Modicon Platform

Cybersecurity

User Guide

Original instructions

EIO0000001999.15
07/2026

www.se.com

Legal Information

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

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

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

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

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

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

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

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

Table of Contents

Table of Contents 3
Safety Information 5
Before You Begin 6
Start-up and Test 7
Operation and Adjustments 8
About the Document 9
Presentation 17
Schneider Electric Guidelines 17
How to Help Secure the Architecture 19
System View 19
Setting Passwords in Control Expert 21
Hardening the PC 23
Disable Unused Embedded Communication Services 31
Restrict Data Flow from Control Network (Access Control) 32
Set Up Encrypted Communication 35
CSPN Security Target 42
Set Up Cybersecurity Audit (Event Logging) 50
Event Log Message Descriptions for Control Expert 58
Event Log Message Descriptions M580 Controllers (as of Firmware Version V4.10), and BMENOR2200H (as of Firmware Version 3.01) 64
Event Log Message Descriptions for M580 Controllers (firmware earlier than V4.10), BMENUA0100 (firmware V3.01 or later) and BMENOR2200H 77
Control Identification and Authentication 90
Control Authorizations 95
Manage Data Integrity Checks 98
Configure a Secure Engineering Link between Control Expert and an M580 Ethernet Controller 102
Features of a Secure Connection 103
Configure a Secure Connection Procedure 105
Operating Mode Considerations 107
Enforced Secure Programming Compatibility and Limitations 108

Communication Adapter Compatibility 110
M580 Ethernet Services and Ports..... 115
Cybersecurity Services Per System 117
Cybersecurity Services 117
Modicon M340 Security Services..... 124
Modicon M580 Security Services..... 124
Modicon Quantum Security Services 125
Modicon X80 Security Services 127
Modicon Premium/Atrium Security Services 129
Modicon Momentum MDI Security Services 130
Modicon MC80 Security Services 131
How to Help Protect M580, M340, Momentum MDI, and MC80 Architecture with EAGLE40 using VPN..... 132
EAGLE40 Firewall..... 132
Prerequisites 133
Typical Architecture 134
Configuring the Firewall 134
Glossary..... 143
Index..... 166

Safety Information

Important Information

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please Note

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

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

Before You Begin

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

⚠ WARNING

UNGUARDED EQUIPMENT

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

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

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

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

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and

other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

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

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

Start-up and Test

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

⚠ WARNING

EQUIPMENT OPERATION HAZARD

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

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

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

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

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

Before energizing equipment:

- Remove tools, meters, and debris from equipment.

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

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

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

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

About the Document

Document Scope

This guide defines the cybersecurity elements that help you configure a system that is less susceptible to cyber attacks.

NOTE: The terms security, secure, secured, and securing are used throughout this document in reference to cybersecurity topics.

Validity Note

This document has been updated for EcoStruxure™ Control Expert V16.4.

Product Related Information

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

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

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

⚠ WARNING

LOSS OF CONTROL

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

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

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

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

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

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION, LOSS OF CONTROL, LOSS OF DATA

You, and anyone owning, designing, operating and/or maintaining equipment using EcoStruxure Control Expert, must read, understand, and follow the instructions outlined in the present document.

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

Information Related to Cybersecurity

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

Documents available for download in the cybersecurity support section:

Title of documentation	Webpage address
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations	www.se.com/ww/en/download/document/STN v2

Available Languages of the Document

The document is available in these languages:

- Chinese (EIO0000002004)
- English (EIO0000001999)
- French (EIO0000002001)
- German (EIO0000002000)
- Italian (EIO0000002002)
- Spanish (EIO0000002003)

Related Documents

Title of documentation	Commercial reference number
Modicon M580 System Planning Guide	HRB65322 (CHS) HRB62666 (ENG) HRB65318 (FRE) HRB65319 (GER) RB65320 (ITA) HRB65321 (SPA)
Modicon M580 Hardware Reference Guide	EIO0000001583 (CHS) EIO0000001578 (ENG) EIO0000001579 (FRE) EIO0000001580 (GER) EIO0000001582 (ITA) EIO0000001581 (SPA)
Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Communications Module, Installation and Configuration Guide	HRB65316 (CHS) HRB62665 (ENG) HRB65311 (FRE) HRB65313 (GER) HRB65314 (ITA) HRB65315 (SPA)
Modicon M340 for Ethernet, Communications Modules and Processors, User Manual	31007493 (CHS) 31007131 (ENG) 31007132 (FRE) 31007133 (GER) 31007494 (ITA) 31007134 (SPA)
Quantum using EcoStruxure™ Control Expert, TCP/IP Configuration, User Manual	31007110 (CHS) 33002467 (ENG) 33002468 (FRE) 33002469 (GER) 31008078 (ITA) 33002470 (SPA)
Premium and Atrium using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual	31007102 (CHS) 35006192 (ENG) 35006193 (FRE) 35006194 (GER) 31007214 (ITA) 35006195 (SPA)
EcoStruxure™ Control Expert, Operating Modes	33003697 (CHS) 33003101 (ENG) 33003102 (FRE) 33003103 (GER) 33003696 (ITA) 33003104 (SPA)

Title of documentation	Commercial reference number
Quantum using EcoStruxure™ Control Expert, Hardware Reference Manual	35012184 (CHS) 35010529 (ENG) 35010530 (FRE) 35010531 (GER) 35013975 (ITA) 35010532 (SPA)
Quantum using EcoStruxure™ Control Expert, 140NOC77101, Ethernet Communication Module, User Manual	S1A33993 (CHS) S1A33985 (ENG) S1A33986 (FRE) S1A33987 (GER) S1A33989 (ITA) S1A33988 (SPA)
Premium using EcoStruxure™ Control Expert, TSXETC101, Ethernet Communication Module, User Manual	S1A34008 (CHS) S1A34003 (ENG) S1A34004 (FRE) S1A34005 (GER) S1A34007 (ITA) S1A34006 (SPA)
Modicon M340, BMXNOC0401 Ethernet Communication Module, User Manual	S1A34014 (CHS) S1A34009 (ENG) S1A34010 (FRE) S1A34011 (GER) S1A34013 (ITA) S1A34012 (Spanish)
Quantum EIO, Control Network, Installation and Configuration Guide	S1A48999 (CHS) S1A48993 (ENG) S1A48994 (FRE) S1A48995 (GER) S1A48997 (ITA) S1A48998 (Spanish)
EcoStruxure™ Control Expert, Communication, Block Library	33003683 (CHS) 33002527 (ENG) 33002528 (FRE) 33002529 (GER) 33003682 (ITA) 33002530 (SPA)
Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual	31007112 (CHS) 33002479 (ENG) 33002480 (FRE) 33002481 (GER) 31007213 (ITA) 33002482 (SPA)
Modicon M580 BMECXM CANopen Modules, User Manual	EIO0000002134 (CHS) EIO0000002129 (ENG) EIO0000002130 (FRE) EIO0000002131 (GER) EIO0000002132 (ITA) EIO0000002133 (SPA)

Title of documentation	Commercial reference number
EcoStruxure Automation Device Maintenance Firmware Upgrade Tool	EIO0000004050 (CHS) EIO0000004033 (ENG) EIO0000004046 (GER) EIO0000004048 (FRE) EIO0000004049 (ITA) EIO0000004047 (SPA)
Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide	HRB44124 (ENG)
Modicon MC80 Program Logic Controller (PLC) User Manual	EIO0000002071 (ENG)

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

Terminology Derived from Standards

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

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

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2020	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design

Standard	Description
IEC 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

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

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems
IEC 62443 series	Security for industrial automation and control systems

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

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

Information on Non-Inclusive or Insensitive Terminology

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

Presentation

Introduction

The goal of this book is to present the cybersecurity solutions implemented in Modicon controllers and associated software applications. In addition to the solutions presented in this book, apply the guidelines provided in Schneider Electric cybersecurity technical notes available on the Schneider Electric website.

Schneider Electric Guidelines

Introduction

Your PC system can run various applications to help enhance security in your control environment. The system has factory default settings that require re-configuration to align with Schneider Electric device hardening guidelines of the defense-in-depth approach.

A topic dedicated to cybersecurity is available in the support area of the Schneider Electric website.

Defense-In-Depth Approach

In addition to the solutions presented in the present document, follow the Schneider Electric defense-in-depth approach as described in the following documents:

- **Book title:** How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations
- **Website link description (book description):** How Can I Reduce Vulnerability to Cyber Attacks in PlantStruxure Architectures?

Managing Vulnerabilities

Reported vulnerabilities from Schneider Electric devices are documented in the **Cybersecurity support** web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page.

A list of security notifications can be accessed by clicking **Security Notifications** which takes you to: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp.

If you face a cybersecurity incident or vulnerability not mentioned in the list provided by Schneider Electric, you can report this incident or vulnerability by clicking **Report a Vulnerability** on the **Cybersecurity support** web page to open: https://www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp

How to Help Secure the Architecture

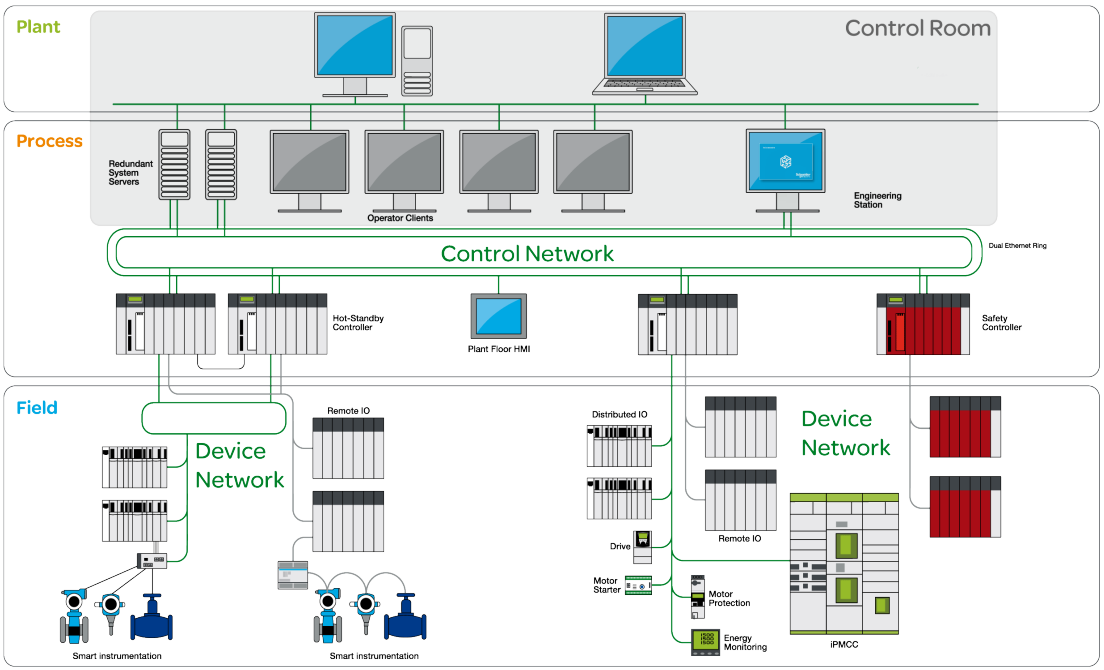
Introduction

This chapter describes how to help make Modicon controllers more secure.

System View

System Architecture

The following architecture highlights the necessity to have a multi-layered architecture (with a control network and a device network) that can be more secured. A flat architecture (all equipment connected to the same network) cannot be secured properly.



More Secured Communication

Equipment in the control room is more exposed to attacks than equipment connected to the device network. Therefore, implement more secured communication between the control room and the controller and devices. Isolate the device network from the other network levels (such as control networks and remote networks).

In the system architecture above, the control room area is grayed to distinguish it from the controller and other devices.

More Secured Access to the USB Ports

Physical access to the USB ports must be controlled.

NOTE: Securing the USB ports can be done only by physical means (for example cabinet or physical key).

More Secured Access to the Hot Standby Link and Device Network

Control the physical access to the Hot Standby link and to the device network.

Testing

Control Expert provides a simulator to test your application before commissioning it as part of your industrial automation system. The simulator conforms to the cybersecurity requirements.

- The simulator can be operated only with an application open in Control Expert.
- The application open in the simulator cannot be uploaded from the simulator to the controller.

For information on how to operate the simulator, refer to the help for the *EcoStruxure™ Control Expert, Controller Simulator* (https://youtu.be/RrkorSe0G8s)..

Setting Passwords in Control Expert

Use Control Expert software to set passwords that help secure your project. The following passwords can be set:

- Application password, with or without file encryption
- Safety-related area password
- Firmware upgrade password
- Program unit, section, and subroutine password
- Data storage/web password

Application Password

Control Expert provides a password mechanism to help guard against unauthorized access to the application. Control Expert uses the password when you:

- Open the application in Control Expert.
- Connect to the controller in Control Expert.

Application protection by a password helps prevent unwanted application modification, download, or opening of application files. The password is stored encrypted in the application.

In addition to the password protection, you can encrypt the .STU, .STA and .ZEF files. The file encryption feature in Control Expert helps prevent unauthorized modifications by unqualified personnel and reinforces protection against theft of intellectual property and other malicious intentions. The file encryption option is protected by a password mechanism.

NOTE: When a controller is managed as part of a system project, the application password and file encryption are disabled.

For information on how to set and use application passwords, refer to the *Application Protection* topic in the *EcoStruxure™ Control Expert, Operating Modes* guide.

Safety-Related Area Password

Safety controllers include a safety-related area password protection function, which is accessible from the **Properties** screen of the project. This function is used to help protect project elements located within the safety-related area of the functional safety project.

When the safety-related area password protection function is active, the safety-related parts of the application cannot be modified.

For information on how to set and use safety-related area passwords, refer to the *Safety-related Area Password Protection* topic in the *EcoStruxure™ Control Expert, Operating Modes* guide.

Firmware Update Password

Firmware protection by a password helps prevent unwanted access to the module firmware.

For M580 controllers, management of the firmware updates depends on the controller firmware version used to create the application.

For controller firmware versions earlier than 4.01:

- Firmware update is managed using FTP.
- Firmware update access *can* be password protected.

For controller firmware versions 4.01 and later:

- Firmware update access is managed using HTTPS (more secure than FTP).
- Firmware update access *must* be password protected.
- Data storage and web page access are protected using the same password.

For information on how to set and use firmware passwords, refer to the *Firmware Protection* topic in the *EcoStruxure™ Control Expert, Operating Modes* guide.

Program Unit, Section, and Subroutine Password

The program unit, section, and subroutine protection function, when enabled, uses a password to help protect these program elements. This function can be set and accessed from the **Properties** screen of the project in offline mode.

For information on how to set and use program unit, section, and sub-routing passwords, refer to the *Program Unit, Section, and Subroutine Protection* topic in the *EcoStruxure™ Control Expert, Operating Modes* guide.

Data Storage/Web Password

Protection by a password helps prevent unwanted access to the data storage zone of the SD memory card (if a valid card is inserted in the controller).

For M580 controllers in a project created by Control Expert with a version:

- Earlier than version 15.1, you can provide password protection for data storage access.
- Version 15.1 and later, you can provide password protection for both web diagnostics and data storage access.

For M580 controllers, management of the Data Storage and Web interfaces depends on the controller firmware version used to create the application.

For controller firmware versions earlier than 4.01:

- Data storage is managed using FTP.
- Data storage access *can* be password protected.
- Web page access cannot be password protected.

For controller firmware versions 4.01 and later:

- Data storage is managed using HTTPS (more secure than FTP).
- Both data storage and web page access *must* be password protected.
- Data storage and web page access are protected using the same password.

For information on how to set and use data storage/web passwords, refer to the *Data Storage/Web Protection* topic in the *EcoStruxure™ Control Expert, Operating Modes* guide.

Hardening the PC

Workstation PCs located in the control room are highly exposed to attacks. Those PCs supporting EcoStruxure™ Control Expert or EcoStruxure™ Server Expert need to be hardened.

As these applications all run on the Windows OS, this chapter offers guidelines on how to how to harden a PC by focusing on security for Windows 10.

Hardening the Engineering Workstation

The following key features are used to help secure the workstation. Click on an item for more information about that feature:

- Attack Surface Reduction, page 24
- Security Policy Configuration and Checking, page 24
- User Account Management, page 25
- Access Control Management, page 25

- Securing Network Services, page 26, including:
  - Disabling Remote Desktop Protocol, page 27
  - Disabling LANMAN and NTLM, page 27
  - Disabling Unused Network Interface Cards, page 28
  - Configuring the Local Area Connection, page 28
- Enable or Install Antivirus Protection Tool, page 28
- Systematic Patch Management, page 29
- Backup Management, page 29
- Confidentiality Management, page 30
- Audit Management, page 30

This topic also includes references to several Windows 10 cybersecurity configuration guides, page 30.

Attack Surface Reduction

The attack surface of your networked system is the collection of areas where an intruder can attempt to add or extract data.

To help reduce the potential attack surface:

- Disable all software applications, services, and communication ports that are not used.
- Disable or restrict access to removable storage devices (for example, USB).
- Use the workstation for only a single function (for example, install OPC UA Server Expert and Control Expert on different PCs).

Security Policy Configuration and Checking

Windows Security Policy can be set through Group Policy objects.

A Group Policy Object (GPO) is a set of configuration changes that can be applied to a PC workstation. For more information about Local Group Policy Editor, refer to the security configuration guides from the Center for Internet Security (CIS) referenced below, page 30.

Domain GPOs can also be defined in Windows Active Directory.

Security configurations need to be checked regularly and automatically.

User Account Management

- **Change Default Passwords**:

  Before deploying any new asset, change all default passwords to values that are consistent with administrative level accounts.

  Disable Windows automatic login.

  For a description of Windows account password settings, refer to the security configuration guides from the Center for Internet Security (CIS) referenced below, page 30.

- **Setup User Accounts**:

  The user accounts can be defined either locally (workgroup) on a standalone computer or through a Windows Active Directory domain controller that allow to centralize the management of all users in a system.

  Follow these guidelines when setting up user accounts:

  - Use a standard individual user account (without Administrator privilege) to run the software applications that are configured to run as standalone applications (for example, Control Expert).
  - Use a local system account for the software applications that are configured to run as a Service (for example, OFS UA).
  - Use a dedicated Administrative account to install the software applications and to configure IPSec.
  - Set up a password manager to manage your passwords (for example, KeyPass).
  - Disable all accounts that are not associated to business (for example, Debug accounts). Refer to CIS control 16.8, page 30.
  - Automatically disable dormant accounts after a set period of inactivity. Refer to CIS control 16.9, page 30.
  - Automatically lock workstation sessions after a standard period of inactivity. Refer to CIS control 16.11, page 30.

Access Control Management

Access to all information stored on systems with file system, network share, claims, application, or database needs to be controlled. These controls enforce the **Least Privilege Principle**, meaning that only authorized individuals can access information, and the information they can access is the information they minimally require given their responsibilities.

Permissions are related to objects. Depending on the objects, permission can be implemented based on:

- Windows Active Directory objects.
- NTFS Files access through discretionary access control list (DACLs).
- Shared folder permissions.
- Remote Registry service (enable/disable).

Privileges are user rights that are not tied to an object, but are instead machine-specific. They can be managed through Group Policy settings, for example, “Removable storage access” settings in Local group policy editor can restrict access to USB device storage (read or write).

Helping Secure Network Services

Uninstall or disable unnecessary or unused network services.

There are several ways to disable a service (Services Tool, Security Template, Group Policy Objet, PowerShell, SC.exe).

Use Windows firewall with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

- **Firewall usage**:

  The Windows firewall is needed for IPSEC configuration on Windows 10. In recent versions of Windows operating systems, including Windows 10, the firewall is enabled by default. More details on Windows Firewall settings refer to the security configuration guides from the Center for Internet Security (CIS) referenced below.

- **Server Manager tool**:

  Server Manager lets you view all the dependencies of a feature so you can determine if it is wise to remove it from a Windows Server.

  Server roles can be selected (for example, Web Server (IIS), DNS Server, and so forth).

  Server features can be selected (for example, BitLocker, .NET Framework, and so forth).

- **Internet Information Server (IIS) – Web Server Security**:

  Use a minimal installation of the latest version.

  Configure IIS Access Control (TLS and user authentication).

  Enable logging and review the logs for hacking signatures.

  More details on IIS settings are provided in the CIS benchmark document (Refer to the link, below, page 30.

- **Disabling SMBv1**:

  Server Message Block version 1 (SMBv1) is a protocol used for sharing services (such as printing, files and communication) between PCs on a network. SMBv1 has been demonstrated to present the vulnerability of allowing remote code execution on the host PC.

  You can disable SMBv1 to help minimize vulnerabilities.

Disabling the Remote Desktop Protocol

Schneider Electric's defense-in-depth approach guidelines include disabling remote desktop protocol (RDP) unless your application requires the RDP. The following steps describe how to disable the protocol:

Step	Action
1	In Windows 10, disable RDP using **Computer** > **System Properties** > **Advanced System Settings**.
2	On the **Remote** tab, deselect the **Allow Remote Assistance Connections to this Computer** check box.
3	Select the **Don't Allow Connection to this Computer** check box.

Disabling LANMAN and NTLM

Disable both the Microsoft LAN Manager protocol (LANMAN) and its successor NT LAN Manager (NTLM) to help minimize vulnerabilities.

The following steps describe how to disable LANMAN and NTLM in a Windows 10 system:

Step	Action
1	In a command window, execute `secpol.msc` to open the **Local Security Policy** window.
2	Open **Security Settings** > **Local Policies** > **Security Options**.
3	Select **Send NTLMv2 response only. Refuse LM & NTLM** in the **Network Security: LAN Manager authentication level** field.
4	Select the **Network Security: Do not store LAN Manager hash value on next password change** check box.
5	In a command window, enter `gpupdate` to commit the changed security policy.

Disabling Unused Network Interface Cards

Disable network interface cards not required by the application. For example, if your system has 2 cards and the application uses only one, verify that the other network card (Local Area Connection 2) is disabled.

To disable a network card in Windows 10:

Step	Action
1	Open **Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings**.
2	Right-click the unused connection. Select **Disable**.

Configuring the Local Area Connection

Various Windows network settings provide enhanced security aligned with the defense-in-depth approach.

In Windows 10 systems, access these settings by opening **Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings > Local Area Connection (x).**

This list is an example of the configuration changes you might make to your system on the **Local Area Connection Properties** screen:

- Disable all IPv6 stacks on their respective network cards.
- Deselect all **Local Area Connection Properties** items except for **QoS Packet Scheduler** and **Internet Protocol Version 4**.
- Under the **Wins** tab on **Advanced TCP/IP Settings**, deselect the **Enable LMHOSTS** and **Disable NetBIOS over TCP/IP** check boxes.
- Enable **File and Print Sharing for Microsoft Network**.

Schneider Electric's defense-in-depth guidelines also include the following:

- Define only static IPv4 addresses, subnet masks, and gateways.
- Do not use DHCP or DNS in the control room.

Enable or Install Antivirus Protection Tools

You can improve the system response against viruses and malicious code using your built-in tools in Windows 10. You can also install additional antivirus software if necessary.

Enterprise editions of Windows 10 include *Windows Defender Advanced Threat Protection*, a security platform that monitors endpoints, such as Windows 10 PCs using behavioral sensors. Microsoft's *SmartScreen* technology is another built-in feature that scans, downloads and blocks the access to websites and downloads that are known to be malicious.

More details on *Windows Defender* settings are provided in the Center for Internet Security (CIS) document referenced below, including:

- Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis (CIS Control 8.2).
- Configure Anti-Malware Scanning of Removable Media: USB (Refer to CIS Control 8.4), page 30.
- Configure devices to not auto-run content from removable media: USB (Refer to CIS control 8.5), page 30.

Systematic Patch Management

Always install the last stable version of any security-related updates of the Operating System, Applications (including web browsers and e-mail client), Drivers.

Enable auto update in Windows 10.

More details are provided in the Center for Internet Security (CIS) document referenced below, page 30.

Backup Management

Ensure that:

- All system data is automatically backed up on a regular basis (Refer to CIS control 10.1), page 30.
- The organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system. (Refer to CIS control 10.2), page 30.
- Backups are properly protected using physical security or encryption when they are stored, and also when they are moved across the network. This includes remote backups and cloud services. (Refer to CIS control 10.4), page 30.
- All backups have at least one offline (not accessible using a network connection) backup destination (Refer to CIS control 10.5), page 30.

You can:

- Use *File History* and other free tools in Windows 10 to create file backups.

- Create a recovery drive to restore your system from an image backup.
- Use a storage-sync-and-share service, to put your backups in the cloud, like *OneDrive*, *Dropbox*, or *Google Drive*.

More details on Windows File History, backup/restore settings are provided in CIS document referenced below.

Confidentiality Management

Remove sensitive data or systems not regularly accessed by the organization from the network. These systems can be used as stand-alone systems (disconnected from the network) of the business unit that needs to occasionally use them, or can be completely virtualized and powered off until needed. Refer to the CIS document referenced below. (Refer to CIS control 13.2), page 30.

Turn on disk encryption with *Bitlocker*. More details on *Bitlocker* settings are provided in the CIS Document referenced below.

Audit Management

Ensure that local security logging has been configured on Windows hosts. For details on Audit Policy configuration, refer to the CIS Document referenced below, page 30.

Windows 10 Cybersecurity Configuration Guides

Have a complete set of Windows 10 Cybersecurity settings to use Windows configuration guides, including:

- Security configuration guides from Center for Internet Security – CIS

  https://www.cisecurity.org/press-release/cis-controls-microsoft-windows-10-cyber-hygiene-guide/

  - IG1 Level:

    https://www.cisecurity.org/cis-benchmarks/

    https://www.cisecurity.org/benchmark/microsoft_windows_desktop/

    https://www.cisecurity.org/benchmark/microsoft_iis/
- Security configuration guidelines developed by United States Department of Defense (DISA STIG)

  https://www.stigviewer.com/stig/windows_10/2020-06-15/

Both the "CIS benchmarks" document and “STIG Windows 10 Security technical implementation guide” propose optional profiles. Your choice of a profile depends on the criticality of your applications running on Windows.

