 1.04*, which is abbreviated below as *OPC UA Part 4*, followed by the appropriate section reference. The borrowed content appears in *italics*.

OPC UA Support for Redundant Servers, Clients, and Networks

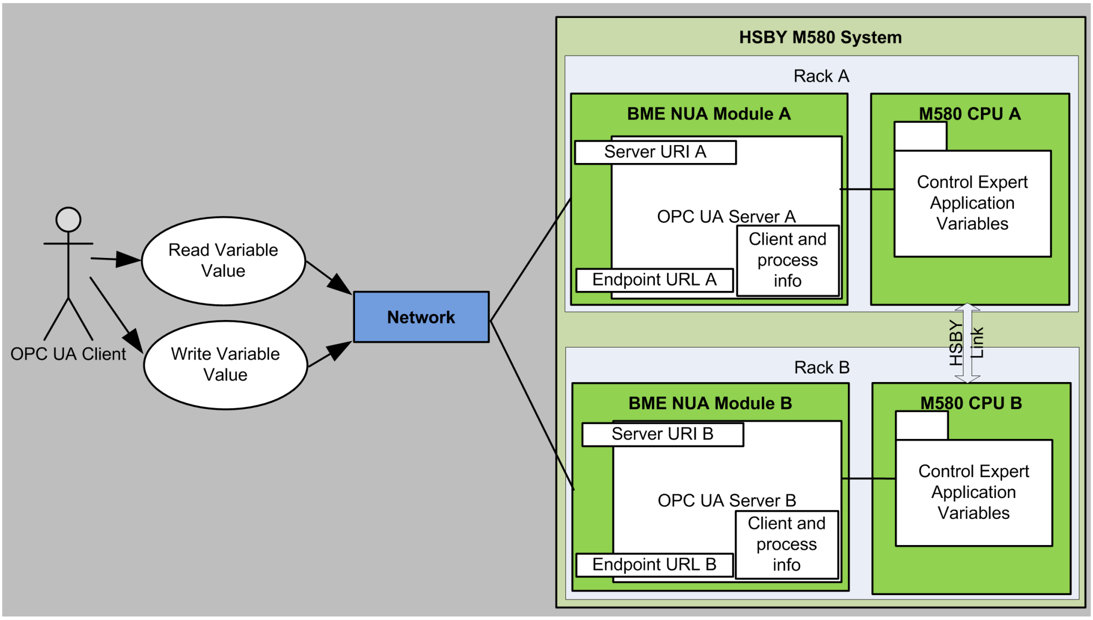
OPC UA enables Servers, Clients and networks to be redundant. OPC UA provides the data structures and Services by which Redundancy may be achieved in a standardized manner.

Server Redundancy allows Clients to have multiple sources from which to obtain the same data. Server Redundancy can be achieved in multiple manners, some of which require Client interaction, others that require no interaction from a Client. Redundant Servers could exist in systems without redundant networks or Clients. Redundant Servers could also coexist in systems with network and Client Redundancy...

Client Redundancy allows identically configured Clients to behave as if they were single Clients, but not all Clients are obtaining data at a given time. Ideally there should be no loss of information when a Client Failover occurs. Redundant Clients could exist in systems without redundant networks or Servers. Redundant Clients could also coexist in systems with network and Server Redundancy...

Network Redundancy allows a Client and Server to have multiple communication paths to obtain the same data. Redundant networks could exist in systems without redundant Servers or Clients. Redundant networks could also coexist in systems with Client and Server Redundancy...
OPC UA Part 4, section 6.6.1.

The following diagram illustrates how an OPC UA client interacts with redundant OPC UA servers in an M580 Hot Standby system:



Server Redundancy

There are two general modes of Server Redundancy, transparent and non-transparent.

In transparent Redundancy the Failover of Server responsibilities from one Server to another is transparent to the Client. The Client is unaware that a Failover has occurred and the Client has no control over the Failover behaviour. Furthermore, the Client does not need to perform any actions to continue to send or receive data.

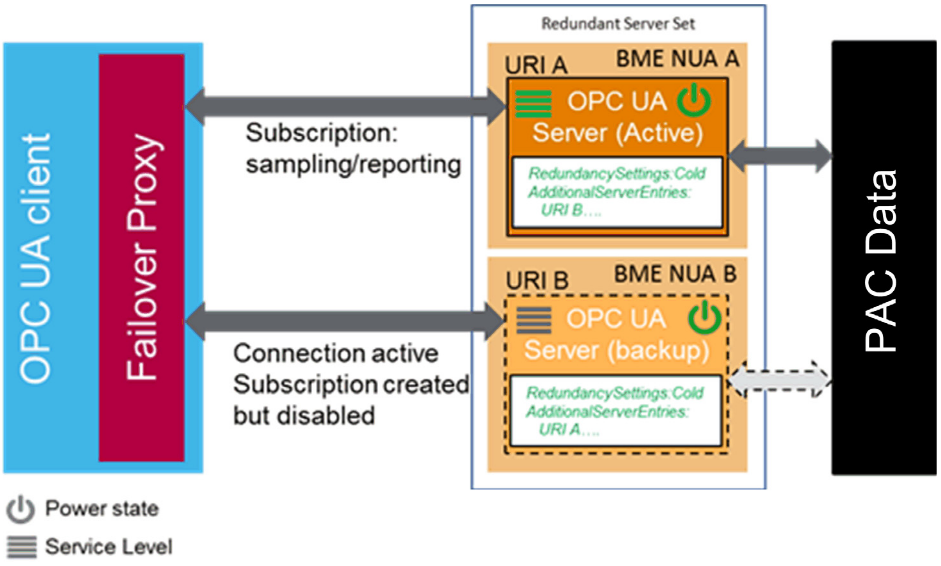
In non-transparent Redundancy the Failover from one Server to another and actions to continue to send or receive data are performed by the Client. The Client must be aware of the Redundant Server Set and must perform the required actions to benefit from the Server Redundancy.

The ServerRedundancy Object ... indicates the mode supported by the Server. The ServerRedundancyType ObjectType and its subtypes TransparentRedundancyType and NonTransparentRedundancyType ... specify information for the supported Redundancy mode. OPC UA Part 4, section 6.6.2

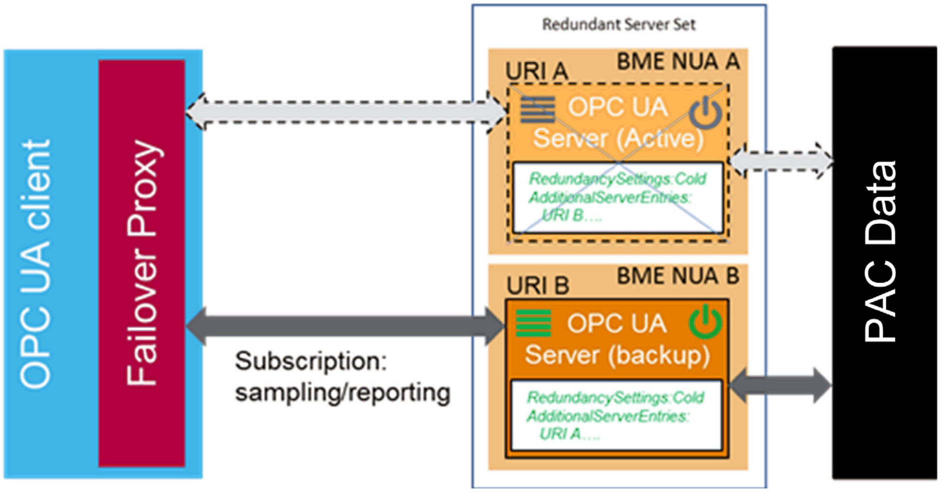
As noted above, the OPC UA server in the BMENUA0100 supports non-transparent server redundancy in warm failover mode.

OPC UA Server Warm Failover Mode

Warm failover mode *is where the backup Server(s) can be active, but cannot connect to actual data points*. Therefore, only a single server will be able to consume data of the Control Expert application. *The ServiceLevel Variable ... indicates the ability of the Server to provide its data to the Client. OPC UA Part 4, section 6.6.2.4.4*



When there is failover, action by the OPC UA client is needed; the OPC UA server embedded in BMENUA0100 becomes inactive:



Client Failover Behavior

Each Server maintains a list of ServerUris for all redundant Servers in the Redundant Server Set.

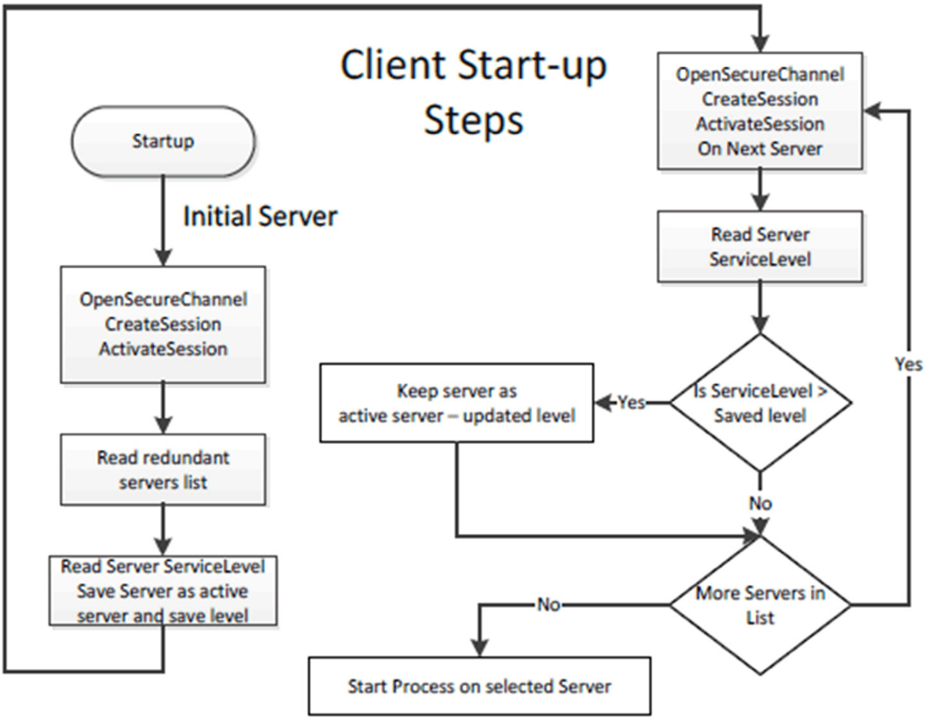
NOTE: A Redundant Server Set is the collection of OPC UA servers in the Control Expert application that are configured to provide redundancy.

The list is provided together with the Failover mode in the ServerRedundancy Object. To enable Clients to connect to all Servers in the list, each Server in the list shall provide the ApplicationDescription for all Servers in the Redundant Server Set through the FindServers Service. This information is needed by the Client to translate the ServerUri into information needed to connect to the other Servers in the Redundant Server Set. Therefore, a Client needs to connect to only one of the redundant Servers to find the other Servers based on the provided information. A Client should persist information about other Servers in the Redundant Server Set.
OPC UA Part 4, section 6.6.2.4.5.1

Client options in warm failover mode include:

- On initial connection, in addition to actions on Active Server:
  - Connect to more than one OPC UA Server.
  - Create Subscriptions and add monitored items.
- At failover:
  - Activate sampling on the subscriptions.
  - Activate publishing.

Clients communicating with a non-transparent Redundant Server Set of Servers require some additional logic to be able to handle Server failures and to Failover to another Server in the Redundant Server Set. The following figure *provides an overview of the steps a Client typically performs when it is first connecting to a Redundant Server Set.*



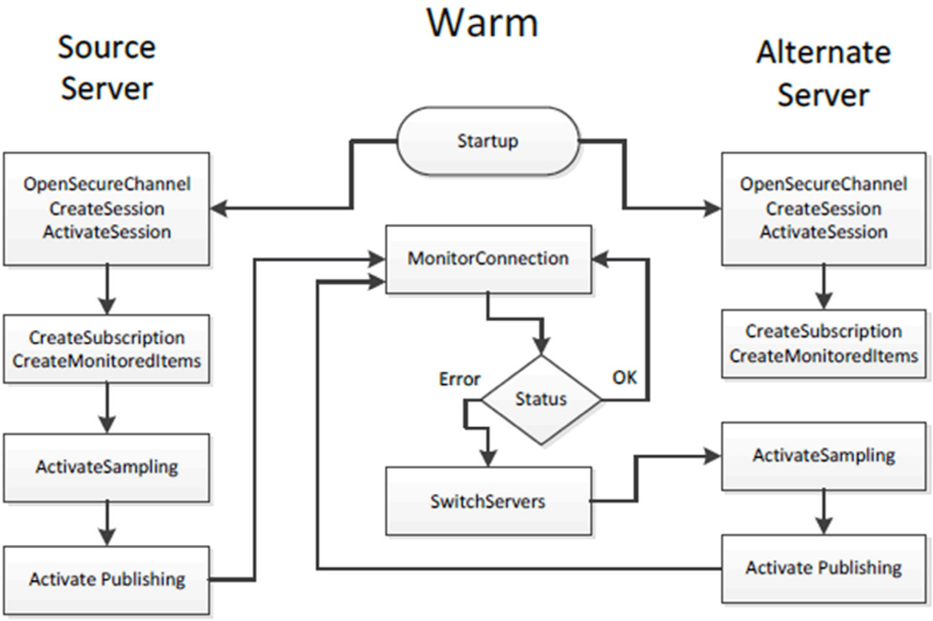
The initial Server may be obtained via standard discovery or from a persisted list of Servers in the Redundant Server Set. But in any case the Client needs to check which Server in the Server set it should connect to. Individual actions will depend on the Server Failover mode the Server provides and the Failover mode the Client will make use.

Clients once connected to a redundant Server have to be aware of the modes of Failover supported by a Server since this support affects the available options related to Client behaviour. A Client may always treat a Server using a lesser Failover mode, i.e. for a Server that provide Hot Redundancy, a Client might connect and choose to treat it as if the Server was running in Warm Redundancy or Cold Redundancy. This choice is up to the client. In the case of Failover mode HotAndMirrored, the Client shall not use Failover mode Hot or Warm as it would generate unnecessary load on the Servers. OPC UA Part 4, section 6.6.2.4.5.1

OPC UA Client Warm Failover Mode

In Warm Failover mode, *the Client should connect to one or more Servers in the Redundant Server Set primarily to monitor the ServiceLevel. A Client can connect and create Subscriptions and MonitoredItems on more than one Server, but sampling and publishing can only be active on one Server. However, the active Server will return actual data, whereas the other Servers in the Redundant Server Set will return an appropriate error for the MonitoredItems in the Publish response such as Bad_NoCommunication. The one Active Server can be found by reading the ServiceLevel Variable from all Servers.*

The Server with the highest ServiceLevel is the Active Server. For Failover the Client activates sampling and publishing on the Server with the highest ServiceLevel. Figure 30 illustrates the steps a Client would perform when communicating with a Server using Warm Failover mode.


Warm
Source Server
Alternate Server
Startup
OpenSecureChannel CreateSession ActivateSession
OpenSecureChannel CreateSession ActivateSession
MonitorConnection
CreateSubscription CreateMonitoredItems
CreateSubscription CreateMonitoredItems
Error
Status
OK
ActivateSampling
SwitchServers
ActivateSampling
Activate Publishing
Activate Publishing

OPC UA Part 4, section 6.6.2.4.5.3

Chapter 4
Supported Architectures

Introduction

This chapter describes the topological architectures supported by the BMENUA0100 Ethernet communication module with embedded OPC UA server.

What Is in This Chapter?

This chapter contains the following topics:

Supported BMENUA0100 Module Configurations

Placement of the BMENUA0100 Module

The BMENUA0100 module can be placed into an Ethernet slot on the local main rack (i.e. in the same rack as the CPU) in the following configurations:

- an M580 standalone configuration.
- an M580 standalone Safety PAC configuration.
- an M580 Hot Standby configuration.
- an M580 Hot Standby Safety PAC configuration.

NOTE:

- The BMENUA0100 module can be used with all M580 CPUs.
- In the event a network loop is created, the BMENUA0100 module goes into NOCONF (Not configured) state.

Connecting via the HTTPS Protocol

If your application experiences connection problems, check with your local IT support to confirm that your network configuration and security policies are consistent with HTTPS (port 443) access to the BMENUA0100 module IP address.

The BMENUA0100 module accepts the HTTPS connections with transport layer security (TLS) protocol v1.2 or later. For example, Windows 7 could require an update to enable TLS 1.2 to upgrade the firmware of the BMENUA0100 or access to its web site.

Installation of the BMENUA0100 Module in a Flat Network

For multiple M580 racks connected on a single subnet (i.e., a flat network architecture) that include BMENUA0100 modules with the control port disabled, install each BMENUA0100 module in a different slot number in its respective rack (except for Hot Standby configurations, where the BMENUA0100 modules are installed in the same slot number). Alternatively, it is strongly recommended that you use a router to isolate the racks and thereby avoid potential address conflicts among BMENUA0100 modules.

Access to the BMENUA0100 embedded OPC UA Server

In the topological architectures described in this chapter, the BMENUA0100 communication module Ethernet backplane port and its control port do not simultaneously provide access to the OPC UA server embedded in the module. OPC UA clients can access the OPC UA server embedded in the BMENUA0100 module either via the control port when it is enabled, or via the Ethernet backplane port when the control port is disabled.

