

Modicon Controllers Platform

Cyber Security Reference Manual

05/2015

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.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

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.

© 2015 Schneider Electric. All rights reserved.

Table of Contents



	Safety Information	5
	About the Book	7
Chapter 1	Presentation	11
	Schneider Electric Guidelines	11
Chapter 2	How to Secure the Architecture	13
	System View	14
	Hardening the PC	15
	Disable Unused Embedded Communication Services	17
	Restrict Data Flow from Control Network (Access Control)	18
	Set Up Secured Communication	20
	Set Up Cyber Security Audit (Event Logging)	25
	Control Identification and Authentication	33
	Control Authorizations	36
	Manage Data Integrity Checks	39
Chapter 3	Cyber Security Services Per Platform	41
	Cyber Security Services	42
	Modicon M340 Security Services	47
	Modicon M580 Security Services	48
	Modicon Quantum Security Services	49
	Modicon X80 Security Services	51
	Modicon Premium/Atrium Security Services	52
Glossary	53
Index	71

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, 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.

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 Unity Pro 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 Unity Pro 10.0 or later.

The technical characteristics of the devices described in this document also appear online. To access this 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. <ul style="list-style-type: none">● 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 data sheet.
6	To save or print a data sheet as a .pdf file, click Download XXX product datasheet .

The characteristics that are presented in this manual 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 manual and online information, use the online information as your reference.

Related Documents

Title of Documentation	Reference Number
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cyber Security Recommendations	–
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 BME NOC 03•1 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)
Quantum with Unity Pro, TCP/IP Configuration, User Manual	33002467 (English), 33002468 (French), 33002469 (German), 31008078 (Italian), 33002470 (Spanish), 31007110 (Chinese)
Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual	35006192 (English), 35006193 (French), 35006194 (German), 31007214 (Italian), 35006195 (Spanish), 31007102 (Chinese)
Unity Pro Operating Modes	33003101 (English), 33003102 (French), 33003103 (German), 33003696 (Italian), 33003104 (Spanish), 33003697 (Chinese)
Quantum with Unity Pro Hardware Reference Manual	35010529 (English), 35010530 (French), 35010531 (German), 35010532 (Spanish), 35013975 (Italian), 35012184 (Chinese)

Title of Documentation	Reference Number
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 www.schneider-electric.com.

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?

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?

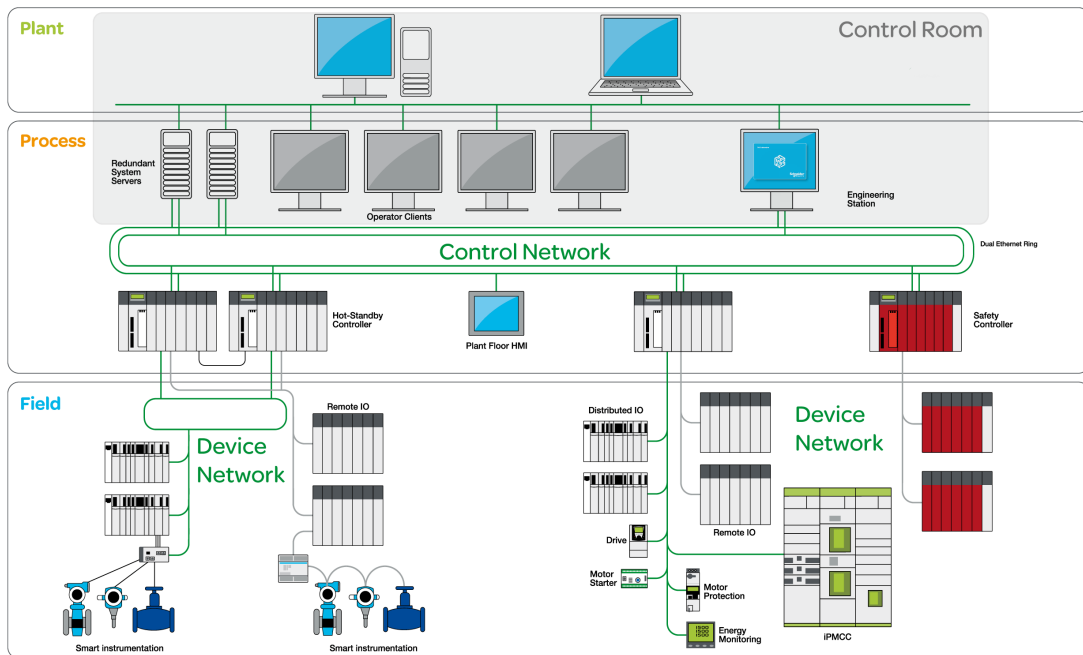
This chapter contains the following topics:

Topic	Page
System View	14
Hardening the PC	15
Disable Unused Embedded Communication Services	17
Restrict Data Flow from Control Network (Access Control)	18
Set Up Secured Communication	20
Set Up Cyber Security Audit (Event Logging)	25
Control Identification and Authentication	33
Control Authorizations	36
Manage Data Integrity Checks	39

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 are more exposed to attacks than equipment connected to the device network. Therefore secured communication needs to be implemented between the control room and the PAC and devices.

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

Hardening the PC

Introduction

The PCs located in the control room are highly exposed to attacks. Those PCs supporting Unity Pro 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 <code>secpol.msc</code> 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 <code>gpupdate</code> 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 Unity Pro

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

- Modicon M340 ([see page 47](#))
- Modicon M580 ([see page 48](#))
- Modicon Quantum ([see page 49](#))
- Modicon X80 modules ([see page 51](#))
- Modicon Premium/Atrium ([see page 52](#))

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 Unity Pro, Communication, Block Library*) function block allows to disable a service enabled after configuration in Unity Pro 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

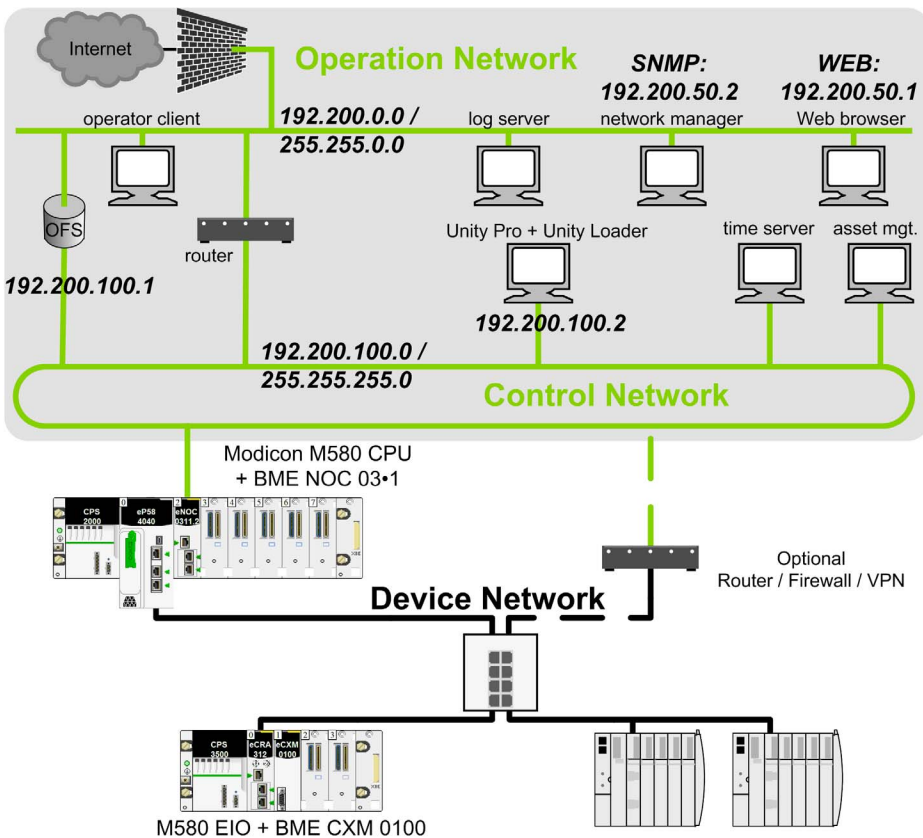
Data flow from control network is an IP-based data flow initiated on the control network.