Disable Unused Embedded Communication Services

Embedded Communication Services

Embedded communication services are IP-based communication services used in server mode on an embedded product (for example HTTP or FTP).

Disable Unused Services

To help reduce attack risks, disable any unused embedded service, for example HTTP and FTP, to close potential communication doors.

Disable Ethernet Services in Control Expert

You can enable/disable Ethernet services using the Ethernet tabs in Control Expert. Tab descriptions are provided for each of the following systems:

- Modicon M340, page 124
- Modicon M580, page 124
- Modicon Quantum, page 125
- Modicon X80, page 127
- Modicon Premium/Atrium, page 129
- Modicon Momentum MDI, page 130
- Modicon MC80, page 131

Set the Ethernet tabs parameters before you download the application to the controller.

The default settings (maximum security level) reduce the communication capacities. If services are needed, they have to be enabled.

NOTE: On some products, the `ETH_PORT_CTRL (see EcoStruxure™ Control Expert, Communication, Block Library)` function block can disable an enabled service after configuration is complete in Control Expert. The respective service can be enabled again using the same function block.

Restrict Data Flow from Control Network (Access Control)

Data Flow from Control Network

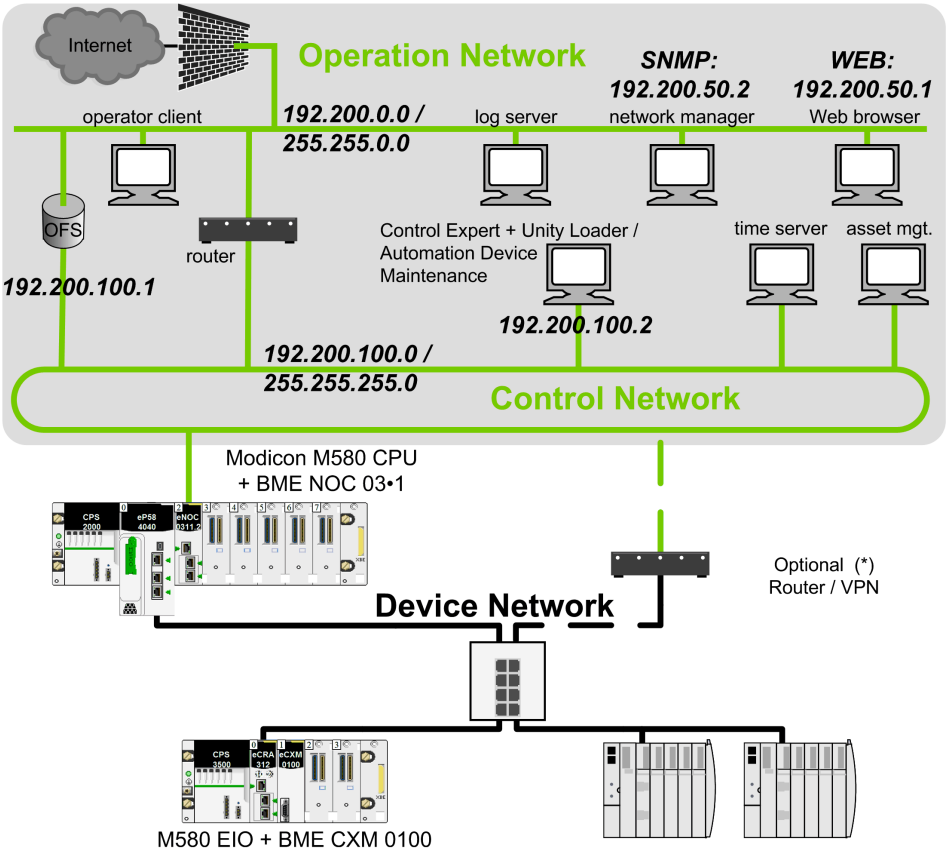
Data flow from control network is an IP-based data flow initiated on the control network.

Description

In order to control the access to communication servers in an embedded product, the access control management restricts the IP-based data flow from control network to an authorized source or subnet IP address.

Architecture Example

The purpose of the following figure is to show the role and impact of the access control settings. The access control manages the Ethernet data flow from devices communicating on the operation and control networks (located in the grayed out area).



(*) Some services require access to the device network (for example: firmware update, at source time stamping). In such cases, an optional router/VPN helps secure the access control.

Setting the Authorized Addresses in the Architecture Example

Access control goals:

- Any equipment connected to the operation network (IP address = 192.200.x.x) can access the controller Web server.
- Any equipment connected to the control network (IP address = 192.200.100.x) can communicate with the controller with Modbus TCP and can access the Web server.

To restrict data flow in previous architecture example, the authorized addresses and services are set as follows in EcoStruxure Control Expert access control table:

Source	IP address	Subnet	Subnet mask	FTP	TFTP	HTTP / HTTPS	Por-t502	EIP	SN-MP
Network manager	192.200.50.2	No	–	–	–	–	–	–	+
Operation network	192.200.0.0	Yes	255.255.0.0	–	–	+	–	–	–
Automation Device Maintenance	192.200.100-.2	No	–	+ [1]	–	– [2]	+	–	–
Control network	192.200.100-.0	Yes	255.255.255-.0	–	–	–	+	–	–

+ Selected

– Not selected or no content

[1] For M580 firmware versions equal to or greater than v4.10, FTP is not selected.

[2] For M580 firmware versions equal to or greater than v4.10, HTTP/HTTPS is selected.

Settings Description

An authorized address is set for devices authorized to communicate with the controller using Modbus TCP or EtherNet/IP.

Services settings explanation for each IP address in previous example:

192.200.50.2 (SNMP)	Set to authorize the access from the network manager using SNMP.
192.200.0.0 (HTTP/HTTPS)	Operation network subnet is set to authorize all Web browsers connected to the operation network to access the controller web browser.
192.200.100.2 (FTP) [1)]	Set to authorize the access from Automation Device Maintenance with FTP.
192.200.100.0 (Port502)	Control network subnet is set to authorize all equipment connected to the control network (OFS, Control Expert, Automation Device Maintenance) to access the controller using Port502 Modbus.
[1)] For M580 firmware versions equal to or greater than v4.10, FTP is not used. Instead, use HTTP/HTTPS.	

NOTE: The access list analysis goes through each access control list entry. If a successful match (IP address + allowed service) is found, then the other entries are ignored.

In the EcoStruxure Control Expert **security** screen, for a dedicated subnet enter the specific rules before the subnet rule. For example: To give a specific SNMP right to device 192.200.50.2, enter the rule before the global subnet rule 192.200.0.0/255.255.0.0 which allows HTTP access to all the devices of the subnet.

Set Up Encrypted Communication

Introduction

The goal of encrypted communication is to help protect the communication channels that allow remote access to the critical resources of the system (such as Modicon M580 PAC embedded application, firmware). IPsec (Internet Protocol Security) is an open standard defined by the IETF to provide protected and private communications on IP networks provided by using a combination of cryptographic and protocol security mechanisms. Our IPsec protection implementation includes anti-replay, message integrity check, and message origin authentication.

IPsec is supported on Microsoft Windows versions 7 and 10. It is initiated from the PC operating system.

Description

The IPsec function helps to secure:

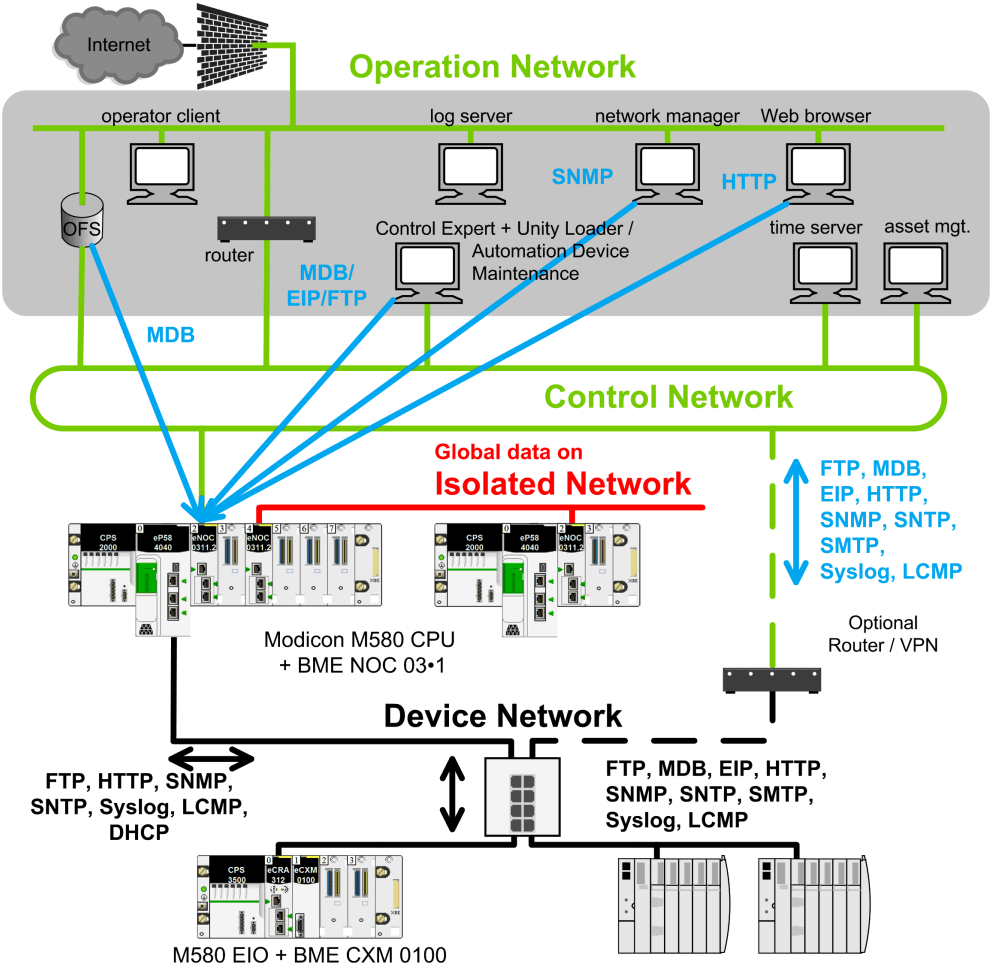
- The control room Modbus access to the controller through the BMENOC0301 and BMENOC0311 modules.
- The control room access to the communication services running inside the BMENOC0301 and BMENOC0311 modules in server mode (Modbus, EtherNet/IP, HTTP, FTP, SNMP).

NOTE: IPsec is intended to help secure services running in server mode in the controller. Secure client services initiated by the Modicon M580 PAC are outside the scope of this manual.

Wireless connection: When a PMXNOW0300 wireless module is used to configure a wireless connection, configure this module with the maximum security settings available (WPA2-PSK).

Architecture Example

The purpose of the following figure is to illustrate through an example the various protocols or services involved in a encrypted communication from the control room to a Modicon M580 controller.



Encrypted communication (IPsec).

Non IPsec communication.

Data Flow with Encrypted Communication Capability

Use these services to facilitate communications when IPsec is enabled:

Ethernet Service	Data Flows Security
EIP class 3 server	These services are supported through encrypted connections.
FTP server, TFTP server	
HTTP	
ICMP	
Modbus server (port 502)	
ARP	These services are supported through encrypted and unencrypted connections. **NOTE:** This traffic bypasses the IPsec protocol handling in the BMENOC and therefore does not use IPsec.
LLDP	
loop check protocol	
Modbus scanner	
RSTP	
DHCP, BootP client	These services are not supported when IPSec is enabled. **NOTE:** Before IKE/IPsec is initiated by the peer (PC), this traffic is not secured by IPSec. After IKE/IPSec is established, this traffic is encrypted by IPsec. Protocol could be supported, but only if packet recipient is a PC with IPSec configured and enabled.
DHCP, BootP server	
EIP class 1, TCP (forward open)	
EIP class 1, UDP (data exchange)	
Modbus client	
NTP client	
SNMP agent	
SNMP traps	
Syslog client (UDP)	

NOTE:

- IPsec is an OSI layer 3 protection. OSI layer 2 protocols (ARP, RSTP, LLDP, loop check protocol) are not protected by IPsec.
- **Global Data** communication flow (using BMXNGD0100 modules) cannot be secured by IPsec. Use such a configuration on an isolated network.

Limitations

IPsec limitations in the architecture: BMENOC0301 and BMENOC0311 modules do not support IP forwarding to device network.

If transparency is required between control and device network, an external router/vpn is needed to provide an encrypted communication between the control and device network (as shown in previous architecture example figure, page 37).

Transparency is required to perform the following operations from the control network:

- Update an M580 controller firmware from the Automation Device Maintenance through HTTPS service.
- Perform a network diagnostic of M580 controller from a network management tool through SNMP service.
- Diagnose an M580 controller from a DTM through EIP service.
- Diagnose an M580 controller from a Web browser through HTTP service.
- Log an M580 controller cybersecurity events in a syslog server through syslog service.
- Synchronize an M580 controller time from a global time server through NTP service.

Setting Up IPsec Communication in the System Architecture

Proceed with the following steps to set up the IPsec communication:

- In the control room, identify the client authorized applications that need to communicate with the Modicon M580 PAC system using Modbus (Control Expert, Automation Device Maintenance, OFS, customer applications such as SGBackup, ...).

  Configure IPsec on each PC supporting these authorized applications.
- In the control room, identify the client authorized applications that need to communicate with the BMENOC0301 and BMENOC0311 modules configured in the local rack (Control Expert DTM, Automation Device Maintenance, SNMP manager, Web browser, Web designer for FactoryCast BMENOC0301 and BMENOC0311 modules).

  Configure IPsec on each PC supporting these authorized applications.

- Incorporate BMENOC0301 and BMENOC0311 modules with IPsec function on the backplane of each Modicon M580 PAC system connected to the control network.

  To configure the IPsec function on BMENOC0301 and BMENOC0311 modules, proceed in 2 steps:

  - Enable IPsec function.
  - Configure a pre-shared key. A pre-shared key is used to build a shared secret allowing two devices to authenticate each other.

    NOTE: Because IPsec relies on this shared secret, it is a key element in the security policy that is managed by the security administrator. To help increase the security of the pre-shared key, use an external tool such as KeePass, page 40 to generate an appropriate character string.

Configuration of the BMENOC0301 and BMENOC0311 modules is performed with Control Expert. In order to help secure this configuration, the first download is best accomplished through a point to point connection, such as the USB port. Thereafter, future downloads may be performed through Ethernet with an IPsec function, assuming IPsec is enabled.

Each PC supporting IPsec needs to comply with the following requirements for IPsec configuration:

- Use Microsoft Windows 10 OS.
- Have the administrator rights to configure IPsec.

  Once the IPsec configuration is performed, set the Windows account as a normal user account without administrator privilege.
- **Harden the PC as explained in the *Hardening the PC* topic**, page 23.

More details on configuration are provided in the *Configuring IP Secure Communications* topic (see Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Communications Module, Installation and Configuration Guide).

Generate Pre-Shared Keys with the Highest Security

The security of IPsec communications relies on the complexity of the pre-shared key. Use specialized tools to generate pre-shared keys of the highest security.

One such tool is KeePass, which you can download as freeware from the Internet. Download and install KeePass to your PC and launch it.

Configure and use KeePass v2.34 to generate passwords that can be used as pre-shared keys:

Step	Action
1	Create a new key database folder (**File > New**),
2	In the **Create New Password Database** dialog box, enter a folder name in the **File name** field and record your modifications.
3	In the **Create Composite Master Key** dialog box, enter a **Master password**. Enter the password again in the **Repeat** password field.
4	Press **OK** to open **Step 2** and press **OK** again.
5	In the new database dialog box, expand **New Database**.
6	Select **Network** and add an entry (**Edit > Add Entry**).
7	In the **Title** field, enter a name for your module (for example, eNOC).
8	In the **User name** field, enter a user name.
9	Click the **Generate a password** icon.
10	Select **Open password generator**.
11	Press **OK** to populate the **Password** and **Repeat** fields.
12	Open the **Password Generation Options** dialog box (**Tools > Generate Password**).
13	Make these selections at **Generate using character set**: • Upper-case (A, B, C, …) • Lower-case (a, b, c, …) • Digits (0, 1, 2, …) • Minus (-) • Underline (_) • Special (!, $, %, &, …) • Brackets ([,], [, (,), <, >) **NOTE:** These characters are not accepted for use in the pre-shared key: • { • } • ; • #
14	Press **OK**.
15	Right-click on your device in the **Database** list and scroll to **Copy Password**.
16	Open the security configuration screen in Control Expert.
17	Paste the key in the IPsec configuration screen.

Diagnose IPsec Communication in the System Architecture

Information on IPsec diagnostic in the system architecture is provided in the *Configuring IP Encrypted Communications* topic (see Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Communications Module, Installation and Configuration Guide).

CSPN Security Target

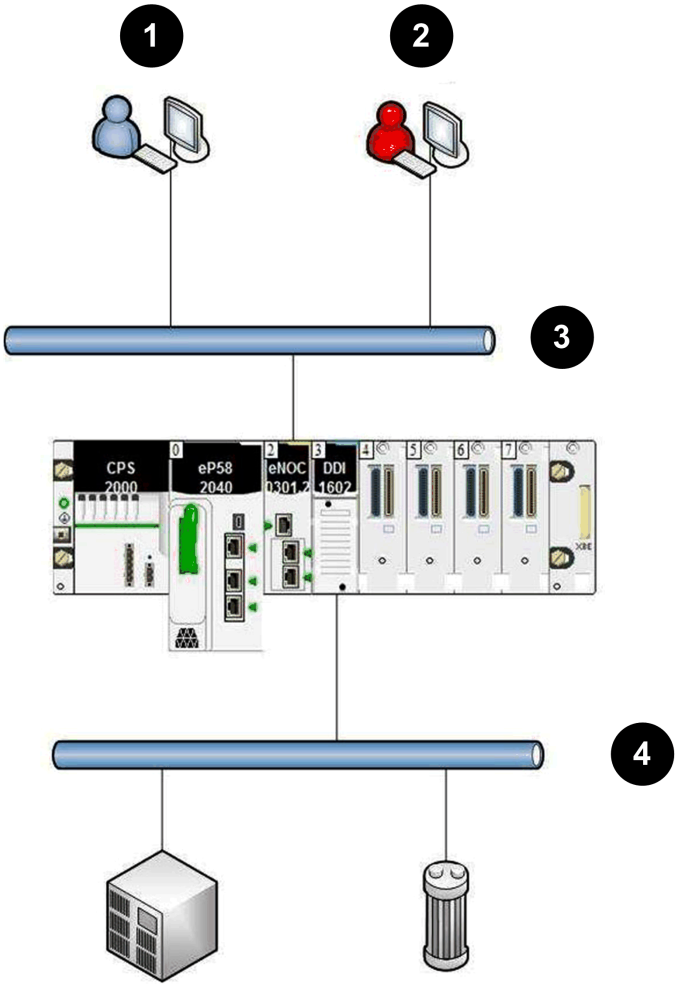
CSPN Introduction

CSPN (Certification de Sécurité de Premier Niveau) is a cybersecurity certification currently used in the country of France. A product with CSPN certification is expected to withstand a cyber attack driven by two-person months of skilled hackers. The M580 system is CSPN-certified. This topic describes the environment, programmable automation controller configurations, and parameters that meet CSPN requirements to effect the highest level of security.

Modicon M580 Introduction

The Modicon M580 PAC system is designed to control and command an industrial process continuously without human intervention. At each step, the controller processes the data received from its inputs, the sensors, and sends commands to its outputs, the actuators. Exchanges with the supervision (HMI, SCADA) are performed with BMENOC0301 and BMENOC0311 Ethernet communication modules on the local rack with the controller.

The following illustration describes a typical M580 system architecture that can be vulnerable to a security attack:



1 operator using EcoStruxure Control Expert

2 attacker

3 supervision network

4 field network with no attacker

M580 Features

The M580 controller offers the following features:

Feature	Description
user program execution	An M580 controller runs a user program that processes the inputs and updates the outputs.
input/output management	An M580 controller can read local inputs and write local outputs. These inputs/outputs can be digital or analog and allow the M580 controller to control and command the industrial process.
communication with the supervision	An M580 controller can communicate with SCADA to receive commands and transmit process data using the Modbus protocol.
administrative functions	An M580 controller includes administrative functions, which are provided in EcoStruxure Control Expert, for configuration and programming.
remote logging	An M580 controller supports the definition of a remote logging policy; it can log security and administrative events.

M580 Configuration

A CSPN-certified M580 configuration includes these components:

Module	Firmware	Description
BMEP58•0•0	as of version 2.20	The controller follows the security rules described in the security documents (see assumptions).
BMENOC0301 and BMENOC0311	as of version 2.11	This Ethernet module manages the encrypted communications with the upper layer (EcoStruxure Control Expert supervision and engineering software).

NOTE: EcoStruxure Control Expert programming software, PCs, other controller modules, and backplane components are not included in the scope of the certification.

User Profiles

Users that interact with the controller for an improved implementation have the following predefined EcoStruxure Control Expert Security Editor's profiles:

User Profile	Description
ReadOnly	No application modification is authorized.
Operate	Only application execution and parameter modification are enabled.
Program	All functions are enabled.

Improved Implementation

These items contribute to a healthy environment for an improved implementation:

Item	Security Considerations
security documentation	All instructions in the documentation (for example, user guides, white papers) are applied prior to the evaluation.
administrators	System administrators are competent, trained, and trustworthy.
premises	Access to the controller location is restricted to trustworthy people. In particular, an attacker does not have access to the physical ports of the controllers. Since identical products can be purchased freely, the attacker can obtain one to research vulnerabilities by any possible means.
unevaluated services disabled	Any services that are not covered by the security target are disabled in the configuration or by a user program (as described in the security documentation).
user application verification	The integrity of the EcoStruxure Control Expert application is controlled by the administrator before it is loaded in the controller.
active logging	The logging function is operational and the logs are not corrupt.
log checking	System administrators regularly check the local and remote logs.
first configuration	The initial configuration is uploaded to the controller through the USB interface, and the controller is unplugged from the network.
firmware upgrade	The firmware upgrade is performed through the USB interface, and the controller is unplugged from the network.
strong passwords	System administrators employ strong passwords that combine uppercase letters, lowercase letters, numbers, and special characters.

Operating Modes

The following operating modes are compliant with CSPN requirements:

- During commissioning phase, initial configuration of the controller can be done with **either** a Control Expert engineering station connected in point-to-point to the Ethernet port **or** to the local USB port of the controller.
- In normal operating conditions (running mode, SCADA connected on the Ethernet control network), confirm that Control Expert is disconnected.
- Perform any further modification of the configuration or application program with Control Expert connected to the USB port of the controller.

Cybersecurity Parameters

This table describes the cybersecurity parameters:

Parameter	Topic	User Guide
ACL activated.	Configuring Security Services	Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Communications Module, Installation and Configuration Guide
IPsec activated on BMENOC0301/0311 with maximum security.	Configuring Security Services	
Enforce security selected (FTP, TFTP, HTTP, DHCP/BOOTP, SNMP, EIP, NTP protocols deactivated).	Configuring Security Services	
Log activated.	Logging DTM and Module Events to the Syslog Server	
RUN/STOP by input only activated.	Managing Run/Stop Input	M580 Hardware Reference Guide
Memory protection activated.	Memory Protect	
Helping secure a project: • Application locked with login and password. • Section protection activated.	Helping Secure a Project in Control Expert	
No upload information stored inside controller.	Controller Embedded Data	EcoStruxure™ Control Expert, Operating Modes
Default password for FTP service changed.	Firmware Protection	
Application sections are set with no read/write access.	Section and Subroutine Protection	

Critical Assets

Environment: This table shows the assets that are critical to the environment:

Asset	Description for Proper Use
control-command of the industrial process	The controller controls and commands an industrial process by reading inputs and sending commands to actuators. The availability of these actions is protected.
engineering workstation flows	The flows between the controller and the engineering workstation are protected in integrity, confidentiality, and authenticity.

Security requirements for the environmental critical assets:

Asset	Availability	Confidentiality	Integrity	Authenticity
control-command of the industrial process	X			
engineering workstation flows		X	X	X

controller: This table shows the assets that are critical to the controllers:

Asset	Description for Proper Use
firmware	The firmware is protected both in integrity and authenticity.
controller memory	The controller memory contains the controller configuration and a program that is loaded by the user. Its integrity and authenticity are protected while it is running.
execution mode	The integrity and authenticity of the execution mode of the controller are protected.
user secrets	All passwords that are used to perform authentication are held in the confidence by the appropriate users.

Security requirements for the controller critical assets:

Asset	Availability	Confidentiality	Integrity	Authenticity
firmware			X	X
controller memory			X	X
execution mode			X	X
user secrets		X	X	

Security Threats

Threats considered by attackers controlling a device plugged into the supervision network:

Type of Threat	Control-Command of the Industrial Process	Engineering Workstation Flows	Firmware	Controller Memory	Execution Mode	User Secrets
denial of service	Av					
firmware alteration		I, Au				
execution mode alteration					Au, I	
memory program alteration				I, Au		
flows alteration	Av	Au, C, I				C, I
Av: availability I: integrity C: confidentiality Au: authenticity						

Type of Threat	Description
denial of service	The attacker manages to generate a denial of service on the controller by performing an unexpected action or by exploring a vulnerability (sending a malformed request, using a corrupted configuration file...). This denial of service affect the entire controller or some of its functions.
firmware alteration	The attacker manages to inject and run a corrupted firmware on the controller. The code injection may be temporary or permanent, and does not include any unexpected or unauthorized code execution. A user may attempt to install that update on the controller by legitimate means. Finally, the attacker manages to modify the version of the firmware installed on the controller without having the privilege to do so.
execution mode alteration	The attacker manages to modify the execution mode of the controller without being authorized (a stop command for instance).
memory alteration	The attacker manages to modify, temporarily or permanently, the user program or configuration that run in the controller memory.
flows alteration	The attacker manages to corrupt exchanges between the controller and an external component without being detected. The attacker can perform attacks such as credential theft, access control violation, or control-command of the industrial process mitigation.