Maximum Number of BMENUA0100 modules per Configuration

The maximum number of BMENUA0100 modules supported in an M580 configuration are:

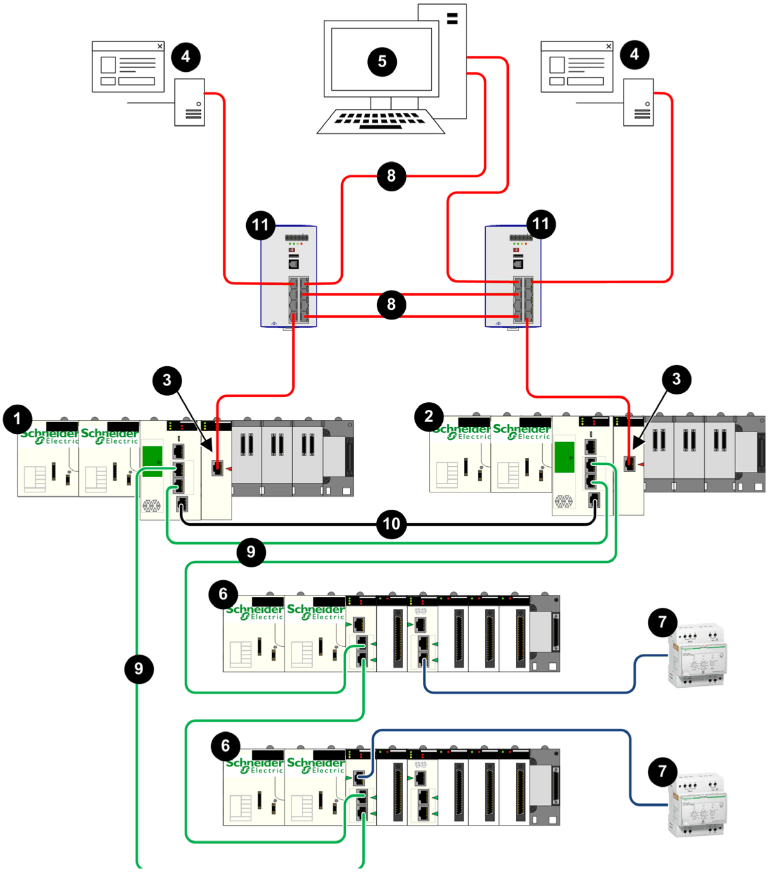
M580 Configuration Type	Maximum Number of BMENUA0100 Modules
Standalone	Two (2) in the local main rack[1].
Safety PAC	
Hot Standby	One (1) in each Hot Standby local main rack.[2]
Hot Standby Safety PAC	
1. When 2 BMENUA0100 modules are used in a standalone main rack: ● Performance of each module will be slower than if a single module had been used. ● Enable the control port in the configuration for both modules. 2. In a Hot Standby design, place each BMENUA0100 module in the same slot number in its respective local main rack.	

Change Configuration on the Fly (CCOTF)

The BMENUA0100 module does not support CCOTF.

Isolated Control Network with M580 Hot Standby PACs

Architecture



1 Primary Hot Standby PAC
2 Standby Hot Standby PAC
3 BMENUA0100 Ethernet communications module with embedded OPC UA server
4 OPC UA client (SCADA system)
5 Engineering workstation with dual Ethernet connections
6 X80 Ethernet RIO drop
7 Distributed equipment
8 Control network
9 Ethernet RIO main ring
10 Hot Standby communication link
11 Dual ring switch (DRS)

Description

This architecture provides redundant connections to dual OPC UA clients (SCADA systems). Cybersecurity can be either enabled or disabled in this architecture. The control network (8) is logically isolated from both the Ethernet devices that reside in the Ethernet RIO main ring (9), including the CPU, and the distributed Ethernet devices (7). This is accomplished at the Network layer of the OSI model via IP addressing.

The BMENUA0100 control port (3), with its dual IPv6/IPv4 stacks, allows upstream connectivity to the control network. When communicating via IPv6, it supports both stateless address auto-configuration (SLAAC) and static IP addressing.

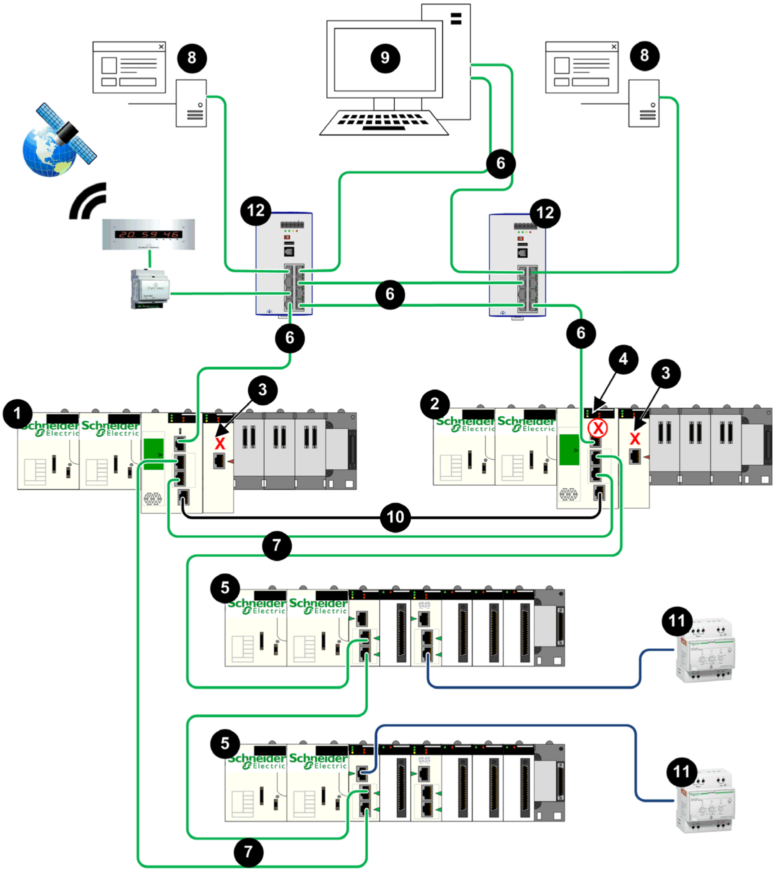
The BMENUA0100 provides Modbus peer-to-peer communication between the two Hot Standby CPUs. The CPU device ports provide downstream connectivity to the Ethernet devices on the Ethernet RIO main ring.

Each BMENUA0100 is a client of an NTP server that resides in the control network. The connection is made through the BMENUA0100 control port. The BMENUA0100 modules also serve as NTP servers for other devices in the Ethernet RIO main ring. In this Hot Standby design, the BMENUA0100 module configured as “A” acts is the primary NTP server, and the BMENUA0100 module configured as “B” acts is the standby NTP server. In this way, the CPU time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the PAC, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Non-Isolated Flat Network with M580 Hot Standby

Architecture



1 Primary Hot Standby PAC
2 Standby Hot Standby PAC
3 BMENUA0100 with control port disabled
4 Standby CPU with automatic blocking of service port
5 X80 Ethernet RIO drop
6 Control network
7 Ethernet RIO main ring
8 OPC UA client (SCADA system)
9 Engineering workstation with dual Ethernet connections
10 Hot Standby communication link
11 Distributed equipment
12 Dual ring switch (DRS)

Description

This architecture provides redundant connections from M580 Hot Standby CPUs to dual OPC UA clients (SCADA systems). Its primary purpose is to provide high availability to the Hot Standby PACs. For that reason, this architecture presents a non-isolated flat network, joining together the control network and the Ethernet RIO main ring in a single subnet.

The BMENUA0100 control port is disabled. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port. Upstream communication from the Hot Standby PACs to the SCADA servers is accomplished via the primary CPU service port. The CPU device ports provide downstream connectivity to the Ethernet devices on the Ethernet RIO main ring.

The standby CPU service port (4) is automatically disabled, which is accomplished by using the Control Expert configuration software to select **Automatic blocking of service port on Standby CPU** in the **ServicePort** tab of the configuration for both the primary and standby CPUs.

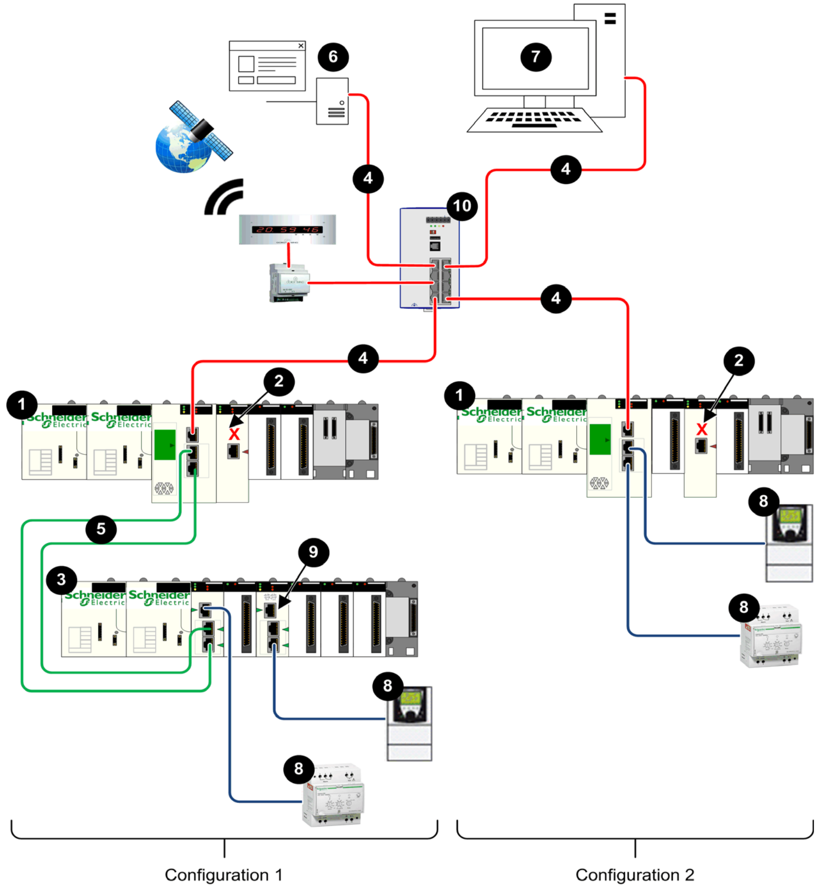
NOTE: The service port of the standby CPU is disabled to help prevent the unintended creation of an Ethernet communications loop, where both the control network and the Ethernet RIO main ring are part of the same subnet. Refer to the *M580 Hot Standby System Planning Guide* and the topic Managing Flat Ethernet Networks with M580 Hot Standby *(see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures)* for additional information.

In this flat network design, all devices, including the CPU, CRAs, and the BMENUA0100 can be clients of the same NTP server that resides in the control network. Hence, CPU time is synchronized with the BMENUA0100 module.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the PAC, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Flat Network with Multiple M580 Standalone CPUs and Single SCADA

Architecture



1 Standalone PAC
2 BMENUA0100 with control port disabled
3 X80 Ethernet RIO drop
4 Control network
5 Ethernet RIO main ring
6 OPC UA client (SCADA system)
7 Engineering workstation with single Ethernet connection
8 Distributed equipment
9 BMENOS0300 switch
10 Dual ring switch (DRS)

Description

This architecture provides a connection to a single OPC UA client (a SCADA system) from multiple M580 standalone CPUs. It is a cost-optimized architecture that does not require high availability. This architecture presents a non-isolated flat network, joining together the control network and the Ethernet RIO main ring in a single subnet.

The BMENUA0100 control port is disabled for each standalone PAC. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port. Upstream communication from each PAC to the single SCADA server is accomplished via the CPU service port.

In configuration 1, downstream connectivity from the PAC to the X80 Ethernet RIO drop (4) from the PAC is provided by the CPU dual device network ports. Further downstream connectivity is provided from the CRA service port and a BMENOS0300 switch (9) to distributed Ethernet equipment.

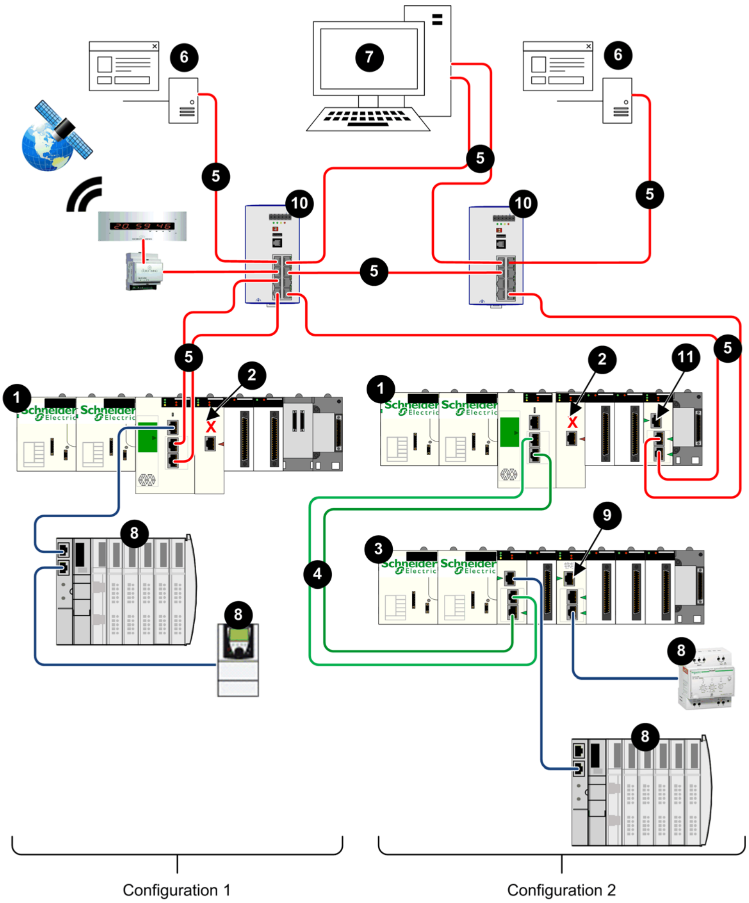
In configuration 2, downstream connectivity is provided by the dual device network ports to distributed Ethernet equipment.

In this flat network design, all network devices – including the CPU, CRAs and the BMENUA0100 – are NTP clients of an NTP server that resides in the control network. As a result, the CPU time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the PAC, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Flat Network with Multiple M580 Standalone CPUs and Redundant SCADA

Architecture



1 Standalone PAC
2 BMENUA0100 with control port disabled
3 X80 Ethernet RIO drop
4 Ethernet RIO main ring
5 Control network
6 OPC UA clients (SCADA systems)
7 Engineering workstation with dual Ethernet connections
8 Distributed equipment
9 BMENOS0300 switch
10 Dual ring switch (DRS)
11 BMENOS0300 or a BMENOC0301/11 module

Description

This architecture provides high availability of the control network, via redundant connections between OPC UA clients (SCADA systems) and multiple M580 standalone CPUs. This architecture presents a non-isolated flat network, joining together the control network and the Ethernet RIO main ring in a single subnet.

The BMENUA0100 control port is disabled for each standalone PAC. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

In configuration 1, upstream communication to the SCADA servers is accomplished via the dual CPU device network ports, using the RSTP redundancy protocol to assign roles to each port to avoid logical Ethernet loops. Downstream connectivity to the Ethernet distributed equipment is provided by the CPU service port.

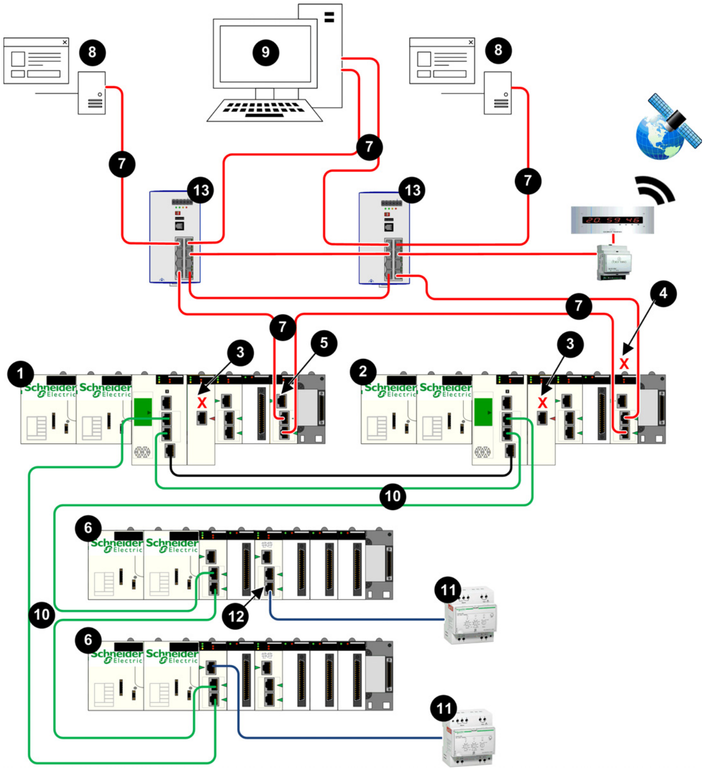
In configuration 2, upstream connectivity to the SCADA servers is provided by the device network ports of a BMENOS0300 or a BMENOC0301/11 module. The RSTP redundancy protocol is used to assign roles to each port to avoid logical Ethernet loops. Downstream connectivity from the PAC is provided from the CPU device network ports to the X80 Ethernet remote I/O drop. Further downstream connectivity is provide by both the CRA service port and a BMENOS0300 switch (9) to distributed Ethernet equipment.