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).



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 Unity Pro access control table:

Source	IP address	Subnet	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
Network manager	192.200.50.2	No	–	–	–	–	–	–	X
Operation network	192.200.0.0	Yes	255.255.0.0	–	–	X	–	–	–
Unity Loader	192.200.100.2	No	–	X	–	–	–	–	–
Control network	192.200.100.0	Yes	255.255.255.0	–	–	–	X	–	–
X 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 Unity Loader with FTP.

192.200.100.0 (Port502): Control network subnet is set to authorize all equipment connected to the control network (OFS, Unity Pro, 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 Unity Pro **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 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 7 and initiated from the PC operating system.

Description

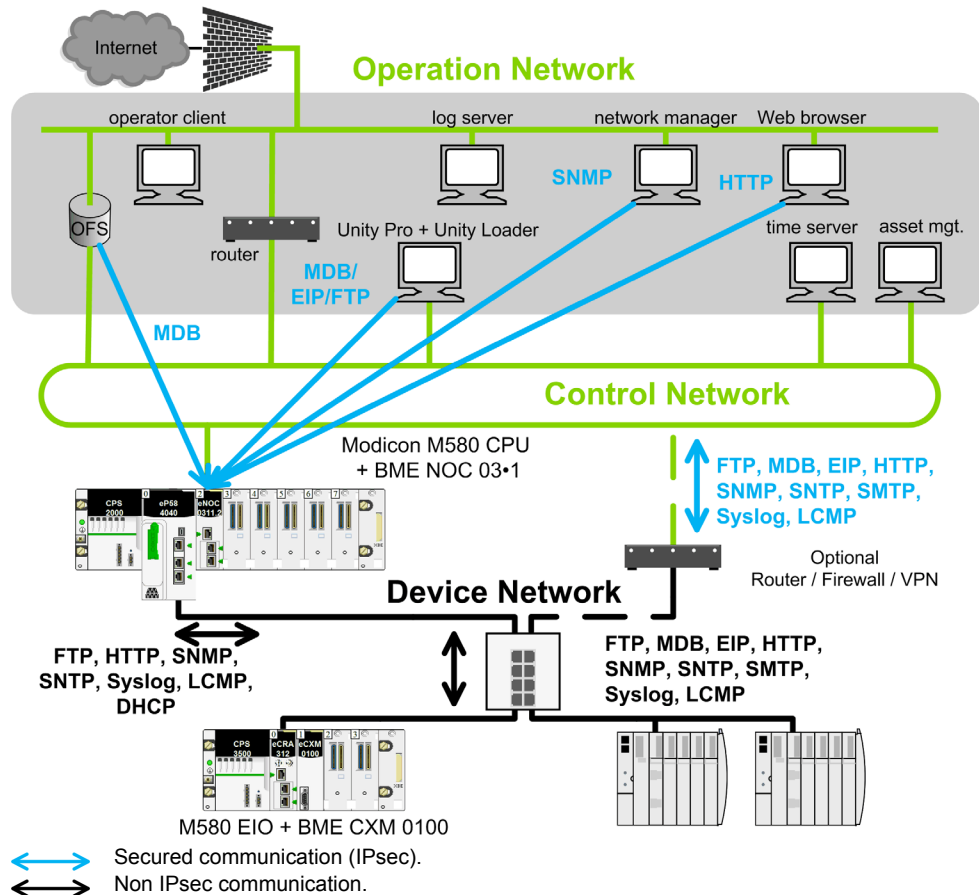
The IPsec function allows to secure:

- The control room Modbus access to the PAC CPU through the BME NOC 03•1 module.
- The control room access to the communication services running inside the BME NOC 03•1 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.

