Modicon Controllers Platform

Cyber Security

Reference Manual

Original instructions

09/2020

EIO0000001999.08

www.schneider-electric.com

Schneider Electric

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

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

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

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

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

Table of Contents

Safety Information

Important Information

NOTICE

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

PLEASE NOTE

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

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

BEFORE YOU BEGIN

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

⚠ WARNING

UNGUARDED EQUIPMENT

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

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

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

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

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

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

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

START-UP AND TEST

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

⚠ WARNING

EQUIPMENT OPERATION HAZARD

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

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

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

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

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

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

OPERATION AND ADJUSTMENTS

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

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

About the Book

At a Glance

Document Scope

⚠ **WARNING**

UNINTENDED EQUIPMENT OPERATION, LOSS OF CONTROL, LOSS OF DATA

The system owners, designers, operators, and those maintaining equipment utilizing Control Expert software must read, understand, and follow the instructions outlined in this document, *Modicon Controllers Platform Cyber Security, Reference Manual* (part number: EIO0000001999).

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

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

NOTE: The term security is used throughout this document in reference to cyber security topics.

Validity Note

This documentation is valid for EcoStruxure™ Control Expert 15.0 or later.

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

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

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

Information Related to Cyber Security

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

Document available for download on cyber security support section:

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

Related Documents

Title of Documentation	Reference Number
Modicon M580 System Planning Guide	HRB62666 (English), HRB65318 (French), HRB65319 (German), HRB65320 (Italian), HRB65321 (Spanish), HRB65322 (Chinese)
Modicon M580 Hardware Reference Manual	EIO0000001578 (English), EIO0000001579 (French), EIO0000001580 (German), EIO0000001582 (Italian), EIO0000001581 (Spanish), EIO0000001583 (Chinese)
Modicon M580 BMENOC0301/11, Ethernet Communication Module, Installation and Configuration Guide	HRB62665 (English), HRB65311 (French), HRB65313 (German), HRB65314 (Italian), HRB65315 (Spanish), HRB65316 (Chinese)
Modicon M340 for Ethernet, Communications Modules and Processors, User Manual	31007131 (English), 31007132 (French), 31007133 (German), 31007494 (Italian), 31007134 (Spanish), 31007493 (Chinese)

Title of Documentation	Reference Number
Quantum using EcoStruxure™ Control Expert, TCP/IP Configuration, User Manuall	33002467 (English), 33002468 (French), 33002469 (German), 31008078 (Italian), 33002470 (Spanish), 31007110 (Chinese)
Premium and Atrium using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manuall	35006192 (English), 35006193 (French), 35006194 (German), 31007214 (Italian), 35006195 (Spanish), 31007102 (Chinese)
EcoStruxure™ Control Expert, Operating Modes	33003101 (English), 33003102 (French), 33003103 (German), 33003104 (Spanish), 33003696 (Italian), 33003697 (Chinese)
Quantum using EcoStruxure™ Control Expert, Hardware Reference Manual	35010529 (English), 35010530 (French), 35010531 (German), 35013975 (Italian), 35010532 (Spanish), 35012184 (Chinese)
Quantum using EcoStruxure™ Control Expert, 140 NOC 771 01, Ethernet Communication Module, User Manual	S1A33985 (English), S1A33986 (French), S1A33987 (German), S1A33989 (Italian), S1A33988 (Spanish), S1A33993 (Chinese)
Premium using EcoStruxure™ Control Expert, TSX ETC 101, Ethernet Communication Module, User Manual	S1A34003 (English), S1A34004 (French), S1A34005 (German), S1A34007 (Italian), S1A34006 (Spanish), S1A34008 (Chinese)
Modicon M340, BMX NOC 0401 Ethernet Communication Module, User Manual	S1A34009 (English), S1A34010 (French), S1A34011 (German), S1A34013 (Italian), S1A34012 (Spanish), S1A34014 (Chinese)

Title of Documentation	Reference Number
Quantum EIO, Control Network, Installation and Configuration Guide	S1A48993 (English), S1A48994 (French), S1A48995 (German), S1A48997 (Italian), S1A48998 (Spanish), S1A48999 (Chinese)
EcoStruxure™ Control Expert, Communication, Block Library	33002527 (English), 33002528 (French), 33002529 (German), 33003682 (Italian), 33002530 (Spanish), 33003683 (Chinese)
Quantum using EcoStruxure™ Control Expert, Ethernet Network Modules, User Manual	33002479 (English), 33002480 (French), 33002481 (German), 31007213 (Italian), 33002482 (Spanish), 31007112 (Chinese)
Modicon M580 BME CXM CANopen Modules, User Manual	EIO0000002129 (English), EIO0000002130 (French), EIO0000002131 (German), EIO0000002132 (Italian), EIO0000002133 (Spanish), EIO0000002134 (Chinese)
MC80 Programmable Logic Controller, User Manual	EIO0000002071 (English)

You can download these technical publications and other technical information from our website at https://www.se.com/ww/en/download/ .

Chapter 1
Presentation

Schneider Electric Guidelines

Introduction

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

The following guidelines describe procedures in a Windows 7 operating system. They are provided as examples only. Your operating system and application may have different requirements or procedures.

A topic dedicated to cyber security is available in the support area of the *Schneider Electric website*.

Defense-In-Depth Approach

In addition to the solutions presented in this book, the recommendation is to follow the Schneider Electric defense-in-depth approach as described in the following STN guide:

- **Book title:** How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cyber Security 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 notified in the **Cybersecurity support** webpage: *http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page*.