Type of Threat	Persistent Denial of Service	Firmware Alteration	Execution Mode Alteration	Memory Alteration	Flows Alteration
malformed input management	X				
storage of secrets				X	

Type of Threat	Persistent Denial of Service	Firmware Alteration	Execution Mode Alteration	Memory Alteration	Flows Alteration
athentication on administrative interface					X
access control policy					X
firmware signature		X			
integrity and authenticity of controller memory				X	
integrity of the controller execution mode			X		
more secure communication					X

Type of Threat	Description
malformed input management	The controller has been developed to correctly handle malformed input, particularly malformed network traffic.
strength of secrets	The controller has been developed to correctly handle malformed input, particularly malformed network traffic. • the PSK used to mount the IPsec tunnel • the application password used to read the .STU Control Expert file and connect the file to the controller • other services passwords (like FTP)
authentication on administrative interface	Session tokens are protected against hijack and replay; they have a short lifespan. The identity and permissions of the user account are systematically checked before any privileged action. An application password is set in each configuration, which helps prevent any modification of the controller from a non-authentic user.
access control policy	The access control policy helps control the authenticity of privileged operations, which are operations that can alter identified critical assets. The access control list (ACL) is activated in each configuration, and only identified IP addresses can connect to the controller.
firmware signature	At each firmware update, integrity and authenticity of the new firmware are checked before updating.

Type of Threat	Description
integrity and authenticity of controller memory	The memory protection feature is activated in each configuration, which helps prevent the modification of the running program without an action in specific inputs or outputs. If no input/output module is installed, the programming interface is blocked. The controller helps ensure the integrity and authenticity of the user program, so that authorized users can modify the program. The memory protection also helps ensure the configuration protection, which includes several security parameters: • Access control policy. • RUN/STOP by input only activated. • Memory protection activated. • Enabled/disabled services (FTP, TFTP, HTTP, DHCP, SNMP, EIP, NTP). • IPsec parameters. • Syslog parameters.
integrity of the controller execution mode	The controller helps ensure that the execution mode can be modified by authorized users that are authenticated. The RUN/STOP by input only feature is activated, which helps prevent the possibility of changing the RUN/STOP status through the Ethernet interface.
encrypted communication	The controller supports encrypted communication, protected in integrity, confidentiality, and authenticity (IPsec encrypted with ESP).The FTP protocol is disabled, and IPsec helps secure Modbus communication through the BMENOC0301 and BMENOC0311 modules.

Set Up Cybersecurity Audit (Event Logging)

Logging events and logging analysis are essential. The analysis traces user actions for maintenance and abnormal events that can indicate a potential attack.

The complete system needs to have a robust logging system distributed in all devices. The events related to cybersecurity are logged locally and sent to a remote server using Syslog protocol.

In the system architecture, event logging involves two parties:

- A log server that receives all the cybersecurity events of the system through Syslog protocol.
- Log clients (Ethernet connection points where cybersecurity events are monitored: device, Control Expert).

NOTE:

- When the M580 controller (4.60 or later) is in secure mode, the controller retrieves its syslog configuration from the cybersecurity configuration provided by Cybersecurity Admin Expert (CAE). Devices that do not use CAE for cybersecurity configuration (example: BMENOC0301, BMECRA31210), retrieve their syslog configuration from the syslog configuration panel in Control Expert 16.4 or later.
- When the M580 controller (4.60 or later) is in standard mode, the controller retrieves its configuration from the syslog configuration panel in Control Expert 16.4 or later.

Event Log Service Description

Each log client role is to:

- Detect and time-stamp events.

  A single NTP reference needs to be configured in the system to time-stamp the cybersecurity events.
- Send the detected events to the event logging server.

  The events are exchanged between the client and the server using Syslog protocol (RFC 5424 specification).

  The Syslog messages respect the format described in RFC 5424 specification.

  Syslog exchanges are done with TCP protocol.

  On devices, events are not lost in case of transient network breakdown. Events are lost in case of device reset (except for Modicon M580 controller firmware ≥ 4.0).

Facility Values for Event Types

Syslog message facility values as per RFC 5424 specification associated with event types:

Facility value	Description
0	Kernel messages.
1	User-level messages.
2	Mail system.
3	System daemons.
4	Security / authorization messages.
5	Messages generated internally by Syslog.

Facility value	Description
6	Line printer subsystem.
7	Network news subsystems.
8	UUCP subsystem
9	Clock daemon.
10	Security / authorization messages.
11	FTP daemon.
12	NTP subsystem.
13	Log audit.
14	Log alert.
15	Clock daemon.
16...23	Local use 0...7.

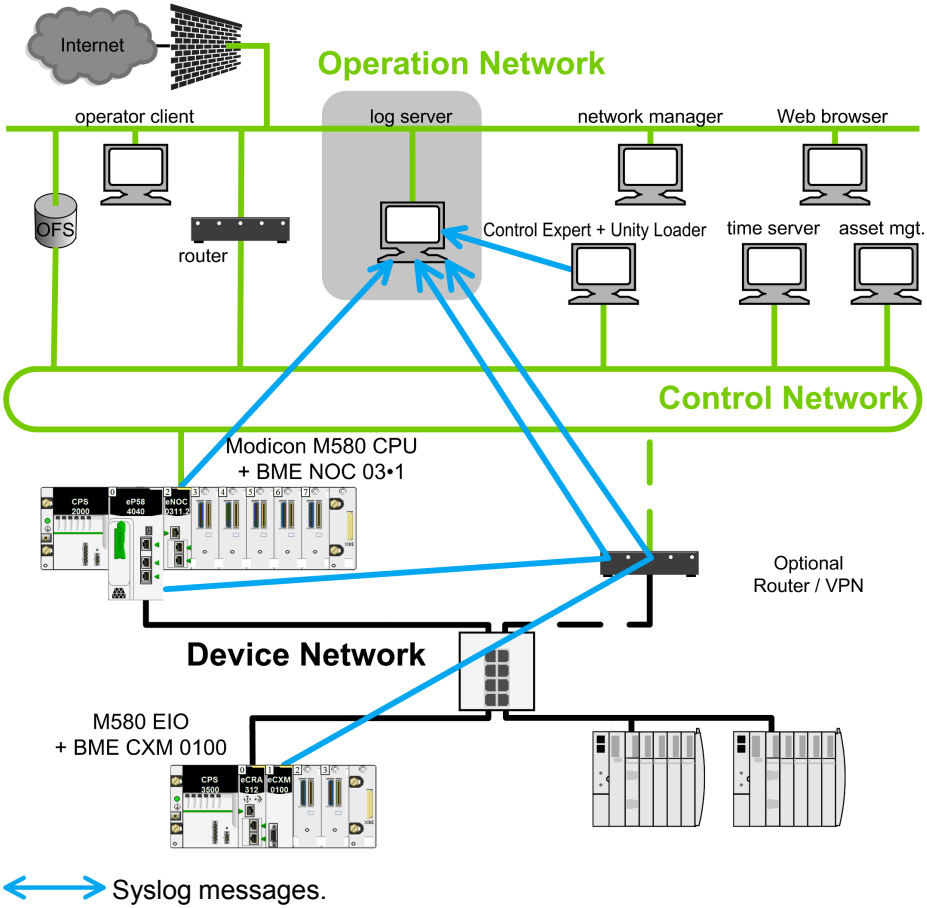
Severity Values for Event Types

Syslog message severity values as per RFC 5424 specification associated with event types:

Severity Value	Keyword	Description
0	Emergency	System is unusable.
1	Alert	Action must be taken immediately.
2	Critical	Critical conditions.
3	Error	Error conditions.
4	Warning	Advisory conditions.
5	Notice	Normal but significant condition.
6	Informational	Informal messages.
7	Debug	Debug-level messages.

Architecture Example

The following figure highlights the position of logging server in a system architecture:



Logged Event Message Structure for Modicon M580 Controller (as of Firmware Version 4.10) and BMENOR2200H (as of Firmware Version 3.01)

Fields	Description
PRI	Facility and severity information: "FACILITY" = 10 for cybersecurity events
VERSION	Version of the Syslog protocol specification (Version = 1 for RFC 5424).

Fields	Description
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: Minute • 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. Source @IP address = @IP address A OR @IP address B in case of HSBY controller
APP-NAME	Identifies the application that initiates the Syslog message. It contains information that identifies the entity sending the message (for example, subset of commercial reference).
PROCID	Process or protocol name that originated the message (for example, Modbus, HTTPS, LocalHMI)
MSGID	An identifier of the type of the event. (for example, CONNECTION_FAILURE_AND_ BLOCK).
Event information	<ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac: macro-id="30296255-e8b7-4cf1-982e-2c45b17b1f06"><ac:plain-text-body><![CDATA[**[authn@3833]**, **[authz@3833]**, **[config@3833]**, **[cred@3833], [backup@3833], [plc@3833] [system@3833]** See STRUCTURED-DATA description below.
MSG	Message containing the event-specific result (see Event Log Message Descriptions for Control Expert, page 58)

- **STRUCTURED-DATA** Description: mandatory event information.
  - **[meta]**: mandatory structured-data to provide meta-information about the message. Where parameter is:
    - **sequenceId**: the event identifier (rollover to 1 when maximum value 2147483647 is reached).
    - **sysUpTime**: this value should be included when component is incapable of obtaining system time (integer containing the time in 1/100th of the second since the system was last re-initialized).

- **STRUCTURED-DATA** Description: event information depending on event category.
  - **[authn@3833]**: structured-data used for authentication events. Where parameters are:
    - **itf**: the interface where the user is connected to, either a network port or a local interface (hmi, usb , …).
    - **peer**: the FQDN or IP address of the component from which the user is connected, plus its port (ipAddress:port), optional in case of local interface
    - **user**: the user name (component or human), optional if user name unknown.
  - **[authz@3833]**: structured-data used for authorization events. Where parameters are:
    - **user**: the user name (component or human)
    - **object**: the object access by the user, object is product dependant.
    - **action**: the action performed on the object: Create, Read, Update, Delete (CRUD)
  - **[config@3833]**: structured-data used for configuration events. Where parameters are:
    - **object**: the name of the security object to configure (Firmware, RBAC, Security Policy, Device Setting, Trust Anchor, product dependant objects)
    - **value**: optional version or value of the new object
  - **[cred@3833]**: structured-data used for credential management events. Where parameters are:
    - **name**: the common name of the certificate or the user login name
  - **[system@3833]** structured-data for system events. Where parameters are:
    - **object**: the name of the system object that change (controller, module, Rotary Switch, SD Card, product dependant object)
  - **[backup@3833]**: structured data used for backup. Where parameters are:
    - **object**: the part of the component that has been backup/restore, object is product dependant.
  - Structured data can also be defined by each application for specific events.

Logged Event Message Structure for Modicon M580 Controller (Firmware earlier than Version 4.10), BMENUA0100 (Firmware Versions 1.10 & 2.0), and BMENOR2200H (Firmware earlier than Version 3.01)

Syslog message structure for Modicon M580 controller firmware and BMENUA0100:

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: Minute • 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.
APP-NAME	Identifies the application that initiates the Syslog message. It contains information that identifies the entity sending the message (for example, subset of commercial reference).
PROCID	Process or protocol name that originated the message (for example, Modbus, HTTPS, LocalHMI, ….) 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: • 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. Not used (null). • Type: Unique number to identify a message (see Event Log Message Descriptions for Control Expert, page 58). • Comment: String that describes the message (see Event Log Message Descriptions M580 Controllers (as of Firmware Version V4.10), and BMENOR2200H (as of Firmware Version 3.01), page 64).

Setting Up a Syslog Server in the System Architecture

Several Syslog servers are available for various operating systems.

NOTE: Syslog servers must be compliant with RFC 5424.

Examples of Syslog server providers:

- WinSyslog: For Windows operating system.

  Link: www.winsyslog.com/en/.
- Kiwi Syslog: For Windows operating system.

  Link: www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx.
- Splunk: For Windows and Unix operating systems.

  Link: www.splunk.com/.
- Rsyslog: For Unix operating system.

  Link: www.rsyslog.com/.
- Syslog-ng: Open source for Unix operating system.

  Link: www.balabit.com/network-security/syslog-ng/opensource-logging-system.
- Syslog Server: Open source for Windows operating system.

  Link: sourceforge.net/projects/syslog-server/.

Setting Up Syslog Clients in the System Architecture

Event logging is managed in Control Expert for all devices and Device Type Managers (DTMs).

The event logging function, server address, and port number are configured in Control Expert as follows, and these parameters are sent to each client in the system after the **Build** action:

Step	Action
1	Click **Tools** > **Project Settings**.
2	Click **Project Settings** > **General** > **PLC diagnostics**.
3	Select **Event Logging** check box (cleared by default). **NOTE:** A project with this setting selected can only be opened as of Unity Pro 10.0. Unity Pro is the former name of Control Expert for version 13.1 or earlier.
4	Enter a valid **SYSLOG server address** and **SYSLOG server port number**.
5	Perform a **Build** after configuring this setting (you are not required to select **Analyze Project**).

Diagnose Event Logging

The following table displays the type of event logging diagnostics available for various devices:

Devices	Diagnostic information
Control Expert	If a communication error with the Syslog server occurs, the detected error is recorded in the event viewer. To enable the event viewer in Control Expert, select the **Audit** check box in the **Policies** tab of the Security Editor (see EcoStruxure™ Control Expert, Security Editor, Operation Guide).
BMENOC0301 and BMENOC0311 device DDT (*SERVICE_STATUS2* parameter)	Two diagnostic information is available: • EVENT_LOG_STATUS: Value = 1 if event log service is operational. Value = 0 if event log service is not operational. • LOG_SERVER_NOT_REACHABLE: Value = 1 if the Syslog client does not receive acknowledgment of the TCP messages from the Syslog server. Value = 0 if the acknowledgment is received.
Modicon M580 controller device DDT	
BMECXM Device DDT	

Event Log Message Descriptions for Control Expert

Logged Event: Application Action

The following table presents the message descriptions when the logged event is: Application action.

MSG(1)	Facility	Severity	Description
Create a new project	10	6	Create a new Control Expert application.
Open an existing project	10	6	Open an existing Control Expert application.
Save a project	10	6	Save the presently opened application.
Save as a project	10	6	Save the presently opened application using a different file.
Import a project	10	6	Import an application.
Build offline	10	6	Build application in offline mode.
Build online stop	10	6	Build application in online mode; controller in STOP mode.

MSG(1)	Facility	Severity	Description
Build online run	10	6	Build application in online mode; controller in RUN mode.
Start stop or initialize the PAC	10	6	Start / stop / initialize the controller.
Update init values with present values	10	6	Update initial values with present values.
Transfer project from PAC	10	6	Upload the application from the controller.
Transfer project to PAC	10	6	Download the application to the controller.
Transfer data values from file to PAC	10	6	Transfer data values from the file to the controller.
Restore project backup in PAC	10	6	Restore project backup in the controller.
Save to project backup in PAC	10	6	Save to project backup in the controller.
Set address	10	6	Change the controller address connection.
Modify options	10	6	Control Expert option modifications.
Modify variable values	10	6	Variable value is modified in the controller.
Force internal bits	10	6	Variable forces value modification in the controller: internal bits.
Force outputs	10	6	Variable forces value modification in the controller: outputs.
Force inputs	10	6	Variable forces value modification in the controller: inputs.
Task management	10	6	Task management
Task cycle time modification	10	6	Modify task cycle time.
Suppress message in diag viewer	10	6	Suppress message in diagnostics viewer.
Debug executable	10	6	Debug executable.
Replace project variable	10	6	Replace project variable.
Create libraries or families	10	6	Create libraries or families inside the library.
Delete libraries or families	10	6	Delete libraries or families inside the library.
Put object into library	10	6	Copy elements (DFB/DDT) from the application to the library.
Delete object from library	10	6	Delete elements (DFB/DDT) in the library.
Get object from library	10	6	Copy elements (DFB/DDT/EF/EFB) from the library to the application.

MSG(1)	Facility	Severity	Description
Modify documentation	10	6	Modify documentation (application printing).
Modify functional view	10	6	Modify functional view.
Modify animation tables	10	6	Modify animation tables.
Modify constant values	10	6	Modify constant values.
Modify program structure	10	6	Modify program structure.
Modify program sections	10	6	Modify program sections.
Modify Project settings	10	6	Modify project settings.
Variable Add Remove	10	6	Create/remove variable in the data editor.
Variable Main Attributes modification	10	6	Modify variable attribute.
Variable Minor Attributes modification	10	6	Modify variable attribute.
DDT modification	10	6	Modify the DDT in the data editor.
DFB type Add Remove	10	6	Create/remove DFB in the data editor.
DFB type structure modification	10	6	Modify DFB structure in the data editor.
DFB type sections modification	10	6	Modify DFB sections.
DFB instance Modification	10	6	Modify DFB instance in the data editor.
DFB instance Minor Attributes modification	10	6	Modify DFB instance minor attributes in the data editor.
Modify configuration	10	6	Modify controller configuration.
IO sniffing	10	6	Sniff controller I/O.
Modify the IO configuration	10	6	Modify controller I/O configuration.
Adjust the IO	10	6	Adjust controller I/O configuration.
Save param	10	6	Save parameters from the I/O screen in the controller I/O configuration.
Restore param	10	6	Restore parameters from the I/O screen in the controller I/O configuration.
Modify screens	10	6	Modify operator screens.
Modify messages	10	6	Modify messages.
Add/Remove screens or families	10	6	Operator screens/families: add/remove.
Cybersecurity Configuration change	10	6	Cyber-security configuration imported successfully.
Product certificate (and/or keys) expired	10	6	Product certificate expired.

MSG[1]	Facility	Severity	Description
Move component	13	6	Move FFB block.
Move component	13	6	Move contact/coil.
Insert component	13	6	Insert FFB block.
Insert component	13	6	Insert contact/coil.
Delete component	13	6	Delete FFB block.
Delete component	13	6	Delete contact/coil.
Add variable	13	6	Set effective parameter on FFB block.
Add variable	13	6	Set effective parameter on contact/coil.
Delete variable	13	6	Remove effective parameter on FFB block.
Delete variable	13	6	Remove effective parameter on contact/ coil.
Modify variable	13	6	Change effective parameter on FFB block.
Modify variable	13	6	Change effective parameter on contact/ coil.
Link pin	13	6	Make a link between two pins.
Scale component	13	6	Change size of extendable FFB block.
Scale component	13	6	Change size of vertical/horizontal link.
Rename variable	13	6	Rename effective parameter.
Delete row	13	6	Delete one single row.
Delete rows from	13	6	Delete multiple rows.
Delete column	13	6	Delete one single column.
Delete columns from	13	6	Delete multiple columns.
Insert row	13	6	Insert one single row.
Insert rows from	13	6	Insert multiple rows.
Insert column	13	6	Insert one single column.
Insert columns from	13	6	Insert multiple columns.
[1] MSG content includes the concatenation of the username, the PID of Control Expert, plus the message.			

NOTE: The fields HOSTNAME, APP-NAME, PROCID, MSGID, and STRUCTURED-DATA do not apply to Control Expert messages.

Logged Event: DTM Action

The following table presents the message descriptions when the logged event is: DTM action.

MSG(1)	Facility	Severity	Description
Download parameters to device service finished in error	9	6	DTM download parameter finished in error.
Download parameters to device service finished without error	9	6	DTM download parameter finished without error.
Upload parameters from device service finished in error	9	6	DTM upload parameter finished in error.
Upload parameters from device service finished without error	9	6	DTM upload parameter finished without error.
Go on-line service failed	9	6	Connection to the DTM is not established.
Go on-line service succeeded	9	6	Connection to the DTM succeeded.
Go offline service failed	9	6	Connection to the DTM is not closed.
Go offline service succeeded	9	6	Connection to the DTM closed successfully.
FDR download parameters service failed	9	6	DTM FDR download parameters service is not performed.
FDR download parameters service succeeded	9	6	DTM FDR download parameters service succeeded.
FDR upload parameters service failed	9	6	DTM FDR upload parameters service is not performed.
FDR upload parameters service succeeded	9	6	DTM FDR upload parameters service succeeded.
Download parameters to device service failed	9	6	Download parameters to device service is not performed.
Download parameters to device service succeeded	9	6	Download parameters to device service succeeded.
Upload parameters from device service failed	9	6	Upload parameters from device service is not performed.
Upload parameters from device service succeeded	9	6	Upload parameters from device service succeeded.
Audit Trail Function Event	9	6	Audit trail function event
Audit Trail Device Status Event	9	6	Audit trail device status event
No device status message	9	6	No device status message
Status information	9	6	Status information
Access right : Read / Write	9	6	Access right : read/write

MSG(1)	Facility	Severity	Description
Enumerator entry	9	6	Enumerator entry
(1) MSG content includes the concatenation of the Username, the PID of Control Expert, plus the message.			

Logged Event: Password Action

The following table presents the message descriptions when the logged event is: Password action.

MSG(1)	Facility	Severity	Description
CyberSecurity - Modifying Password > Incorrect Password	2	6	Problem at application password changing
CyberSecurity - Verifying Password > Incorrect Password	2	6	Problem at application password verification
CyberSecurity - Verifying Section Password > Incorrect Password	2	6	Problem at section password verification
CyberSecurity - Data Storage Password Modified	2	6	Password DataStorage changed
CyberSecurity - Firmware Password Modified	2	6	Password FW Download changed
CyberSecurity - Verifying Password > Incorrect Password	2	6	Problem at application password verification
(1) MSG content includes the concatenation of the username, the PID of Control Expert, plus the message.			

Logged Event: SYSLOG Configuration Changed

The following table presents the message descriptions when the logged event is: SYSLOG configuration changed.

MSG(1)	Facility	Severity	Description
SYSLOG address changed	-	-	CyberSecurity - Event logging project setting has changed - Event Logging, SYSLOG server address, port or protocol.
(1) MSG content includes the concatenation of the username, the PID of Control Expert, plus the message.			

Logged Event: File Action

The following table presents the message descriptions when the logged event is: File action.

MSG[1]	Facility	Severity	Description
XXXXX file has been opened	0	6	File XXXXX is open.
Disconnection from PAC @=XXXXXX dirver= YYYYY	0	6	The controller disconnected = @XXXXXX driver = YYYYYY.
Close application XXXXXX	0	6	Close application XXXXXX.
Project has been transfered from PAC to PC	0	6	The project is transferred from the controller to the PC.
[1] MSG content includes the concatenation of the username, the PID of Control Expert, plus the message.			