In this flat network design, all network devices – including the CPU, CRAs and the BMENUA0100 – are NTP clients of an NTP server that resides in the control network. As a result, the CPU time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the PAC, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Flat Network with M580 Hot Standby CPUs and Redundant SCADA

Architecture



1 Primary Hot Standby PAC
2 Standby Hot Standby PAC
3 BMENUA0100 with control port disabled
4 BMENOS0300 or BMENOC0301/11 with backplane port disabled
5 BMENOS0300 or BMENOC0301/11 with backplane port enabled
6 X80 Ethernet RIO drop
7 Control network
8 OPC UA client (SCADA system)
9 Engineering workstation with dual Ethernet connections
10 Ethernet RIO main ring
11 Distributed equipment
12 BMENOS0300 switch
13 Dual ring switch (DRS)

Description

This architecture provides high availability with redundant connections linking redundant OPC UA clients (SCADA systems) to redundant Hot Standby PACs in a single subnet.

Each PAC is connected to SCADA via either a BMENOS0300 or BMENOC0301/11 module. To guard against the unintended creation of Ethernet loops, the backplane port of one of the BMENOS0300 or BMENOC0301/11 module is disabled. In this example, it is the module in the standby PAC (4) with a disabled backplane port. Additionally, RSTP redundancy protocol is used to assign roles to each port to avoid logical Ethernet loops

The BMENUA0100 control port is disabled (3) for each standalone PAC. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

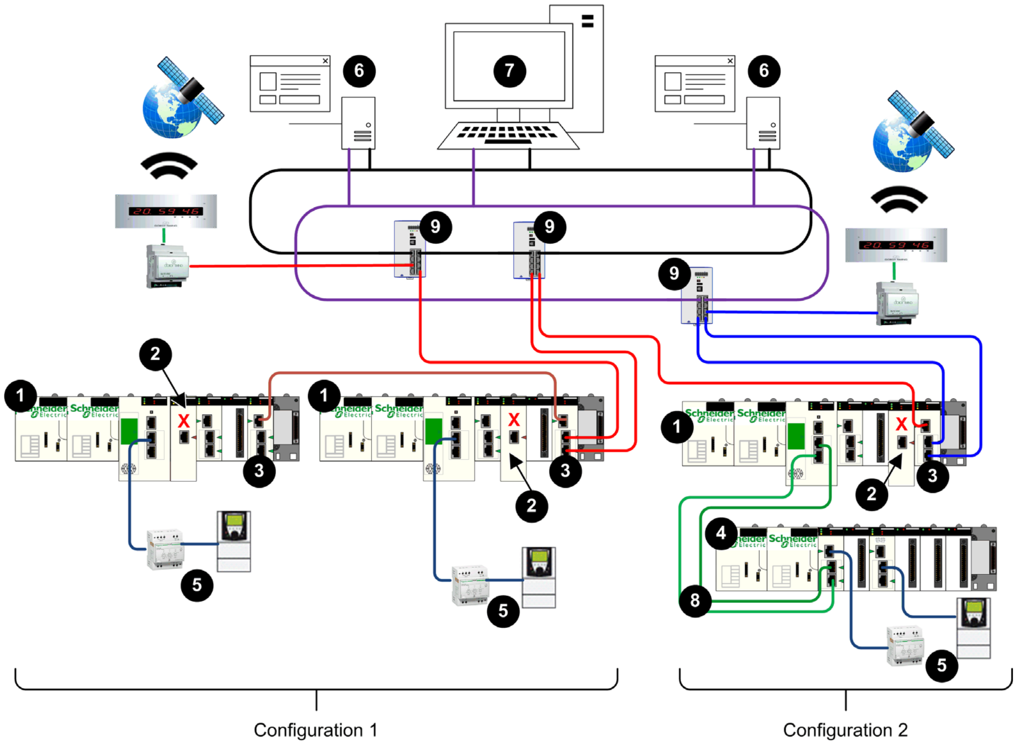
Downstream connectivity to the X80 Ethernet RIO drops is provided by the CPU device network ports. Further downstream connectivity from the X80 Ethernet RIO drops is provided by both the CRA service port and a BMENOS0300 switch (12) to distributed Ethernet equipment.

In this flat network design, all network devices – including each Hot Standby CPU and BMENUA0100 module – are NTP clients of an NTP server that resides in the control network. As a result, the CPU time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the PAC, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Hierarchical Network featuring Multiple M580 Standalone CPUs Connected to Control Network and Redundant SCADA

Architecture



1 Standalone PAC
2 BMENUA0100 with control port disabled
3 BMENOC0321 Ethernet communications module
4 X80 Ethernet RIO drop
5 Distributed equipment
6 OPC UA client (SCADA system)
7 Engineering workstation with dual Ethernet connections
8 Ethernet RIO main ring
9 Dual ring switch (DRS)

Description

This architecture features a hierarchical network, which relies on BMENOC0321 communication modules to route network traffic between subnets. Upstream communication from the PACs to the OPC UA clients (SCADA systems) is accomplished via the dual device network ports of the BMENOC0321 module, using the RSTP redundancy protocol to avoid logical Ethernet loops.

NOTE: This architecture requires the configuration of static routes in the control network equipment to redirect the various subnets of the several CPU PACs.

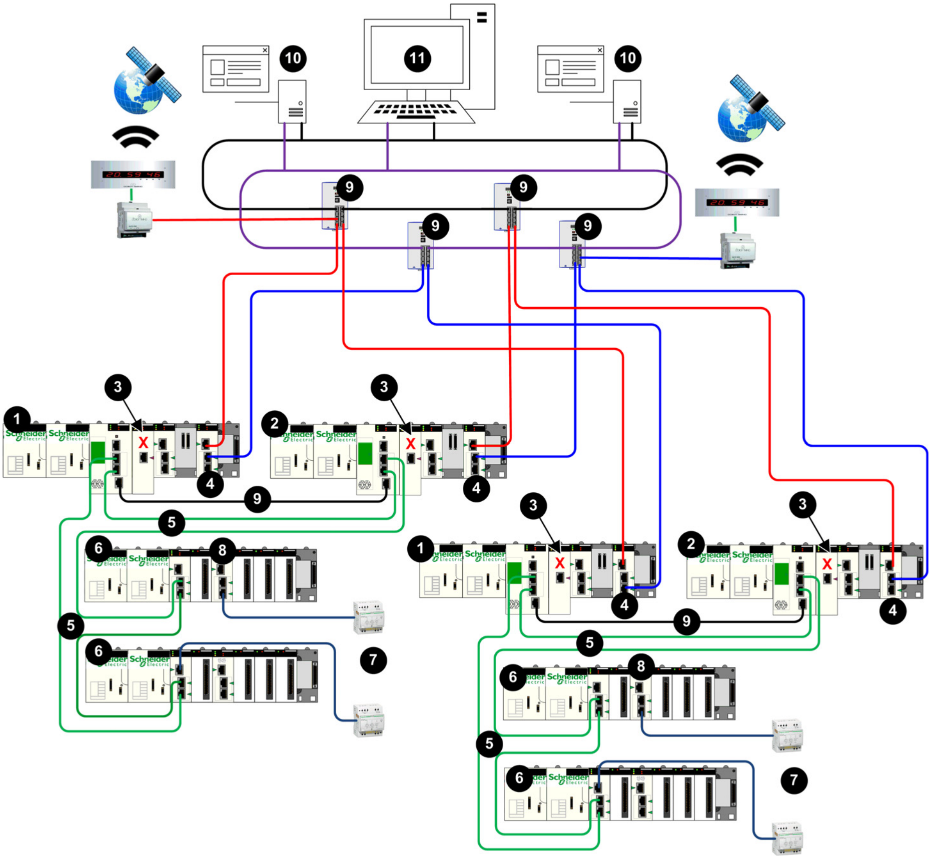
The BMENUA0100 control port (2) is disabled for each standalone PAC. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

Configuration 1 includes two PACs that reside in the same subnet. This configuration employs the BMENOC0321 module to provide redundant upstream communications to the redundant SCADA servers. The BMENOC0321 module employs the RSTP redundancy protocol to avoid logical Ethernet loops. The dual device network ports of the two CPUs provide downstream communication to the distributed Ethernet equipment.

Configuration 2 includes a single PAC, with X80 Ethernet RIO drop. This PAC uses the BMENOC0321 module for upstream communication to the redundant SCADA servers. The BMENOC0321 accomplishes this using two independent subnets. Downstream communication from the X80 Ethernet RIO drop is provided by both the CRA service port and a BMENOS0300 switch to distributed Ethernet equipment.

Hierarchical Network with Multiple M580 Hot Standby CPUs and Redundant SCADA Connections

Architecture



1 Primary Hot Standby PAC
2 Standby Hot Standby PAC
3 BMENUA0100 with control port disabled
4 BMENOC0321 Ethernet communications module
5 Ethernet RIO main ring
6 X80 Ethernet RIO drop
7 Distributed equipment
8 BMENOS0300 switch
9 Dual ring switch (DRS)
10 OPC UA client (SCADA system)
11 Engineering workstation with dual Ethernet connections

Description

This architecture features a hierarchical network, which relies on BMENOC0321 communication modules (4) to route network traffic between subnets. Upstream communication from the Hot Standby PACs to the OPC UA clients (SCADA systems) is accomplished via the dual device network ports of the BMENOC0321 modules, using the RSTP redundancy protocol to avoid logical Ethernet loops.

NOTE: This architecture requires the configuration of static routes in the control network equipment to redirect the various subnets of the several CPU PACs.

The BMENUA0100 control port (3) is disabled for each PAC. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

This configuration employs the BMENOC0321 module to provide redundant upstream communications via redundant connections to the redundant SCADA servers. The dual device network ports of the CPUs provide downstream communication to the X80 Ethernet RIO drops. Farther downstream communication from the X80 Ethernet RIO drop to the distributed Ethernet equipment is provided by both the CRA service port and a BMENOS0300 switch (8).

Chapter 5
Commissioning and Installation

Introduction

This chapter describes how to select an operating mode and install the BMENUA0100 Ethernet communications module with embedded OPC UA server.

What Is in This Chapter?

This chapter contains the following topics:

Commissioning the BMENUA0100 Module

Introduction

The BMENUA0100 module with embedded OPC UA server appears in the Control Expert hardware catalog as a communications module. It consumes one I/O channel.

When a new BMENUA0100 module comes from the factory, its cybersecurity operating mode is set to Secured mode by default. To configure the new module for Secured mode operations, follow the scenario for Secured Mode Commissioning *(see page 28)* set forth below.

To change the cybersecurity operating mode for a module that has previously been configured, including a new module you plan to configure for Standard mode operations, perform a Security Reset operation *(see page 78)* for the module. After the Security Reset operation, you can follow the scenario for either Secured Mode Commissioning *(see page 28)* or Standard Mode Commissioning *(see page 28)*.

Secured Mode Commissioning

Commissioning a BMENUA0100 module to operate in Secured mode, requires the completion of two configuration processes:

- Cybersecurity configuration, using the module web pages.
- IP address, NTP client, and SNMP agent configuration, using the Control Expert configuration tool.

Only a Security Administrator, using the Secured mode default username / password combination *(see page 29)* can commission the module in Secured mode.

NOTE: You need to complete these two configuration processes in the order set forth above, i.e., first complete the cybersecurity configuration, then configure IP, NTP and SNMP settings. When the rotary selector switch on the back of the module is set to the Secured position, placed on a rack, and then powered-up, it is not possible to configure IP, NTP and SNMP settings for the module until it receives a cybersecurity configuration.

The following procedure is intended for a new module that has not been previously configured. If you are using a module that has previously been configured, perform a Security Reset operation *(see page 78)* before proceeding with the following steps.

To commission the module in Secured operating mode:

1. Configure cybersecurity settings:
   a. With the module detached from the rack, use the plastic screwdriver that ships with the module *(see page 18)* to set the rotary switch to the **[Secured]** position.
   b. Install *(see page 79)* the module into an Ethernet slot on the local, main Ethernet rack and cycle power.
   c. Connect your configuration PC to the module control port, and use your Internet browser to navigate to the module web pages at the default IPv4 address.
   NOTE: The default IPv4 address is 10.10.MAC5.MAC6, where MAC5 is the fifth octet and MAC 6 is the sixth octet of the module MAC address. The module MAC address is printed on the face of the module.

  d. If your Internet browser displays a message *(see page 84)* indicating a potential security risk, proceed to make the connection by clicking **Accept the Risk and Continue** (or similar, browser-specific language).
  e. In the user login page, enter the default username / password combination *(see page 29)*.
  f. Change and confirm the password. Refer to the User Management topic *(see page 96)* for password requirements. The module **Home** page *(see page 87)* is displayed.
  g. Starting from the **Home** page, navigate to the module web pages and configure its cybersecurity settings.

2. Configure IP address, NTP client, and SNMP agent settings:
   a. Open the Control Expert configuration tool.
   b. In Control Expert, create a **New Project** add a BMENUA0100 module to the project from the **Hardware Catalog** then configure the IP address, NTP client, and SNMP agent settings. *(see page 100)*
   c. When the Control Expert project configuration is complete, connect to the PAC and transfer the project to the PAC.

NOTE: When the configuration is loaded in the BMENUA0100 module the module state changes from NOT CONFIGURED to CONFIGURED. The SECURE LED *(see page 114)* indicates if the module is not configured or configured, and if the OPC UA server is connected to an OPC UA client.

Standard Mode Commissioning

In Standard mode, a cybersecurity configuration is not required. Only the IP address, NTP client, and SNMP agent settings are configured using the Control Expert configuration tool. In Standard mode, the module begins to communicate when it is placed on the rack, power is applied, and it receives a valid configuration from Control Expert.

Use the Installer default username / password combination *(see page 29)* to commission the module in Standard mode.

To commission the module in Standard mode:

1. With the module detached from the rack, use the plastic screwdriver that ships with the module *(see page 18)* to set the rotary switch to the **Standard** position.
2. Place the module an Ethernet slot on the local, main Ethernet rack and cycle power.
3. Open the Control Expert configuration tool.
4. In Control Expert, create a **New Project**, add a BMENUA0100 module to the project from the **Hardware Catalog**, then configure the IP address *(see page 101)*, NTP client *(see page 104)*, and SNMP agent *(see page 107)* settings.
5. When the Control Expert project configuration is complete, connect to the PAC and transfer the project to the PAC.

NOTE: When operating in Standard mode, the SECURE LED will be OFF.

Security Reset Operation

For a module that has previously been configured, or for a new module you want to configure for Standard mode cybersecurity operations, perform a Security Reset operation before proceeding with cybersecurity configuration. A reset operation sets the cybersecurity settings to their factory default values. You can perform a reset by using the module web pages, or the rotary switch located on the back of the module.

Web pages: For a BMENUA0100 module that is presently configured for Secured mode operations:

1. Navigate to the **Configuration Management → RESET** web page.
2. Click **Reset**.
   NOTE: The Security Reset operation is complete when the RUN LED is solid green, and both the NS control port LED and BS backplane port LED are solid red.
3. Cycle power to the module in one of the following ways:
   - Turn off power to the module rack, then turn power back on.
   - Physically remove the module from the rack, then re-insert it.

   You can now proceed with Secured mode commissioning.

Rotary Switch: For any BMENUA0100 module:

1. With the module detached from the rack, use the plastic screwdriver that ships with the module *(see page 18)* to set the rotary switch to the **Security Reset** position.
2. Install *(see page 79)* the module into an Ethernet slot on the local, main Ethernet rack, and cycle power.
   NOTE: This restores the factory default settings to the module, including the control port default IP address *(see page 101)* of 10.10.MAC5.MAC6.

   Upon completion, the RUN LED is solid green, and both the NS control port LED and BS backplane port LED are solid red. You can turn off power, remove the module from the rack, and proceed with either Secured Mode Commissioning *(see page 28)* or Standard Mode Commissioning *(see page 28)*

Installing the BMENUA0100

Introduction

You can install the BMENUA0100 module only into a local, Ethernet main rack by placing it into any Ethernet slot not reserved for the safety power supply or CPU.

NOTE: If your application includes multiple PACs (that are not paired Hot Standby PACs) each with a BMENUA0100 module, install the modules so that the slot number of each BMENUA0100 module is unique. For example, for an application that includes two PACs, if a BMENUA0100 module in the PAC1 rack is placed into slot 4, place a BMENUA0100 module in the PAC2 rack into a slot other than slot 4.

Grounding Precautions

Each BMENUA0100 module is equipped with ground connection contacts.

Schneider Electric recommends the use of a BMXXSP•••• bar to help protect the rack from electromagnetic disturbances.

Follow all local and national safety codes and standards.