If you face a cyber security incident or vulnerability not mentioned in the list provided by Schneider Electric, you can report this incident or vulnerability by clicking **Report an incident or vulnerability** button in the **Cybersecurity support** webpage.

Chapter 2
How to Secure the Architecture

Introduction

This chapter describes the actions to accomplish in Modicon controllers platform architecture in order to make it more secure.

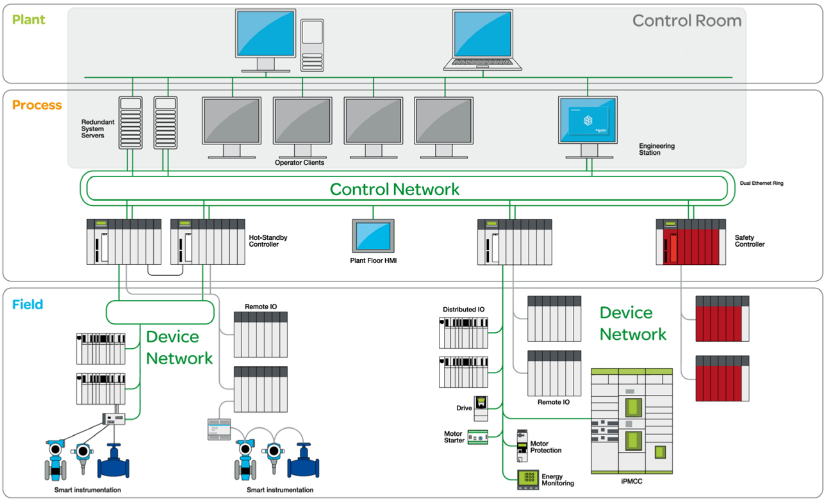
What Is in This Chapter?

This chapter contains the following topics:

System View

System Architecture

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



Secured Communication

Equipment in the control room is more exposed to attacks than equipment connected to the device network. Therefore, implement secured communication between the control room and the PAC 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 PAC and devices.

Secured Access to the USB Ports

The physical access to the CPU USB ports needs to be controlled.

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

Secured Access to the Hot Standby Link and Device Network

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

Hardening the PC

Introduction

The PCs located in the control room are highly exposed to attacks. Those PCs supporting Control Expert or OFS need to be hardened.

Hardening Engineering Workstations

Customers may choose from various commercial PC systems for their engineering workstation needs. Key hardening techniques include:

- Strong password management.
- User account management.
- Methods of least privilege applied to applications and user accounts.
- Removal or disabling unneeded services.
- Removing remote management privileges.
- Systematic patch management.

Disabling Unused Network Interface Cards

Verify that network interface cards not required by the application are disabled. 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 7:

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 that Schneider Electric recommends.

In Windows 7 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 recommendations also include the following:

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

Disabling the Remote Desktop Protocol

Schneider Electric’s defense-in-depth approach recommendations 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 2008R2 or Windows 7, disable RDP via **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.

Updating Security Policies

Update the security policies on the PCs in your system by `gpupdate` in a command window. For more information, refer to the Microsoft documentation on `gpupdate`.

Disabling LANMAN and NTLM

The Microsoft LAN Manager protocol (LANMAN or LM) and its successor NT LAN Manager (NTLM) have vulnerabilities that make their use in control applications inadvisable.

The following steps describe how to disable LM and NTLM in a Windows 7 or Windows 2008R2 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 Manger 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.

Managing Updates

Before deployment, update all PC operating systems using the utilities on Microsoft’s **Windows Update** Web page. To access this tool in Windows 2008R2, or Windows 7, select **Start** → **All Programs** → **Windows Update**.

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).

Description

In order to reduce the attack field, disable any unused embedded service to close potential communication doors.

Disable Ethernet Services in Control Expert

You can enable/disable Ethernet services using the Ethernet tabs in control Expert. Tabs description is provided for each of the following platform:

- Modicon M340 *(see page 59)*
- Modicon M580 *(see page 60)*
- Modicon Quantum *(see page 61)*
- Modicon X80 modules *(see page 63)*
- Modicon Premium/Atrium *(see page 65)*

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

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 allows to disable a service enabled after configuration in Control Expert application. The service can be enabled again using the same function block.

Restrict Data Flow from Control Network (Access Control)

Data Flow from Control Network

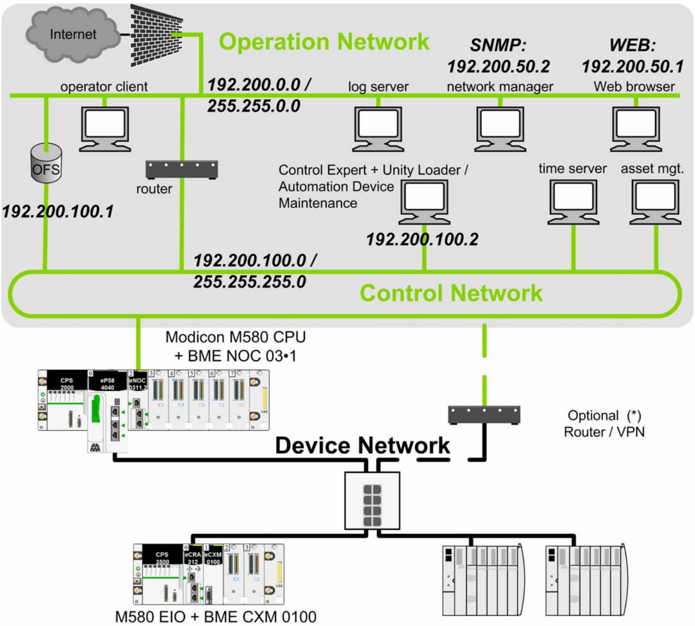
Data flow from control network is an IP-based data flow initiated on the control network.