Event Log Message Descriptions M580 Controllers (as of Firmware Version V4.10), and BMENOR2200H (as of Firmware Version 3.01)

This topic presents event log message descriptions for:

- M580 controllers as of firmware version 4.10 (abbreviated **CPU** in the**Devices** column)
- BMENOR2200H RTU modules as of firmware version 3.01 (abbreviated eNOR in the **Devices** column)

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
Successful connection	All successful connections from a user (human or a component) to a component whether through an encrypted protocol or an unencrypted protocol if allowed by the customer security policy	Successful login (web server through HTTPS)	6	HTTPS	CONNECTION_SUCCESS	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN:peerPort* user= *username*]	Logon	CPU eNOR
		Successful login (firmware upgrade through HTTPS)	6	HTTPS	CONNECTION_SUCCESS	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN:peerPort* user= *username*]	Logon	CPU eNOR
		Successful login (OPC UA)	6	OPC-UA	CONNECTION_SUCCESS	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN:peerPort* user= *username*]	Socket connection	CPU
		Successful login (Control Expert application password through Modbus-Umas) **Mode standard only**	6	MODBUS-UMAS	CONNECTION_SUCCESS	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN:peerPort* user= *username*]	Logon	CPU

Logged event	Descrip-tion	Additional descrip-tion	Severi-ty	PROCID	MSGID	Structured – data	Msg	Devices
		Successful Modbus TCP connection (no user)	6	MODBUS	CON-NEC-TION_ SUC-CESS	[meta sequen-ceId=*num*] [auth-n@3833 itf=*localPort* | *localInterfa-ce*peer= *peerFQDN: peerPort* user= *username*]	Socket connection	CPU eNOR
		Successful HTTP/ DPWS connection	6	HTTP	CON-NEC-TION_ SUC-CESS	[meta sequen-ceId=*num*] [auth-n@3833 itf=*localPort* | *localInterfa-ce*peer= *peerFQDN: peerPort* user= *username*]	Socket connection	CPU
		Successful EtherNet/IP (EIP) / explicit TCP connection (no user)	6	EIP	CON-NEC-TION_ SUC-CESS	[meta sequen-ceId=*num*] [auth-n@3833 itf=*localPort* | *localInterfa-ce*peer= *peerFQDN: peerPort* user= *username*]	Socket connection	CPU
		Successful DNP3 connection (no user)	6	DNP3	CON-NEC-TION_ SUC-CESS	[meta sequen-ceId=num] [auth-n@3833 itf=localPort | localInter-face peer= peerFQDN: peerPort user= username]	Socket connection	eNOR

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
		Successful IEC 60870 connection (no user)	6	IEC60870	CONNECTION_SUCCESS	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer= peerFQDN: peerPort user= username]	Socket connection	eNOR
Connection problem	All unsuccessful connections from a user (human or a component) to a component whether through an encrypted protocol or an unencrypted protocol if allowed by the customer security policy	Login problem (Control Expert application password through Modbus-Umas)	5	MODBUS-UMAS	CONNECTION_FAILURE	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN: peerPort* user= *username*]	Invalid password	CPU
		Modbus TCP connection problem (no user)	5	MODBUS	CONNECTION_FAILURE	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN: peerPort* user= *username*]	Max connections reached. Filtered data flow.	CPU eNOR
		EIP explicit TCP connection problem (no user)	5	EIP	CONNECTION_FAILURE	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN: peerPort* user= *username*]	Max connections reached. Filtered data flow.	CPU

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
		DNP3 connection problem (no user)	5	DNP3	CONNECTION_FAILURE	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer= peerFQDN: peerPort user= username]	Max connections reached.	eNOR
		IEC60870 connection problem (no user)	5	IEC60870	CONNECTION_FAILURE	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer= peerFQDN: peerPort user= username]	Max connections reached.	eNOR
Human user account locking due to too many problems during the authentication attempts	The security policy may request to block a human user account after a number of failed attempts. This event informs the administrator about potential attacks and that the human user account must be locked.	Login problem (Web Server through HTTPS). Human user account locking due to too many problems during the authentication attempts	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN: peerPort* user= *username*]	Invalid certificate Invalid password	CPU eNOR
		Login problem (firmware upgrade through HTTPS), human user account locking due to too many	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer= *peerFQDN: peerPort*	Invalid certificate Invalid password	CPU eNOR

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
		unsuccessful authentication attempts				user=*username*]		
		Login problem (OPC UA), human user account locking due to too many problems during the authentication attempts	1	OPC-UA	CONNECTION_FAILURE_AND_BLOCK	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*username*]	Invalid certificate, Invalid password	—
Denied login (blocked account)	Human user tries to connect to a blocked account.	Login problem (web server through HTTPS), denied login (blocked account)	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*username*]		CPU eNOR
		Login problem (firmware upgrade through HTTPS), denied login (account is blocked)	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*username*]		CPU
		Login problem (OPC UA), denied login (blocked account)	1	OPC UA	CONNECTION_FAILURE_ON_BLOCKED	[meta sequenceId=*num*] [authn@3833 itf=*localPort* |		—

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
						localInterfacepeer=peerFQDN:peerPort user=*username*]		
Disconnection	Human user or component disconnected manually after a time out due to inactivity.	HTTPS disconnection (web server)	6	HTTPS	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*username*]	Manual logout	CPU eNOR
		HTTPS disconnection (firmware upgrade)	6	HTTPS	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*username*]	Manual logout	CPU eNOR
		OPC UA disconnection	6	OPC-UA	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*username*]	Socket disconnection	CPU
		Modbus disconnection	6	MODBUS	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* |	Socket disconnection	CPU

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
						*localInterface*peer=*peerFQDN:peerPort* user=*username*]		
		EIP explicit disconnection	6	EIP	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*username*]	Socket disconnection	CPU
		HTTP disconnection (DPWS)	6	HTTP	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*username*]	Socket disconnection	CPU
		HTTPS disconnection triggered by a time out	6	HTTPS	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*username*]	Time-out logout	CPU eNOR
		OPC UA disconnection triggered by a time out	6	OPC-UA	DISCONNECTION	[meta sequenceId=*num*] [authn@3833 itf=*localPort* |	Time-out logout	—

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
						*localInterface*peer= *peerFQDN: peerPort* user= *username*]		
		DNP3 disconnection	6	DNP3	DISCONNECTION	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer= peerFQDN: peerPort user= username]	Socket disconnection	eNOR
		IEC 60870 disconnection	6	IEC60870	DISCONNECTION	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer= peerFQDN: peerPort user= username]	Socket disconnection	eNOR
Major parameter change at RUN time	Major parameters at run time that change and can cause significant impact on the system	Controller application parameters change: cycle time	6	Configuration	PARAMETER_SET	[meta sequenceId=*num*] [config@3833 object= "PLC application" value= *value*]	Scan time	CPU
Backup operation.	Backup part or all of component.	Download application from the controller.	6	Backup	BACKUP	[meta sequenceId=*num*] [backup@3833 object= "PLC application"]		CPU

Logged event	Descrip-tion	Additional descrip-tion	Severi-ty	PROCID	MSGID	Structured – data	Msg	Devices
		Export Cyberse-curity configura-tion from BMENUA or BMENOR web pages.	6	Backup	BACKUP	[meta sequen-ceId=*num*] [back-up@3833 object= "Cyberse-curity configura-tion"]		eNOR
Restore operation.	Restore part or all of compo-nent.	Upload controller application/ configura-tion inside the controller.	6	Configu-ration	CONFIG-URA-TION_ CHANG-E	[meta sequen-ceId=*num*] [con-fig@3833 object= *Object* *Object* = "PLC application" or "PLC configura-tion		CPU
		Restore controller application inside the controller.	6	Backup	RE-STORE	[meta sequen-ceId=*num*] [back-up@3833 object= "PLC applica-tion"]		CPU
		Import Cyberse-curity configura-tion from BMENUA or BMENOR web pages.	6	Backup	RE-STORE	[meta sequen-ceId=*num*] [back-up@3833 object= "Cyberse-curity configura-tion"]		eNOR
Firmware update	A new firmware has been success-fully verified and installed.	Upload a new firmware in the controller.	6	Configu-ration	FIRM-WARE_ UPDATE	[meta sequen-ceId=*num*] [con-fig@3833 object= *Object* value= *versio-n*]"Object =		CPU eNOR

Logged event	Descrip-tion	Additional descrip-tion	Severi-ty	PROCID	MSGID	Structured – data	Msg	Devices
						"Firmware", "Safety copro", "Web pages		
Invalid firmware update	A new firmware was not installed due to an error.	A new firmware was not installed because of an incompati-ble version or invalid signature.	1	Configu-ration	FIRM-WARE_ INVALID	[meta sequen-ceId=*num*] [con-fig@3833 object= *Object* value= *versio-n*]"Object = "Firmware", "Safety copro", "Web pages”	Incompati-ble version, invalid signature	CPU eNOR
Modifica-tion of the time of the device	A human user request to change time and date	—	5	Configu-ration	TIME_ CHANG-E	[meta sequen-ceId=*num*] [con-fig@3833 object= *"Time"* value= *datetime*]		CPU
Time signal out of tolerance	The compo-nent validates time synchroni-zation messages received through time synchroni-zation channels. It sounds an alarm if the time synchroni-zation message is not within the tolerances of the	—	1	Configu-ration	TIME_ UNEX-PECTED	[meta sequen-ceId=*num*] [con-fig@3833 object= "Time" value= *datetime*]	Time signal out of tolerance	

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
	component internal/ local clock (time in the past, far away, …)							
Hardware change	Change detected in network topology.	Network physical port change: port link up/ down	6	System	HARDWARE_CHANGE	[system@3833 object= *Object*] Object = "eth" followed by decimal number	Port link up, port link down	CPU
		Any topology change detected from RSTP / HSR / PRP	6	System	HARDWARE_CHANGE	[system@3833 object= *Object*] Object = "eth" followed by decimal number	Port enable, port disable, port learning, port forward, port blocking	CPU
	Change detected in hardware.	M580 SD card insertion/ extraction	6	System	HARDWARE_CHANGE	[system@3833 object= "SDCard"]	Insertion, extraction	CPU
Operating mode change	Program operating mode change (Run, Stop, Init, Halt) Mode maintenance / SafeRun / Stop SAFE task	—	5	System	OPERATING_MODE_CHANGE	[system@3833 object= Object] Object = "PLC" or "PLC safe task" or "Module"	"Init" "Run" "Stop" "Halt" "Maintenance mode" "Safe mode" "Hsby primary" "Hsby secondary" "Hsby wait" "Master" "Non master"	CPU
Invalid configuration (outside	A new (not Cybersecurity) configuration was	Data integrity error (controller	1	Configuration	CONFIGURATION_INVALID	[meta sequenceId=*num*] [config@3833	Invalid format, incompatible version	

Logged event	Description	Additional description	Severity	PROCID	MSGID	Structured – data	Msg	Devices
Cybersecurity)	not installed due to an error.	application, …)				object= *Object* value= *version*]"*Object*= "PLC application" or "Module configuration"		
Reboot	Hardware reset or automatic reset after firmware upload	—	1	System	REBOOT	—	Firmware update, reset button	CPU
Product certificate (and/or keys) modification	Certificate management: SL1Product self-signed certificate creation	—	6	Credential	CERTIFICATE_CHANGE	[meta sequenceId=*num*] [cred@3833 name= *CommonName*]	Certificate creation	CPU

NOTE: In addition to the previously described structure, each message also contains the following fields and values:

- Facility = 10
- HOSTNAME = fully qualified domain name (FQDN) or local IP address
- APPNAME = Commercial reference name, for example, BMEP584040

Example of Syslog Server Messages

Date	Time	Priority	Hostname	Message
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="331"][authn@3833 if="eth" peer="192.168.11.50:52470"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="330"][authn@3833 if="eth" peer="192.168.11.50:52468"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="329"][authn@3833 if="eth" peer="192.168.11.50:52466"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="328"][authn@3833 if="eth" peer="192.168.11.50:52464"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="327"][authn@3833 if="eth" peer="192.168.11.50:52462"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="326"][authn@3833 if="eth" peer="192.168.11.50:52460"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="325"][authn@3833 if="eth" peer="192.168.11.50:52458"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="324"][authn@3833 if="eth" peer="192.168.11.50:52456"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="323"][authn@3833 if="eth" peer="192.168.11.50:52454"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="322"][authn@3833 if="eth" peer="192.168.11.50:52452"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="321"][authn@3833 if="eth" peer="192.168.11.50:52450"] Socket connection
11-08-2021	11:54:33	System0.Info	192.168.11.1	1 2021-08-26T11:22:12.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="320"][authn@3833 if="eth" peer="192.168.11.50:52442"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:07.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="319"][authn@3833 if="eth" peer="192.168.1.100:34246"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="318"][authn@3833 if="eth" peer="192.168.11.50:52440"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="317"][config@3833 object="Module"]
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:04.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="316"][config@3833 object="Module"]
11-08-2021	11:54:24	System0.Notice	192.168.11.1	1 2021-08-26T11:22:03.000Z 192.168.11.1 BMEP585040 System OPERATING_MODE_CHANGE [meta sequenceId="315"][system@3833 object="PLC"] Init
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="314"][config@3833 object="PLC application"]
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Backup RESTORE [meta sequenceId="313"][backup@3833 object="PLC application"]
11-08-2021	11:54:07	System0.Info	192.168.11.1	1 2021-08-26T11:21:46.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="312"][authn@3833 if="eth" peer="192.168.1.100:34235"] Socket connection
11-08-2021	11:53:20	System0.Info	192.168.11.1	1 2021-08-26T11:20:59.000Z 192.168.11.1 BMEP585040 Backup BACKUP [meta sequenceId="311"][backup@3833 object="PLC application"]

Event Log Message Descriptions for M580 Controllers (firmware earlier than V4.10), BMENUA0100 (firmware V3.01 or later) and BMENOR2200H

This topic presents event log message descriptions for:

- M580 controllers with firmware earlier than version 4.10 (abbreviated CPU in the **Devices** column)
- BMENUA0100 OPC UA communication modules (abbreviated NUA in the **Devices** column)
- BMENOR2200H remote terminal unit (abbreviated eNOR in the **Devices** column)

Logged event	Description	Facility	Severity	MSGID	MSG: peerAddr	MSG: type	MSG: appMsg	Devices
Successful connection to or from a tool or a device: • successful login • successful TCP connection	Successful login (data storage using FTP, FDR server using FTP, firmware upload using FTP)	10	6	FTP	Remote IP address	Li1: Successful connection (MNT_ENG_MSG_TYP_CNCTN_SUCCESS)	Successful login	CPU
	Successful login (web			HTTP-S	(null)		Successful login	NUA

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
	server using HTTPS)							
	Successful login (firmware upgrade using HTTPS)			HTTP-S	(null)		Successful login	NUA
	Successful login (OPC-UA)			OPC UA	(null)		Successful login	NUA
	Successful login (Control Expert application password using Modbus-Umas)			DE-VICE_ MAN-AGER	(null)		Successful login	CPU
	Successful login (web server using HTTP)			HTTP	(null)		Successful login OR successful connection (if no user login on M580 web pages)	CPU
	Successful TCP connection (no user)			MOD-BUS	Remote IP address		Successful connection	CPU
	Successful TCP connection (no user)			EIP	(null)		Successful connection	CPU
	Successful connection on DNP3 communica-tion protocol (about DNP3 master and outstation)			DNP3	Remote IP address		Successful connection	eNOR
	Successful connection on IEC60870 communica-tion protocol (about			IE-C608-70	Remote IP address		Successful connection	eNOR

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
	IEC60870 client and server)							
Connection problem to or from a tool or a device: • TCP connection problem due to ACL check (source IP address/ TCP port filtering) • Login problem	Login problem (data storage using FTP, FDR server using FTP, firmware upload using FTP)	10	4	FTP	Remote IP address	Li2: Unsuccess-ful connection (wrong credential) (MNT_ ENG_ MSG_TYP_ CNCTN_ FAILURE)	Failed login	CPU
	Login problem (web server using HTTPS)			HTTP-S	(null)		Failed login	NUA
	Login problem (firmware upgrade using HTTPS)			HTTP-S	(null)		Failed login	NUA
	Login problem (OPC UA)			OPC UA	(null)		Failed login	NUA
	Login problem (web server using HTTP)			HTTP	Remote IP address		Failed login OR failed connection (if no user login)	CPU
	Login problem (Control Expert application password using Modbus-Umas)			DE-VICE_ MAN-AGER	Remote IP address		Failed login	CPU
	TCP connection problem (no user)			MOD-BUS	Remote IP address		Failed connection	CPU
	TCP connection problem (no user)			EIP	Remote IP address		Failed connection	CPU
	Connection problem on DNP3			DNP3	Remote IP address		Failed connection	eNOR

Logged event	Description	Facility	Severity	MSGID	MSG: peerAddr	MSG: type	MSG: appMsg	Devices
	communication protocol (about DNP3 master and outstation)							
	Connection problem on IEC60870 communication protocol (about IEC60870 client and server)			IEC608-70	Remote IP address		Failed connection	eNOR
Disconnection triggered by local or peer: • TCP disconnection • On demand logout	Disconnection triggered by either the peer/user/local	10	6	FTP	(null)	Li5: Disconnection triggered by the peer/user (MNT_ENG_MSG_TYP_DISCONNECTION)	Disconnection	—
	Disconnection triggered by either the peer/user/local			HTTP-S	(null)		Disconnection	NUA
	Disconnection triggered by either the peer/user/local			OPC UA	(null)		Disconnection	NUA
	Disconnection triggered by either the peer/user/local			MODBUS	Remote IP address		Disconnection	CPU
	—			DNP3	(null) or remote IP address		Disconnection	eNOR
	—			IEC608-70	(null) or remote IP address		Disconnection	eNOR

Logged event	Description	Facility	Severity	MSGID	MSG: peerAddr	MSG: type	MSG: appMsg	Devices
Automatic logout (inactivity timeout) HTTPS OPC UA	Disconnection triggered by a timeout	10	6	HTTPS	(null)	Li6: Disconnection triggered by a timeout (MNT_ENG_MSG_TYP_DSCNCT_TIMEOUT)	Auto logout	NUA
	Disconnection triggered by a timeout			OPC UA			Auto logout	NUA
Major changes in the system: Parameters run time change outside configuration.	Major change of cycle time or watch dog controller application parameters change (cycle time, watch dog)	13	5	DEVICE_MANAGER	(null)	Li87: System parameter update (MNT_ENG_MSG_TYP_PARAMETER_UPDATE)	XXXX parameter update (with XXXX that identifies the parameter) XXXX = Cycle time example: Cycle time parameter update	CPU
Major changes in the system: • Application or configuration download from the device • Export (recording) cybersecurity configuration files from the device	Download of a configuration file from the device	13	6	MODBUS	(null)	Li8: Download of a configuration file from the device (MNT_ENG_MSG_TYP_CONF_DL)	Application download OR configuration download	CPU
				HTTPS			Cybersecurity configuration backup	NUA
Major changes in the system	Upload of application/ configuration OR configuration only into the device	13	6	MODBUS	(null)	Li9: Upload of a configuration file into the device (MNT_ENG_	Application upload OR configuration upload	CPU NUA

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
	(including CCOTF)					MSG_TYP_ CONF_UL)		
	Import (restore) cybersecurity configuration file into the device			HTTP-S			Cybersecur-ity configura-tion restore	NUA
Major changes in the system	Upload of web pages into the device	13	6	FTP	(null)	Li10: Upload of a new firmware in the device (MNT_ ENG_ MSG_TYP_ FIRM-WARE_ UPDATE)	Web pages upload	CPU
	Upload of new safety co-controller firmware			FTP			Safety co-controller firmware upload	CPU
	Upload of a new firmware in the device			FTP			Firmware upload	CPU
	Upload of a new firmware in the device			HTTP-S			Firmware upload	NUA
Major changes in the system	Modification of the time of the device	13	6	DE-VICE_ MAN-AGER	(null)	LI15: Modification of the time of the IED	Time major update	NUA
Communication parameters run time, successful change outside configuration	Enable/ disable of communica-tion services	10	4	DE-VICE_ MAN-AGER	(null)	Li18: Any port, either physical (serial, USB) or logical (telnet, FTP) activation/ deactivation (MNT_ ENG_ MSG_TYP_ PORT_ MANAGE-MENT)	Major communica-tion parameter update: XXXX YYYY XXXX = EIP or DHCP or FTP or MODBUS or SNMP or HTTP or SECURITY or NTP or IPSEC or	CPU NUA eNOR

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
							DEVICE_ MANAGER For NUA only:XXXX = Control Expert data flows to controller only. OR Control Expert data flows to device network. OR CPU to CPU data flows for NOR only: XXXX = "DNP3 over TLS channel *channel name*] OR IEC60870 over TLS YYYY= enable OR disable, example: Major communica-tion parameter update: FTP enable	
Network physical port change: port link up/down	Any network physical port status change. Can be the simple status of an Ethernet port or information gathered from RSTP / HSR / PRP algorithm for redundant systems	10	4	DE-VICE_ MAN-AGER	(null)	LI19: Any network physical port status change. Can be the simple status of an Ethernet port or information gathered from RSTP / HSR / PRP algorithm for redundant	Major network physical port status change: XXXX link YYYY XXXX = ETH following by decimal number for the port OR front port YYYY = link up OR link down, example:	CPU NUA

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
						systems (MNT_ ENG_ MSG_TYP_ NETWK_ PORT_ CHG)	Major network physical port status change: ETH1 link up)	
Any topology change detected	Any topology change detected from RSTP / HSR / PRP	10	4	RSTP	(null)	LI20: Any topology change detected from RSTP / HSR / PRP algorithms for redundant systems (MNT_ ENG_ MSG_TYP_ NTWK_ TPLGY_ CHG)	Topology change detected OR topology change detected: XXXX YYYY XXXX = ETH following by decimal number for the port OR front port YYYY = enable, disable, learning, forward, blocking	CPU NUA
Integrity check error: • Digital signature error • Integrity only (hash mac) • Configura-tion files, CRC error	Firmware integrity error	10	6	DE-VICE_ MAN-AGER	(null)	LI84: Data integrity error (MNT_ ENG_ MSG_ DATA_ INTEGRI-TY_ ERROR) CONFIGU-RATION_ INVALID	Firmware integrity error	CPU NUA
	Data integrity error; CS Conf, cert, whitelist, or RBAC			DE-VICE_ MAN-AGER			Data integrity error	NUA
	Configuration file integrity error, CRC error			EVT-LO_ PRO-TO-COL_ NA			Integrity error	eNOR
Major changes in the system: Reboot	Reboot after firmware upload	13	4	DE-VICE_ MAN-AGER	(null)	LI14: MNT_ ENG_ MSG_TYP_ REBOOT_ ORDER	Restart	CPU NUA

Logged event	Description	Facility	Severity	MSGID	MSG: peerAddr	MSG: type	MSG: appMsg	Devices
Major changes in the system	• Controller operating mode change (Run, Stop, Init, Halt) • Maintenance mode • Safety-related operating modes change (SafeRun, Stop Safe task)	13	5	DEVICE_MANAGER	(null)	LI85: Operating mode change (MNT_ENG_MSG_OPERATING_MODE_CHANGE)	XXXX state update: YYYY (with XXXX that identifies the object which state change and YYYY that identifies the new state) XXXX = PLC OR PLC safe task OR device YYYY = INIT OR Stop OR Run OR Halt OR Maintenance mode OR Safe mode, Examples: PLC state update: RUN, PLC state update: Maintenance mode	CPU
Major changes in the system: Hardware change	Operation on SD card	13	6	DEVICE_MANAGER	(null)	LI26: Hardware change (MNT_ENG_MSG_HARDWARE_CHANGE)	Hardware update: XXXX (with XXXX that describes the update) XXXX = SD card insertion OR SD card extraction	CPU
	Rotary wheel position change: Reset, Advanced			DEVICE_MANAGER			Hardware update: XXXX (with XXXX that describes the update) XXXX = Back to factory mode OR	NUA

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
							Secure mode	
Major change in Cybersecurity RBAC (done through Cybersecurity configuration web pages)	• Create user account. • Delete user account. • Update user account.			HTTP-S	(null)	Li11: MNT_ENG_MSG_TYP_RBAC_UPDATE	Update RBAC	NUA
Major change in Cybersecurity policy (done through Cybersecurity configuration web pages)	• Network services • Event log • Security policy • Security banner	10	4	HTTP-S	(null)	Li12: MNT_ENG_MSG_TYP_SECURI-TY_UPDATE_UPDATE	Major cybersecuri-ty parameter update: Network services, Major cybersecuri-ty parameter update: event log" "Major cybersecuri-ty parameter update: security policy" "Major cybersecuri-ty parameter update: Security banner	NUA
Major change in Cybersecurity device specific parameters (done through Cybersecurity configuration web pages)	• Enable/disable and configure IPSEC. • Enable/disable and configure OPC UA.	10	4	HTTP-S	(null)	Li13: MNT_ENG_MSG_TYP_DSS_UPDATE	Major cybersecuri-ty parameter update: IPSEC, Major cybersecuri-ty parameter update: OPC UA	NUA

Logged event	Description	Facility	Severity	MSGID	MSG: peerAddr	MSG: type	MSG: appMsg	Devices
	• Enable/disable and configure DNP3.							
Authorization problem	An action on a resource from a user or machine is not authorized.	10	4	HTTP-S	(null)	Li21: MNT_ENG_MSG_TYP_AUTH_REQ	Failed authorization	—
Certificate management	Add/remove client certificate	10	4	HTTP-S	(null)	Li89: Certificate management (MNT_ENG_MSG_TYP_CERT_MGT)	Add client certificate. OR Remove client certificate.	NUA
• Certificate management • Certificate expired	Server certificate expiration detection on restart	10	3	DEVICE_MANAGER	(null)	Li29: Certificate management (MNT_ENG_MSG_TYP_CERT_EXPIRE)	Certificate expired	NUA
Specific for eNOR project								
Authentication problem	—	10	4	DNP3_Master OR DNP3_Outstation	Remote IP address	Li100: MNT_ENG_MSG_TYPE_AUTHENTICATION_FAILURE	Channel [*channel name*] authentication failed	eNOR
Unexpected response	—	10	4	DNP3_Master OR DNP3_Outstation	Remote IP address	Li101: MNT_ENG_MSG_TYPE_UNEXPECTED_RESPONSE	Channel [*channel name*] unexpected response	eNOR
No response	—	10	4	DNP3_Master	Remote IP address	Li102: MNT_ENG_	Channel [*channel*	eNOR

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
				OR DN-P3_ Out-station		MSG_ TYPE_NO_ RE-SPONSE	*name*] no response	
Aggressive mode not supported.	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li103: MNT_ ENG_ MSG_ TYPE_ AGGRES-SIVE_ MODE_ NOT_ SUPPOR-TED	Channel [*channel name*] aggressive mode not supported	eNOR
MAC algorithm not supported.	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li104: MNT_ ENG_ MSG_ TYPE_ MAC_ ALGO-RITHM_ NOT_ SUPPOR-TED	Channel [*channel name*] MAC algorithm not supported	eNOR
Key wrap algorithm not supported.	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li105: MNT_ ENG_ MSG_ TYPE_ KEY-WRAP_ ALGO-RITHM_ NOT_ SUPPOR-TED	Channel [*channel name*] key wrap algorithm not supported	eNOR
Authorization problem	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li86: MNT_ ENG_ MSG_TYP_ AUTHORI-ZATION_ FAILURE	Channel [*channel name*] authoriza-tion failed	eNOR
Update key change method not permitted.	—	10	4	DN-P3_ Master OR	Remote IP address	Li106: MNT_ ENG_ MSG_ TYPE_	Channel [*channel name*] update key change	eNOR

Logged event	Description	Facili-ty	Severi-ty	MSGI-D	MSG: peer-Addr	MSG: type	MSG: appMsg	Devices
				DN-P3_ Out-station		UPDATE_ KEY_ CHANGE_ METHOD_ NOT_ PERMIT-TED	method not permitted	
Invalid signature	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li107: MNT_ ENG_ MSG_ TYPE_ INVALID_ SIGNA-TURE	Channel [*channel name*] invalid signature	eNOR
Invalid certification data	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li108: MNT_ ENG_ MSG_ TYPE_ INVALID_ CERTIFI-CATION_ DATA	Channel [*channel name*] invalid certification data	eNOR
Unknown User	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li109: MNT_ ENG_ MSG_ TYPE_ UN-KNOWN_ USER	Channel [*channel name*] unknown user	eNOR
Max session key status request exceeded.	—	10	4	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li110: MNT_ ENG_ MSG_ TYPE_ MAX_ SESSION_ KEY_ STATUS_ REQ_ EXCEED	Channel [*channel name*] max session key status request exceeded	eNOR
Session key change success	—	10	6	DN-P3_ Master OR DN-P3_ Out-station	Remote IP address	Li111: MNT_ ENG_ MSG_ TYPE_ SESSION_ KEY_ CHANGE_ SUCCESS	Channel [*channel name*] session key change success	eNOR

NOTE: In addition to the structure described above, each message will also contain the following fields and values following the Severity field:

- HOSTNAME = local IP address or null
- APPNAME = commercial reference name, for example, BMEP584040
- PROCID = not used
- MSG:IssuerAdress = local IP address
- MSG:Peer = not used

Control Identification and Authentication

Managing Accounts

The following are best practices for account management:

- Create a standard user account with no administrative privileges.
- Use the standard user account to launch applications. Use more privileged accounts to launch an application only if the application requires higher privilege levels to perform its role in the system.
- Use an administrative level account to install applications.