⚠ ⚠ DANGER

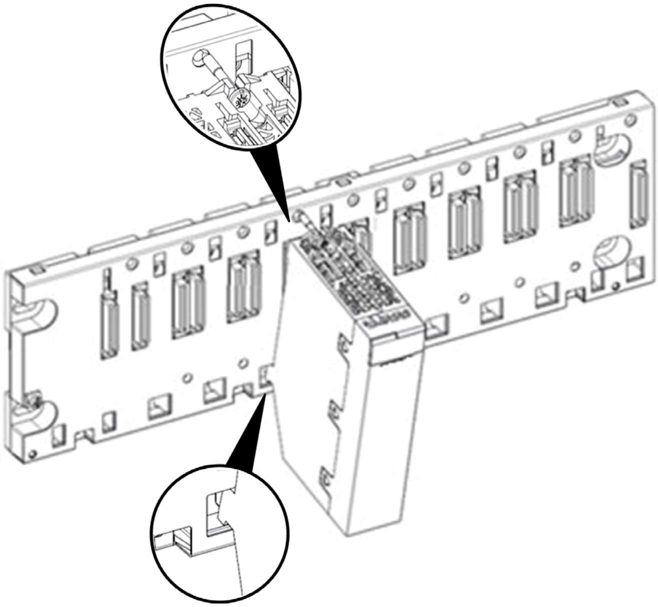
HAZARD OF ELECTRICAL SHOCK

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

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

Installing a Safety I/O Module in the Rack

A BMENUA0100 module requires a single rack Ethernet slot. You can install the module into any Ethernet slot not reserved for the power supply or CPU. Follow these steps to install a BMENUA0100 module in a rack:

Step	Action	
1	Position the locating pins situated at the bottom rear of the module in the corresponding slots on the rack.	
2	Swivel the module towards the top of the rack so that the module sits flush with the back of the rack. The module is now set in position.	
3	Tighten the single screw on top of the module to maintain the module in place on the rack. Tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).	

Grounding the I/O Modules

For information on grounding, refer to the topic *Grounding the Rack and Power Supply Module* in the document *Modicon X80 Racks and Power Supplies Hardware Reference Manual*.

Chapter 6
Configuration

Introduction

This chapter describes how to configure the BMENUA0100 Ethernet communications module with embedded OPC UA server.

What Is in This Chapter?

This chapter contains the following sections:

Section 6.1
Configuring the BMENUA0100 Cybersecurity Settings

Introduction

This section describes how to use the web pages of the BMENUA0100 Ethernet communication module with OPC UA server. Use the web pages to create a cybersecurity configuration for the module, and to view diagnostic data.

What Is in This Section?

This section contains the following topics:

Introducing the BMENUA0100 Web Pages

Introduction

Use the BMENUA0100 web pages to create, manage and diagnose a cybersecurity configuration for the module, and to view event and OPC UA diagnostic data.

For the BMENUA0100 module to operate in Secured mode, a cybersecurity configuration is required and must be performed before its IP address, NTP client, and SNMP settings can be configured using Control Expert *(see page 100)*. A cybersecurity configuration can be configured only locally for each BMENUA0100 module by connecting a configuration PC, running an HTTPS browser, to the BMENUA0100 module:

- Control port, if the control port is enabled.
- Backplane port (via a BMENOC0301/11 or the CPU), if the control port is disabled.

For the BMENUA0100 module to operate in Standard mode, cybersecurity settings are not required and cannot be configured.

NOTE:

- When using a self-signed certificate, some browsers may report the connection between the PC and the module as “Unsecured”.
- For BMENUA0100 modules operating in Secured mode in a Hot Standby system, verify that the cybersecurity settings for the BMENUA0100 module in the primary PAC are the same as the cybersecurity settings for the BMENUA0100 module in the standby PAC. The system will not automatically perform this check for you.

The accessibility of web pages depends on the cybersecurity operating mode:

Web Page or Group	Secured Mode	Standard Mode
Home *(see page 87)*	✓	✓
Settings (device security) *(see page 90)*	✓	–
Certificates Management *(see page 94)*	✓	–
Access Control *(see page 96)*	✓	–
Configuration Management *(see page 98)*	✓	–
Diagnostic *(see page 131)*	✓	✓
✓ : web pages are accessible. – : web pages are not accessible.		

Initial Configuration of Cybersecurity Settings

You can configure initial cybersecurity settings for a BMENUA0100 module that has:

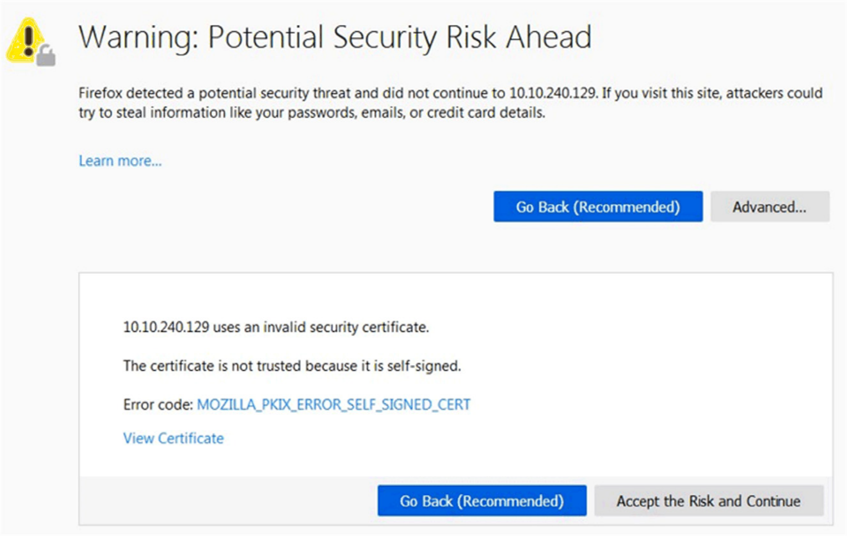
- Never been configured, and retains its initial factory default configuration.
- Previously been configured, but had its factory default configuration restored by executing the Security Reset command *(see page 28)*.

After a module has been configured with cybersecurity settings, and is operating in Secured mode, you can also modify the cybersecurity settings using the web pages.

Refer to the commissioning topic *(see page 76)* for instructions on how to apply an initial configuration to the module.

First Login to the Web Pages

When you login to an unconfigured BMENUA0100 module, the following screen displays:



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 10.10.240.129. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more...

10.10.240.129 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

View Certificate

Despite the warning language, the connection is secured via HTTPS. Proceed with the initial login by clicking **[Accept the Risk and Continue]** (or other similar browser-specific language).

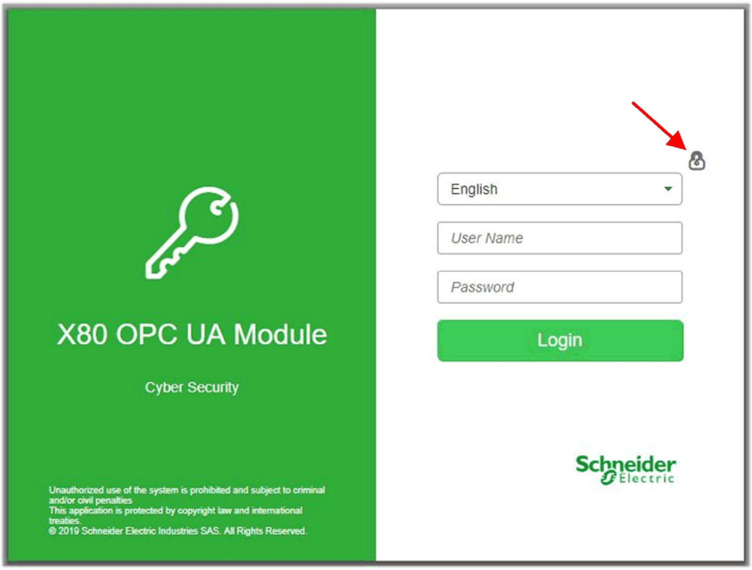
NOTE: The above message appears because the module does not yet have a valid configuration and is using a self-signed certificate.

Logging In to the Web Pages

On the first login, the security administrator enters the default User Name and Password combination *(see page 29)*. Immediately thereafter, the administrator is required to change the administrator's default password.

You need to login each time you open the web pages for the BMENUA0100 module. Only persons that have been assigned a valid user account – with a valid username and password combination created by a security administrator in the **Access Control** → **User Management** web page *(see page 96)* – can access the module web pages.

In the login page, select a language from the drop-down list, then enter your **User Name** and **Password**.



X80 OPC UA Module

Cyber Security

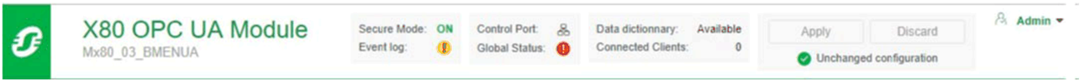
Unauthorized use of the system is prohibited and subject to criminal and/or civil penalties
This application is protected by copyright law and international treaties.
© 2019 Schneider Electric Industries SAS. All Rights Reserved.

NOTE: The module cybersecurity operating mode is displayed by the lock icon in the upper-right part of the dialog (indicated by the red arrow, above). If the lock is:

- Closed (as shown above): the module in operating in Secured mode *(see page 28)*.
- Open: the module is operating in Standard mode *(see page 28)*.

Web Page Banner

Every web page presents a banner at the top of the page:



X80 OPC UA Module
Mx80_03_BMENUA

Secure Mode: ON
Event log:
Control Port:
Global Status:
Data dictionnary: Available
Connected Clients: 0
Unchanged configuration

The banner presents the following information about the BMENUA0100 module:

- Secure Mode:
  - ON: the module is operating in Secured mode *(see page 28)*.
  - OFF: the module is operating in Standard mode *(see page 28)*.
- Event log:
  - ✓ The Event log service is disabled.
  - ✓ The Event log service is enabled; the log server is reachable.
  - ! The Event log service is enabled; the log server is not reachable.
  - ! The Event log service is enabled, but an error has been detected.

- Control Port:
  - The control port is enabled.
  - The control port is disabled.
- Global Status:
  - ✓ All services are operational.
  - ! At least one service is not operational.
- Data dictionary:
  - Available: the data dictionary functionality is available.
  - NotAvailable: the data dictionary functionality is not available or is not enabled.
- Connected Clients: the number of currently connected OPC UA clients.
- Apply/Discard Configuration: Indicates the state of the current module cybersecurity web page configuration:
  - ✓ Unchanged configuration: The cybersecurity configuration contains no pending or invalid edits. The **Apply** and **Discard** commands are disabled.
  - ! Pending configuration: One or more changes to the cybersecurity configuration has not yet been applied. Both the **Apply** and the **Discard** commands are enabled.
  - X Invalid configuration: The cybersecurity configuration is incomplete or incorrect. The **Apply** command is disabled; the **Discard** command is enabled. In this state, the web page GUI displays, next to each affected menu item, a red circle that contains the number of invalid configuration settings reachable via that menu path. When you navigate to a page with an invalid configuration setting, the GUI identifies the invalid configuration setting.

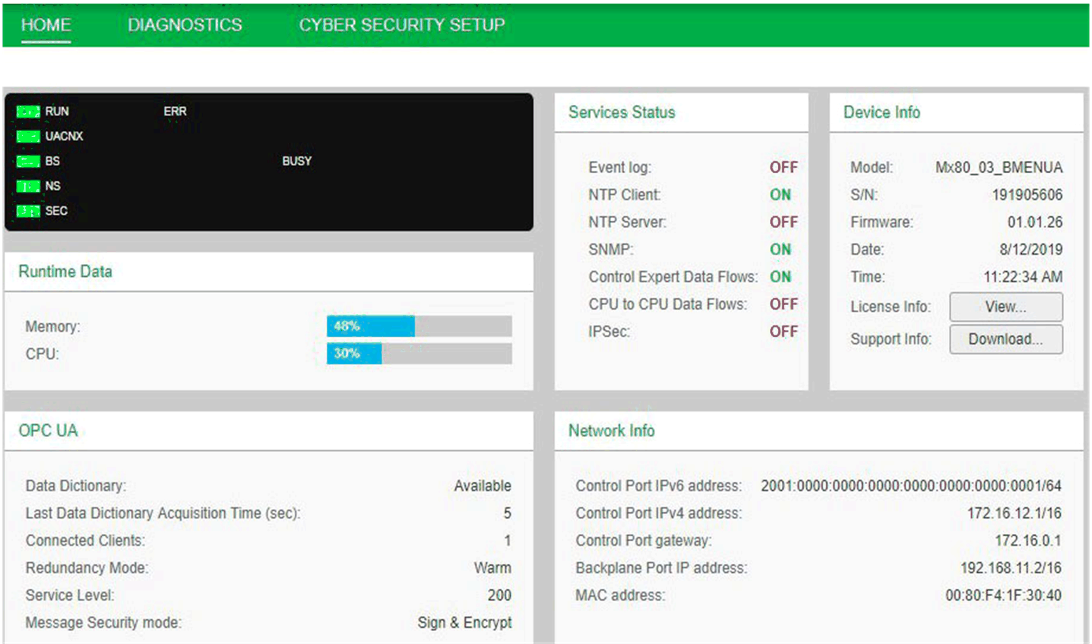
Web Page Help

Many Web pages offer parameter-level context sensitive help. To get help for a specific parameter, or field, place your cursor pointer over the i icon.

Home Page

Introducing the Home Page

When you login to the BMENUA0100 web pages, the **Home** page opens by default. If the module has a valid configuration, the page appears as follows:



Runtime Data

Memory:	48%
CPU:	30%

Services Status

Event log:	OFF
NTP Client:	ON
NTP Server:	OFF
SNMP:	ON
Control Expert Data Flows:	ON
CPU to CPU Data Flows:	OFF
IPSec:	OFF

Device Info

Model:	Mx80_03_BMENUA
S/N:	191905606
Firmware:	01.01.26
Date:	8/12/2019
Time:	11:22:34 AM
License Info:	View...
Support Info:	Download...

OPC UA

Data Dictionary:	Available
Last Data Dictionary Acquisition Time (sec):	5
Connected Clients:	1
Redundancy Mode:	Warm
Service Level:	200
Message Security mode:	Sign & Encrypt

Network Info

Control Port IPv6 address:	2001:0000:0000:0000:0000:0000:0000:0001/64
Control Port IPv4 address:	172.16.12.1/16
Control Port gateway:	172.16.0.1
Backplane Port IP address:	192.168.11.2/16
MAC address:	00:80:F4:1F:30:40

Use the **Home** page to:

- Access the navigation tree, which contains links to the BMENUA0100 module web pages. When the module is operating in:
  - Secured mode *(see page 28)*, both the DIAGNOSTICS and CYBER SECURITY SETUP menus are displayed and accessible to the security administrator.
  - Standard mode *(see page 28)*, only the DIAGNOSTICS menu is accessible.
- View the state *(see page 112)* of the module LEDs *(see page 20)*.
- View collections of data for the module, including:
  - Runtime Data *(see page 88)*
  - OPC UA *(see page 88)*
  - Services Status *(see page 88)*
  - Network Info *(see page 88)*
  - Device Info *(see page 89)*

NOTE: When the rotary switch on the back of the module is set to the Security Reset *(see page 28)* position, there can be no communication with the module. Hence, the web pages – including the **Home** page – are not accessible.

Runtime Data

The **OPC UA** area displays:

- **Memory**: The percentage of internal RAM used by the OPC UA server (MEM_USED_PERCENT).
- **CPU**: The percentage of currently used CPU processing capacity (CPU_USED_PERCENT).

NOTE: The items described above are based on elements in the T_BMENUA0100 DDT *(see page 115)*.

OPC UA

The **Runtime Data** area displays:

- **Data dictionary**: The availability state of the data dictionary (DATA_DICT).
- **Last Data Dictionary Acquisition Time (sec)**: The duration of the last data dictionary acquisition (DATA_DICT_ACQ_DURATION).
- **Connected clients**: The number of connected OPC UA clients (CONNECTED_CLIENTS).
- **Redundancy mode**: The failover mode supported for a Hot Standby system (REDUNDANCY_MODE).
- **Service Level**: The OPC UA server health, based on data and service quality (REDUNDANCY_MODE).
  NOTE: The five items described above are based on elements in the T_BMENUA0100 DDT *(see page 115)*.
- **Message Security mode**: The setting configured in the OPC UA web page *(see page 93)*: None, Sign, or Sign&Encrypt.

Services Status

The **Service Status** area displays the status – enabled (ON) or disabled (OFF) – of the following services as reported in the T_BMENUA0100 DDT *(see page 115)*:

- **Event log** (EVENT_LOG_SERVICE)
- **NTP Client** (NTP_CLIENT_SERVICE)
- **NTP Server** (NTP_SERVER_SERVICE)
- **SNMP** (SNMP_SERVICE)
- **Control Expert Data Flows** (CONTROIL_EXPERT_IP_FORWARDING)
- **CPU to CPU Data Flows** (CPU_TO_CPU_IP_FORWARDING)
- **IPSEC** (IPSEC)

Network Info

This area displays:

- The IP configuration settings for the BMENUA0100 module control port (CONTROL_PORT_IPV6, CONTROL_PORT_IPV4, and CONTROL_PORT_GTW) and backplane port (ETH_BKP_PORT_IPV4), entered in Control Expert *(see page 101)*, and reported in the T_BMENUA0100 DDT *(see page 115)*.
- The module MAC address, a unique hexadecimal value assigned to each module at the factory.