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, the secure access is provided by an optional router/VPN.

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

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

Source	IP address	Subnet	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
Network manager	192.200.50.2	No	–	–	–	–	–	–	+
Operation network	192.200.0.0	Yes	255.255.0.0	–	–	+	–	–	–
Automation Device Maintenance / Unity Loader	192.200.100.2	No	–	+	–	–	–	–	–
Control network	192.200.100.0	Yes	255.255.255.0	–	–	–	+	–	–
+ Selected – Not selected or no content									

Settings Description

An authorized address is set for devices authorized to communicate with the CPU 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): Operation network subnet is set to authorize all Web browsers connected to the operation network to access the CPU web browser.
192.200.100.2 (FTP): Set to authorize the access from Automation Device Maintenance / Unity Loader 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, Unity Loader) to access the CPU via Port502 Modbus.

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 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 Secured Communication

Introduction

The goal of secured communication is to help protect the communication channels that allow remote access to the critical resources of the system (such as 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 allows to secure:

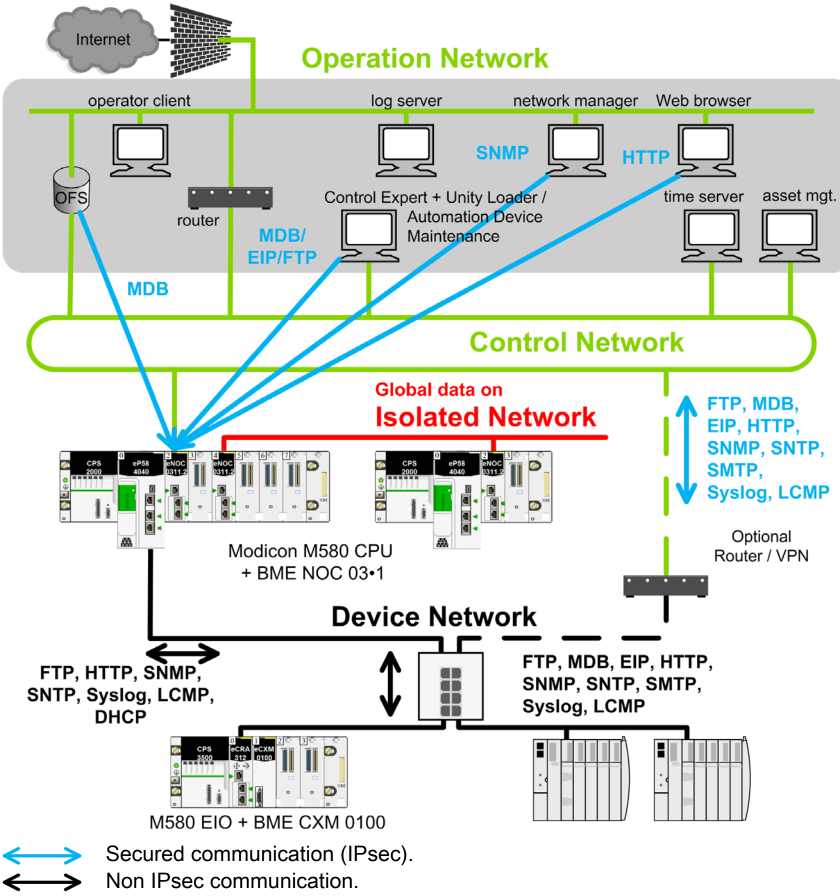
- The control room Modbus access to the PAC CPU through the BMENOC0301/11 module.
- The control room access to the communication services running inside the BMENOC0301/11 module in server mode (Modbus, EtherNet/IP, HTTP, FTP, SNMP).

NOTE: IPsec is intended to secure services running in server mode in the PAC. Secure client services initiated by the 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 secured communication from the control room to a Modicon M580 PAC.



Data Flow with Secured 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 secure connections.
FTP server, TFTP server	
HTTP	
ICMP (ping, etc.)	
Modbus server (port 502)	
ARP	These services are supported through secure and unsecure 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 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 secured 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: BMENOC0301/11 does not support IP forwarding to device network.

If transparency is required between control and device network, an external router/vpn is needed to provide a secured communication between the control and device network (as shown in previous architecture example figure *(see page 24)*).

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

- Update Modicon M580 CPU firmware from the Automation Device Maintenance or Unity Loader software through FTP service.
- Perform a network diagnostic of Modicon M580 CPU from a network management tool through SNMP service.
- Diagnose a Modicon M580 CPU from a DTM through EIP service.
- Diagnose a Modicon M580 CPU from a Web browser through HTTP service.
- Log Modicon M580 CPU cyber security events in a syslog server through syslog service.
- Synchronize Modicon M580 CPU time from a global time server through NTP service.

NOTE: The BMENOC0301/11 is the only module that provides secure communication between the plant floor and the control room.