Managing User Account Controls (UAC) Using Windows 10

To help minimize unauthorized PC operating system changes, Windows 10 grants applications the permission levels of a normal user with no administrative privileges. Without administrative privileges, applications cannot make changes to the system. UAC prompts the user to grant or deny additional permissions to an application. Set UAC to its maximum level. At the maximum level, UAC prompts the user before allowing an application to make any changes that require administrative permissions.

To access UAC settings in Windows 10, open **Control Panel > User Accounts and Family Safety > User Accounts > Change User Account Control Settings**, or enter **UAC** in the Windows 10 **Start Menu** search field.

Managing Passwords

Password management is one of the fundamental tools of device hardening, which is the process of configuring a device against communication-based threats. It is a good practice to apply the following password management guidelines:

- Enable password authentication on all e-mail and Web servers, controllers, and Ethernet interface modules.
- Change all default passwords immediately after installation, including those for:
  - user and application accounts on Windows, SCADA, HMI, and other systems
  - scripts and source code
  - network control equipment
  - devices with user accounts
  - FTP servers
  - SNMP and HTTP devices
  - Control Expert
- Grant passwords only to people who require access. Prohibit password sharing.
- Do not display passwords during password entry.
  - Require passwords that are difficult to guess. They should contain at least 8 characters and should combine upper and lower case letters, digits, and special characters when permitted.
- Require users and applications to change passwords on a scheduled interval.
- Remove employee access accounts when employment has terminated.
- Require different passwords for different accounts, systems, and applications.
- Maintain a secure master list of administrator account passwords so they can be quickly accessed in the event of an emergency.
- Implement password management so that it does not interfere with the ability of an operator to respond to an event such as an emergency shutdown.
- Do not transmit passwords by e-mail or other manner over the insecure Internet.

Managing HTTP

Hypertext transfer protocol (HTTP) is the underlying protocol used by the Web. It is used in control systems to support embedded Web servers in control products. Schneider Electric Web servers use HTTP communications to display data and send commands using webpages.

If the HTTP server is not required, disable it. Otherwise, use *hypertext transfer protocol secure* (HTTPS), which is a combination of HTTP and a cryptographic protocol, instead of HTTP if possible. Only allow traffic to specific devices, by implementing access control mechanisms such as a firewall rule that restricts access from specific devices to specific devices.

You can configure HTTPS as the default Web server on the products that support this feature.

Import and trust the self-signed certificates of your M580 controllers into your web browsers from a trusted network. This helps prevent the notification from being displayed when connecting to the web pages of your trusted controllers.

NOTE: This process must be repeated when the certificates of your controllers are renewed, such as when changing the IP addresses of your controller from the application.

Managing FTP

File transfer protocol (FTP) provides remote file handling services through a TCP/IP-based network, such as Internet. FTP uses a client-server architecture as well as separate control and data connections between the client and the server.

Consider the following behavior of the FTP service provided by Schneider Electric:

- FTP protocol is disabled by default.
- FTP protocol is necessary for specific maintenance and configuration activities only. It is a good practice to disable the entire set of FTP services when they are not required.
- FTP protocol is an unsecure protocol and must be used with care to avoid sensitive information disclosure and unauthorized access to the controllers:
  - Change the default passwords of all devices that support FTP, when possible.
  - Use Access Control List to restrict communication to the authorized IP addresses. Refer to “Cybersecurity Services Per System” for details on the concerned module.
  - When using BMENOC module, configure the IPSEC feature (Set Up Encrypted Communication, page 35).
  - Block all inbound and outbound FTP traffics at the boundary of the enterprise network and operations network of the control room.
  - Filter FTP commands between the control network and operations network to specific hosts or communicate them over a separate, encrypted management network.
  - Use external module to setup a VPN between the controller impacted modules and the engineering workstation on control network.

- BMENOC0301 and BMENOC0311 modules do not support IP forwarding to the device network.

  If transparency is required between the control and device networks, an external router/VPN is needed to provide an encrypted communication between the control and device networks (refer to the illustration in CSPN Security Target, page 42).

In FTP protocol, transparency is required to perform the following operations from the control network:

- Update of M580 controller firmware from the Automation Device Maintenance.
- Network diagnostics of M580 controller executed from a network management tool through SNMP service.

Managing SNMP

Simple network management protocol (SNMP) provides network management services between a central management console and network devices such as routers, printers, and controllers. The protocol consists of three parts:

- Manager: an application that manages SNMP agents on a network by issuing requests, getting responses, and listening for and processing agent-issued traps.
- Agent: a network-management software module that resides in a managed device. The agent allows configuration parameters to be changed by managers. Managed devices can be any type of device: routers, access servers, switches, bridges, hubs, controllers, drives.
- Network management system (NMS): the terminal through which administrators can conduct administrative tasks.

Schneider Electric Ethernet devices have SNMP service capability for network management.

Often SNMP is automatically installed with **public** as the read string and **private** as the write string. This type of installation allows an attacker to perform reconnaissance on a system to create a denial of service.

To help reduce the risk of an attack using SNMP:

- If SNMP v1 is required, use access settings to limit the devices (IP addresses) that can access the switch. Assign different read and read/write passwords to devices.
- Change the default passwords of all devices that support SNMP.
- Block all inbound and outbound SNMP traffic at the boundary of the enterprise network and operations network of the control room.
- Filter SNMP v1 commands between the control network and operations network to specific hosts or communicate them over a separate, encrypted management network.
- Control access by identifying which IP address has privilege to query an SNMP device.

- Use an external module to set up a VPN between the controller impacted modules and the engineering workstation on the control network.

Managing Control Expert Application, Section, Data Storage, and Firmware Password

In Control Expert, passwords apply to the following (depending on the controller):

- **Application**

  Control Expert and controller application protection by a password helps prevent unwanted application modification, download, or opening (.STU, .STA and .ZEF files). The password is stored encrypted in the application.

  In addition to the password protection you can encrypt the .STU, .STA and .ZEF files. The file encryption feature in Control Expert helps prevent unauthorized modifications by unqualified personnel and reinforces protection against theft of intellectual property and other malicious intentions. The file encryption option is protected by a password mechanism.

  NOTE: When a controller is managed as part of a system project, the application password and file encryption are disabled.

  More details are provided in the *Application Protection* topic (see EcoStruxure™ Control Expert, Operating Modes).

- **Section**

  The section protection function is accessible from the **Properties** screen of the project in offline mode. This function is used to help protect the program sections. More details are provided in the *Section and Subroutine Protection* topic (see EcoStruxure™ Control Expert, Operating Modes).

  NOTE: The section protection is not active as long as the protection is not activated in the project.

- **Data Storage/Web**

  Data storage protection by a password can help prevent unwanted access to the data storage zone of the SD memory card (if a valid card is inserted in the controller). It can also help prevent unwanted access to web diagnostics (for M580 controller firmware ≥ 4.0). More details are provided in the *Data Storage Protection* topic (see EcoStruxure™ Control Expert, Operating Modes).

- **Firmware**

  Firmware download protection by a password helps prevent download of malicious firmware. More details are provided in the *Firmware Protection* topic (see EcoStruxure™ Control Expert, Operating Modes).

Control Authorizations

Control Expert Security Editor

A security configuration tool is used to define software users and their respective authorizations. EcoStruxure Control Expert access security affects the terminal or terminals on which the software is installed and not the project, which has its own protection system.

For more detailed information, refer to *EcoStruxure™ Control Expert, Security Editor, Operation Guide*.

It is a good practice to establish a dedicated password to the security administrator (*SecurityAdmin*) and limit other users authorizations with a restricting profile.

Programming and Monitoring Mode

Two modes are available to access the controller in **Online** mode:

- **Programming** mode: The controller program can be modified. When a terminal is first connected to the controller, the controller becomes reserved and another terminal cannot be connected as long as the controller is reserved.
- **Monitoring** mode: The controller program cannot be modified, but the variables can be modified. The monitoring mode does not reserve the controller, and an already reserved controller can be accessed in monitoring mode.

To choose a mode in EcoStruxure Control Expert , select: **Tools > Options... > Connection > Default connection mode**.

More details on those modes are provided in the *Services in Online Mode* topic (see EcoStruxure™ Control Expert, Operating Modes).

It is a good practice to set the **Online** controller access mode to **Monitoring** whenever possible.

Program Sections Protection

The section protection function is accessible from the **Properties** screen of the project in offline mode. This function is used to protect the program sections. More details are provided in the *Section and Subroutine Protection* topic (see EcoStruxure™ Control Expert, Operating Modes).

NOTE: The section protection is not active as long as the protection has not been activated in the project.

It is a good practice to activate the sections protection.

Controller Memory Protection

The memory protection prohibits the transfer of a project into the controller and modifications in online mode, regardless of the communication channel.

NOTE: The controller memory protection cannot be configured with Hot Standby controllers. In such cases, use IPsec encrypted communication.

The memory protection is activated as follows:

- Modicon M340 controller: Input bit. For details, refer to the *Configuration of Modicon M340 processors* section (see EcoStruxure™ Control Expert, Operating Modes).
- Modicon M580 controller: Input bit. For details, refer to the *Managing Run/Stop Input* section (see Modicon M580, Hardware, Reference Manual).
- Modicon Quantum controller: Physical key switch on the controller module, either for low end (see Quantum using EcoStruxure™ Control Expert, Hardware, Reference Manual) or high end (see Quantum using EcoStruxure™ Control Expert, Hardware, Reference Manual) controller.
- Modicon Premium controller: Input bit. For details, refer to the *Configuration of Premium processors* section (see EcoStruxure™ Control Expert, Operating Modes).
- Modicon MC80 controller: Input bit. For details, refer to the Modicon MC80 Program Logic Controller (PLC) User Manual.
- Modicon Momentum MDI controller: Input bit. For details, refer to the EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide.

It is a good practice to activate the controller memory protection whenever possible.

Controller Remote Run/Stop Access

The remote run/stop access management defines how a controller can be started or stopped remotely and depends on the system.

NOTE: The controller remote run/stop access cannot be configured with Hot Standby controllers. In such cases, use IPsec encrypted communication.

Controller	Access
Modicon M580:	Controller remote access to run/stop allows one of the following: • Stop or run the controller remotely by request. • Stop the controller remotely by request. Rejects requests to run the controller remotely. Only a run controlled by the input is available when a valid input is configured. • Rejects requests to run or stop the controller remotely by request. Refer to the *Managing Run/Stop Input* for controller configuration options that help prevent remote commands from accessing the Run/Stop modes section (see Modicon M580, Hardware, Reference Manual).
Modicon M340:	Controller remote access to run/stop allows one of the following: • Stop or run the controller remotely by request. • Stop the controller remotely by request. Rejects requests to run the controller remotely. Only a run controlled by the input is available when a valid input is configured. Refer to the *Configuration of Modicon M340 Processors section* (see EcoStruxure™ Control Expert, Operating Modes).
Modicon Premium:	Controller remote access to run/stop allows one of the following: • Stop or run the controller remotely by request. • Stop the controller remotely by request. Rejects requests to run the controller remotely. Only a run controlled by the input is available when a valid input is configured. Refer to the *Configuration of Premium\Atrium Processors section* (see EcoStruxure™ Control Expert, Operating Modes).
Modicon Quantum:	Controller remote access to run/stop allows to: • Stop or run the controller remotely with a request.
Modicon MC80:	Controller remote access to run/stop allows one of the following: • Stop or run the controller remotely by request. • Stop the controller remotely by request. Rejects requests to run the controller remotely. Only a run controlled by the input is available when a valid input is configured. • Reject running or stopping the controller remotely by request. Refer to the *Configuration of Modicon MC80 Processors* section in the Modicon MC80 Program Logic Controller (PLC) User Manual.
Modicon Momentum MDI	Controller remote access to run/stop allows one of the following: • Stop or run the controller remotely by request. • Rejects requests to stop the controller remotely. Only a stop controlled by the input is available when a valid input is configured. Refer to the *Configuration of Modicon Momentum MDI Processors* section in the Modicon Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide.

It is a good practice to deny running or stopping the controller remotely by request.

Controller Variables Access

To help protect controller data from unauthorized read or write access, use the following best practices whenever possible:

- Use unlocated data.
- Configure EcoStruxure Control Expert to store only HMI variables: **Tools > Project Settings... > PLC embedded data > Data dictionary > Only HMI variables**.

  Only HMI variables can be selected only if **Data dictionary** is selected.
- Tag as *HMI* the variables that are accessed from HMI or SCADA. Variables that are not tagged as *HMI* cannot be accessed by external clients.
- Connection with SCADA has to rely on OFS.

Data Memory Protection

You can activate data memory protection in EcoStruxure Control Expert by navigating to **Tools > Project Setting > PLC embedded data**, then select **Apply**. This feature helps protect both located and unlocated data.

For more information on the data memory protection feature, refer to the topic Data Memory Protection in the EcoStruxure Control Expert Operating Modes document.

Manage Data Integrity Checks

Introduction

The integrity check feature helps prevent EcoStruxure Control Expert files and software from being changed by a virus or malware.

Automatic Integrity Check

The servers are configured to start automatically when the computer is powered-on or restarted. Before the servers start, an integrity check is performed on both.

The server starts only if the integrity check completes without detecting data corruptions. If the integrity check detects data corruption, an error is logged that you can view using the **Event viewer**.

A message box indicates the corrupted files. Click **OK** and the EcoStruxure Control Expert instance closes. For details, refer to the *EcoStruxure™ Control Expert, Installation Manual* and the chapter *Enabling Client/server Communication*.

Manual Integrity Check with Control Expert Classic

To perform a manual integrity check when an instance of Control Expert Classic is started, follow these steps:

Step	Action
1	Click **Help > About Control Expert XXX**.
2	In the **Integrity check** field, click **Perform self-test**. **Result**: The integrity check runs in the background. Control Expert creates a log of the successful and unsuccessful component login. The log file contains the IP address, the date and time, and the result of the login. **NOTE:** If an integrity check displays an unsuccessful component login, the **Event Viewer** displays a message. Click **OK**. Manually fix the items in the log.

M580 Firmware Integrity Check

The M580 controller firmware integrity check is performed automatically after a new firmware upload or restart of the Modicon M580 PAC.

Management of SD Card

Activate the application signature in order to avoid running an incorrect application from an SD card.

The SD card signature is managed using the `SIG_WRITE` and `SIG_CHECK` functions (see *EcoStruxure™ Control Expert, Communication, Block Library*).

Configuring the SD Card Port Protection

An SD Card Protection mechanism is available for controllers with firmware version 4.30 or later.

This feature can be enabled or disabled from the **Configuration** tab on the controller's web pages.

Open the **Home** page:

Step	Action
1	Open an Internet browser.
2	In the address bar, enter the IP address of the controller.
3	Enter the username **modbususer** and the application password.
4	Press **Enter** and wait for the page to open.
5	Select the **Configuration > Cyber Security**.
6	In the drop-down list, select **SD Card Port** to configure this feature: • **Enabled** (SD cards are not considered by the controller). • **Disabled** (SD cards are considered by the controller). **NOTE:** If an SD card is already inserted in the controller, the protection is activated when the SD card is removed or when the controller is power cycled. **NOTE:** When the SD Card Port Protection is enabled, the controller backup memory zone is the controller NAND. Therefore, clearing the backup zone when the protection is enabled results in clearing the controller NAND.

Operating Modes on SD Card and %SW97 Related Values

SD Card Protection by Web Page	Operating Mode	%SW97 Value	Result
Disabled	Sign in with modbususer and plug the SD Card in.	%SW97 value is 0 and SD Card led is on. A refresh on the data storage Web page leads to the apparition of any error about SD Card.	The SD Card is mounted when the protection is off.
Enabled	Enable the protection and plug the SD Card in.	%SW97 value is 15 and the SD Card led is flashing. A refresh on the data storage Web page for Web user leads to the apparition of an error indicating that there is no SD Card available for data storage.	The SD Card is not mounted when the protection is on.

SD Card Protection by Web Page	Operating Mode	%SW97 Value	Result
Enabled	Reboot the controller with reset controller or power cut.	After reboot,%SW97 value is 3 and SD Card led is flashing. After plugging/unplugging the SD Card, the % SW97 value is 15.The controller has the same application asEcoStruxure Control Expert and the application in the SD Card is different.	The protection value is saved in the non-volatile memory and backup feature does not work when the protection is on.
Disabled	Disable the protection and reboot the Controller with reset controller or power cut.	After reboot,%SW97 value is 0 and SD Card led is on. The controller has the same application as the SD Card and a different flag is raised on EcoStruxure Control Expert.	The protection value is saved in the non-volatile memory and the backup feature does work when the protection is off.

NOTE: For more information about %SW97 value, refer to the *Description of System Words %SW70 to %SW99* topic in the *EcoStruxure™ Control Expert System Bits and Words Reference Manual.*

Configure a Secure Engineering Link between Control Expert and an M580 Ethernet Controller

Compatibility

- M580 PV < 25 (white controllers) and PV >= 25 (grey controllers).
- Control Expert Classic V16.0 and later
- M580 firmware V4.20 and later
- Control Expert Application V4.20 and later
- Cybersecurity Admin Expert (CAE) V4.2.0 and later

Purpose of a Secure Connection

Using the software, hardware, and application versions referenced above, you can configure a secure connection between Control Expert and an M580 Ethernet controller. You can also use CAE to create secure configurations and download them to your application in Control Expert. This connection is based on Transport Layer Security (TLS) protocol and provides end-to-end encrypted communication.

A secure engineering link helps protect the M580 controller against cyberattacks by providing:

- Controller authentication relying on a self-signed M580 certificate.
- Encryption of data flows between Control Expert and the M580 controller.
- Control Expert client authentication by requiring a login/password to establish the HTTPS tunnel.

A secure connection helps protect against the following network attacks:

- Replay attacks.
- Password recovery (hash).
- Application binary recovery.
- Man-in-the-middle (MITM) attacks that can modify data or the application.

Features of a Secure Connection

The following features have been added to the **Security Editor**, M580 controller firmware, and Control Expert to support the creation of a secure engineering link:

- Secure communication protocol drivers, page 103
- Three Engineering Link Modes, page 103
- Modbus Secure Mode (TLS/TCP)
- Centralized Mode

Communication Protocol Drivers

HTTPS and **HTTPS via USB** are new drivers that support secure engineering links.

NOTE: For clarity, two pre-existing drivers have been renamed:

- **TCPIP** is now **Modbus TCP**
- **USB** is now **Modbus TCP via USB**

Engineering Link Modes

Depending on the level of targeted cybersecurity, you can select one of the following three **Engineering Link Modes**:

- **Full Access**:

  The controller operates as in previous firmware versions. Secure and non-secure communications are accepted.

  - For Control Expert communication, the controller accepts the non-secure drivers **Modbus TCP** and **Modbus TCP via USB** or secure drivers **HTTPS** and **HTTPS via USB**.
  - For SCADA or controller to controller communication, **Modbus TCP** (port 502) is accepted.

- **Filtered** (default):

  A hybrid mode you can use to apply cybersecurity on the engineering link, and non-secure connectivity on links to SCADA or other controllers.

  - For Control Expert communication, the controller accepts the secure drivers **HTTPS** and **HTTPS via USB**.
  - For SCADA or controller to controller communication, **Modbus TCP** (port 502) or **UMAS** (OFS) are accepted.

    NOTE: In **Filtered** mode, the controller accepts the non-secure drivers **Modbus TCP** and **Modbus TCP via USB** but only with **Connection mode** set to **monitoring** in the options of the project. Monitoring mode is a read-only mode, where it is not possible to download an application to the controller or stop the controller.

- **Enforced**

  This mode provides the highest level of security. Only secure protocols are accepted by the controller.

  - For Control Expert communication, the controller accepts only the secure drivers **HTTPS** and **HTTPS via USB**.
  - For SCADA or controller to controller communication, **Modbus TCP** (port 502) or **UMAS** (OFS) are **NOT** accepted.

NOTE: Application download time could be significantly impacted if **Full Access** mode is configured and secure drivers **HTTPS** or **HTTPS via USB** are used. If you intend to use secure drivers, consider using **Filtered** or **Enforced** mode to preserve performance.

Protocol Availability Summary

Each **Engineering Link Mode** option supports logical port and communication protocol combinations, as follows:

Purpose of link:		**Secure Engineering Link**	**Non-Secure Engineering Link**		**HMI / SCADA**
Drivers:		**HTTPS** or **HTTPS via USB**	**Modbus TCP** and **Modbus TCP via USB**		Modbus TCP/IP or UMAS
Communication Logical Port:		443	502		502
Connection mode:		**Monitoring** or **Programming**	**Program-ming**	**Monitoring**	N/A
Engineering Link Mode:	Enforced	✓	X	X	X
	Filtered	✓	X	✓	✓
	Full Access	✓	✓	✓	✓

Modbus Secure Mode

Refer to the *Cybersecurity Secure Mode Configuration* topic in the *Modicon M580 Hardware, User Guide* for details about creating a Secure Mode cybersecurity configuration using port 802.

The *Create a New CAE Cybersecurity Configuration* topic in the *Modicon M580 Hardware, User Guide* will get you started. You can perform discovery and trust certificates using CAE as well as Control Expert before you put your controller into Secure or Centralized Mode. These tasks are discussed in the *Modicon M580 Hardware, User Guide*.

Centralized Mode

Refer to the *Cybersecurity Centralized Mode Configuration* topic in the *Modicon M580 Hardware, User Guide* for details about creating a Secure Mode cybersecurity configuration for controllers not in an out-of-box state.

Security Editor Certificate Whitelist

A **Certificate Whitelist** is introduced to the **Security Editor** and includes the following features:

- **Add**: Use this command to configure the IP address of the M580 controller on which you want to create a secure engineering link.
- **Get Certificate**: Use this command to retrieve the HTTPS certificate from the device.
- A dialog box that allows you to trust the certificate and add it to the Windows certificate store.
- **View Certificate**: Use this command to display and verify the certificate.
- **Remove**: Use this command to remove a certificate from the list.

NOTE: In this release, only self-signed certificates are supported.

Configure a Secure Connection Procedure

Use Control Expert and Security Editor to configure the Secure Engineering Link. Perform the following tasks.

Preliminary Tasks

1. Upgrade your controller to:
   a. V4.20 or later for standard controllers
   b. V4.21 or later for safety controllers
2. Upgrade Control Expert to V16.0 or later.
3. Open an existing project and change the application level to V4.20 or later, or create a new project with application level to V4.20 or later.
4. Enable HTTPS, if disabled, in the Security tab.
5. Select an Engineering Link Mode setting.
6. Configure the definitive M580 Ethernet controller IP address settings, if not previously done.

   NOTE: As the certificate of an M580 controller contains its IP address, every time you change the IP address setting, the controller renews its certificate. You must trust the certificate in the Security Editor each time.
7. Create an application password for the new project.
8. Create firmware and web passwords for the new project.
9. Download the application to the controller using **Modbus TCP** or **Modbus TCP via USB**.

Task 1: Trust the M580 Certificate in Security Editor

1. Open Security Editor.
2. At first launch of Security Editor, configure a password for SecurityAdmin and wait for Security Editor to install.
3. Log in as SecurityAdmin with configured password.
4. Select the **Certificate whitelist** tab.
5. Select**Add**. The **Add Connection Configuration** dialog opens.
6. Select **HTTPS** or **HTTPS over USB** as the **Communication Protocol**. Then set **IP Address** to the configured IP address of the controller.
7. Select **OK**.
8. Select the row corresponding to the controller.

9. Select **Trust Certificate**, then select **Yes** to add it.

   The certificate **Status** column is updated and indicates:

   - valid: The certificate was successfully added.
   - unknown: No certificate was added. Use the tooltip to view the detected error details.

10. If certificate is valid, select the ellipsis (...) to display its device name and details.

Task 2: Configure a Secure Connection

1. Select **PLC > Set Address...** in Control Expert.
2. In the PLC area, enter either the M580 controller's IP address, or SYS if you are using a USB cable.
3. In the **Communication Protocol** area, select **HTTPS** or **HTTPS via USB**.
4. Select **OK**.
5. In Control Expert, select **PLC > Connect**.
6. Enter the application password.

Operating Mode Considerations

Out-of-the-Box Communication

When you first start-up a new out-of-the-box M580 controller, the following restrictions are applied:

- An HTTPS connection between Control Expert and the M580 controller is not supported.
- Communication is possible only by using USB or TCPIP.

Reset M580 Controller to NOCONF

You can switch your M580 controller to the NOCONF in the following ways:

- Set the rotary wheel to reset a Hot Standby M580 controller.

- Use an SD Card as follows:
  1. Create an application without a password.
  2. Load the application into another M580 controller of the same reference.
  3. Insert the SD card on this controller.
  4. Set %S66 to TRUE to backup application on the SD card.
  5. Insert the SD card into the original M580 controller and cycle power to the controller.

Reset the Application Password

Resetting the application password procedure through technical support is still available in **Filtered** and **Full Access Engineering Link Mode**.

Online application password change is supported.

Enforced Secure Programming Compatibility and Limitations

Compatibility

Refer to the topic Configure a Secure Engineering Link between Control Expert and an M580 Ethernet Controller, page 102.

Engineering Link Mode Limitations

For any physical connection, the following limitations apply to the **Enforced Engineering Link Mode** option:

- The Data Dictionary feature is not functional.
- BMENUA0100•• is not supported in Enforced Engineering Link Mode.
- Upgrade to M580 with a product version (PV) 3 or later.