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

The following table shows Ethernet services that can benefit from IPsec secured communication:

Ethernet service or traffic	Secured communication
SNMP agent	IPsec ⁽¹⁾
SNMP traps	IPsec
EIP class 1 scanner	No
EIP class 3 client	No ⁽²⁾
EIP class 3 server	IPsec ⁽¹⁾
Modbus scanner	No ⁽³⁾
Modbus client (port502)	No ⁽²⁾
Modbus server (port502)	IPsec ⁽¹⁾
HTTP	IPsec ⁽¹⁾
ICMP (ping, ...)	IPsec ⁽¹⁾
DHCP, BOOTP client	No ⁽²⁾
DHCP, BOOTP server	No
FTP server, TFTP server	IPsec ⁽¹⁾
Syslog client (UDP)	No ⁽²⁾
<p>(1) Before IKE/IPsec is initiated by the peer (PC), this traffic is in clear. Once IKE/IPsec has been established, this traffic is secured by IPsec.</p> <p>(2) This client service initiated by BME NOC 03•1 is not available when IPsec is enabled.</p> <p>(3) This client service is available without IPsec protection.</p>	

NOTE: IPsec is an OSI layer 3 protection. OSI layer 2 protocols (ARP, RSTP, LLDP, loop check protocol) are not protected by IPsec.

Limitations

IPsec limitations in the architecture: BME NOC 03•1 does not support IP forwarding to device network.

If transparency is required between control and device network, an external router/firewall/vpn (such as a ConneXium firewall) is needed to provide a secured communication between the control and device network (as shown in previous architecture example figure ([see page 21](#))).

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

- Update Modicon M580 CPU firmware from Unity Loader 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.

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 (Unity Pro, Unity Loader, OFS, customer applications such as SGBBackup, ...).

Configure IPsec on each PC supporting these authorized applications.

- In the control room, identify the client authorized applications that need to communicate with each BME NOC 03•1 module configured in the local rack (Unity Pro DTM, Unity Loader, SNMP manager, Web browser, Web designer for FactoryCast BME NOC 03•1 module).

Configure IPsec on each PC supporting these authorized applications.

- Incorporate a BME NOC 03•1 module with IPsec function on the backplane of each PAC connected to the control network.

To configure the IPsec function on a BME NOC 03•1 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: As IPsec relies on this shared secret, it is a key element in the security policy and has to be managed by the security administrator.

The BME NOC 03•1 module configuration is performed with Unity Pro. 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 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 topic on Hardening the PC (see page 15).**

More details on configuration are provided in the topic on Configuring IP Secure Communications (see *Modicon M580, BME NOC 03•1 Ethernet Communications Module, Installation and Configuration Guide*).

Diagnose IPsec Communication in the System Architecture

Information on IPsec diagnostic in the system architecture is provided in the topic on Configuring IP Secure Communications (see *Modicon M580, BME NOC 03•1 Ethernet Communications Module, Installation and Configuration Guide*).

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, Unity Pro or DTM).