Device Info

This area displays the name, serial number, and firmware version (FW_VERSION in the T_BMENUA0100 DDT *(see page 115)*), date, and time for the BMENUA0100 module.

Click the **View...** button to display licensing information.

Click the **Download...** button to display tech support contact information.

Settings

Introduction

In the BMENUA0100 module web pages, starting in the **Home** page, select **Settings** to display links to the following configuration pages, where you can enter settings for device security:

- User Account Policy *(see page 90)*
- Event Logs *(see page 90)*
- Network Services *(see page 91)*
- IPSEC *(see page 92)*
- OPC UA *(see page 93)*
- Security Banner *(see page 93)*

The configurable parameters for each node are described below.

Use these settings to configure device security for the BMENUA0100 module. After changing settings, select **Submit** or **Cancel**.

User Account Policy

Use these settings to configure user account policy:

Parameter	Description
Session maximum inactivity (minutes)	The idle session timeout period for HTTPS connections. If a connection is inactive for this period, the user session is automatically closed. Default = 15 min. **NOTE:** There exists no inactivity period timeout for OPC UA connections.
Maximum login attempts	The number of times a user may attempt, and fail, to login. Default = 5 attempts. When the configured maximum is reached, the user account is locked.
Login attempt timer (minutes)	The maximum time period to login. Default = 3 min.
Account locking duration (minutes)	Time period during which no additional logins may be attempted after the maximum login attempts is reached. Upon the expiration of this period, a locked user account is automatically unlocked. Default = 4 min.

Event Logs

Use these settings to configure the syslog client that resides in the BMENUA0100 module. The logs are stored locally in the module and exchanged with a remote syslog server *(see page 126)*.:

Parameter	Description
Service activation	Turns ON and OFF the syslog client service. Default = OFF.
Syslog server IP address	IPv4 address of the remote syslog server.
Syslog server port	The port number used by the syslog client service. Default = 601.

Network Services Activation

These services together constitute a firewall that permits or denies the passage of communications through the BMENUA0100 module. Use these settings to enable or disable the following services:

GLOBAL POLICY:

Service	Description
Enforce Security	Disables all network services, except IPSec which is enabled.
Unlock Security	Enables all network services, except IPSec which is disabled.

NETWORK SERVICES ACTIVATION: The default setting for the following services depends on the cybersecurity operating mode (CS Op Mode), as follows:

Service	Description	CS Op Mode default	
		Standard	Secure
SNMP Agent	Enables and disables SNMP Agent communications.	Enabled	Disabled
NTP Server	Enables and disables NTP server communications.	Enabled	Disabled
IPSec	Enables and disables IPSec communications.	Disabled	Enabled[1]
Control Expert Data Flows to CPU only (Refer to *Configuring Communication for Control Expert Data Flow (see page 92)*.)	Enables and disables Modbus, EtherNet/IP, Ping, explicit messaging, and FTP communications, passing through the BMENUA0100 module, between Control Expert configuration software and the CPU only.	Enabled	Disabled
Control Expert Data Flows to Device Network (Refer to *Configuring Communication for Control Expert Data Flow (see page 92)*.)	Enables and disables Modbus, EtherNet/IP, Ping, explicit messaging, and FTP communications, passing through the BMENUA0100 module, between Control Expert configuration software and network devices, including the CPU.	Enabled	Disabled
CPU to CPU Data Flows Refer to *Configuring Communication for CPU to CPU Data Flows (see page 92)*.)	Enables and disables Modbus communications, passing through the BMENUA0100 module, between M580 CPUs.	Enabled	Disabled
HTTPS on control port	Enables and disables HTTPS communications over the control port. **NOTE:** If HTTPS is disabled, and the change applied, the web pages can not be accessed via the control port. To regain access to the web pages from the control port, you can either reset the cybersecurity configuration, or access the web pages from the backplane port and enable HTTPS.	Disabled	Enabled
1. IPSec is enabled with no rules defined. The service needs to be configured.			

NOTE: SNMP, NTP, Syslog and Modbus services are not inherently secure protocols. They are rendered secure when encapsulated within IPSEC. It is recommended that you do not disable IPSEC if any one of the SNMP, NTP, Modbus, or Syslog services is enabled.

Configuring Communication for Control Expert Data Flows

Modbus, EtherNet/IP, FTP, and Ping communications from an online DTM in Control Expert will address the target device (e.g., the M580 CPU) using the IP address of the target device. To support this communication, set up two default gateways, as follows:

- On the host PC running Control Expert, set up a PC default gateway to the BMENUA0100 module control port IP address.
- On the target device (e.g. the M580 CPU), set up a device default gateway to the BMENUA0100 module backplane port IP address.

Modbus communications from Control Expert Connect screen will address the BMENUA0100 control port IP address. Gateways are not needed for this communication.

Configuring Communication for CPU to CPU Data Flows

Modbus TCP/IP communications from CPU to CPU through the BMENUA0100 module will use the BMENUA0100 module control port address, and not the address of the target CPU.

NOTE: EtherNet/IP CPU to CPU data flows are not forwarded.

IPSEC

Use these settings to configure a maximum of 8 IKE / IPSEC channels for the BMENUA0100 module:

Parameter	Description
IPSEC SERVICE	● ON: Enables IPSec service. ● OFF: Disables IPSec service.
NTP authorized outside IPSEC	● De-selected (disabled): NTP is exchanged only through IPSEC. ● Selected (enabled): NTP is exchanged through IPSEC if IPSEC channel is opened, and outside IPSEC if IPSEC channel is not opened.
New link	Creates a new IKE / IPSEC channel and adds it to the list for editing. **NOTE:** A maximum of 8 IKE / IPSec channels are supported.
For each IKE / IPSEC channel, configure the following settings:	
Remote IP address	IPv4 address of the remote device at the other end of the IPSEC connection.
Confidentiality	● Selected: Communication will be encrypted. ● De-selected: No encryption. **NOTE:** Confidentiality is disabled if *NTP without IPSEC* is enabled.
PSK	A pre-shared key that is 32 hexadecimal characters long, the result of a random number generated by the BMENUA0100 module. It can be copied and edited in this web page. **NOTE:** PSK is disabled if *NTP without IPSEC* is enabled.

NOTE: To support IKE/IPSEC communication, configure Windows firewall settings *(see page 143)* for any PC that hosts an OP UA client connected to the OPC UA server in the BMENUA0100 module.

OPC UA

Use these settings to configure the connection for the OPC UA server embedded in the BMENUA0100 module:

Parameter	Description
Message Security mode	● Sign&Encrypt (default): Each message is given a signature and is encrypted. ● Sign: A signature is applied to each message. ● None: No security policy is applied. In this case, the following two fields are disabled.
Security Policy	● Basic256Sha256 (default): It defines a security policy for configurations with valid crypto suite. ● Basic256: It defines a security policy for configurations with deprecated crypto suite. **NOTE:** This selection is not used unless needed for interoperability with remote client. ● Basic128Rsa15: It defines a security policy for configurations with deprecated crypto suite. **NOTE:** This selection is not used unless needed for interoperability with remote client.
User Identifier token types	● Anonymous: No user information is available. ● User Name (default): User is identified by username & password.

NOTE: Cybersecurity configuration changes to the OPC UA server settings cause the server to restart and apply the new settings. As a result, if one or more OPC UA sessions exist when configuration changes are made, these sessions are suspended. When the *SessionTimeout* period expires, these sessions finally will be closed. The *SessionTimeout* is part of the OPC UA SCADA client configuration.

Security Banner

This page contains editable text that is displayed when a user accesses the BMENUA0100 module web pages:

Parameter	Description
Banner text	A string of up to 128 characters that is displayed to a user on the login page. The following editable text is displayed by default: “Unauthorized use of the system is prohibited and subject to criminal and/or civil penalties.'

Certificates Management

Introduction

OPC UA clients and BMENUA0100 modules are authenticated by means of self-signed certificates. In order to provide the required level of cybersecurity, each entity (OPC UA client, BMENUA0100) needs to manage a trust list of all certificates of devices/applications that communicate with it.

The BMENUA0100 module creates two certificates:

- HTTPS certificate for:
  - configuration of the cybersecurity settings via the module web pages
  - diagnostic of the module via its web pages
  - firmware upgrade
- OPC UA application instance certificates to permit OPC UA clients to access the embedded OPC UA server in the BMENUA0100 module.

NOTE:

- The expiration dates of the trusted certificates are made by reference to the internal Date and Time settings of the BMENUA0100 module. To avoid inconsistency, use the NTP service to update the Date and Time settings of the BMENUA0100 module, and check that the NTP server is accessible and has a updated Time and Date settings.
- If you receive a *BadCertificateHostnameInvalid* error when attempting to connect your OPC UA client to the BMENUA0100 server in IPv6, it may be caused by a compressed IPv6 address (i.e., shortened IPv6 address). In this case check the IPv6 address that was used and, if necessary, replace it using an uncompressed format.

Managing Certificates

In the BMENUA0100 module web pages, starting in the **Home** page, select **Certificates Management** to display links to the following application instance certificate management pages:

- Trust List Management *(see page 94)*
- Device Certificates Export *(see page 95)*

Trust List Management

Only OPC UA clients that have provided the BMENUA0100 module with an application instance certificate can communicate with the OPC UA server embedded in the module. The module implements local (module-based) management of OPC UA application instance certificates, which are stored in a trust list. Use the commands on the **Certificates Management** web pages to:

- Add a certificate to the trust list.
- Remove a certificate from the trust list.
- Download a trust list certificate.

NOTE: OPC UA application instance trust list certificates are encoded in ANSI CRT.

To add a certificate to the list:

Step	Action
1	In the trust list, right click to open a menu
2	Select **Add**.
3	Click **Browse**, then navigate to and select the certificate you want to add to the list.
4	Click **Submit** to add the certificate.

To remove a certificate from the list:

Step	Action
1	In the trust list, right click on the certificate you want to remove
2	Select **Delete**.
3	Click **OK** to remove the certificate from the list.

Device Certificate Export

An OPC UA application instance certificate of a BMENUA0100 module needs to be exported, so that it can be imported into the trust list of a remote OPC UA client.

To export a certificate:

Step	Action
1	Click **Browse**, then navigate to and select the certificate you want to export.
2	Click **Download** to add the certificate to a newly generated file in the CRT format. **NOTE:** If your OPC UA client supports only DER encoded certificates, change the extension of the certificate from .crt to .der.

Access Control

Introduction

The BMENUA0100 module supports local authentication of users based on the use of username/password combinations for:

- Configuration of the module cybersecurity settings via HTTPS
- Firmware download via HTTPS
- Module web page diagnostics via HTTPS

NOTE: Only a user with the role of Security Administrator can create, edit, or delete user accounts.

The BMENUA0100 web pages provide tools for the management of users. Starting in the **Home** page, click on **Access Control** to display a list of existing OPC UA users, including their roles and permissions. In this page you can:

- Add a user *(see page 97)*.
- Update the profile *(see page 97)* of an existing user.
- Delete *(see page 97)* a user.

User Management

The BMENUA0100 module provides role based access control (RBAC). All users are assigned a role and can perform only those tasks associated with that role.

The following roles and permissions are supported:

Role	Permissions			
	Cybersecurity Configuration	Firmware Upgrade	Diagnostic Web Page Access	OPC UA Protocol Access
SECADM	Update, Read, Delete	–	Read	–
OPERATOR	–	–	Read	Connect
ENGINEER	–	–	Read	Connect
INSTALLER	–	Update	Read	–

Each BMENUA0100 module supports a maximum of 15 simultaneous users.

No custom roles or custom permission sets can be configured. No IP address-based access control whitelist can be configured.

Add a User

A Security Administrator can click **New User** then complete the following parameters to add a new user:

Parameter	Description
User name	The user ID. The user will enter this along with the password to gain access to the permitted functions.
Password	The user password. Because the password is not displayed in clear text, enter this value twice to confirm its accuracy. **NOTE:** Each password must be at least 8 characters long, and must contain at lest one of the following characters: ● an upper-case alpha character (A...Z) ● a lower-case alpha character (a...z) ● a base 10 digit (0...9) ● a special character ~ ! @ $ % ^ & * _ + - = ` | \ ( ) [ ] : “ ‘ < >
Confirm Password	
Roles	Select the user role, which will define the permissions granted to the user: ● Security Administrator ● Operator ● Engineer ● Installer

Click **Apply Changes** after these parameters are configured to create the new user.

Update User

To edit the settings of an existing user, a Security Administrator can click on the edit icon (pencil) for the profile you want to edit. Click **Apply Changes** to save your edits. The same dialog used to add a new user opens, letting you update some or all of the selected user’s configuration,

Delete User

To delete an existing user, a Security Administrator can right click on that user in the list, and under **Delete User** click **OK**.

Configuration Management

Introduction

To facilitate system configuration, you can export the cybersecurity settings of a configured BMENUA0100 module, and import that configuration into another module. In the BMENUA0100 module web pages, starting in the **Home** page, select **Configuration Management** to display links to the following cybersecurity configuration management pages:

- EXPORT
- IMPORT *(see page 99)*
- RESET *(see page 99)*

NOTE: Only a security administrator, with the role SECADM, can perform the configuration management tasks described in this topic.

Export Config

Use the **EXPORT** page to export the cybersecurity configuration file of the local BMENUA0100 module. The exported configuration file is encrypted with the password assigned in this page. An exported configuration file can be stored and re-used.

To export the cybersecurity configuration file of the local BMENUA0100 module:

Step	Description
1	In the **EXPORT** page, assign the configuration file a **Password**. **NOTE:** The password needs to be a minimum of 16 characters, and applies the same rules that are used in the creation of user passwords *(see page 97)*.
2	Re-enter the assigned password in the **Confirm password** field.
3	Click **Download**.

NOTE: The configuration file is produced with the name: Mx80_xx_BMENUA.cfg, where “xx” indicates the slot number occupied by the module in the rack.

Import a Configuration

Use the **IMPORT** page to import a cybersecurity configuration file and apply it to the local BMENUA0100 module. The cybersecurity settings applied using this command overwrite the module's existing cybersecurity settings.

To import a cybersecurity configuration file and apply it to the local BMENUA0100 module:

Step	Description
1	In the **IMPORT** page, click the file icon to open a window where you can select a **Configuration archive**.
2	Navigate to and select the configuration file you want to import, and click **OK**.
3	In the **IMPORT** page, enter the configuration file **Password** that was assigned to the file when the file was exported. **NOTE:** Optionally, you can select **Save** to automatically apply the imported configuration immediately after it is uploaded.
4	Click **Upload**. A dialog opens informing you that your session has been closed. The configuration has been uploaded to the server.
5	Click **Reconnect** to close the dialog and open the login screen *(see page 84)*.
6	Enter your security administrator username and password and click **Login**. The Home page opens. If **Save** was not selected in step 3, the banner indicates a pending configuration exists.
7	In the banner, click **Apply**, then click **Yes** to confirm that you want to apply the pending configuration. The new configuration is applied. **NOTE:** If you previously selected **Save** in the **IMPORT** page (as indicated in step 3, above) the configuration is automatically applied, and this step 7 is automatically performed.

Reset Config

Click **Reset** in the **RESET** page to restore the "out of the box" factory default cybersecurity settings to the local BMENUA0100 module. This action has the same effect as setting the rotary selector switch to the Security Reset *(see page 28)* position.

Section 6.2
Configuring the BMENUA0100 in Control Expert

Introduction

This section describes how to configure IP address settings, the NTPv4 client, and the SNMPv1 agent for the BMENUA0100 Ethernet communication module with embedded IPC UA server.

What Is in This Section?

This section contains the following topics:

Configuring IP Address Settings

Introduction

The BMENUA0100 Ethernet communications module with embedded OPC UA server includes two Ethernet ports:

- the control port located on the front of the module.
- a backplane port connecting the module to the local main rack Ethernet backplane.

The control port can be enabled or disabled, and is enabled by default. The backplane port is always enabled.

Static IP address settings for both the control port and the backplane port can be configured in the **IPConfig** tab of the BMENUA0100 configuration dialog. In addition, IP address settings can be dynamically assigned to the control port via the Stateless Address Auto-configuration (SLAAC) method of DHCP.

When the BMENUA0100 module is used in a standalone PAC, IP address settings are configured for only a single module. When two instances of the BMENUA0100 module are used in a Hot Standby PAC architecture (one BMENUA0100 module in each PAC), the Control Expert **IPConfig** configuration tab includes settings for two modules (A and B). In a Hot Standby PAC architecture, the IP address for each module can be in different subnets.

IPv4 and IPv6 Stack Support

The control port can be configured to support IP stacks (each of which consists of a collection of Internet-enabling protocols) as follows:

- IPv4 stack: Supports only 32-bit addressing. An example of an IPv4 IP address is: 192.168.1.2.
- IPv4/IPv6 dual stack: Supports both 32-bit and 128-bit addressing. When both the IPv4 and IPv6 stacks are configured, the control port can receive and handle both IPv4 and IPv6 Ethernet packets An example of an IPv6 128-bit IP address is: 2001:0578:0123:4567:89AB:CDEF:0123:4567.