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 PAC using Modbus (Control Expert, Automation Device Maintenance, Unity Loader, 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 each BMENOC0301/11 module configured in the local rack (Control Expert DTM, Automation Device Maintenance, Unity Loader, SNMP manager, Web browser, Web designer for FactoryCast BMENOC0301/11 module).
  Configure IPsec on each PC supporting these authorized applications.
- Incorporate a BMENOC0301/11 module with IPsec function on the backplane of each PAC connected to the control network.
  To configure the IPsec function on a BMENOC0301/11 module, 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 only. To increase the security of the pre-shared key, we recommend that you use an external tool such as KeePass *(see page 27)* to generate an appropriate character string.

The BMENOC0301/11 module configuration is performed with Control Expert. The application is initially downloaded through USB link, future downloads are performed through Ethernet with an IPsec function if IPsec is enabled.

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

- Use Microsoft Windows 7 or 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 *(see page 17)*.

More details on configuration are provided in the *Configuring IP Secure Communications* topic *(see Modicon M580, BMENOC0301/0311 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. We recommend the use of 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 save the folder.
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**).

Step	Action
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 Secure Communications* topic *(see Modicon M580, BMENOC0301/0311 Ethernet Communications Module, Installation and Configuration Guide)*.

CSPN Security Target

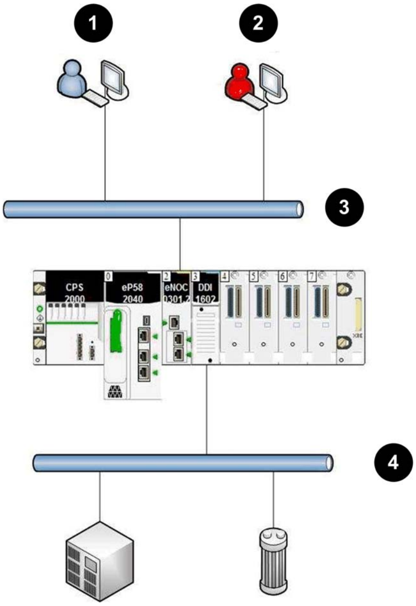
CSPN Introduction

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

M580 Introduction

The M580 PAC is designed to control and command an industrial process continuously without human intervention. At each step, the PAC 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 via a BMENOC0301/0311 Ethernet communication module on the local rack with the PAC.The PAC can run in a hostile environment despite humidity, dust, or unusual temperatures for IT systems and strong EMC or mechanical constraints.

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



1 operator using Control Expert
2 attacker
3 supervision network
4 field network with no attacker

M580 Features

The M580 PAC offers the following features:

Feature	Description
user program execution	An M580 PAC runs a user program that processes the inputs and updates the outputs.
input/output management	An M580 PAC can read local inputs and write local outputs. These inputs/outputs can be digital or analog and allow the M580 PAC to control and command the industrial process.
communication with the supervision	An M580 PAC can communicate with SCADA to receive commands and transmit process data using the Modbus protocol.
administrative functions	An M580 PAC includes administrative functions, which are provided in Control Expert , for configuration and programming.
remote logging	An M580 PAC 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	V2.20 or later	This CPU follows the security rules described in the security documents (see assumptions).
BMENOC0301/0311	V2.11 or later	This Ethernet module manages the secure communications with the upper layer (supervision and engineering software Control Expert).

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

User Profiles

Users that interact with the PAC for a secure implementation have the following predefined 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.

Secure Implementation

These items contribute to a healthy environment for a secure implementation:

Item	Security Considerations
security documentation	The product documentation (user guides, white papers, etc. includes instructions for secure usage. All recommendations in the documentation are applied prior to the evaluation).
administrators	System administrators are competent, trained, and trustworthy.
premises	The PAC is located in secure location. Access is restricted to trustworthy people. In particular, an attacker does not have access to the physical ports of the PACs. 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 Control Expert application is controlled by the administrator before it is loaded in the PAC.
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 PAC through the USB interface, and the PAC is unplugged from the network.
firmware upgrade	The firmware upgrade is performed through the USB interface, and the PAC 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 PAC 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 PAC.
- 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 PAC.

Cyber Security Parameters

This table describes the cyber security parameters:

Parameter	Topic	User Guide
ACL activated.	Configuring Security Services	Modicon M580 BMENOC0301/0311 Ethernet Communications Module User 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	Modicon M580 Hardware Reference Guide
Memory protection activated.	Memory Protect	
Project fully secured: ● Application secured with login and password. ● Section protection activated.	Helping Secure a Project in Control Expert	
No upload information stored inside CPU.	PAC 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 PAC 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 PAC 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

PAC: This table shows the assets that are critical to the PACs:

Asset	Description for Proper Use
firmware	The firmware is protected both in integrity and authenticity.
PAC memory	The PAC memory contains the PAC 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 PAC 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 PAC critical assets:

Asset	Availability	Confidentiality	Integrity	Authenticity
firmware			X	X
PAC 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:

	Control-Command of the Industrial Process	Engineering Workstation Flows	Firmware	PAC Memory	Execution Mode	User Secrets
denial of service	Av					
firmware alteration		I, Au				
execution mode alteration					, AuI	
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 PAC 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 PAC or only some of its functions.
firmware alteration	The attacker manages to inject and run a corrupted firmware on the PAC. 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 PAC by legitimate means. Finally, the attacker manages to modify the version of the firmware installed on the PAC without having the privilege to do so.
execution mode alteration	The attacker manages to modify the execution mode of the PAC 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 PAC memory.
flows alteration	The attacker manages to corrupt exchanges between the PAC and an external component without being detected. He can perform attacks such as credential theft, access control violation, or control-command of the industrial process mitigation.