- The controller is not accessible using the following function blocks:
  - READ_VAR
  - WRITE_VAR
  - DATA_EXCH
  - READ_REMOTE
- The controller cannot be scanned by a Modbus scanner.
- The M580 controller's Modbus scanner cannot scan Modbus devices.
- Depending on the selected communication protocol (Modbus TCP or EtherNet/IP), some DTM diagnostic services are not available, as follows:

DTM Services	Protocol	Availability
EtherNet/IP DTM Connect	EtherNet/IP	✓
EtherNet/IP DTM Disconnect	EtherNet/IP	✓
Modbus DTM Connect	Modbus TCP	X
Modbus DTM Disconnect	Modbus TCP	X
Ethernet Diagnostic	EtherNet/IP	✓
Bandwidth Diagnostic	Modbus TCP	X
RSTP Diagnostic	Modbus TCP	X
Network Time Service Diagnostic	EtherNet/IP	✓

Communication Adapter Compatibility

The following table summarizes the services available on a controller or communication adaptor, depending on the selected engineering mode.

The rows correspond to the available services:

- Engineering link: The connection between Control Expert and the controller.
- Client mode communication: Scanner, Modbus, EtherNet/IP (implicit or explicit), OPCUA, DNP3, IEC 61850
- Server mode communication: Modbus, EtherNet/IP, OPCUA, DNP3, IEC 61850

The columns correspond to the different possible configurations. For example:

- Controller alone: A controller is used without any communication adapter.
- Controller+NOC with backplane on: A controller and a BMENOC03•• module exist in the main rack. The backplane port of the BMENOC03•• module is enabled. Control Expert is connected to the BMENOC03•• module.
- Controller+NOC with backplane off: A controller and a BMENOC03•• module exist in the main rack. The backplane port of the BMENOC03•• module is disabled. Control Expert is connected to the BMENOC03•• module.

When a communication adapter is used, some services are available on the adapter itself or from the controller through the adapter. To distinguish these two cases, the letters C for controller and M for module are used. For example:

- If the connection from Control Expert to the controller is made using the IP address of the controller, the letter C applies.
- If the connection from Control expert is made using the IP address of the BMENUA0100 module, the letter M applies.

Modicon M580 system		Controller alone			Controller + NOCs (NOC301, NOC311, NOC321)			Controller + NOCs (NOC301, NOC311, NOC321)			Controller + NOC321			Controller + NUA (sec mode)			Controller + BMXNOR			Controller + BMENOR			Controller + NOP			Controller + NOP		
Communication adapter parameter					Backplane port enabled			Backplane port disabled			Backplane port disabled IP forwarding			IP forwarding			Backplane isolated			Backplane port disabled			Backplane port enabled no IP forwarding			Backplane port disabled IP forwarding		
Topology																												
Security mode		🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒
Engineering link	HTTPS	C	C	C	C	C	C	X	X	X	C	C	C	C* M	C* M	X	X	X	X	X	X	X	C	C	C	X	X	X
	Modbus TCP monitoring	C	C	X	C M	C M	X	C	C	X	C	C	X	C* M	C* M	X	M	M	X	M**	M**	X	C M	C M	X	M	M	X
	Modbus TCP programming	C	X	X	C M	X	X	C	X	X	C	X	X	C* M	X	X	M	X	X	M**	X	X	C M	X	X	M	X	X

Modicon M580 system		Controller alone			Controller + NOCs (NOC301, NOC311, NOC321)			Controller + NOCs (NOC301, NOC311, NOC321)			Controller + NOC321			Controller + NUA (sec mode)			Controller + BMXNOR			Controller + BMENOR			Controller + NOP			Controller + NOP		
Communication adapter parameter					Backplane port enabled			Backplane port disabled			Backplane port disabled IP forwarding			IP forwarding			Backplane isolated			Backplane port disabled			Backplane port enabled no IP forwarding			Backplane port disabled IP forwarding		
Topology																												
Security mode		🔓	🔒	🔒	🔓	🔒	🔒	🔓	🔒	🔒	🔓	🔒	🔒	🔓	🔒	🔒	🔓	🔒	🔒	🔓	🔒	🔒	🔓	🔒	🔒	🔓	🔒	🔒
Client mode	IO scanner — Modbus	C	C	X	C M	C M	M	M	M	M	C M	C M	M	C*	C*	X	-	-	-	-	-	-	C	C	X	-	-	-
Client mode	EIP — Scanner	C	C	C	C M	C M	C M	M	M	M	C M	C M	C M	C*	C*	C*	-	-	-	-	-	-	C	C	C	-	-	-
Client mode	EFB Modbus	C	C	X	C	C	X	C	C	X	C	C	X	C*	C*	X	C	C	X	C	C	X	C	C	X	C	C	X
Client mode	EFB — EIP	C	C	C	C	C	C	C	C	C	C	C	C	C*	C*	C*	C	C	C	C	C	C	C	C	C	C	C	C
Client mode	EFB — OPC UA	C	C	C	-	-	-	-	-	-	C	C	C	C*	C*	C*	-	-	-	-	-	-	C	C	C	C	C	C
Client mode	DNP3 IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-
Client mode	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X
Server mode	Modbus server / UMAS	C	C	X	M	M	X	M	M	X	C	C	X	C* M-*	C* M*	X	M	M	X	M**	M**	X	C M	C M	X	M	M	X

Modicon M580 system		Controller alone			Controller + NOCs (NOC301, NOC311, NOC321)			Controller + NOCs (NOC301, NOC311, NOC321)			Controller + NOC321			Controller + NUA (sec mode)			Controller + BMXNOR			Controller + BMENOR			Controller + NOP			Controller + NOP		
Communication adapter parameter					Backplane port enabled			Backplane port disabled			Backplane port disabled IP forwarding			IP forwarding			Backplane isolated			Backplane port disabled			Backplane port enabled no IP forwarding			Backplane port disabled IP forwarding		
Topology																												
Security mode		🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒	🔓	🔰	🔒
SCADA communication	OPC UA server	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	-	-	-	-	-	-	-	-	-	-	-	-
	EherNet/IP Adapter (Local server)	C	C	C	M	M	M	M	M	M	C M	C M	C M	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	HTTPS web server of the controller	C	C	C	C	C	C	-	-	-	C	C	C	C*	C*	C*	-	-	-	-	-	-	C	C	C	-	-	-
	DNP3 - IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-
	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X

Symbol	Description
	Engineering link mode set to **Full Access**
	Engineering link mode set to **Filtered**
	Engineering link mode set to **Enforced**
C	• In client mode, C indicates the communication is initiated by the controller. • In server mode, C indicates the destination IP address is the controller.
M	• In client mode, M indicates the communication is initiated by the communication adapter. • In server mode, M indicates the destination IP address is the communication adapter. In both cases the module communicates with the controller over XBUS.
X	Not supported
*	Depending on forwarding rules configured in the BMENUA0100 module
**	If the Modbus server is enabled in the BMENOR00200
-	Not applicable

M580 Ethernet Services and Ports

This topic presents the Modicon M580 Ethernet services available and their status by default in the EcoStruxure Control Expert application.

“Out of box” indicates the configuration applies to a controller from the factory, with no application installed. Once an application has been installed on the controller, this "out of box" configuration can never again be realized.

“Default” indicates the configuration applies to a default EcoStruxure Control Expert application.

M580 Controllers with Firmware Version ≤ 4.01

Service	Port number	Out of box	Default	Notes
HTTP	80/tcp	Closed	Closed	Webserver
Modbus TCP	502/tcp	Open	Open	-
EtherNet/IP	44818/tcp-udp	Closed	Closed	EtherNet/IP Explicit (Class 3)
DHCP	67/udp	Closed	Closed	-
FTP	21/tcp	Open	Closed	Firmware, data storage, FDR
TFTP	69/udp	Closed	Closed	FDR (X80)
SNMP	161/udp	Closed	Closed	-
EtherNet/IP	2222/udp	Closed	Closed	EtherNet/IP implicit (Class 1)
NTP/SNTP	123/udp	Closed	Closed	NTPV4 or SNTP

M580 Controllers with Firmware Version ≥ 4.20 and < 4.60

Service	Port number	Out of box	Default	Notes
HTTPS	443/tcp	Open	Open	Web, firmware, data storage
Modbus TCP	502/tcp	Open	Open	NOTE(1)
EtherNet/IP	44818/tcp-udp	Closed	Closed	EtherNet/IP Explicit (Class 3)
DHCP	67/udp	Closed	Closed	-
FTP	21/tcp	Closed	Closed	FDR
TFTP	69/udp	Closed	Closed	FDR (X80)

Service	Port number	Out of box	Default	Notes
SNMP	161/udp	Closed	Closed	-
EtherNet/IP	2222/udp	Closed	Closed	EtherNet/IP implicit (Class 1)
NTP/SNTP	123/udp	Closed	Closed	NTPV4 or SNTP
DPWS	9867/tcp	Open	Open	Firmware update, NOTE(1)
NOTE(1): The port and related service are primary to customer to ensure fundamental functions are operational under desired industrial environment. The port keeps open for safety and availability purpose. Users cannot disable the port.				

M580 Controllers with Firmware Version ≥ 4.60

Service	Port number	Out of box	Default	Notes
HTTPS	443/tcp	Open	Open	Web, firmware, data storage
Modbus TCP	502/tcp	Open	Open	NOTE(1)
Modbus Secure (TLS/TCP)	802	Open	Open	—
EtherNet/IP	44818/tcp-udp	Closed	Closed	EtherNet/IP explicit (class 3)
DHCP	67/udp	Closed	Closed	—
FTP	21/tcp	Closed	Closed	FDR
TFTP	69/udp	Closed	Closed	FDR (X80)
SNMP	161/udp	Closed	Closed	—
EtherNet/IP	2222/udp	Closed	Closed	EtherNet/IP implicit (class 1)
NTP/SNTP	123/udp	Closed	Closed	NTPV4 or SNTP
DPWS	9867/tcp	Open	Open	Firmware update, NOTE(1)
NOTE(1): The port and related service are primary to customer to help ensure fundamental functions are operational under desired industrial environment. You cannot disable the port; it remains open for safety and availability purposes.				

Cybersecurity Services Per System

Introduction

This chapter lists the main cybersecurity services available for each system and indicates where to find detailed information in Control Expert help.

Cybersecurity Services

Overview

Software, DTM, or devices are elements providing cybersecurity services in a global system. The available cybersecurity services are listed for the following elements:

- Control Expert software, page 118
- Modicon M340 controller, page 118
- Modicon M580 controller, page 119
- Modicon Quantum controller and communication modules, page 120
- Modicon X80 modules, page 121
- Modicon Premium/Atrium controller and communication modules, page 122
- Modicon Momentum MDI, page 123
- Modicon MC80, page 123

The cybersecurity services listed below are described in previous chapter:

- Disable unused services, page 31
- Access control, page 32
- Set Up Encrypted Communication, page 35
- Event logging, page 50
- Authentication, page 90
- Authorizations, page 95
- Integrity checks, page 98

Cybersecurity Services in Unity Pro/Control Expert Software

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

Cybersecurity services availability

Software	Cybersecurity services							
Reference	**Disable unused services**	**Access control**	**Encrypted communication**	**Encrypted communication with confidentiality**	**Event logging**	**Authentication**	**Authorizations**	**Integrity checks**
Unity Pro v8.1	–	N.A.	–	–	–	X	X	X
Unity Pro≥v10.0	–	N.A.	X	–	X	X	X	X
Unity Pro≥v13.0	–	N.A.	X	X	X	X	X	X
Control Expert≥v14.0	X	X	X	X	X	X	X	X

X Available, at least one service is implemented.

– Not available

N.A. Not applicable

There are more robust password recovery mechanisms available when using Control Expert versions greater than or equal to v.15.1 targeting applications for M580 firmware versions greater than or equal to v4.01.

Cybersecurity Services in Modicon M340 Controller

Minimum firmware version and cybersecurity services availability in Modicon M340 controller:

Controller		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encryp-ted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
BMX P34 1000	2.60	–	–	–	–	X	X	–
BMX P34 2000	2.60	–	–	–	–	X	X	–
BMX P34 2010	2.60	–	–	–	–	X	X	–
BMX P34 20102	2.60	–	–	–	–	X	X	–
BMX P34 2020	2.60	X	X	–	–	X	X	–
BMX P34 2030	2.60	X	X	–	–	X	X	–
BMX P34 20302	2.60	X	X	–	–	X	X	–
X Available, at least one service is implemented. **–** Not available								

Cybersecurity Services in Modicon M580 Controller

Minimum firmware version and cybersecurity services availability in Modicon M580 controller:

Controller		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
BME P58 1020	1.00	X	X	–	X	X	X	X
BME P58 2020	1.00	X	X	–	X	X	X	X
BME P58 2040	1.00	X	X	–	X	X	X	X
BME P58 3020	1.00	X	X	–	X	X	X	X
BME P58 3040	1.00	X	X	–	X	X	X	X
BME P58 4020	1.00	X	X	–	X	X	X	X
BME P58 4040	1.00	X	X	–	X	X	X	X
BME P58 5040	2.10	X	X	–	X	X	X	X
BME P58 6040	2.10	X	X	–	X	X	X	X
BME H58 2040	2.10	X	X	–	X	X	X	X
BME H58 4040	2.10	X	X	–	X	X	X	X

Controller		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
BME H58 6040	2.10	X	X	–	X	X	X	X
X Available, at least one service is implemented. **–** Not available								

Cybersecurity Services in Modicon Quantum Controller and Modules

Minimum firmware version and cybersecurity services availability in Modicon Quantum controller:

Controller		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encryp-ted commu-nication**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
140CPU31110	3.20	–	–	–	–	X	X	–
140CPU43412•	3.20	–	–	–	–	X	X	–
140CPU53414•	3.20	–	–	–	–	X	X	–
140CPU651•0	3.20	X	X	–	–	X	X	–
140CPU65260	3.20	X	X	–	–	X	X	–
140CPU65860	3.20	X	X	–	–	X	X	–
140CPU67060	3.20	X	X	–	–	X	X	–
140CPU67160	3.20	X	X	–	–	X	X	–
140CPU6726•	3.20	X	X	–	–	X	X	–
140CPU67861	3.20	X	X	–	–	X	X	–
X Available, at least one service is implemented. **–** Not available								

Modicon Quantum modules supporting cybersecurity services:

Module		Cybersecurity services						
Reference	**Min. firmware**	**Disable unused services**	**Access control**	**Encrypted communication**	**Event logging**	**Authentication**	**Authorizations**	**Integrity checks**
140NOC7710•	1.00	–	X	–	–	X	–	–
140NOC78000	2.00	X	X	–	–	X	–	–
140NOC78100	2.00	X	X	–	–	X	–	–
140NOE771••	X	X	–	–	–	X	–	–
140NWM10000	–	X	–	–	–	–	–	–

X Available, at least one service is implemented.

– Not available

Cybersecurity Services in Modicon X80 Modules

Modicon X80 modules supporting cybersecurity services:

Module		Cybersecurity services							
Reference	**Min. firmware**	**Disable unused services**	**Access control**	**Encrypted communication**	**Encrypted communication with confidentiality**	**Event logging**	**Authentication**	**Authorizations**	**Integrity checks**
BMECXM0100	1.01	X	X	–	–	X	–	–	X
BMENOC0301	1.01	X	X	X	–	X	X	–	X
BMENOC0311	1.01	X	X	X	–	X	X	–	X
BMXNOC0401.2	2.05	X	X	–	–	–	–	–	–
BMXNOE0100.2	2.90	X	X	–	–	–	–	–	–
BMXNOE0110.2	6.00	X	X	–	–	–	–	–	–
BMXPRA0100	2.60	X	X	–	–	–	X	–	–
BMENOC0301	2.11	X	X	X	X	X	X	–	X
BMENOC0311	2.11	X	X	X	X	X	X	–	X

X Available, at least one service is implemented.

– Not available

Cybersecurity Services in Modicon Premium/Atrium Controller and Modules

Minimum firmware version and cybersecurity services availability in Modicon Premium/ Atrium controller:

Controller		**Cybersecurity services**						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
TSXH57•4M	3.10	–	–	–	–	X	X	–
TSXP570244M	3.10	–	–	–	–	X	X	–
TSXP57•04M	3.10	–	–	–	–	X	X	–
TSXP57•54M	3.10	–	–	–	–	X	X	–
TSXP571634M TSXP572634M TSXP573634M (through ETY port)	3.10	X	X	–	–	X	X	–
TSXP574634M TSXP575634M TSXP576634M (embedded Ethernet port)	3.10	X	X	–	–	X	X	–
X Available, at least one service is implemented. **–** Not available								

Modicon Premium/Atrium modules supporting cybersecurity services:

Module		**Cybersecurity services**						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
TSXETC101.2	2.04	X	X	–	–	–	–	–
TSXETY4103	5.70	X	X	–	–	–	–	–

Module		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
TSXETY5103	5.90	X	X	–	–	–	–	–
X Available, at least one service is implemented. **–** Not available								

Cybersecurity Services in Modicon Momentum MDI Controller and Modules

Minimum firmware version and cybersecurity services availability in Modicon Momentum MDI:

Controller		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
171CBU78090	1.0	X	X	–	–	X	X	–
171CBU98090	1.0	X	X	–	–	X	X	–
171CBU98091	1.0	X	X	–	–	X	X	–
X Available, at least one service is implemented. **–** Not available								

Cybersecurity Services in Modicon MC80 Controller and Modules

Minimum firmware version and cybersecurity services availability in Modicon MC80:

Controller		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
BMKC8020301	1.2	X	X	–	–	X	X	–
BMKC8020310	1.0	X	X	–	–	X	X	–

Controller		Cybersecurity services						
Reference	**Min. firm-ware**	**Disable unused services**	**Access control**	**Encrypted communi-cation**	**Event logging**	**Authenti-cation**	**Authori-zations**	**Integrity checks**
BMKC8030311	1.2	X	X	–	–	X	X	–
X Available, at least one service is implemented. **–** Not available								

Modicon M340 Security Services

Overview

Communication security services settings description is provided for the Modicon M340 controller in different manuals as described in the following topic.

Modicon M340 Controller with Embedded Ethernet Ports

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security* section (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual).
Access control:	Refer to *Messaging Configuration Parameters* section (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual).

Modicon M580 Security Services

Modicon M580 Controller

Cybersecurity communication parameters are described in the *Security Tab* topic in the *Modicon M580 Hardware, User Guide*.

Cybersecurity Mode Configuration

Refer to the Cybersecurity Secure Mode Configuration topic in the *Modicon M580 Hardware, User Guide* to configure an M580 controller in secure mode or standard mode for standalone, Hot Standby, and Safety controllers.

You can also configure an M580 controller in centralized mode (see the *Modicon M580 Hardware, User Guide*).

In this mode, use Cybersecurity Admin Expert to decommission the controller, restore to out-of-box state, and apply cybersecurity configuration features.

Modicon Quantum Security Services

Overview

Communication security services settings description is provided for the Modicon Quantum controller and Ethernet modules in different manuals as described in the following topics.

Modicon Quantum Controller with Embedded Ethernet Ports

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security (Enable / Disable HTTP, FTP, and TFTP)* section (see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).
Access control:	Refer to *Modicon Quantum with Control Expert Ethernet Controller Messaging Configuration* section (see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).

140 NOC 771 0x Module

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security (Enable / Disable HTTP, FTP, and TFTP)* section (see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).
Access control:	Refer to *Configuring Access Control* section (see Quantum using EcoStruxure™ Control Expert, 140 NOC 771 01 Ethernet Communication Module, User Manual).

140 NOC 780 00 Module

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security* section (see Quantum EIO, Control Network, Installation and Configuration Guide).
Access control:	Refer to *Configuring Access Control* section (see Quantum EIO, Control Network, Installation and Configuration Guide).

140 NOC 781 00 Module

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security* section (see Quantum EIO, Control Network, Installation and Configuration Guide).
Access control:	Refer to *Configuring Access Control* section (see Quantum EIO, Control Network, Installation and Configuration Guide).

140 NOE 771 xx Module

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security (Enable / Disable HTTP, FTP, and TFTP)* section (see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual), *Security* section (see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual), and *Establishing HTTP and Write Passwords* section (see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).

140 NWM 100 00 Module

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security (Enable / Disable HTTP, FTP, and TFTP)* section (see Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).

Modicon X80 Security Services

Overview

Communication security services settings description is provided for the Modicon X80 Ethernet modules in different manuals as described in the following topics.

BMXNOC0401.2 Module

A description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to the *Security* section (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual).
Access control:	Refer to the *Configuring Access Control* section (see Modicon M340, BMX NOC 0401 Ethernet Communication Module, User Manual).

BMXNOE0100.2 and BMXNOE0110.2 Module

A description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to the *Security* section (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual).
Access control:	Refer to the *Messaging Configuration Parameters* section (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual).

BMXPRA0100 Module

The BMXPRA0100 module is configured as an Modicon M340 controller. A description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to the *Security* topic (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual).
Access control:	Refer to the *Messaging Configuration Parameters* topic (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual).

BMXNOR0200H Module

A description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to the *Security* topic (see Modicon X80 , BMXNOR0200H RTU Module, User Manual).
Access control:	Refer to the *Messaging Configuration Parameters* topic.

BMENOR2200H Module

A description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to the *Security* topic.
Access control:	Refer to the *Messaging Configuration Parameters* topic.

BMECXM0100 Module

A description of communication parameters related to cybersecurity is provided in the *Ethernet Services Configuration* chapter (see Modicon M580, BMECXM CANopen Modules, User Manual).

BMENOC0301 and BMENOC0311 Modules

A description of communication parameters related to cybersecurity is provided in the *Configuring Security Services* topic (see Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Communications Module, Installation and Configuration Guide).

BMENUA0100 Module

A description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to the Cybersecurity Settings topic (see M580, BMENUA0100 OPC UA Embedded Module, Installation and Configuration Guide).
Access control:	Refer to the *Access Control* topic.

Modicon Premium/Atrium Security Services

Overview

Communication security services settings description is provided for the Modicon Premium/ Atrium controller and Ethernet modules in different manuals as described in the following topics.

Modicon Premium/Atrium Controller with Embedded Ethernet Ports

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security Service Configuration Parameters* section (see Premium and Atrium Using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).
Access control:	Refer to *Configuration of TCP/IP Messaging (TSX P57 6634/5634/4634)* section (see Premium and Atrium Using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).

Modicon Premium/Atrium Controller through ETY Ports

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security Service Configuration Parameters* section (see Premium and Atrium Using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).
Access control:	Refer to *Configuration of TCP/IP Messaging* section (see Premium and Atrium Using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).

TSX ETC 101.2 Module

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security* section (see Premium using EcoStruxure™ Control Expert, TSX ETC 101 Ethernet Communication Module, User Manual).
Access control:	Refer to *Configuring Access Control* section (see Premium using EcoStruxure™ Control Expert, TSX ETC 101 Ethernet Communication Module, User Manual).

TSX ETY x103 Module

Description of communication parameters related to cybersecurity is provided in the listed topics:

Ethernet communication:	Refer to *Security Service Configuration Parameters* section (see Premium and Atrium Using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).
Access control:	Refer to *Configuration of TCP/IP Messaging* section (see Premium and Atrium Using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual).

Modicon Momentum MDI Security Services

Communication security services settings description is provided for the Modicon Momentum MDI controller described in the *Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide*.

Modicon MC80 Security Services

Communication security services settings description is provided for the MC80 controller described in the *Modicon MC80 Program Logic Controller (PLC) User Manual*.

How to Help Protect M580, M340, Momentum MDI, and MC80 Architecture with EAGLE40 using VPN

Introduction

This chapter explains how to help increase protection of controllers against cyber attacks by relying on a firewall device such as the EAGLE40-07 from Belden, configured to establish VPN connections. Deploying such device in an architecture can help mitigate vulnerabilities existing in the devices and help reduce the attack surface of different products.

It is a good practice to harden the network, workstations and devices, as described in the *Modicon Controller Systems CyberSecurity, User Guide* available for download at: https://www.se.com/us/en/download/document/EIO0000001999/

EAGLE40 Firewall

Why use a Firewall?

Relying on a firewall to reinforce the cybersecurity of an existing architecture brings the following advantages:

- The cybersecurity of control networks and devices is reinforced.
- Reinforced cybersecurity relies on the IPSEC protocol.
- Impact on existing architecture and performances can be minimized.

EAGLE40 Main Features

The EAGLE40 firewall is a solution to cover or mitigate cybersecurity residual issues.

- Through powerful IPSEC VPN, EAGLE40 firewall provides expected confidentiality on network traffic to help prevent attacks conducted by *man in the middle*. It ensures the authentication of the sender by helping to prevent spoofing attacks. Message integrity is reinforced by cryptographic methods and cannot be tampered.
- Usual filtering capabilities are available, allowing you to control traffic and protocols based on IP, Mac address, and port of network devices.

- The EAGLE40 firewall is a scalable product that can be included in multi-point architectures, with rate and bandwidth performances helping ensure network transparency.

Prerequisites

Software Installation

A compatible VPN client software is necessary to establish a VPN tunnel based on IPSEC protocol between the client and the firewall.

The EAGLE40 firewall requires the use of the VPN client IPSEC/IKEV2.

NOTE: Use the VPN client solution provided by TheGreenBow.