NOTE: On initial power up (or after the module rotary switch has been set to **Security Reset**, powered up, then re-set to **Secured**, and then powered up again), the control port is assigned a default IPv4 address of 10.10.MAC5.MAC6, where MAC5 is the decimal value of the 5th octet of the module MAC address, and MAC6 is the decimal value of the 6th octet. The MAC address of the module appears on its front face.

Configuring IP Addresses

Configure IP addressing in Control Expert, as follows:

Step	Action
1	In the **Project Browser** expand the **PLC Bus** node and open the BMENUA0100 module configuration dialog.
2	Click on the **IPConfig** tab.
3	Enter changes in the appropriate fields on the **IPConfig** configuration page. (The following table describes the configuration page parameters.)

Configurable Parameters

Configure these IP address parameters for each BMENUA0100 communications module in your project:

Parameter	Description
Control Port	Enables/disables the control port of the BMENUA0100 module. When set to: ● Enabled: the control port is the exclusive interface for IPv4 or IPv6 communication to the embedded OPC UA server. ● Disabled: the Ethernet backplane port can support IPv4 communication to the OPC UA server.
IPv6 Control Port configuration	
IPv6	Enables/disables IPv6 IP addressing for the control port.Default = disabled.
Mode	Identifies the source of the IPv6 address: ● SLAAC: Indicates the IPv6 IP address will be served to the control port from a DHCP server using the SLAAC method. ● Static (default): Enables the IPv6@ field for inputting a static IPv6 IP address.
IPv6 @	If **Static** is selected as the **Mode**, above, enter a valid IPv6 address for the control port. **NOTE:** The BMENUA0100 cannot detect duplicate IPv6 addresses. Please check with your network administrator to ensure there are no duplicate IPv6 addresses within the same network segment.
Subnet prefix length	The number of bits of the SLAAC assigned IPv6 address that are used to define the subnet network prefix. (default = 64).
IPv4 control port configuration	

Parameter		Description
	Mode	Identifies the source of the IPv4 address: ● Default: Indicates the IPv4 IP address based on the module MAC address is used. ● Static (default): Enables the **IPv4 @**, **Subnet Mask**, and **Default Gtw** fields for inputting a static IPv4 IP address for the control port.
	IPv4 @	If the selected mode is: ● **Default**: Replace the Control Expert auto-filled value (10.10.0.2) with the address 10.10.MAC5.MAC6 where: ❍ MAC5 is the fifth octet of the module MAC address. ❍ MAC6 is the sixth octet of the module MAC address. ● **Static**: Enter a valid IPv4 address for the control port.
	Subnet Mask	If **Static** is selected as the **Mode**, above, enter a valid IPv4 subnet mask for the control port, which will determine the network portion of the IPv4 address.
	Default Gtw	If **Static** is selected as the **Mode**, above, enter a valid IPv4 address for the default gateway.
Backplane port		
	IPv4 @	Enter a valid IPv4 address for the backplane port.

NOTE: When configuring your application in Control Expert, the **Ethernet Network** window (opened via **Tools → Ethernet Network Manager...**) displays only the backplane port identifier for the BMENUA0100 module. Information concerning the control port, NTP server, SNMP manager, and - for a Hot Standby system - the standby BMENUA0100 module (B) is not displayed.

Configuring the Network Time Service

Introduction

The BMENUA0100 Ethernet communications module with embedded OPC UA server supports version 4 of the network time protocol (NTP). The NTP service synchronizes the clock in the BMENUA0100 module with the clock of a time server. The synchronized value is used to update the clock in the module.

NOTE: If the NTP server resides in the CPU, the BMENUA0100 module can update its time settings without introducing delay.

When the BMENUA0100 module is used in a standalone PAC, NTP settings are configured for only a single module. When two instances of the BMENUA0100 module are used in a Hot Standby PAC architecture (one BMENUA0100 module in each PAC), the Control Expert **NTP Client** configuration tab includes settings for two modules (A and B).

NOTE: When a new NTP server is reached or if there is a time offset on an NTP server, it can take up to 5 minutes to update the BMENUA0100. The ERR LED *(see page 112)* remains ON until the BMENUA0100 time is synchronized with the NTP server.

Enabling and Disabling the NTP Client and the NTP Server

The BMENUA0100 module includes both an NTP server and an NTP client.

NTP Client:

If either the primary or secondary NTP server IP address is set to a value other than 0.0.0.0, the NTP client is enabled. If both the primary and secondary NTP server IP address settings are set to 0.0.0.0, the NTP client is disabled.

NOTE: When both **Primary NTP Server** and **Secondary NTP Server** IP address settings are set to 0.0.0.0, the BMENUA0100 module cannot operate as either NTP client or NTP server.

NTP Server:

The NTP server is enabled, depending on the cybersecurity operating mode:

- In Secured mode, the NTP server is enabled if:
  - Either the primary or secondary NTP server IP address setting is set to a non-null value (i.e., set to a value other than 0.0.0.0); and
  - The NTP Server is set to enabled, in the **Network Services** web page *(see page 91)* configuration settings.
- In Standard mode, the NTP server is enabled if either the **Primary NTP Server** or **Secondary NTP Server** IP address setting is set to a non-null value (i.e., set to a value other than 0.0.0.0).

NOTE: If the BMENUA0100 is configured as NTP client of a server on the backplane network (**Primary NTP Server** or **Secondary NTP Server**), the BMENUA0100 NTP server will not be enabled in any case, even if there is no NTP server on the backplane network.

When both the NTP server and NTP client are enabled in the BMENUA0100 module, the module NTP client receives time settings over its control port from a remote NTP server. The module NTP server forwards these time settings over its backplane port to NTP clients.

NOTE: The BMENUA0100 module cannot operate as NTP server over its control port.

NTP Polling

The BMENUA0100 module optimally and dynamically manages the NTP polling period with the NTP server. No configuration is necessary.

Power Up

To establish the accurate Ethernet system network time, the system performs these tasks at power up:

- The BMENUA0100 communications module powers up.
- The BMENUA0100 communications 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 impacts the accuracy of the time.

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

The BMENUA0100 communications module does not maintain the time. Upon power up or power cycle, the clock value of the module is 0, which is equivalent to January 1st 1980 00:00:00:00.

Configuring the Service

Configure the network time synchronization service in Control Expert, as follows:

Step	Action
1	In the **Project Browser** expand the **PLC Bus** node and open the BMENUA0100 module configuration dialog.
2	Click on the **NTP Client** tab.
3	Select **Enable NTP Client**.
4	Enter changes in the appropriate fields on the **Network Time Service** configuration page. (The following table describes the configuration page parameters.)

Configurable Parameters

Configure these time synchronization parameters for each BMENUA0100 communications module in your project:

Parameter		Description
IPv4 NTP server configuration		
	Primary NTP Server[1]	Enter a valid IPv4 address for the primary NTPv4 server. **NOTE:** Set to the CPU main IP address by default.
	Secondary NTP Server[1]	Enter a valid IPv4 address for the secondary NTPv4 server.
1. Configure NTP server address that can be reached by BMENUA0100 module. If the control port is disabled, enter NTP server IP addresses that are in the same subnet as the backplane port.		

SNMP Agent Configuration

About SNMP

An SNMP V1 agent is a software component of the SNMP service that runs on the BMENUA0100 module and provides access to diagnostic and management information for the module. You can use SNMP browsers, network management software, and other tools to access this data.

In addition, the SNMP agent can be configured with the IP addresses of 1 or 2 devices (typically PCs that run network management software) to be the targets of event-driven trap messages. Such messages inform the management device of events like cold starts and the inability of the software to authenticate a device.

Termination of SNMP Service

The SNMP service running on the BMENUA0100 module is terminated if:

- the module is in the ERROR state.
- the SNMP service is in the FAULT state.

Access the SNMP Tab

Double-click the BMENUA0100 module in the Control Expert configuration to access the **SNMP** tab.

The SNMP agent can connect to and communicate with 1 or 2 SNMP managers. The SNMP service includes:

- authentication checking by the BMENUA0100 module of any SNMP manager that sends SNMP requests.
- management of events or traps.

SNMP Parameters

These parameters are found on the Control Expert **SNMP** tab:

Field	Parameter	Description	Value
IP Address managers	IP Address manager 1	The address of the first SNMP manager to which the SNMP agent sends notices of traps.	0.0.0.0...255.255.255.255
	IP Address manager 2	The address of the second SNMP manager to which the SNMP agent sends messages of traps.	
Agent	Location (SysLocation)	device location	31 characters (maximum)
	Contact (SysContact)	information about the person to contact for device maintenance	
	Enable SNMP manager	*unchecked* (default): You can edit the **Location** and **Contact** parameters. *checked*: You cannot edit the **Location** and **Contact** parameters.	checked/unchecked
Community names	Set	password that the SNMP agent requires to read commands from an SNMP manager (default = **Public**)	15 characters (maximum)
	Get		
	Trap		
Security	Enable "Authentication failure" trap	*unchecked* (default): not enabled. *checked*: Enabled. The SNMP agent sends a trap message to the SNMP manager if an unauthorized manager sends a **Get** or **Set** command to the agent.	checked/unchecked

Supported Traps

By default, the BMENUA0100 module SNMP agent supports the following traps:

- Linkup
- Linkdown

The Authentication failure trap is also supported, if enabled.

Offline IP Address Verification

Offline tests are done to verify that the IP addresses of the managers do not include the following types of IP addresses:

- multicast: 224.0.0.0 or higher
- loopback: Any address that starts with 127
- broadcast: 255.255.255.255

SNMP MIB-2 Object Identifiers

Under the **Vendor Name** Schneider Electric, the BMENUA0100 module presents the following object identifier (OID) values:

Object Name	OID	Value
SysDesc	1.3.6.1.2.1.1.1	Product: BMENUA0100 - OPC UA communication module. Firmware ID: xx.yy
SysObjectID	1.3.6.1.2.1.1.2	1.3.6.1.4.1.3833.1.7.255.53
SysName	1.3.6.1.2.1.1.5	BMENUA0100
SysServices	1.3.6.1.2.1.1.7	74, representing the sum of (2**7-1 + 2**4-1 + 2**2-1) and indicating support of protocols in the following OSI layers: ● 7: application layer ● 4: transport layer ● 2: data-link layer
ifDesc	1.3.6.1.2.1.2.2.1.2	This OID contains information describing the interface, including the product name, and port name.

Chapter 7
Diagnostics

Overview

This chapter describes the diagnostic tools available for the BMENUA0100 Ethernet communication module with embedded OPC UA server.

What Is in This Chapter?

This chapter contains the following topics:

LED Diagnostics

Display Panel LED Diagnostics

The state of the BMENUA0100 module display panel LEDs *(see page 20)* are presented, below, for the several operating states of the module.

NOTE: The state of the SECURE LED for the configured and non-configured state of the module are separately presented, below, following the initial presentation.

Operating State		RUN LED (Green)	UACNX LED (Green/Red)	ERR LED (Red)	BS Backplane LED (Green/Red)	NS Control Port LED (Green/Red)	BUSY LED (Yellow)	SECURE LED (Green/Red)
Power on sequence	1	OFF	OFF	ON	Green OFF Red ON	Green OFF Red ON	OFF	Green OFF Red ON
	2 (All LEDs ON)	ON	ON	ON	Green ON Red ON	Green ON Red ON	ON	Green ON Red ON
	3 (All LEDs OFF)	OFF	OFF	OFF	Green OFF Red OFF	Green OFF Red OFF	OFF	Green OFF Red OFF
	4	ON	OFF	ON	Green OFF Red OFF	Green OFF Red OFF	OFF	Green OFF Red OFF
	5 (Autotest[1])	Flashing	Flashing	Flashing	Green Flashing Red OFF	Green Flashing Red OFF	Flashing	Green Flashing Red OFF
Not configured		OFF	OFF	Blinking	Red blinking if not connected to an Ethernet Backplane port. Blinking green otherwise.	OFF if not cable plugged and connected to another powered device. Blinking green otherwise.	OFF	Refer to cyber-security LEDs, below *(see page 114)*.

1. The autotest is performed quickly and LED flashing cannot be visually detected.
2. Refer to SERVICES_STATUS detected error codes in the T_BMENUA0100 DDT *(see page 115)*.
3. This state results from changing the rotary switch from Standard to Secured mode, or from Secured to Standard mode without performing a Security Reset *(see page 26)* as an intermediate step.

Operating State		RUN LED (Green)	UACNX LED (Green/Red)	ERR LED (Red)	BS Backplane LED (Green/Red)	NS Control Port LED (Green/Red)	BUSY LED (Yellow)	SECURE LED (Green/Red)
Configured	After detecting a duplicated IPv4 address on backplane port	Blinking	Refer to description of UACNX LED, below *(see page 114)*	OFF	Green OFF Red ON	/	/	Refer to description of Secure Communication Status LED, below *(see page 114)*.
	After detecting a duplicated IPv4 address on Control Port	Blinking		OFF	/	Green OFF Red ON	/	
	RUN State	ON		OFF	Green ON Red OFF	Steady green if connected; Off if no cable	ON if data-dictionary acquisition in progress; Flashing if data dictionary overflow; otherwise OFF	
Power Off		OFF	OFF	OFF	Green OFF Red OFF	Green OFF Red OFF	OFF	Green OFF Red OFF
Recoverable Detected Error or Inconsistent Configuration[2]		/	/	ON	/	/	/	/
Non-recoverable Detected Error (Module will reboot)		OFF	OFF	ON	Green OFF Red ON	Green OFF Red ON	OFF	Green OFF Red ON
Security Reset	In progress	Blinking	OFF	OFF	Green OFF Red ON	Green OFF Red ON	ON	Green OFF Red OFF
	Complete	ON	OFF	OFF	Green OFF Red ON	Green OFF Red ON	OFF	Green OFF Red OFF
Missing Security Reset[3]		OFF	OFF	ON	Green OFF Red ON	Green OFF Red ON	OFF	Blinking Red
OS Update		Blinking	OFF	OFF	Green OFF Red ON	Green OFF Red ON	ON	Green OFF Red OFF

1. The autotest is performed quickly and LED flashing cannot be visually detected.
2. Refer to SERVICES_STATUS detected error codes in the T_BMENUA0100 DDT *(see page 115)*.
3. This state results from changing the rotary switch from Standard to Secured mode, or from Secured to Standard mode without performing a Security Reset *(see page 26)* as an intermediate step.

UACNX LED When the Module is in Configured State

The color (red or green) and state (blinking or steady) describe the state of the OPC UA connections:

Data Dictionary State	OPC UA Client Connection State	
	No OPC UA Client Connected	At Least 1 OPC UA Client Connected
Data Dictionary Unavailable	Blinking Red	Steady Red
Data Dictionary Available	Blinking Green	Steady Green

Secure Communications Status LED When the Module is Configured/Not Configured State

The states of the SECURE LED, when the module is in the configured or not configured state, are described below:

LED State	Description
OFF	The module is not operating in secure operating mode (i.e., the rotary switch is not set to the secure position).
RED	A secure communications critical error is detected. For example, no security configuration is present, a certificate has expired and communications have stopped, and so forth.
GREEN	Secure communications are enabled and running without detected error. A client is connected to the module and the module has received a valid cybersecurity configuration. The session is opened and the module is ready to respond to client requests.
FLASHING RED	Secure communications are enabled and running, but an error has been detected. For example, a certificate has expired but the configuration authorizes communications to continue.
FLASHING GREEN	The module has received a valid cybersecurity configuration and is ready to communicate with a client which will initiate a communication.

Control Port LED Diagnostics

The control port LEDs *(see page 20)* can be used to diagnose the state of Ethernet communications over the control port:

LED	State	Description
ACT	Off	No link established.
	Green	Link established, no activity.
	Blinking Green	Link established, activity detected.
LNK	Off	No link established.
	Yellow	Link established at speed less than module maximum capability (10/100Mbps).
	Green	Link established at speed equal to module maximum capability (1000Mbps).

BMENUA0100 Derived Data Type (DDT)

Introduction

Each BMENUA0100 Ethernet communication module with embedded OPC UA server that you add to your application instantiates a common collection of data elements. You can use the tools presented in the Control Expert software to access these data elements and diagnose the module.

NOTE:

- DDT data returned in response to a Modbus request cannot exceed 256 bytes in length.
- Given the organization of the Control Expert data dictionary, requests for data stored in bits of words need to be extracted by the requesting client.

The contents of the DDT can be accessed using the READ_DDT *(see page 120)* elementary function (EF) in Control Expert software.