	Persistent Denial of Service	Firmware Alteration	Execution Mode Alteration	Memory Alteration	Flows Alteration
malformed input management	X				
secure storage of secrets				X	
secure authentication on administrative interface					X
access control policy					X
firmware signature		X			
integrity and authenticity of PAC memory				X	
integrity of the PAC execution mode			X		
secure communication					X

Type of Threat	Description
malformed input management	The PAC has been developed to correctly handle malformed input, particularly malformed network traffic.
secure strength of secrets	The PAC 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 PAC ● other services passwords (like FTP)
secure 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 PAC from a non-authentic user.
access control policy	The access control policy helps guarantee the authenticity of privileged operations, i.e., 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 PAC.
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 PAC 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 PAC helps ensure the integrity and authenticity of the user program, so that only 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 PAC execution mode	The PAC helps ensure that the execution mode can only 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.
secure communication	The PAC supports secured communication, protected in integrity, confidentiality, and authenticity (IPsec encrypted with ESP).The FTP protocol is disabled, and IPsec helps ensure Modbus secured communication through the BMENOC0301/0311 module.

Set Up Cyber Security Audit (Event Logging)

Introduction

Logging events and logging analysis are essential in a secured system. 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 cyber security 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 cyber security events of the system through syslog protocol.
- Log clients (Ethernet connection points where cyber security events are monitored: device, Control Expert or DTM).

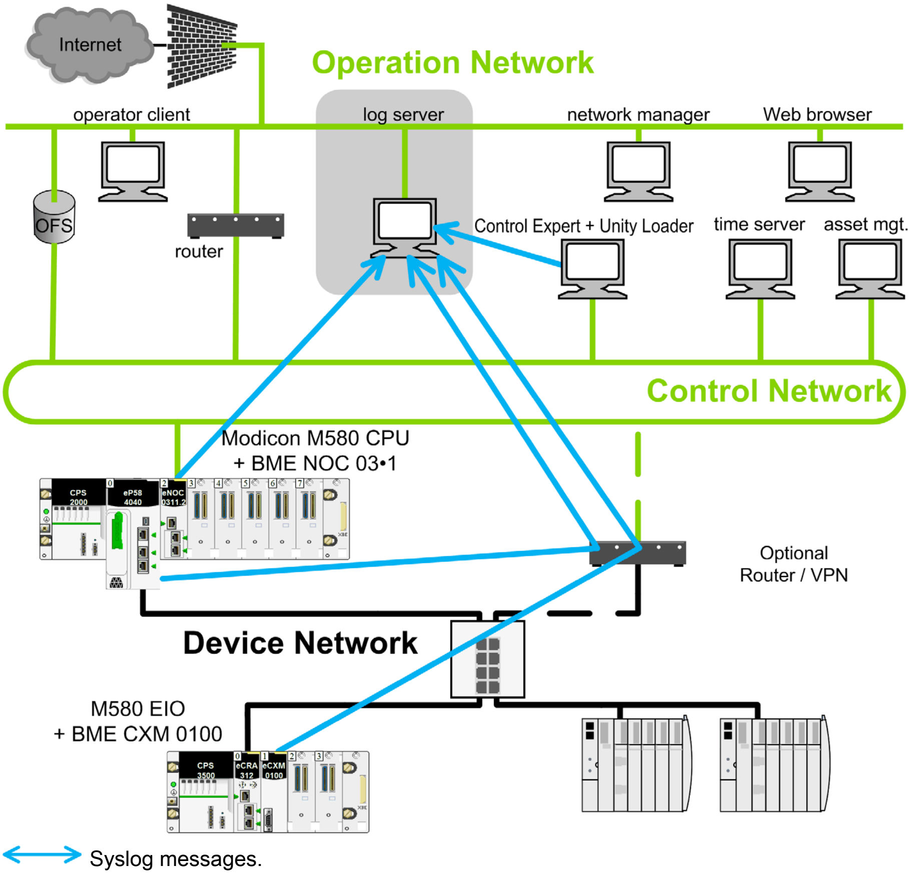
Event Log Service Description

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 cyber security 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.

Architecture Example

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



Events Logged

Syslog message structure:

Field	Description
PRI	Facility and severity information (description provided in following tables).
VERSION	Version of the syslog protocol specification (Version = 1 for RFC 5424.).
TIMESTAMP	Time stamp format is issued from RFC 3339 that recommends the following ISO8601 Internet date and time format: YYY-MM-DD**T**hh:mm:ss.nnn**Z** **NOTE:** -, **T**, :, . , **Z** are mandatory characters and they are part or the time stamp field. **T** and **Z** need to be written in uppercase. **Z** specifies that the time is UTC. Time field content description: **YYY** Year **MM** Month **DD** Day **hh** Hour **mm** Month **ss** Second **nnn** Fraction of second in millisecond (0 if not available)
HOSTNAME	Identifies the machine that originally sent the syslog message: fully qualified domain name (FQDN) or source static IP address if FQDN is not supported.
APP-NAME	Identifies the application that initiates the syslog message. It contains information that allows to identify the entity that sends the message (for example, subset of commercial reference).
PROCID	Identifies the process, or entity, or component that sends the event. Receives NILVALUE if not used.
MSGID	Identifies the type of message on which the event is related to, for example HTTP, FTP, Modbus. Receives NILVALUE if not used.
MESSAGE TEXT	This field contains several information: ● Issuer address: IP address of the entity that generates the log. ● Peer ID: Peer ID if a peer is involved in the operation (for example, user name for a logging operation). Receives null if not used. ● Peer address: Peer IP address if a peer is involved in the operation. Receives null if not used. ● Type: Unique number to identify a message (description provided in following tables). ● Comment: String that describes the message (description provided in following tables).