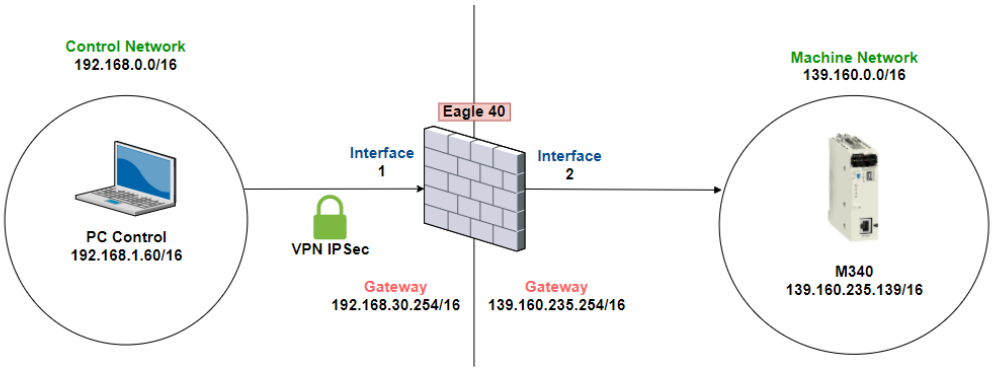
In the configuration procedures described below we use this software that you can download at the following URL:

https://www.thegreenbow.com/en/

Machines and Operating Systems

Before configuring the firewall, you need to prepare all IP address in use in the architectures.

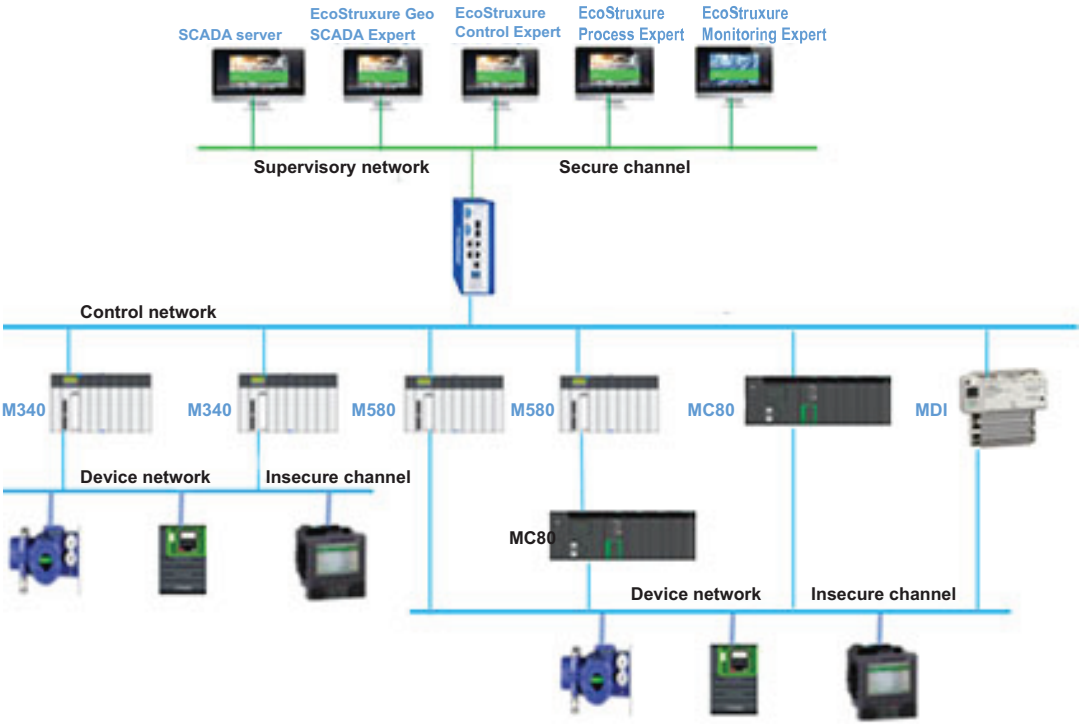
The following diagram is given as an example:



Typical Architecture

The architecture and configuration instructions in this document are provided as examples and can be adapted to various architectures and systems.

As an example, the following mixed architecture, combining Modicon M340, M580, Momentum MDI, and MC80 controllers is a typical architecture:



NOTE: Install EAGLE40 firewall near the controllers.

Configuring the Firewall

Web Configuration

To configure the firewall, open an Internet browser and enter the following URL:

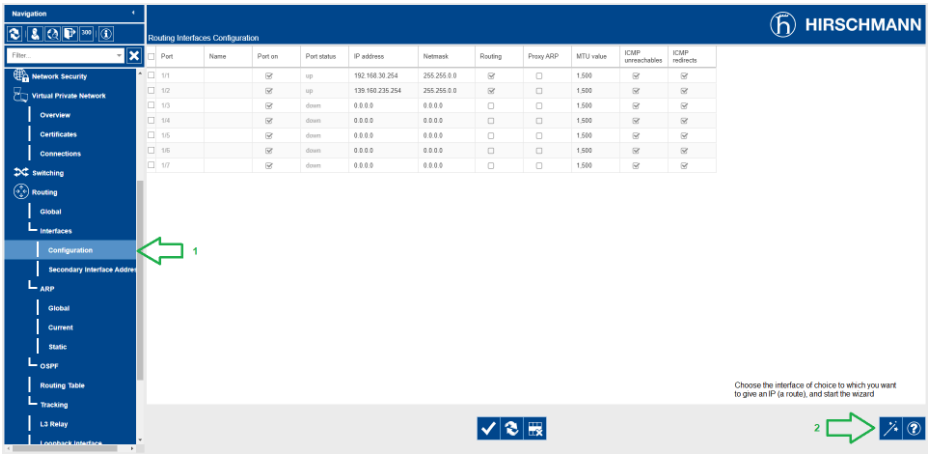
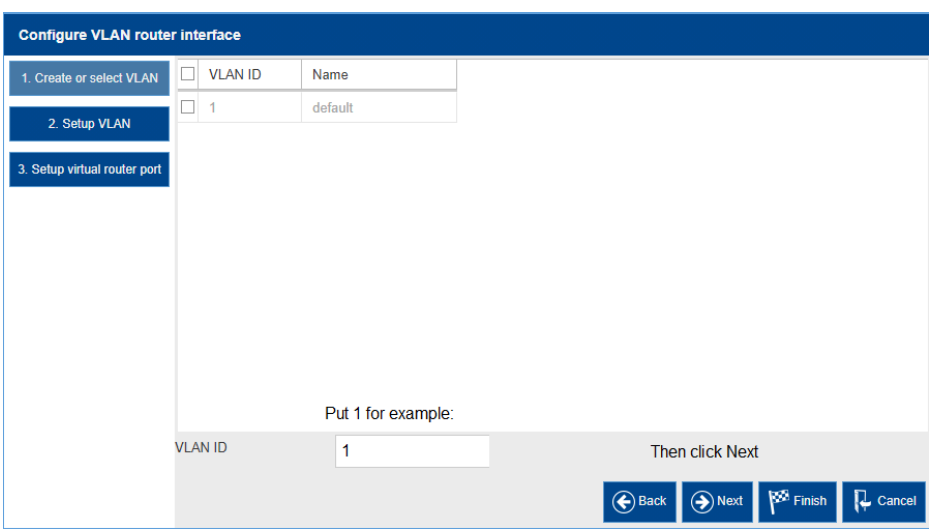
`https://[IPFirewall]/admin`

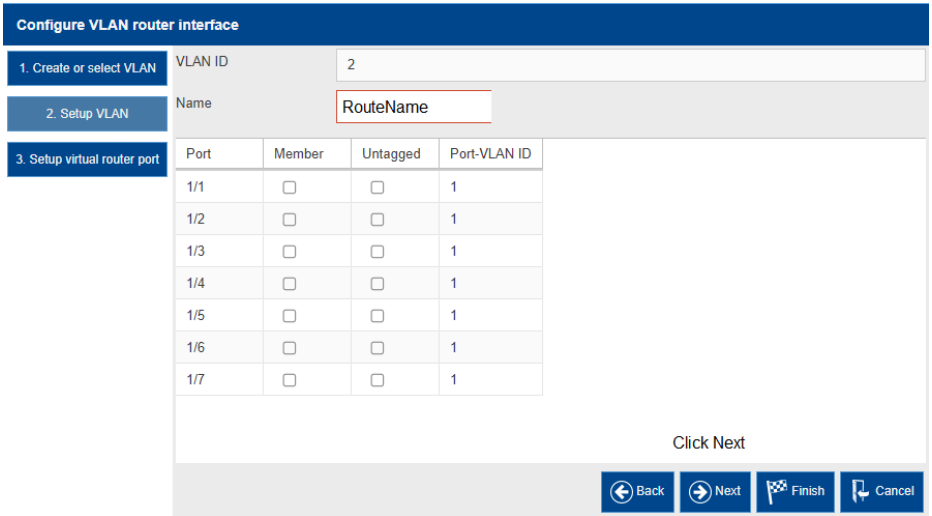
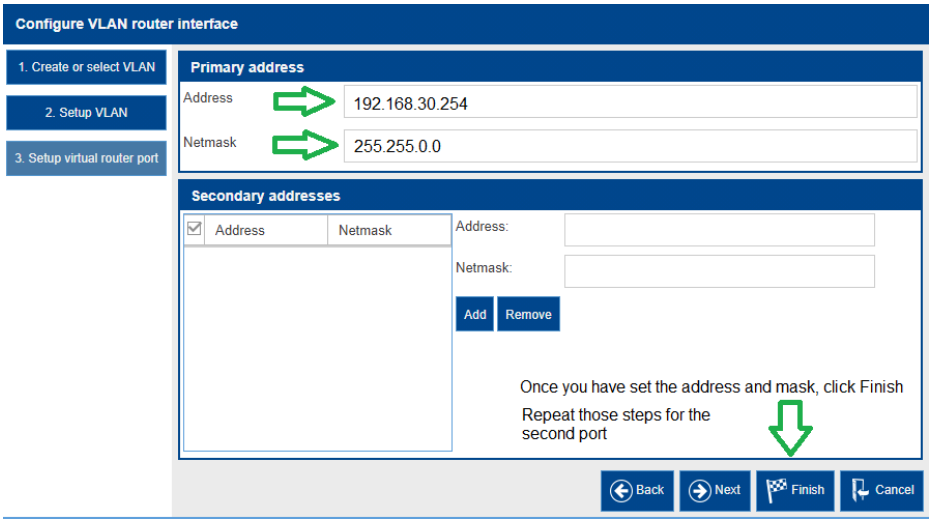
Click **Enter** and use default username/password combination `admin/private` to log in.

NOTE: On the first login you are required to change the password.

Configuring the Routes

To configure the routes, proceed as follows:

Step	Action
1	 **1.** On the **Navigation** left pane open **Routing** > **Interfaces** > **Configuration** webpage. Choose the Ethernet interface you want to configure. **2.** Click the icon to launch the **Configure VLAN Router Interface** window.
2	Set an ID number to the VLAN you want to configure (1 in the example), then click **Next**. 

Step	Action
3	Set a route name to the VLAN you want to configure (RouteName in the example), then click **Next**. 
4	Set the IP address of the Control Network and its mask, (`192.168.30.254/16` in the example), then click **Finish**. 
5	Repeat the steps 1 to 4 for the Machine Network using the second Ethernet interface.

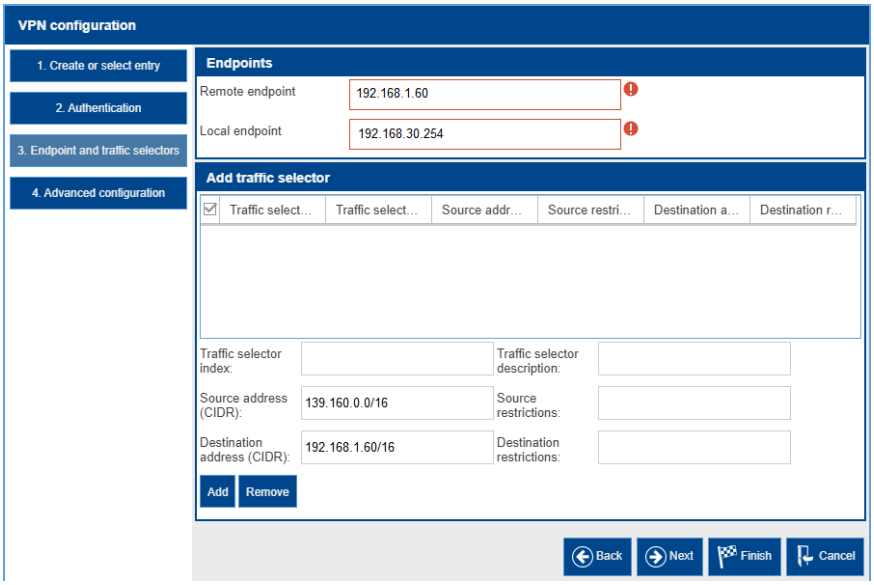
In the following example we have set the control network gateway interface of the firewall to `192.168.30.254/16` on the first physical port and machine network to `139.160.235.254/16` on the second physical port.

Port	Name	Port on	Port status	IP address	Netmask	Routing	Proxy ARP	MTU value	ICMP unreachables	ICMP redirects
1/1		☑	up	192.168.30.254	255.255.0.0	☑	☐	1,500	☑	☑
1/2		☑	up	139.160.235.254	255.255.0.0	☑	☐	1,500	☑	☑
1/3		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/4		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/5		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/6		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/7		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑

Configuring the VPN in the Firewall

To configure the VPN, proceed as follows:

Step	Action
1	On the left pane of the web page, click on **Virtual Private Network** > **Connections** menu. Click the icon.
2	Choose an index number and a name then click **Next**.
3	Choose a password (PSK) then click **Next**.

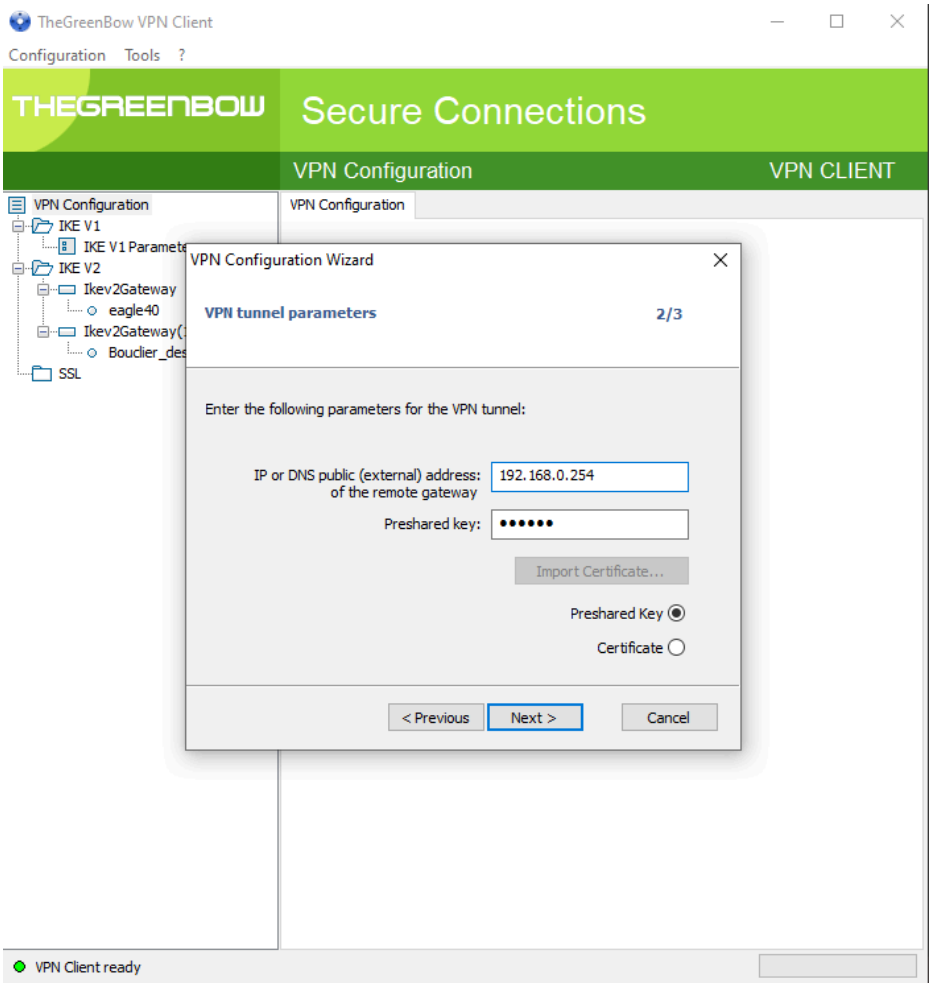
Step	Action
4	Fill up the IP addresses and masks according to your network. • **Remote endpoint**: The computer connecting to the firewall using a VPN. • **Local endpoint**: The gateway configured in the Routes. • **Source address (CIDR)**: The protected machine network accessible only once connected using a VPN. • **Destination address (CIDR)**: The computer connecting to the firewall using a VPN.  Click **Next**.
5	Set a margin time. The default value is 150. Set **IKE Version** to ikev2 then click **Finish**.

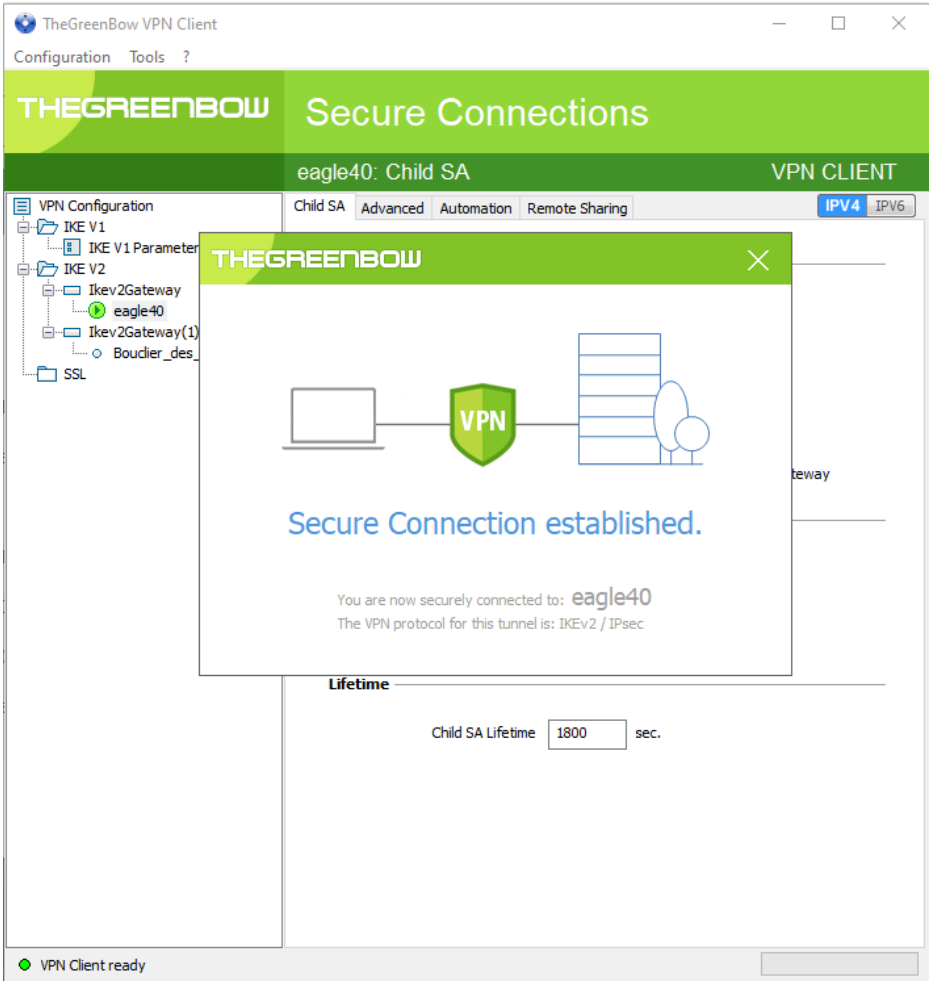
Configuring the VPN Client

NOTE: In our example we use the VPN client solution provided by TheGreenBow.

To configure the VPN client, proceed as follows:

Step	Action
1	Download and install the VPN client software.
2	On the left pane of the VPN Client window, right click **VPN Configuration** and choose **Wizard**.
3	Choose **IKEv2 Tunnel** and click **Next**.

Step	Action
4	Set the IP address of the firewall accessible using the Control Network interface (192.168.0.254 in the example). Enter the PSK previously selected.  Click **Next**, then click **Finish**.
5	On the left pane of the VPN Client window, right click on the Ikev2 tunnel just created and rename it.

Step	Action
6	Right click on the just renamed Ikev2 tunnel and select **Open Tunnel**. A notification confirms that the secure connection has been established. 

Glossary

802.1Q:

The IEEE protocol designator for Virtual Local Area Network (VLAN). This standard provides VLAN identification and quality of service (QoS) levels.

A

adapter:

An adapter is the target of real-time I/O data connection requests from scanners. It cannot send or receive real-time I/O data unless it is configured to do so by a scanner, and it does not store or originate the data communications parameters necessary to establish the connection. An adapter accepts explicit message requests (connected and unconnected) from other devices.

advanced mode:

In Control Expert, advanced mode is a selection that displays expert-level configuration properties that help define Ethernet connections. Because these properties should be edited only by people with a good understanding of EtherNet/IP communication protocols, they can be hidden or displayed, depending upon the qualifications of the specific user.

applicative time stamping:

Use the applicative time stamping solution to access time stamp event buffers with a SCADA system that does not support the OPC DA interface. In this case, function blocks in the Control Expert application read events in the buffer and formats them to be sent to the SCADA system.

architecture:

Architecture describes a framework for the specification of a network that is constructed of these components:

- physical components and their functional organization and configuration
- operational principles and procedures
- data formats used in its operation

ARRAY:

An `ARRAY` is a table containing elements of a single type. This is the syntax: `ARRAY [<limits>] OF <Type>`

Example: `ARRAY [1..2] OF BOOL` is a one-dimensional table with two elements of type `BOOL`.

`ARRAY [1..10, 1..20] OF INT` is a two-dimensional table with 10x20 elements of type `INT`.

ART:

(*application response time*) The time a controller application takes to react to a given input. ART is measured from the time a physical signal in the controller turns on and triggers a write command until the remote output turns on to signify that the data has been received.

AUX:

An (AUX) task is an optional, periodic processor task that is run through its programming software. The AUX task is used to execute a part of the application requiring a low priority. This task is executed only if the MAST and FAST tasks have nothing to execute. The AUX task has two sections:

- IN: Inputs are copied to the IN section before execution of the AUX task.
- OUT: Outputs are copied to the OUT section after execution of the AUX task.

B

BCD:

(*binary-coded decimal*) Binary encoding of decimal numbers.

BOOL:

(*boolean type*) This is the basic data type in computing. A `BOOL` variable can have either of these values: 0 (`FALSE`) or 1 (`TRUE`).

A bit extracted from a word is of type `BOOL`, for example: `%MW10.4`.

BOOTP:

(*bootstrap protocol*) A UDP network protocol that can be used by a network client to automatically obtain an IP address from a server. The client identifies itself to the server using its MAC address. The server, which maintains a pre-configured table of client device MAC addresses and associated IP addresses, sends the client its defined IP address. The BOOTP service utilizes UDP ports 67 and 68.

broadcast:

A message sent to all devices in a broadcast domain.

C

CCOTF:

(*change configuration on the fly*) A feature of Control Expert that allows a module hardware change in the system configuration while the system is operating. This change does not impact active operations.

CIP™:

(*common industrial protocol*) A comprehensive suite of messages and services for the collection of manufacturing automation applications (control, safety, synchronization, motion, configuration and information). CIP allows users to integrate these manufacturing applications with enterprise-level Ethernet networks and the internet. CIP is the core protocol of EtherNet/IP.

class 1 connection:

A CIP transport class 1 connection used for I/O data transmission using implicit messaging between EtherNet/IP devices.

class 3 connection:

A CIP transport class 3 connection used for explicit messaging between EtherNet/IP devices.

connected messaging:

In EtherNet/IP, connected messaging uses a CIP connection for communication. A connected message is a logical relationship between two or more application objects on different nodes. The connection establishes a virtual circuit in advance for a particular purpose, such as frequent explicit messages or real-time I/O data transfers.

connection originator:

The EtherNet/IP network node that initiates a connection request for I/O data transfer or explicit messaging.

connection:

A virtual circuit between two or more network devices, created prior to the transmission of data. After a connection is established, a series of data is transmitted over the same communication path, without the need to include routing information, including source and destination address, with each piece of data.

connectionless:

Describes communication between two network devices, whereby data is sent without prior arrangement between the two devices. Each piece of transmitted data also includes routing information, including source and destination address.

control network:

An Ethernet-based network containing PACs, SCADA systems, an NTP server, PCs, AMS, and switches, among other things. Two kinds of topologies are supported:

- flat: All modules and devices in this network belong to same subnet.
- 2 levels: The network is split into an operation network and an inter-controller network. These two networks can be physically independent, but are generally linked by a routing device.

CPU:

(*central processing unit*) The CPU, also known as the processor or controller, is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. CPUs are computers suited to survive the harsh conditions of an industrial environment.

D

DDT:

(*derived data type*) A derived data type is a set of elements with the same type (`ARRAY`) or with different types (structure).

determinism:

For a defined application and architecture, you can predict that the delay between an event (change of value of an input) and the corresponding change of a controller output is a finite time *t*, smaller than the deadline required by your process.

Device DDT (DDDT):

A Device DDT is a DDT predefined by the manufacturer and not modifiable by user. It contains the I/O language elements of an I/O module.

device network:

An Ethernet-based network within a remote I/O network that contains both remote I/O and distributed I/O devices. Devices connected on this network follow specific rules to allow remote I/O determinism.

DFB:

DFB is the abbreviation for Derived Function Block.

DFB types are function blocks that can be programmed in ST, IL, LD, FBD or SFC.

By using DFB types in an application, it is possible to:

- simplify the design and input of the program,
- increase the legibility of the program,
- facilitate the debugging of the program,
- reduce the volume of the generated code.

DHCP:

(*dynamic host configuration protocol*) An extension of the BOOTP communications protocol that provides for the automatic assignment of IP addressing settings, including IP address, subnet mask, gateway IP address, and DNS server names. DHCP does not require the maintenance of a table identifying each network device. The client identifies itself to the DHCP server using either its MAC address, or a uniquely assigned device identifier. The DHCP service utilizes UDP ports 67 and 68.