T_BMENUA0100 DDT Structure

The BMENUA0100 DDT includes the following elements:

Element	Type	Address	Description
DEVICE_NAME	STRING[16]	MW1...8	The module name.
CONTROL_PORT_IPV6	STRING[44]	MW9...30	Control Port IPv6 / subnet prefix length.
CONTROL_PORT_IPV4	STRING[18]	MW31...39	Control Port IPv4 / subnet prefix length.
CONTROL_PORT_GTW	STRING[16]	MW40...47	Control Port default gateway.
ETH_BKP_PORT_IPV4	STRING[18]	MW48...56	Backplane Port IPv4 / subnet prefix length.
ETH_STATUS	WORD	MW57	–
PORT_CONTROL_LINK	BOOL	MW57.0	● 0: Control port link is down. ● 1: Control port link is up.
ETH_BKP_PORT_LINK	BOOL	MW57.1	● 0: Backplane port link is down. ● 1: Backplane port link is up.
GLOBAL_STATUS	BOOL	MW57.2	● 0: Module is not operational. ● 1: Module is operational.
NETWORK_HEALTH	BOOL	MW57.3	● 0: Network overload condition is detected. ● 1: Network is operating normally.
Reserved	–	MW57.4...15	–
OPCUA_STATUS	T_OPCUA_STATUS	MW58...61	–

Element	Type	Address	Description
DATA_DICT	BYTE	MW58[0]	● 1: Not available. Possible causes: ❍ The data dictionary functionality is not available or enabled in the Control Expert application and cannot be embedded in the PAC. ❍ The loading/browsing of the data dictionary is in progress in OPC UA Server. ● 2: Available, for example: ❍ The loading/browsing of the data dictionary by the OPC UA server completed with success. ❍ A pre-loading (in accordance with Control Expert data dictionary project settings) can be in progress. ● 4: Busy. ● 8: Data dictionary overflow.
DATA_DICT_ACQ_DURATION	BYTE	MW58[1]	Duration of last acquisition (0...255 seconds).
CONNECTED_CLIENTS	BYTE	MW59[0]	Number of connected OPC UA clients.
DATA_DICT_PRELOAD_ DURATION	BYTE	MW59[1]	Duration of last data dictionary pre-load (0...255 seconds). **NOTE:** You can use the information contained in this element to adjust and optimize the **Effective Build changes time-out** setting in the **Tools → Project Settings → General → PLC embedded data** configuration window. Refer to Control Expert online help for information on how to configure this setting.
REDUNDANCY_MODE	BYTE	MW60[0]	● 0: None (Transparent) ● 2: Non-transparent (“Warm”) redundancy mode.
SERVICE_LEVEL	BYTE	MW60[1]	OPC UA server health *(see page 124)*, depending on the data and service quality.
Reserved	WORD	MW61	–
SERVICES_STATUS	T_SERVICE S _STATUS	MW62...68	–
NTP_CLIENT_SERVICE	BYTE	MW62[0]	NTP client status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code: ❍ 1 = Invalid Time (Time never updated) ❍ 2 = Time catch up

Element	Type	Address	Description
NTP_SERVER_SERVICE	BYTE	MW62[1]	NTP server status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code (secured mode only): ❍ 1 = Control Port not configured ❍ 2 = NTP client of backplane and server enabled in web pages
SNMP_SERVICE	BYTE	MW63[0]	SNMP server status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code: ❍ 1 = SNMP is enabled in Secured mode and no SNMP IP address is defined in Control Expert (0.0.0.0)
Reserved	BYTE	MW63[1]	–
WEB_SERVER	BYTE	MW64[0]	Web server status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code: ❍ 1 = Non-recoverable detected error
FW_UPGRADE	BYTE	MW64[1]	Firmware upgrade status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code: ❍ 1 = Invalid firmware package or blacklisted firmware package ❍ 2 = Last firmware update was not successful (managed as a non-recoverable detected error)
Reserved	BYTE	MW65[0]	–
Reserved	BYTE	MW65[1]	–
CONTROL_EXPERT_IP_ FORWARDING	BYTE	MW66[0]	Control Expert IP forwarding status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code (Secured mode only): ❍ 1 = Control port not configured
CPU_TO_CPU_IP_ FORWARDING	BYTE	MW66[1	CPU to CPU forwarding status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code (Secured mode only): ❍ 1 = Control port not configured
IPSEC	BYTE	MW67[0]	IPSEC status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code (Secured mode only): ❍ 1 = Control port not configured

Element	Type	Address	Description
Reserved	BYTE	MW67[1]	–
EVENT_LOG_SERVICE	BYTE	MW68[0]	Event log service status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code (Secured mode only): ❍ 1 = Service event log detected error. ❍ 2 = Event log configuration detected error
LOG_SERVER_NOT_ REACHABLE	BYTE	MW68[1]	Log server status: ● Bit 0: 0 = acknowledgement received from syslog server / 1 = No acknowledgement received from syslog server
FW_VERSION	T_FW_ VERSION	MW69...72	Module firmware version.
MAJOR_VERSION	WORD	MW69	Major firmware version.
MINOR_VERSION	WORD	MW70	Minor firmware version.
INTERNAL_REVISION	WORD	MW71	Firmware internal revision.
Reserved	WORD	MW72	–
CONTROL_PORT_STATUS	BYTE	MW73[0]	Control Port IPv4 status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code (Secured mode only): ❍ 1 = Invalid IP ❍ 2 = Duplicate IP
ETH_BKP_PORT_STATUS	BYTE	MW73[1]	Backplane Port IPv4 status: ● Bit 0: 0 = Inactive / 1 = Active ● Bits 4...7: Detected error code (Secured mode only): ❍ 1 = Invalid IP ❍ 2 = Duplicate IP
IN_PACKETS_RATE	UINT	MW74	Number of packets received per second on all Ethernet interfaces.
IN_ERROR_COUNT	UINT	MW75	Number of inbound packets with detected errors since last reset (modulo 65535).
OUT_PACKETS_RATE	UINT	MW76	Number of packets emitted per second on all Ethernet interfaces.
OUT_ERROR_COUNT	UINT	MW77	Number of outbound packets with detected errors since last reset (modulo 65535).
MEM_USED_PERCENT	BYTE	MW78[0]	Percentage of internal RAM used by OPC UA server.
CPU_USED_PERCENT	BYTE	MW78[1]	Percentage of internal CPU used.

Element	Type	Address	Description
CYBERSECURITY_STATUS	T_CYBER SECURITY_ STATUS	MW79...80	Cybersecurity status.
SECURE_MODE	BYTE	MW79[0]	● 0: The module is operating in Secured mode. ● 1: The module is operating in Standard mode.
CYBERSECURITY_STATE	BYTE	MW79[1]	Cybersecurity status: ● 0: Secured mode OFF. (SECURE LED OFF) ● 1: A secure communications enabled and running without detected error. (SECURE LED GREEN) ● 2: Ready to communicate. (SECURE LED FLASHING GREEN) ● 3: Secure communication running with minor detected errors. (SECURE LED FLASHING RED) ● 4: Secure communications stopped because of critical detected error. (SECURE LED RED)
IPSEC_CHANNELS	BYTE	MW80[0]	The number of IPSEC channels opened.
Reserved	BYTE	MW80[1]	–

Configuring the READ_DDT Elementary Function

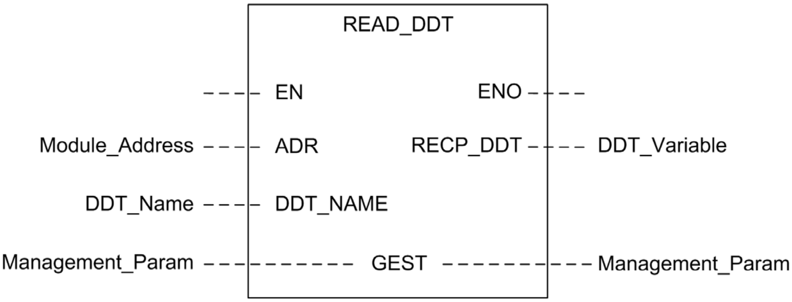
Overview

Use the READ_DDT function block to configure read messages for the BMENUA0100 communication module.

The ADR, the DDT_NAME, and the GEST 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.
ADR	Any Array of INT	Array containing the address of the destination entity of the exchange operation. The address is the result of the ADDMX function. For example: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) indicates the module at IP address 192.168.10.2, with UnitId 100 (local server of the module), connected to the embedded Ethernet port.
DDT_NAME	STRING	Name of DDT to read: T_BMENUA0100

Input/Output Parameters

The GEST array is local:

<table>
<tr><th>Parameter</th><th>Data type</th><th colspan="3">Description</th></tr>
<tr><td rowspan="6">GEST</td><td rowspan="6">Array [0...3] of INT</td><td colspan="3">The management parameters, consisting of four words. Refer to the Control Expert help topic *Structure of the Management Parameters (see EcoStruxure™ Control Expert, Communication, Block Library)* for additional information regarding these parameters.</td></tr>
<tr><td>Word#</td><td><b>Most Significant BYTE</b></td><td><b>Least Significant BYTE</b></td></tr>
<tr><td>0</td><td>Exchange number</td><td>Activity bit: rank 0
Cancel bit: rank 1
Immediate knowledge bit: rank 2</td></tr>
<tr><td>1</td><td>Operation report *(see EcoStruxure™ Control Expert, Communication, Block Library)*</td><td>Communication report *(see EcoStruxure™ Control Expert, Communication, Block Library)*</td></tr>
<tr><td>2</td><td colspan="2">Timeout *(see EcoStruxure™ Control Expert, Communication, Block Library)*</td></tr>
<tr><td>3</td><td colspan="2">Length *(see EcoStruxure™ Control Expert, Communication, Block Library)*</td></tr>
</table>

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.
RECP_DDT	Any	Reception buffer. A DDT variable may be used. Refer to the T_BMENUA0100 DDT description *(see page 115)* for the content of this DDT. The size of the data received (in bytes) is written automatically by the system in the fourth word of the management table.

Considerations when Configuring the Function

When using the READ_DDT EF, consider the following:

- You do not need to specify a value for the length parameter in GEST[3], because there is no data to send. At the end of the operation (when the activity bit in GEST[0] is set to 0), the length will be set with the length of the data copied into the RECP_DDT output parameter if no detected error is reported in GEST[1] or with an additional status code. Refer to the Control Expert help topic *Error Codes of EFBs with STATUS parameter (see EcoStruxure™ Control Expert, Communication, Block Library)* for an description of these additional status code values.
- A timeout value of 0 indicates an infinite waiting period. In this case, a communication delay or loss occurring during the exchange operation is not detected. During this infinite waiting period, the RECP_DDT parameter retains its previous value. To avoid this scenario, set the timeout to a non-zero value.
- In case of operation report 16#01 (Request not processed) or 16#02 (Incorrect response) in the GEST[1] word of the management table, an additional status code may be reported in the length parameter (GEST[3]). Status codes returned in this field correspond to a subrange of the possible STATUS parameter codes of communication EFBs. Possible values for the READ_DDT are 0x30ss and 0x4001. Refer to the Control Expert help topic *Error Codes of EFBs with STATUS parameter (see EcoStruxure™ Control Expert, Communication, Block Library)* for an description of these additional status code values.
- Depending on the DDT specified in the DDT_NAME parameter, some consistency checks will be performed on the data received. If a mismatch is detected, code 16#02 (Incorrect response) is set in the operation report byte (the most significant byte of GEST[1]). Note that the block does not check the data type validity of the variable configured as the reception buffer (RECP_DDT). Verify that the data type of the variable linked to the RECP_DDT parameter matches the type of data received.

⚠ CAUTION

UNEXPECTED BEHAVIOR OF APPLICATION

- Verify that the DDT-type variable associated to the RECP_DDT output parameter corresponds to the type of data written in the reception buffer.
- Verify that the address set in the ADR parameter corresponds to the correct module, especially when several identical modules are configured on the same network.

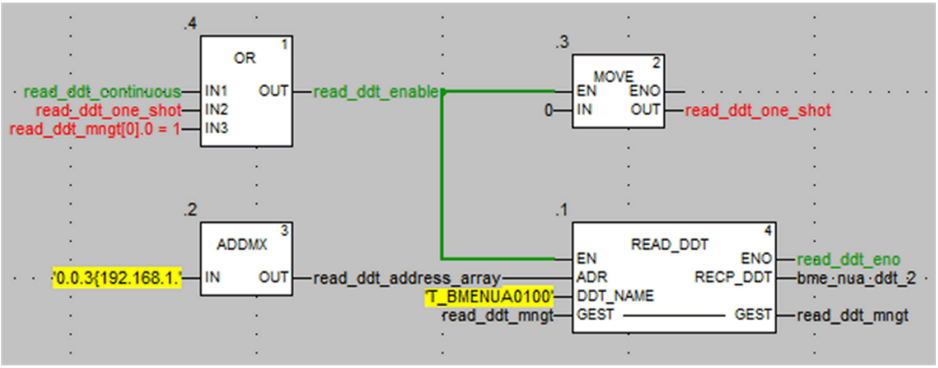
Failure to follow these instructions can result in injury or equipment damage.

Configuring the READ_DDT Elementary Function

To configure the READ_DDT elementary function, follow these steps:

Step	Action
1	Set the address of the destination device in ADR (use an ADDM block to specify this address in an explicit string format).
2	Set DDT_NAME parameter with the name of the DDT to read.
3	Call the READ_DDT function to launch the communication (with EN input pin set to 1 if configured).
4	Monitor the activity bit (in the least significant byte of the GEST[0] parameter) until the communication is completed (the activity bit is set to 0 by the system when the communication has ended). Execute this function only once to avoid erasing the status values. For example, setting the EN pin to 0 during operation would cause the function to be called again.
5	View the report parameters in GEST[1]. If the report reads 16#0000, then RECP_DDT buffer has been filled with received data. Size of the data received (in bytes) is written in the fourth word (GEST[3]) of the management table.

READ_DDT EF Example



In this example, the READ_DDT EF may be started:

- Continuously by setting the read_ddt_continuous variable.
  NOTE: In the event of a detected error, report codes in the second word of the read_ddt_mngt variable cannot be read.
- Only one time, by setting the read_ddt_one_shot variable.

OPC UA Diagnostics

Introduction

The BMENUA0100 module presents both OPC UA server variables and Specific DataItems that can be used to identify the application running in the module, and to diagnose module operations.

OPC UA SERVICE_LEVEL Variable

The SERVICE_LEVEL variable provides information to a client regarding the status of the CPU and the health of the OPC UA server. The SERVICE_LEVEL variable is directly accessible under the OPC UA server node tree. The SERVICE_LEVEL variable is also duplicated in the OPCUA_STATUS.SERVICE_LEVEL element of the BMENUA0100 module DDT *(see page 115)*, and can be programmatically accessed by executing the READ_DDT *(see page 120)* elementary function when the application is in the RUN state.

SERVICE_LEVEL Value	Status of the CPU / OPC UA Server
0	BMENUA0100 is in boot phase. CPU is in NOCONF or ERROR state.
1	OPC UA server has started. Data dictionary list browsing is ongoing.
5	Data dictionary browsing is started.
10	Data dictionary size overflow.
20	Data dictionary type browsing is ongoing.
50	Data dictionary variable browsing is ongoing.
100	Data dictionary browsing is complete. Reading of the CPU status is ongoing.
120[1]	CPU in STOP state.
150[1]	CPU in WAIT STANDBY state (Hot Standby CPU only).
199[1]	CPU in RUN STANDBY state (Hot Standby CPU only).
200...255[2]	CPU in RUN (or RUN PRIMARY for Hot Standby CPU). OPC UA server is fully operational
1. This value does not need to be set before the server becomes operational. 2. The greater the value, the better the server health. A value of 255 indicates the healthiest server state.	

NOTE: The larger the size of the data dictionary, the longer the data dictionary acquisition time (i.e. the time required for the module to browse and load the data dictionary). During data dictionary acquisition, SERVICE_LEVEL remains at the value 100 until acquisition is completed. When a build change is performed in Control Expert generating a new data dictionary, the OPC UA server restarts the process of browsing the data dictionary browsing. During this process updates of the currently monitored items may be halted, with monitored item values frozen at their most recently updated value.

OPC UA Server Variables

You can view these variables online using an OPC UA client device, such as the UaExpert tool from Unified Automation. Navigate the OPC UA server node tree to **ServerStatus** → **BuildInfo** to display the following OPC UA server variables:

Variable	Description
BuildDate	The date the application in the PAC was built.
BuildNumber	The number of the current PAC application build.
ManufacturerName	Always “Schneider Electric”.
ProductName	Always “BMENUA0100”.
ProductUri	The unique Uniform Resource Identifier assigned to the module.
SoftwareVersion	The current version of module firmware.

OPC UA Specific DataItems

The BMENUA0100 module supports the following Specific DataItems. These DataItems are accessible via the OPC UA server stack. While they are much like PAC data items reachable via the Control Expert software, these Special DataItems are not linked to PAC symbols and are not reachable via the Control Expert software:

DataItem	Data type	Default value	Description
#ApplicationName	STRING	0	The PAC application name.
#ApplicationVersion	STRING	0	The PAC application version.
#DeviceIdentity	STRING	0	Always “Schneider Electric”.
#PLCDatadicReady	BYTE	1	Monitors the PAC data dictionary loading status: ● 1: The PAC data dictionary is not available. Possible explanations include: ❍ The data dictionary functionality is not available or enabled in the Control Expert application and cannot be embedded in the PAC. ❍ The loading/browsing of the data dictionary is in progress in OPC UA Server. ● 2: The PAC data dictionary is available, for example: ❍ The loading/browsing of the data dictionary by the OPC UA server completed with success. ❍ A pre-loading (in accordance with Control Expert data dictionary project settings) can be in progress.
#PLCQualStatus	INT16	0	Monitors the communication status of a device. Possible (hex) values include: ● 0x00C0: Communication with the device is correct. ● 0x0040: No communication with the device for a time less than the Device Timeout (5s). ● 0x0: Device is not identified.

Syslog

Introduction

The BMENUA0100 module logs events in a local diagnostic buffer, then sends a record of these events to a remote syslog server where they are stored and made available to syslog clients. To diagnose older events, you can query the syslog server event records. For current module events, you can use the module web pages *(see page 128)* to diagnose the state of the syslog service and to view specified events in the diagnostic buffer.