The following table presents events linked to a PAC that can be logged in a syslog server:

Event description	Facility	Severity (1)	Type	Comment
Successful connection to or from a tool or device: ● Successful login. For example: data storage via FTP, Control Expert application password via Modbus, firmware upload via FTP, FDR ... ● Successful user login to a tool. For example: Control Expert security editor. ● Successful TCP connection (no user). For example: Port502 Modbus TCP/IP explicit messaging for M580 CPU.	10	Informational	1	`Successful login`, or `successful connection`.
Failed connection from a tool or device: ● Failed connection due to access control list (ACL) check (source IP address / TCP port filtering). ● Failed login (with ACL check correct). For example: data storage via FTP, Control Expert application via Modbus, FDR server via FTP... ● Failed user login to a software tool. For example: Control Expert. ● Failed TCP connection (no user). For example: Port502 Modbus TCP/IP explicit messaging for M580 CPU.	10	Warning	2	`Failed login`, `failed connection`, or `connection denied from`.
Disconnection triggered locally or by a peer: ● On logout request (FTP).	10	Informational	5	`Disconnection`.
Automatic logout (for example inactivity time-out).	10	Informational	6	`Auto logout`.
Major changes in the system: ● Firmware upload.	13	Informational	10	`XXXX upload`. For example: `firmware upload`, `web pages upload`.
Communication parameters run time change outside configuration: ● Communication services enabled or disabled (FTP, TFTP, HTTP, function block in M580 PAC device).	10	Warning	18	`Major communication parameter update: XXXX YYYY` (`XXXX` = communication parameter ID, `YYYY` = value). For example: `major communication parameter update: FTP enable`.

(1) NOTE: The terms severity, Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug are used in this table as attributes of syslog event messages and as defined in RFC 5424 specification of the Internet Engineering Task Force (IETF).

Event description	Facility	Severity [1]	Type	Comment
Embedded switch port status change: ● Port link up, port link down, ...	10	Warning	19	ETHXX YYYY (XX = port number, YYYY = port state). For example: ETH3 link down (after a cable disconnection on port 3).
Topology changes detected: ● From RSTP: port role change or root change.	10	Warning	20	topology change detected.
Integrity check error: ● Digital signature error. ● Integrity only (hash) error.	10	Error	84	XXXX integrity error (XXXX identifies the object with an error detected). For example: firmware integrity error.
Major changes in the system: ● Program operating mode change (run, stop, ...).	13	Notice	85	XXXX state update: YYYY (XXXX identifies the object with changing state, YYYY identifies the new state). For example: PLC state update: RUN.
Major changes in the system: ● Restart after RESET	13	Warning	14	Restart
Major changes in the system: ● Program operating mode change: PLC INIT	13	Notice	85	PLC INIT
Major changes in the system: ● Hardware change (SD cart insert, module replacement, ...).	13	Informational	26	XXXX hardware update: YYYY (XXXX identifies the hardware with changing state, YYYY identifies the update). For example: PLC hardware update: SD card insertion.

[1] **NOTE:** The terms severity, Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug are used in this table as attributes of syslog event messages and as defined in RFC 5424 specification of the Internet Engineering Task Force (IETF).

NOTE: Control Expert specific events not described in previous table are defined in the **Security Editor** user profile *(see EcoStruxure™ Control Expert, Security Editor, Operation Guide)* audit column and sent via syslog.

Syslog message facility values as per RFC 5424 specification associated with events type:

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.
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.

Syslog message security values as per RFC 5424 specification associated with events type:

Security 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	Warning conditions.
5	Notice	Normal but significant condition.
6	Informational	Informal messages.
7	Debug	Debug-level messages.

Setting Up a Syslog Server in the System Architecture

A wide variety of syslog servers are available for various operating systems. 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, DTMs, and Control Expert.

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 (deselected by default). **NOTE:** A project with this setting checked can only be opened in Unity Pro (Control Expert) 10.0 or later.
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 diagnostic 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 **Audit** check box in the **Policies** tab of the Security Editor *(see EcoStruxure™ Control Expert, Security Editor, Operation Guide)*.
BMENOC0301/11 device DDT (`SERVICE_STATUS2` parameter)	Two diagnostic information is available: **EVENT_LOG_STATUS:** Value = 1 if event log service is operational or disabled. Value = 0 if event log service is not operational. **LOG_SERVER_NOT_REACHABLE:** Value = 1 if the syslog client does not receive the acknowledge of the TCP messages from the syslog server. Value = 0 if the acknowledge is received.
Modicon M580 CPU device DDT	
BMECXM Device DDT	

Control Identification and Authentication

Managing Accounts

Schneider Electric recommends the following regarding 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) (Windows 7)

To block unauthorized attempts to make system changes, Windows 7 grants applications the permission levels of a normal user, with no administrative privileges. At this level, 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 7, open **Control Panel** → **User Accounts and Family Safety** → **User Accounts** → **Change User Account Control Settings**, or enter **UAC** in the Windows 7 **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. Schneider Electric recommends the following password management guidelines:

- Enable password authentication on all email and Web servers, CPUs, 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 via email 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 via 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.