DIO cloud:

A group of distributed equipment that is not required to support RSTP. DIO clouds require only a single (non-ring) copper wire connection. They can be connected to some of the copper ports on DRSs, or they can be connected directly to the controller or Ethernet communications modules in the *local rack*. DIO clouds **cannot** be connected to *sub-rings*.

DIO network:

A network containing distributed equipment, in which I/O scanning is performed by a controller with DIO scanner service on the local rack. DIO network traffic is delivered after RIO traffic, which takes priority in an RIO network.

DIO:

(*distributed I/O*) Also known as distributed equipment. DRSs use DIO ports to connect distributed equipment.

distributed equipment:

Any Ethernet device (Schneider Electric device, PC, servers, or third-party devices) that supports exchange with a controller or other Ethernet I/O scanner service.

DNS:

(*domain name server/service*) A service that translates an alpha-numeric domain name into an IP address, the unique identifier of a device on the network.

domain name:

An alpha-numeric string that identifies a device on the internet, and which appears as the primary component of a web site's uniform resource locator (URL). For example, the domain name *schneider-electric.com* is the primary component of the URL *www.se.com*.

Each domain name is assigned as part of the domain name system, and is associated with an IP address.

Also called a host name.

DRS:

(*dual-ring switch*) A ConneXium extended managed switch that has been configured to operate on an Ethernet network. Predefined configuration files are provided by Schneider Electric to downloaded to a DRS to support the special features of the main ring / sub-ring architecture.

DSCP:

(*differentiated service code points*) This 6-bit field is in the header of an IP packet to classify and prioritize traffic.

DST:

(*daylight saving time*) DST is also called *summer time* and is a practice consisting of adjusting forward the clock near the start of spring and adjusting it backward near the start of autumn.

DT:

(*date and time*) The `DT` type, encoded in BCD in a 64-bit format, contains this information:

- the year encoded in a 16-bit field
- the month encoded in an 8-bit field
- the day encoded in an 8-bit field
- the time encoded in an 8-bit field
- the minutes encoded in an 8-bit field
- the seconds encoded in an 8-bit field

NOTE: The eight least significant bits are not used.

The `DT` type is entered in this format:

```
DT#<Year>-<Month>-<Day>-<Hour>:<Minutes>:<Seconds>
```

This table shows the upper/lower limits of each field:

Field	Limits	Comment
Year	[1990,2099]	Year
Month	[01,12]	The leading 0 is displayed; it can be omitted during data entry.
Day	[01,31]	For months 01/03/05/07/08/10/12
	[01,30]	For months 04/06/09/11
	[01,29]	For month 02 (leap years)
	[01,28]	For month 02 (non-leap years)
Hour	[00,23]	The leading 0 is displayed; it can be omitted during data entry.
Minute	[00,59]	The leading 0 is displayed; it can be omitted during data entry.
Second	[00,59]	The leading 0 is displayed; it can be omitted during data entry.

DTM:

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

See FDT.

E

EDS:

(*electronic data sheet*) EDS are simple text files that describe the configuration capabilities of a device. EDS files are generated and maintained by the manufacturer of the device.

EFB:

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

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

EF:

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

A function does not have any information on the internal state. Several calls to the same function using the same input parameters will return the same output values. You will find information on the graphic form of the function call in the [*functional block (instance)*]. Unlike a call to a function block, function calls include only an output which is not named and whose name is identical to that of the function. In FBD, each call is indicated by a unique [number] using the graphic block. This number is managed automatically and cannot be modified.

Position and configure these functions in your program to execute your application.

You can also develop other functions using the SDKC development kit.

EIO network:

(Ethernet I/O) An Ethernet-based network that contains three types of devices:

- local rack
- X80 remote drop (using a BM•CRA312•0 adapter module), or a BMENOS0300 network option switch module
- ConneXium extended dual-ring switch (DRS)

NOTE: Distributed equipment may also participate in an Ethernet I/O network using a connection to DRSs or the service port of X80 remote modules.

EN:

EN stands for **EN**able; it is an optional block input. When the EN input is enabled, an ENO output is set automatically.

If EN = 0, the block is not enabled; its internal program is not executed, and ENO is set to 0.

If EN = 1, the block's internal program is run and ENO is set to 1. If a runtime error is detected, ENO is set to 0.

If the EN input is not connected, it is set automatically to 1.

ENO:

ENO stands for **E**rror **NO**tification; this is the output associated with the optional input EN.

If ENO is set to 0 (either because EN = 0 or if a runtime error is detected):

- The status of the function block outputs remains the same as it was during the previous scanning cycle that executed correctly.
- The output(s) of the function, as well as the procedures, are set to 0.

Ethernet DIO scanner service:

This embedded DIO scanner service of M580 controllers manages distributed equipment on an M580 device network.

Ethernet I/O scanner service:

This embedded Ethernet I/O scanner service of M580 controllers manages distributed equipment **and** RIO drops on an M580 device network.

EtherNet/IP™:

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

Ethernet:

A 10 Mb/s, 100 Mb/s, or 1 Gb/s, CSMA/CD, frame-based LAN that can run over copper twisted pair or fiber optic cable, or wireless. The IEEE standard 802.3 defines the rules for configuring a wired Ethernet network; the IEEE standard 802.11 defines the rules for configuring a wireless Ethernet network. Common forms include 10BASE-T, 100BASE-TX, and 1000BASE-T, which can utilize category 5e copper twisted pair cables and RJ45 modular connectors.

explicit messaging client:

(*explicit messaging client class*) The device class defined by the ODVA for EtherNet/IP nodes that only support explicit messaging as a client. HMI and SCADA systems are common examples of this device class.

explicit messaging:

TCP/IP-based messaging for Modbus TCP and EtherNet/IP. It is used for point-to-point, client/server messages that include both data, typically unscheduled information between a client and a server, and routing information. In EtherNet/IP, explicit messaging is considered class 3 type messaging, and can be connection-based or connectionless.

F

FAST:

A FAST task is an optional, periodic processor task that identifies high priority, multiple scan requests, which is run through its programming software. A FAST task can schedule selected I/O modules to have their logic solved more than once per scan. The FAST task has two sections:

- IN: Inputs are copied to the IN section before execution of the FAST task.
- OUT: Outputs are copied to the OUT section after execution of the FAST task.

FBD:

(*function block diagram*) An IEC 61131-3 graphical programming language that works like a flowchart. By adding simple logical blocks (for example, `AND`, `OR`), each function or function block in the program is represented in this graphical format. For each block, the inputs are on the left and the outputs on the right. Block outputs can be linked to inputs of other blocks to create complex expressions.

FDR:

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

FDT:

(*field device tool*) The technology that harmonizes communication between field devices and the system host.

FTP:

(*file transfer protocol*) A protocol that copies a file from one host to another over a TCP/IP-based network, such as the internet. FTP uses a client-server architecture as well as separate control and data connections between the client and server.

full duplex:

The ability of two networked devices to independently and simultaneously communicate with each other in both directions.

function block diagram:

See FBD.

G

gateway:

A gateway device interconnects two different networks, sometimes through different network protocols. When it connects networks based on different protocols, a gateway converts a datagram from one protocol stack into the other. When used to connect two IP-based networks, a gateway (also called a router) has two separate IP addresses, one on each network.

GPS:

(*global positioning system*) The GPS standard consists of a space-based positioning, navigation, and timing signals delivered worldwide for civil and military use. Standard positioning service performance depends on satellite broadcast signal parameters, GPS constellation design, the number of satellites in sight, and various environmental parameters.

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.

HART:

(*highway addressable remote transducer*) A bi-directional communication protocol for sending and receiving digital information across analog wires between a control or monitoring system and smart devices.

HART is the global standard for providing data access between host systems and intelligent field instruments. A host can be any software application from a technician's hand-held device or laptop to a plant's process control, asset management, or other system using any control system.

high-capacity daisy chain loop:

Often referred to as HCDL, a high-capacity daisy chain loop uses dual-ring switches (DRSs) to connect device sub-rings (containing RIO drops or distributed equipment) and/or DIO clouds to the Ethernet RIO network.

HMI:

(*human machine interface*) System that allows interaction between a human and a machine.

Hot Standby:

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

HTTP:

(*hypertext transfer protocol*) A networking protocol for distributed and collaborative information systems. HTTP is the basis of data communication for the web.

I

I/O scanner:

An Ethernet service that continuously polls I/O modules to collect data, status, event, and diagnostics information. This process monitors inputs and controls outputs. This service supports both RIO and DIO logic scanning.

%I:

According to the CEI standard, `%I` indicates a language object of type discrete IN.

IEC 61131-3:

International standard: programmable logic controllers

Part 3: programming languages

IGMP:

(internet group management protocol) This internet standard for multicasting allows a host to subscribe to a particular multicast group.

IL:

(*instruction list*) An IEC 61131-3 programming language that contains a series of basic instructions. It is very close to assembly language used to program processors. Each instruction is made up of an instruction code and an operand.

implicit messaging:

UDP/IP-based class 1 connected messaging for EtherNet/IP. Implicit messaging maintains an open connection for the scheduled transfer of control data between a producer and consumer. Because an open connection is maintained, each message contains primarily data, without the overhead of object information, plus a connection identifier.

inter-controller network:

An Ethernet-based network that is part of the control network, and provides data exchange between controllers and engineering tools (programming, asset management system (AMS)).

INT:

(*INTeger*) (encoded in 16 bits) The upper/lower limits are as follows: -(2 to the power of 15) to (2 to the power of 15) - 1.

Example: `-32768`, `32767`, `2#1111110001001001`, `16#9FA4`.

IODDT:

(*input/output derived data type*) A structured data type representing a module, or a channel of a controller. Each application expert module possesses its own IODDTs.

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.

IPsec:

(*internet protocol security*) An open set of protocol standards that make IP communication sessions private and encrypted for traffic between modules using IPsec, developed by the internet engineering task force (IETF). The IPsec authentication and encryption algorithms require user-defined cryptographic keys that process each communications packet in an IPsec session.

isolated DIO network:

An Ethernet-based network containing distributed equipment that does not participate in an RIO network.

%IW:

According to the CEI standard, `%IW` indicates a language object of type analog IN.

L

LD:

(*ladder diagram*) An IEC 61131-3 programming language that represents instructions to be executed as graphical diagrams very similar to electrical diagrams (for example, contacts, coils).

literal value of an integer:

A literal value of an integer is used to enter integer values in the decimal system. Values may be preceded by the "+" and "-" signs. Underscore signs (_) separating numbers are not significant.

Example:

```
-12,0,123_456,+986
```

local rack:

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

local slave:

The functionality offered by Schneider Electric EtherNet/IP communication modules that allows a scanner to take the role of an adapter. The local slave enables the module to publish data using implicit messaging connections. Local slave is typically used in peer-to-peer exchanges between PACs.

M

%M:

According to the CEI standard, `%M` indicates a language object of type memory bit.

M580 Ethernet I/O device:

An Ethernet device that provides automatic network recovery and deterministic RIO performance. The time it takes to resolve an RIO logic scan can be calculated, and the system can recover quickly from a communication disruption. M580 Ethernet I/O devices include:

- local rack (including a controller with Ethernet I/O scanner service)
- RIO drop (including an X80 adapter module)
- DRS switch with a predefined configuration

main ring:

The main ring of an Ethernet RIO network. The ring contains RIO modules and a local rack (containing a controller with Ethernet I/O scanner service) and a power supply module.

MAST:

A master (MAST) task is a deterministic processor task that is run through its programming software. The MAST task schedules the RIO module logic to be solved in every I/O scan. The MAST task has two sections:

- IN: Inputs are copied to the IN section before execution of the MAST task.
- OUT: Outputs are copied to the OUT section after execution of the MAST task.

MB/TCP:

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

MIB:

(*management information base*) A virtual database used for managing the objects in a communications network. See SNMP.

Modbus:

Modbus is an application layer messaging protocol. Modbus provides client and server communications between devices connected on different types of buses or networks. Modbus offers many services specified by function codes.

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.

%MW:

According to the CEI standard, `%MW` indicates a language object of type memory word.

N

network convergence:

Activity of re-configuring the network in situation of network loss to ensure system availability.

network time service:

Use this service to synchronize computer clocks over the Internet to record events (sequence events), synchronize events (trigger simultaneous events), or synchronize alarms and I/O (time stamp alarms).

network:

There are two meanings:

- In a ladder diagram:

  A network is a set of interconnected graphic elements. The scope of a network is local, concerning the organizational unit (section) of the program containing the network.

- With expert communication modules:

  A network is a set of stations that intercommunicate. The term *network* is also used to define a group interconnected graphic elements. This group then makes up part of a program that may comprise a group of networks.

NIM:

(*network interface module*) A NIM resides in the first position on an STB island (leftmost on the physical setup). The NIM provides the interface between the I/O modules and the fieldbus master. It is the only module on the island that is fieldbus-dependent — a different NIM is available for each fieldbus.

NTP:

(*network time protocol*) Protocol for synchronizing computer system clocks. The protocol uses a jitter buffer to resist the effects of variable latency.

O

O->T:

(*originator to target*) See originator and target.

ODVA:

(*Open DeviceNet Vendors Association*) The ODVA supports network technologies that are based on CIP.

OFS:

(*OPC Factory Server*) OFS enables real-time SCADA communications with the Control Expert family of PLCs. OFS utilizes the standard OPC data access protocol.

OPC DA:

(*OLE for Process Control Data Access*) The Data Access Specification is the most commonly implemented of the OPC standards that provide specifications for real-time data communications between clients and servers.

operation network:

An Ethernet-based network containing operator tools (SCADA, client PC, printers, batch tools, and EMS, among other things.). Controllers are connected directly or through routing of the inter-controller network. This network is part of the control network.

originator:

In EtherNet/IP, a device is considered the originator when it initiates a CIP connection for implicit or explicit messaging communications or when it initiates a message request for un-connected explicit messaging.

P

PAC:

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

port 502:

Port 502 of the TCP/IP stack is the well-known port that is reserved for Modbus TCP communications.

port mirroring:

In this mode, data traffic that is related to the source port on a network switch is copied to another destination port. This allows a connected management tool to monitor and analyze the traffic.

PTP:

(*precision time protocol*) Use this protocol to synchronize clocks throughout a computer network. On a local area network, PDP achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

Q

%Q:

According to the CEI standard, `%Q` indicates a language object of type discrete OUT.

QoS:

(*quality of service*) The practice of assigning different priorities to traffic types for the purpose of regulating data flow on the network. In an industrial network, QoS is used to provide a predictable level of network performance.

%QW:

According to the CEI standard, `%QW` indicates a language object of type analog OUT.

R

rack optimized connection:

Data from multiple I/O modules are consolidated in a single data packet to be presented to the scanner in an implicit message in an EtherNet/IP network.

ready device:

Ethernet ready device that provides additional services to the EtherNet/IP or Modbus module, such as: single parameter entry, bus editor declaration, system transfer, deterministic scanning capacity, alert message for modifications, and shared user rights between Control Expert and the device DTM.

RIO drop:

One of the three types of RIO modules in an Ethernet RIO network. An RIO drop is an M580 rack of I/O modules that are connected to an Ethernet RIO network and managed by an Ethernet RIO adapter module. A drop can be a single rack or a main rack with an extended rack.

RIO network:

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

RPI:

(requested packet interval) The time period between cyclic data transmissions requested by the scanner. EtherNet/IP devices publish data at the rate specified by the RPI assigned to them by the scanner, and they receive message requests from the scanner at each RPI.

RSTP:

(*rapid spanning tree protocol*) Allows a network design to include spare (redundant) links to provide automatic backup paths if an active link stops working, without the need for loops or manual enabling/disabling of backup links.

S

S908 RIO:

A Quantum RIO system using coaxial cabling and terminators.

SCADA:

(*supervisory control and data acquisition*) SCADA systems are computer systems that control and monitor industrial, infrastructure, or facility-based processes (examples: transmitting electricity, transporting gas and oil in pipelines, and distributing water).

scanner class device:

A scanner class device is defined by the ODVA as an EtherNet/IP node capable of originating exchanges of I/O with other nodes in the network.

scanner:

A scanner acts as the originator of I/O connection requests for implicit messaging in EtherNet/IP, and message requests for Modbus TCP.

service port:

A dedicated Ethernet port on the M580 RIO modules. The port may support these major functions (depending on the module type):

- port mirroring: for diagnostic use
- access: for connecting HMI/Control Expert/ConneXview to the controller
- extended: to extend the device network to another subnet
- disabled: disables the port, no traffic is forwarded in this mode

SFC:

(*sequential function chart*) An IEC 61131-3 programming language that is used to graphically represent in a structured manner the operation of a sequential controller. This graphical description of the controller's sequential behavior and of the various resulting situations is created using simple graphic symbols.

SFP:

(*small form-factor pluggable*). The SFP transceiver acts as an interface between a module and fiber optic cables.

simple daisy chain loop:

Often referred to as SDCL, a simple daisy chain loop contains RIO modules only (no distributed equipment). This topology consists of a local rack (containing a controller with Ethernet I/O scanner service), and one or more RIO drops (each drop containing an RIO adapter module).

SMTP:

(*simple mail transfer protocol*) An email notification service that allows controller-based projects to report alarms or events. The controller monitors the system and can automatically create an email message alert with data, alarms, and/or events. Mail recipients can be either local or remote.

SNMP:

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

SNTP:

(*simple network time protocol*) See NTP.

SOE:

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

ST:

(*structured text*) An IEC 61131-3 programming language that presents structured literal language and is a developed language similar to computer programming languages. It can be used to organize a series of instructions.

sub-ring:

An Ethernet-based network with a loop attached to the main ring, using a dual-ring switch (DRS) or BMENOS0300 network option switch module on the main ring. This network contains RIO or distributed equipment.

subnet mask:

The 32-bit value used to hide (or mask) the network portion of the IP address and thereby reveal the host address of a device on a network using the IP protocol.

%SW:

According to the CEI standard, `%SW` indicates a language object of type system word.

switch:

A multi-port device used to segment the network and limit the likelihood of collisions. Packets are filtered or forwarded based upon their source and destination addresses. Switches are capable of full-duplex operation and provide full network bandwidth to each port. A switch can have different input/output speeds (for example, 10, 100 or 1000Mbps). Switches are considered OSI layer 2 (data link layer) devices.

T

T->O:

(*target to originator*) See target and originator.

target:

In EtherNet/IP, a device is considered the target when it is the recipient of a connection request for implicit or explicit messaging communications, or when it is the recipient of a message request for un-connected explicit messaging.

TCP/IP:

Also known as *internet protocol suite*, TCP/IP is a collection of protocols used to conduct transactions on a network. The suite takes its name from two commonly used protocols: transmission control protocol and internet protocol. TCP/IP is a connection-oriented protocol that is used by Modbus TCP and EtherNet/IP for explicit messaging.

TCP:

(*transmission control protocol*) A key protocol of the internet protocol suite that supports connection-oriented communications, by establishing the connection necessary to transmit an ordered sequence of data over the same communication path.

TFTP:

(*trivial file transfer protocol*) A simplified version of *file transfer protocol* (FTP), TFTP uses a client-server architecture to make connections between two devices. From a TFTP client, individual files can be uploaded to or downloaded from the server, using the user datagram protocol (UDP) for transporting data.

TIME_OF_DAY:

See `TOD`.

TOD:

(*time of day*) The `TOD` type, encoded in BCD in a 32-bit format, contains this information:

- the hour encoded in an 8-bit field
- the minutes encoded in an 8-bit field
- the seconds encoded in an 8-bit field

NOTE: The eight least significant bits are not used.

The TOD type is entered in this format: xxxxxxxx: **`TOD#`**`<Hour>`**`:`**`<Minutes>`**`:`**`<Seconds>`

This table shows the upper/lower limits of each field:

Field	Limits	Comment
Hour	[00,23]	The leading 0 is displayed; it can be omitted during data entry.
Minute	[00,59]	The leading 0 is displayed; it can be omitted during data entry.
Second	[00,59]	The leading 0 is displayed; it can be omitted during data entry.

Example: `TOD#23:59:45`.

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.

TR:

(*transparent ready*) Web-enabled power distribution equipment, including medium- and low-voltage switch gear, switchboards, panel boards, motor control centers, and unit substations. Transparent Ready equipment allows you to access metering and equipment status from any PC on the network, using a standard web browser.

U

UDP:

(*user datagram protocol*) A transport layer protocol that supports connectionless communications. Applications running on networked nodes can use UDP to send datagrams to one another. Unlike TCP, UDP does not include preliminary communication to establish data paths or provide data ordering and checking. However, by avoiding the overhead required to provide these features, UDP is faster than TCP. UDP may be the preferred protocol for time-sensitive applications, where dropped datagrams are preferable to delayed datagrams. UDP is the primary transport for implicit messaging in EtherNet/IP.

UMAS:

(*Unified Messaging Application Services*) UMAS is a proprietary system protocol that manages communications between Control Expert and a controller.

UTC:

(*coordinated universal time*) Primary time standard used to regulate clocks and time worldwide (close to former GMT time standard).

V

variable:

Memory entity of type `BOOL`, `WORD`, `DWORD`, and similar types, containing content that can be modified by the program currently running.

VLAN:

(*virtual local area network*) A local area network (LAN) that extends beyond a single LAN to a group of LAN segments. A VLAN is a logical entity that is created and configured uniquely using applicable software.

Index

A

access
USB....20
access control
cybersecurity....117
security....32
access control policy
CSPN....48
accounts
cybersecurity....90
ACL
security....32
administrative interface
CSPN....48
architecture....19
assets
critical, M580 CSPN controller....47
critical, M580 CSPN environment....47
audit trail
security....50
authentication
cybersecurity....117
authorization
security....95
authorizations
cybersecurity....117

C

certification
CSPN....42
communication services
disable....31
communication, secure
CSPN....48
Control Expert
password....94
Control Expert Security Editor....45
controller execution mode
CSPN....48
controller memory
CSPN....48
critical assets
environment, M580 CSPN....47
PAC, M580 CSPN....47
CSPN....42
critical assets, controller....47
critical assets, environment....47
M580 cybersecurity parameters....46
M580 operating modes....46
M580, access control policy....48
M580, denial of service....48
M580, encrypted authentication on administrative interface....48
M580, encrypted communications....48
M580, execution mode alteration....48
M580, firmware alteration....48
M580, firmware signature....48
M580, flows alteration....48
M580, integrity and authenticity of controller memory....48
M580, integrity of the controller execution mode....48
M580, malformed input management....48
M580, memory program alteration....48
M580, secure storage of secrets....48
cybersecurity....17
access control....117
accounts....90
authentication....117
authorizations....117
CSPN....42
CSPN, M580....42
CSPN, M580 operating modes....46
disable unused services....117
event logging....117
firmware....117
FTP....92
guidelines....17
HTTP....91
integrity checks....117
LANMAN / NTLM....27
literature....17
local area connection....28
M340....124
M580....124
M580 Control Expert Security Editor....45
M580 CSPN parameters....46
network interface cards....28
notifications....17
passwords....91

Premium/Atrium 129
Quantum 125
remote desktop 27
secured communication 117
services 117
SNMP 93
vulnerability 17
X80 127

D

denial of service
CSPN 48
disable
communication services 31
disable unused services
cybersecurity 117

E

event log messages 64
BMENOR2200H 77
BMENUA0100 77
Control Expert 58
M580 controller (firmware earlier than V4.10) 77
M580 controller (for firmware V4.10 and any subsequent supporting version(s) 64
event logging
cybersecurity 117
execution mode alteration
CSPN 48
execution mode, controller
CSPN 48

F

firmware
cybersecurity 117
security 117
firmware alteration
CSPN 48
firmware signature
CSPN 48
flows alteration
CSPN 48
FTP
cybersecurity 92

H

hardening
PC 23
HTTP
cybersecurity 91

I

input management, malformed
CSPN 48
integrity check
security 98
integrity checks
cybersecurity 117
interface, administrative
CSPN 48

L

LAN
cybersecurity 28
LANMAN / NTLM
cybersecurity 27
literature
cybersecurity 17
logging
security 50

M

M340
cybersecurity 124
M580
cybersecurity 124
memory
protect 96
memory program alteration
CSPN 48
memory protection
security 98
memory, controller
CSPN 48

N

network interface cards
cybersecurity 28
notifications
cybersecurity 17

O

Operate
M580 Control Expert Security Editor profile 45
operating modes
CSPN, M580 46

P

password
Control Expert 94
passwords
cybersecurity 91
PC
hardening 23
Premium/Atrium
cybersecurity 129
profile
M580 Control Expert Security Editor 45
Program
M580 Control Expert Security Editor profile 45
protect
memory 96
protection
section 95

Q

Quantum
cybersecurity 125

R

ReadOnly
M580 Control Expert Security Editor profile 45
remote desktop
cybersecurity 27
run/stop
security 96

S

section
protection 95
secure communication
CSPN 48
secured communication
cybersecurity 117
security
access control 32
ACL 32
audit trail 50
authorization 95
CSPN 42
CSPN, M580 operating modes 46
firmware 117
integrity check 98
logging 50
M580 Control Expert Security Editor 45
M580 CSPN parameters 46
memory protection 98
run/stop 96
services 117
Syslog 50
services
cybersecurity 117
security 117
signature, firmware
CSPN 48
SNMP
cybersecurity 93
storage of secrets
CSPN 48
Syslog
BMENOR2200H 77
BMENUA0100 77
Control Expert 58
M580 controller (firmware earlier than V4.10) 77
M580 controller (firmware V4.10 and any subsequent supporting version(s)) 64
security 50

U

USB
access 20
user profiles
security, M580 Control Expert Security Editor 45

V

vulnerability
cybersecurity 17

X

X80
cybersecurity 127

Schneider Electric
1884 Boulevard de la Défense
92000 Nanterre
France

www.se.com

© 2026 Schneider Electric. All rights reserved.

EIO0000001999.15