The local buffer operates as a circular buffer, with the most recent events overwriting and replacing the oldest events when the buffer is full.

The module stores events in volatile memory.

Logged events relate to either:

- Security/Authorization *(see page 127)*
  – or –
- Major changes in the system (log audit) *(see page 128)*

The syslog service is configurable in the web pages *(see page 90)* as part of the cybersecurity configuration and, therefore, can be active only when the module is operating in Secured mode. When the module is operating in Standard mode, the service is deactivated.

NOTE: Syslog is not a natively secure protocol, but must be encapsulated within an IPSEC *(see page 92)* secure channel over the control port.

Syslog Message Structure

The syslog protocol – RFC 5424 – defines how events exchanged between the module and the remote server. The syslog message structure is set forth below:

Field	Description
PRI	Facility and severity information (description provided in following tables).
VERSION	Version of the syslog protocol specification (Version = 1 for RFC 5424.).
TIMESTAMP	Time stamp format is issued from RFC 3339 that recommends the following ISO8601 Internet date and time format: YYY-MM-DD**T**hh:mm:ss.nnn**Z** **NOTE:** **-**, **T**, **:**, **.** , **Z** are mandatory characters and they are part or the time stamp field. **T** and **Z** need to be written in uppercase. **Z** specifies that the time is UTC. Time field content description: **YYY.** Year **MM.** Month **DD.** Day **hh.** Hour **mm.** Month **ss.** Second **nnn.** Fraction of second in millisecond (0 if not available)
HOSTNAME	Identifies the machine that originally sent the syslog message: fully qualified domain name (FQDN) or source static IP address if FQDN is not supported.

Field	Description
APP-NAME	Identifies the application that initiates the syslog message. It contains information that allows to identify the entity that sends the message (for example, subset of commercial reference).
PROCID	Identifies the process, or entity, or component that sends the event. Receives NILVALUE if not used.
MSGID	Identifies the type of message on which the event is related to, for example HTTP, FTP, Modbus. Receives NILVALUE if not used.
MESSAGE TEXT	This field contains several information: ● Issuer address: IP address of the entity that generates the log. ● Peer ID: Peer ID if a peer is involved in the operation (for example, user name for a logging operation). Receives null if not used. ● Peer address: Peer IP address if a peer is involved in the operation. Receives null if not used. ● Type: Unique number to identify a message (description provided in following tables). ● Comment: String that describes the message (description provided in following tables).

Events Related to Security/Authorization

- Failed secure channel opening from OPC UA stack: for example, invalid certificate, expired certificate.
- Successful user sessions (Login/Password) from OPC UA stack (successful login)
  NOTE: In case of no login (Standard mode), the log is disabled so a record of the successful connection is not created.
- Failed user sessions (Login/Password) from OPC UA stack (failed login)
  NOTE: In case of no login (Standard mode), the log is disabled so a record of the unsuccessful connection is not created.
- Successful HTTPS connections to or from a tool (successful login): for example, a connection to the web server or a firmware download via HTTPS.
- Failed HTTPS login to or from a tool: for example, a failed connection to the web server or a failed firmware download via HTTPS.
- Successful user session disconnection (on demand logout) for HTTPS.
- Successful user session disconnection (on demand logout) for OPC UA.
- Automatic logout: for example, an inactivity timeout for either OPC UA or HTTPS.
- Integrity check error detected: for example, a digital signature detected error, or an integrity only (hash) detected error.
- Create a new certificate.
- Remove local certificates. This is accomplished by using the rotary selector switch to set the operating mode to the Security Reset position.
- Add a new client certificate from the whitelist into the device.
- Remove a client certificate from the whitelist into the device.

Events Related to Major Changes in the System (log audit)

- Application or cybersecurity configuration download into the device.
- Firmware download into the device.
- Mismatched signature for firmware that failed to download into the device.

Syslog Web Page Diagnostics

Use the module web pages to diagnose the state of the syslog service running on the module, and to diagnose specified parts of the module’s syslog diagnostic buffer.You can also use the SERVICES_STATUS element of the module DDT *(see page 115)* to view the syslog service status.

In the **Diagnostics** → **Event log diagnostic** menu, use the following commands to view the module syslog service status:

Parameter	Description
Status	● Operational: the module is operating in Secured mode and the syslog service is enabled. ● Not operational: the module is operating in Secured mode but the syslog service is disabled.
Log server	● Reachable: a connection can be established to the remote syslog server. ● Not reachable: a connection cannot be established to the remote syslog server.

In the **Diagnostics** → **Event log diagnostic** menu, in the **Diag Buffer to read** field, input the part of the diagnostic buffer to read.

Modbus Diagnostics

Introduction

You can use Modbus function code commands to perform diagnostics on the BMENUA0100 module. Modbus commands can reach the module only over its backplane port. Because Modbus is not an inherently secure protocol, you need to encapsulate Modbus commands within IPSEC.

Modbus function code 43 / subcode 14 is supported by the BMENUA0100 module.

43/14: Read Device Identification

The following device identification data can be returned using function code 43 / subcode 14:

Category	Object ID	Object Name	Type
Basic	0x00	VendorName	ASCII string
	0x01	ProductCode	ASCII string
	0x02	MajorMinorRevision	ASCII string
Regular	0x03	VendorUrl	ASCII string
	0x04	ProductName	ASCII string
	0x05	ModelName	ASCII string
	0x06	UserApplicationName	ASCII string
	0x07...0xFF	Reserved	ASCII string

NOTE: In Secure mode, the BMENUA0100 accepts the Modbus TCP/IP client data flow only from the M580 CPU.

SNMP Diagnostics

Introduction

The BMENUA0100 module enables SNMP diagnostics in the TCP/IP-based Ethernet network by supporting the following MIBs:

- MIB-II
- Link Layer Discovery Protocol (LLDP) MIB

MIB-II

MIB-II provides an SNMP manager with a collection of device management variables. By reading these variables, an SNMP manager can diagnose the operation of a specific device, such as the BMENUA0100.

LLDP MIB

The LLDP MIB contains data collected by operation of the link layer discovery protocol relating to the identity, capabilities, and location on the Ethernet network. Using the LLDP MIB, an SNMP manager can discover the topology of the network and the capabilities of the network devices.

NOTE: SNMP communication of LLDP MIB data is made exclusively over the backplane port.

OPC UA Diagnostics

Introduction

Use the **OPC UA Diagnostics** web page to view dynamic data describing the operation of the OPC UA server embedded in the BMENUA0100 module.

Viewable Data

OPC UA Diagnostics web page displays the following read-only data. Note that all numeric values are in decimal format:

Field	Description
EPAC	CPU IP address.
Device Identity	CPU part number.
Device Version	CPU firmware version.
Device Status	Connection status with CPU: Good, Bad, Uncertain, Unknown, Missing.
Frame Time Out (in ms)	The maximum length of time the OPC UA server will wait for an answer from a device after sending a request. For example, 1000.
Device Time Out (in ms)	Delay for the status change of the device (Missing, Unknown or OK). For example, 5000.
Maximum Channel number	Number of connections opened by OPC UA server on the CPU.
Maximum Pending Request number	Maximum number of requests authorized to be pending (awaiting response).
Request Length	Length of request for communication with CPU.
Number of All Variable descriptor(s)	All CPU variables + specific DataItems requested by OPC UA client.
Number of Specific Variable descriptor(s)	All specific DataItems requested by OPC UA client.
Number of non Specific Variable descriptor(s)	All CPU variables requested by OPC UA client.
Current number of timers (different sampling intervals)	Number or requested sampling intervals, for all subscriptions.
Application Name (Device)	Control Expert project name.
Application Version (Device)	Application checksum and signatures.
Preload data dictionary	Available or Unavailable for application in PAC.

Chapter 8
Optimizing BMENUA0100 Performance

Optimizing BMENUA0100 Performance

Introduction

When optimizing performance of the BMENUA0100, consider the entire system. Pay particular attention to the overall communication efficiency and workload within the network architecture that includes the BMENUA0100 modules. It is in this context that OPC UA client performance optimizations also impact the OPC UA communication effectiveness.

Several settings, at different levels of the architecture, can enhance system performance or make your system more stable and robust during each of the operating mode phases (connections, browse, subscription, monitoring, and so forth).

Performance Example

An OPC UA client can monitor up to 20 000 items in Standard cybersecurity mode.

Example based on:

- BMEP584040 with a MAST task cycle time at 20ms (CPU load less than 80%).
- BMENUA0100 in rotary switch position Standard (i.e. no secure communication, no IPSec channel).
- OPC UA client (UAExpert) initiates communication with Message Security mode set to **None** and monitors 20,000 items by reference to variables based on array of ‘INT’ type from a BMENUA0100 OPC UA server. This server is configured with Publishing Interval to 1 second, Sampling Interval to 1 second, session Timeout to 30 seconds.
- No other communication than OPC UA.

How to Adjust the Performance

Exchange data structure

The Data application memory of the CPU is organized depending on the Data application definition in Control Expert. The more the variable declaration is structured, the more the BMENUA0100 Server generates optimized requests for access to the variables and to the Data Dictionary in Run time.

Thus, for the variables that are accessed by the OPC UA Client, it is recommended to:

- Use Arrays or Data structure whenever possible.
- Enable the option **Only HMI variable** in **PLC embedded data** of the **Project Settings**and set only these variables with the attribute **HMI** to reduce the size of the Data Dictionary.
- In the CPU Safety process, to reduce the data dictionary size, de-select the option **Usage of Process Namespace** (in **Project Settings** → **General** → **PLC embedded data** → **Data dictionary**.

CPU communication capabilities

The capability of the communication system depends on the M580 CPU model and some configuration setting. The CPU model determines:

- The system-wide CPU processing performance capabilities.
- The number of requests per cycle that can be processed, even if configurable by System word %SW90.
- The maximum number of channels available to each BMENUA0100 for establishing connections to the M580 CPU *(see page 141)*.

In addition, the less the MAST cycle time, the greater the number of communication requests that can be processed. Thus, the performance level is directly dependent to the MAST cycle time.

OPC UA client, configuration and usage

The number of monitored variables impacts the performance. The Sampling Rates and Publishing intervals configured for each OPC UA client determine the number of requests needed to animate the variables. Keep in mind that, when several OPC UA clients are connected to the same BMENUA0100 OPC UA server, when the Sampling Rates and Publishing intervals are different in each OPC UA client sides, this configuration generates more requests.

All timeout values configurable from OPC UA client (Browse, Connect, Publish, Session, Watchdog…) need to be tuned to optimize and stabilize - to the extent possible - your overall system. As a side effect, these timeouts could impact the system performance.

Depending on the Message Security mode (None, Sign, Sign&Encrypt), the algorithm to treat the signature and the encryption takes additional time.

CPU to CPU and Control Expert to CPU communications

Each IPSec tunnel used to secure the communications other than OPC UA or HTTPS slows down the traffic, especially when the setting **Confidentiality** is enabled, thereby generating encryption and decryption.

How to Monitor the Performance

There are several ways to monitor performance.

Using Control Expert

Using Control Expert in connected mode, you can access the effective MAST cycle time and the M580 CPU load for the system, for each task and for the total of all tasks by reading the system words %SW110 to %SW116. In addition, the M580 CPU DDDT and the BMENUA0100 DDT can provide different diagnostic information linked to the system performance of the PAC, such as:

- The Service Level of the OPC UA server.
- The number of connected OPC UA clients.
- The data dictionary status, acquisition time, preload duration.
- The Ethernet service status.
- The network health.
- The control port and the backplane port status.
- The number of Ethernet packets per second.
- The number of Ethernet packets that contain detected errors.
- The percentage of BMENUA0100 CPU load and used memory.
- The number of IPSec channels opened.

Using BMENUA0100 Web site

The Home page and the Diagnostic page of the BMENUA0100 Web site provide interesting information related to the performance of OPC UA servers. Some information comes from the BMENUA0100 DDT, and other information is given by the OPC UA server itself:

- Number of monitored items.
- Number of monitored specific items.
- The different sampling intervals currently in execution.
- The number of generated requests for the current animations.
- Detected overruns.
- Number of connected clients.

Using OPC UA client

The OPC UA client can monitor directly some specific items under the OPC UA server, but also the ServiceLevel variable or some BMENUA0100 DDT subfields on demand through application variables.

Other services for diagnostic

In a more technical approach, the SNMP agent and the Syslog server of the BMENUA0100 module can help to get other diagnostic information linked to the performance of the OPC UA servers.

Chapter 9
Firmware Upgrade

EcoStruxure™ Maintenance Expert Tool

Introducing the EcoStruxure™ Maintenance Expert Tool

Use the EcoStruxure™ Maintenance Expert tool to upgrade the firmware of the BMENUA0100 module. EcoStruxure™ Maintenance Expert is a web-based tool that enables you to:

- Automatically or manually discover one or more BMENUA0100 modules in your project based on IP addresses.
- Upgrade the latest firmware version to BMENUA0100 modules over the web.

For details on how to install and use the EcoStruxure™ Maintenance Expert tool, refer to the online help *(see EcoStruxure™ Maintenance Expert, Firmware Upgrade Tool, Online Help)*.

NOTE: Schneider Electric’s Unity Loader™ software tool is not usable for upgrading firmware for the BMENUA0100 module. You cannot connect the Unity Loader software to the BMENUA0100 module control port for the purpose of downloading projects or upgrading CPU or module firmware.

Appendices

What Is in This Appendix?

The appendix contains the following chapters:

Appendix A
CPU Connections

OPC UA Server to CPU Connections

Opened Connections

The number of connections the BMENUA0100 module can open to the M580 CPU depends on the capacity of the CPU. Thus, performance of the BMENUA0100 module will depend on the time required to perform the MAST task and the selected CPU. The maximum number of connections opened by each BMENUA0100 module to the M580 CPU are as follows:

CPU Model	Maximum Number of Connections Opened by each BMENUA0100
BMEP581020	7
BMEP5820•0	7
BMEP5830•0	10
BMEP5840•0	13
BMEP585040	13
BMEP586040	16
BMEH582040	7
BMEH584040	13
BMEH586040	16

Appendix B
IPSEC Windows Scripts

IKE/IPSEC Windows Firewall Configuration Scripts

Introduction

To run IPSEC on a PC that hosts either the Control Expert configuration software or an OPC UA client (e.g. SCADA), you need to run a script that will configure on the host firewall:

- IKE/IPSEC in **transport** mode for the data flows that are local to the BMENUA0100.
- IKE/IPSEC in **tunnel** mode for the data flows that are forwarded to the Ethernet backplane.
- Passthrough rules for OPC UA and HTTPS.

The following examples present Windows firewall configuration scripts with and without IPSEC confidentiality.

In each script example, you need to provide actual values for the following variables:

- **`endpoint1`**: the remote IP address value in the IPSEC configuration.
- **`endpoint2`**: the BMENUA0100 control port IP address.
- **`Auth1psk`**: the PSK setting in the IPSEC configuration.

Windows Firewall Script With Confidentiality

NOTE: If confidentiality is enabled in the IPSEC configuration, `qmsecmethods=esp:sha256-aes128`

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess

netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"

netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout description="IPSECtransport" mode=transport enable=yes profile=public type=static protocol=any auth1=computerpsk auth1psk=b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-aes128+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA" endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=noauthentication description="IPSECpassthroughOPCUA" mode=transport enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS" endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=noauthentication description="IPSECpassthroughHTTPS" mode=transport enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=192.169.1.100 remotetunnelendpoint=192.169.1.50 action=requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes profile=public type=static protocol=any auth1=computerpsk auth1psk= b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-aes128+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Windows Firewall Script Without Confidentiality

NOTE: If confidentiality is enabled in the IPSEC configuration, `qmsecmethods=esp:sha256-None`

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess

netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"

netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout description="IPSECtransport" mode=transport enable=yes profile=public type=static protocol=any auth1=computerpsk auth1psk= b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-None+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA" endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=noauthentication description="IPSECpassthroughOPCUA" mode=transport enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS" endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=noauthentication description="IPSECpassthroughHTTPS" mode=transport enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=192.169.1.100 remotetunnelendpoint=192.169.1.50 action=requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes profile=public type=static protocol=any auth1=computerpsk auth1psk= b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-None+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Glossary

B

broadcast

A message sent to all devices in a broadcast domain.

H

harsh environment

Resistance to hydrocarbons, industrial oils, detergents and solder chips. Relative humidity up to 100%, saline atmosphere, significant temperature variations, operating temperature between -10°C and + 70°C, or in mobile installations. For hardened (H) devices, the relative humidity is up to 95% and the operating temperature is between -25°C and + 70°C.

I

IP address

The 32-bit identifier, consisting of both a network address and a host address assigned to a device connected to a TCP/IP network.

M

multicast

A special form of broadcast where copies of the packet are delivered to only a specified subset of network destinations. Implicit messaging typically uses multicast format for communications in an EtherNet/IP network.

S

SNTP

(*simple network time protocol*) See NTP.

T

trap

A trap is an event directed by an SNMP agent that indicates one of these events:

- A change has occurred in the status of an agent.
- An unauthorized SNMP manager device has attempted to get data from (or change data on) an SNMP agent.

Index