Managing SNMP

Simple network management protocol (SNMP) provides network management services between a central management console and network devices such as routers, printers, and PACs. 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, PACs, 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 via SNMP:

- When possible, deactivate SNMP v1 and v2 and use SNMP v3, which encrypts passwords and messages.
- If SNMP v1 or v2 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 and v2 commands between the control network and operations network to specific hosts or communicate them over a separate, secured management network.
- Control access by identifying which IP address has privilege to query an SNMP device.

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

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

- Application
  Control Expert and CPU application protection by a password prevents unwanted application modification, download, or opening (.STU and .STA files). 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 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.
- Data Storage
  Data storage protection by a password prevents unwanted access to the data storage zone of the SD memory card (if a valid card is inserted in the CPU). More details are provided in the *Data Storage Protection* topic. *(see EcoStruxure ™ Control Expert, Operating Modes)*
- Firmware
  Firmware download protection by a password prevents download of malicious firmware inside the CPU. 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. Control Expert access security concerns the terminal 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*.

Recommendation: Set a dedicated password to the super user and limit other users authorizations with a restricting profile.

Programming and Monitoring Mode

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

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

To choose a mode in 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)*.

Recommendation: Set the **Online** CPU 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.

Recommendation: Activate the sections protection.

CPU Memory Protection

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

NOTE: The CPU memory protection cannot be configured with Hot Standby CPUs. In such cases, use IPsec secured communication.

The memory protection is activated as follows:

- Modicon M340 CPU: Input bit. More details in the *Configuration of Modicon M340 processors* section *(see EcoStruxure™ Control Expert, Operating Modes)*.
- Modicon M580 CPU: Input bit. More details in the *Managing Run/Stop Input* section *(see Modicon M580, Hardware, Reference Manual)*.
- Modicon Quantum CPU: Physical key switch on the CPU 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)* CPU.
- Modicon Premium CPU: Input bit. More details in the *Configuration of Premium processors* section *(see EcoStruxure™ Control Expert, Operating Modes)*.
- Modicon MC80 CPU: Input bit. More details in Modicon MC80 CPU manual.

Recommendation: Activate the CPU memory protection whenever possible.

CPU Remote Run/Stop Access

NOTE: The CPU remote run/stop access cannot be configured with Hot Standby CPUs. In such cases, use IPsec secured communication.

The remote run/stop access management defines how a CPU can be started or stopped remotely and depends on the platform:

Modicon M580: CPU remote access to run/stop allows one of the following:

- Stop or run the CPU remotely by request.
- Stop the CPU remotely by request. Denies running the CPU remotely by request, only a run controlled by the input is available when a valid input is configured.
- Denies to run or stop the CPU remotely by request.

Refer to the *Managing Run/Stop Input* for CPU configuration options that help prevent remote commands from accessing the Run/Stop modes section *(see Modicon M580, Hardware, Reference Manual)*.

Modicon M340: CPU remote access to run/stop allows one of the following:

- Stop or run the CPU remotely by request.
- Stop the CPU remotely by request. Denies running the CPU remotely by request, 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: CPU remote access to run/stop allows one of the following:

- Stop or run the CPU remotely by request.
- Stop the CPU remotely by request. Denies running the CPU remotely by request, 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: CPU remote access to run/stop allows to:

- Stop or run the CPU remotely via request.

Modicon MC80: CPU remote access to run/stop allows one of the following:

- Stop or run the CPU remotely by request.
- Stop the CPU remotely by request. Denies running the CPU remotely by request, only a run controlled by the input is available when a valid input is configured.
- Denies to run or stop the CPU remotely by request.

Refer to the *Configuration of Modicon MC80 Processors* section in MC80 user manual.

Recommendation: Deny running or stopping the CPU remotely by request.

CPU Variables Access

Recommendation: To protect CPU data at run time from illegal read or write access, proceed as follows whenever possible:

- Use unlocated data.
- Configure 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.

Manage Data Integrity Checks

Introduction

You can use an integrity check feature in Control Expert on an authorized PC to help prevent Control Expert files and software from being changed via a virus / malware through the Internet.

Automatic Integrity Check

Control Expert automatically performs an integrity check **only** when you first launch Control Expert. The PAC firmware integrity check is done automatically after a new firmware upload or restart of the PAC

NOTE: If integrity check detects errors, then Control Expert will not start.

Perform a Manual Integrity Check

To perform a manual integrity check in Control Expert, 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 and does not impact your application performance. Control Expert creates a log of the successful and unsuccessful component logins. The log file contains the IP address, the date and hour, 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.

Management of SD Card

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

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

Chapter 3
Cyber Security Services Per Platform

Introduction

This chapter lists the main cyber security services available per platform and indicates where to find detailed information in Control Expert help.

What Is in This Chapter?

This chapter contains the following topics:

Cyber Security Services

Overview

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

- Control Expert software *(see page 54)*
- Modicon M340 CPU *(see page 55)*
- Modicon M580 CPU *(see page 55)*
- Modicon Momentum (Cyber security services are not implemented.)
- Modicon Quantum CPU and communication modules *(see page 56)*
- Modicon X80 modules *(see page 57)*
- Modicon Premium/Atrium CPU and communication modules *(see page 58)*

The cyber security services listed below are described in previous chapter:

- Disable unused services *(see page 20)*
- Access control *(see page 21)*
- Secured communication *(see page 23)*
- Event logging *(see page 37)*
- Authentication *(see page 45)*
- Authorizations *(see page 48)*
- Integrity checks *(see page 51)*

Cyber Security Services in Unity Pro/Control Expert Software

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

Cyber security services availability in Control Expert software:

Software	Cyber security services							
Reference	Disable unused services	Access control	Secured com	Secured com 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

X Available, at least one service is implemented.
– Not available
N.A. Not applicable

Cyber Security Services in Modicon M340 CPU

Minimum firmware version and cyber security services availability in Modicon M340 CPU:

CPU		Cyber security services						
Reference	Min. firmware	Disable unused services	Access control	Secured com	Event logging	Authentication	Authorizations	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								

Cyber Security Services in Modicon M580 CPU:

Minimum firmware version and cyber security services availability in Modicon M580 CPU:

CPU		Cyber security services						
Reference	Min. firmware	Disable unused services	Access control	Secured com	Event logging	Authentication	Authorizations	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
BME H58 6040	2.10	X	X	–	X	X	X	X
X Available, at least one service is implemented. – Not available								

Cyber Security Services in Modicon Quantum CPU and Modules

Minimum firmware version and cyber security services availability in Modicon Quantum CPU:

CPU		Cyber security services						
Reference	Min. firmware	Disable unused services	Access control	Secured com	Event logging	Authentication	Authorizations	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 cyber security services:

Module		Cyber security services						
Reference	Min. firmware	Disable unused services	Access control	Secured com	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								

Cyber Security Services in Modicon X80 Modules

Modicon X80 modules supporting cyber security services:

Module		Cyber security services							
Reference	Min. firmware	Disable unused services	Access control	Secured com	Secured com 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
BMXNOR0200H									
BMENOR2200H									
BMEERT3203(C)									

X Available, at least one service is implemented.
– Not available

Cyber Security Services in Modicon Premium/Atrium CPU and Modules

Minimum firmware version and cyber security services availability in Modicon Premium/Atrium CPU:

CPU		Cyber security services						
Reference	Min. firmware	Disable unused services	Access control	Secured com	Event logging	Authentication	Authorizations	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 cyber security services:

Module		Cyber security services						
Reference	Min. firmware	Disable unused services	Access control	Secured com	Event logging	Authentication	Authorizations	Integrity checks
TSXETC101.2	2.04	X	X	–	–	–	–	–
TSXETY4103	5.70	X	X	–	–	–	–	–
TSXETY5103	5.90	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 CPU in different manuals as described in the following topic.

Modicon M340 CPU with Embedded Ethernet Ports

Description of communication parameters related to cyber security 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 CPU

Description of communication parameters related to cyber security is provided in the topic that describes the *Security Tab (see Modicon M580, Hardware, Reference Manual)*.

Modicon Quantum Security Services

Overview

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

Modicon Quantum CPU with Embedded Ethernet Ports

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

BMENOC0301/11 Module

A description of communication parameters related to cyber security is provided in the *Configuring Security Services* topic *(see Modicon M580, BMENOC0301/0311 Ethernet Communications Module, Installation and Configuration Guide)*.

BMENUA0100 Module

A description of communication parameters related to cyber security 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 CPU and Ethernet modules in different manuals as described in the following topics.

Modicon Premium/Atrium CPU with Embedded Ethernet Ports

Description of communication parameters related to cyber security 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 CPU through ETY Ports

Description of communication parameters related to cyber security 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 cyber security 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 cyber security 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)*.

Glossary

!

%I

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

%IW

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

%M

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

%MW

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

%Q

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

%QW

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

%SW

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

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 PLC 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 CPU application takes to react to a given input. ART is measured from the time a physical signal in the CPU 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 via 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

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.

connection originator

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

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, switches, etc. 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.

device network

An Ethernet-based network within an RIO network that contains both RIO and distributed equipment. Devices connected on this network follow specific rules to allow RIO determinism.

DFB

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

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

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

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

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

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 CPU 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 CPU with DIO scanner service on the local rack. DIO network traffic is delivered after RIO traffic, which takes priority in an RIO network.

distributed equipment

Any Ethernet device (Schneider Electric device, PC, servers, or third-party devices) that supports exchange with a CPU 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.schneider-electric.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.

EF

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

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

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

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

EFB

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

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

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 via 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

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.

Ethernet DIO scanner service

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

Ethernet I/O scanner service

This embedded Ethernet I/O scanner service of M580 CPUs 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.

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.

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.

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 (`AND`, `OR`, etc.), 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 platform.

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.

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.

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`.

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)).

IODDT

(*input/output derived data type*) A structured data type representing a module, or a channel of a CPU. 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 secure for traffic between modules using IPsec, developed by the internet engineering task force (IETF). The IPsec authentication and encryption algorithms require user-defined cryptographic keys that process each communications packet in an IPsec session.

isolated DIO network

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

L

LD

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

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

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 via implicit messaging connections. Local slave is typically used in peer-to-peer exchanges between PACs.

M

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 CPU 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 CPU 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.

N

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.

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).

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, EMS, etc.). 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

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.

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 via 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

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

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.

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 CPU
- 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 CPU. This graphical description of the CPU'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 CPU 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 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, via 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.

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

(*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.

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.

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`.

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.

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.

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`, etc., whose contents 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