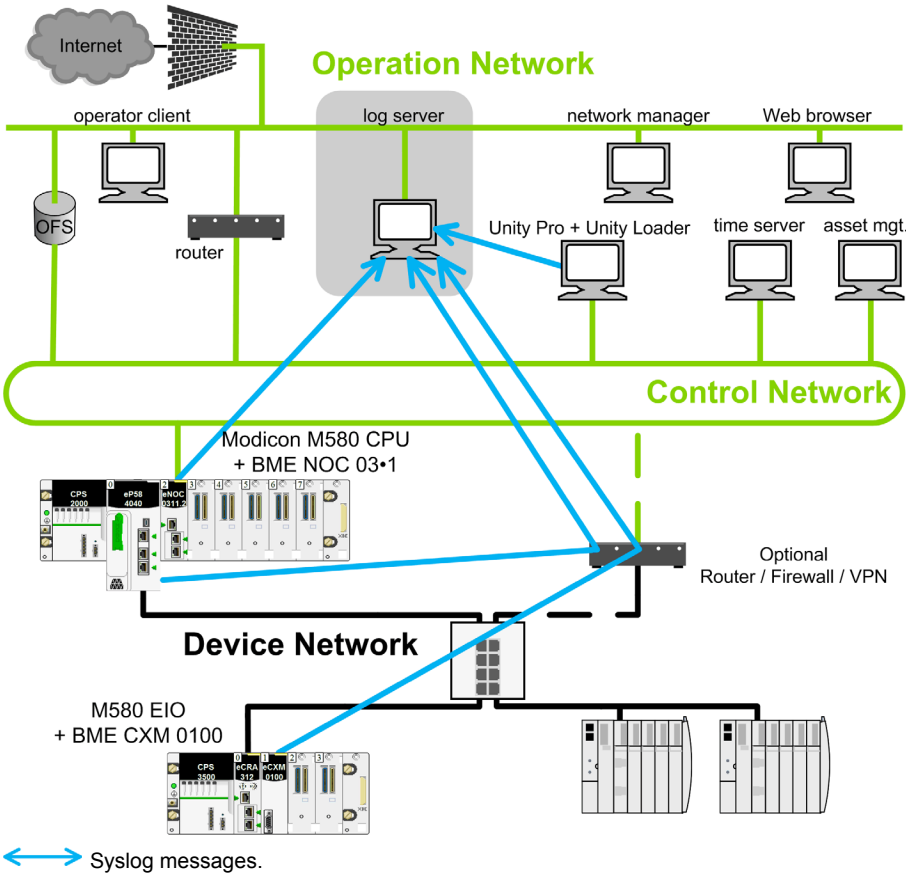
Event Log Service Description

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	<p>Time stamp format is issued from RFC 3339 that recommends the following ISO8601 Internet date and time format: YYY-MM-DDThh:mm:ss.nnnZ</p> <p>NOTE: -, T, :, , , Z are mandatory characters and they are part of the time stamp field. T and Z need to be written in uppercase. Z specifies that the time is UTC.</p> <p>Time field content description:</p> <p>YYY Year MM Month DD Day hh Hour mm Month ss Second nnn Fraction of second in millisecond (0 if not available)</p>
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	<p>This field contains several information:</p> <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> Successful login. For example: data storage via FTP, Unity Pro application password via Modbus, firmware upload via FTP, FDR ... Successful user login to a tool. For example: Unity Pro 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: <ul style="list-style-type: none"> Failed connection due to an erroneous access control list (ACL) check (source IP address or TCP port filtering). Failed login (with ACL check correct). For example: data storage via FTP, Unity Pro application via Modbus, FDR server via FTP... Failed user login to a software tool. For example: Unity Pro. Failed TCP connection (no user). For example: Port502 Modbus TCP/IP explicit messaging for M580 CPU. 	10	Warning	2	Failed login, or failed connection.
Disconnection triggered locally or by a peer: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Parameters run time change outside configuration: CPU application parameters change (for example cycle time or watch dog). 	13	Notice	87	XXXX parameter update (XXXX identifies the parameter). For example: cycle time parameter update.
Major changes in the system: <ul style="list-style-type: none"> Process data run time change outside configuration. 	13	Notice	88	XXXX process update (XXXX identifies the parameter).
Major changes in the system: <ul style="list-style-type: none"> Upload of application and configuration, or upload of configuration only into a device (including CCOTF function). 	13	Informational	9	XXXX upload (XXXX identifies the object uploaded). For example: application upload, configuration upload.
(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
Major changes in the system: <ul style="list-style-type: none"> Download of application and configuration from a device. 	13	Informational	8	XXXX download (XXXX identifies the object downloaded). For example: application download, configuration download.
Major changes in the system: <ul style="list-style-type: none"> Firmware upload. 	13	Informational	10	XXXX upload. For example: firmware upload, web pages upload.
Communication parameters run time change outside configuration: <ul style="list-style-type: none"> 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.
Embedded switch port status change: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> From RSTP: port role change or root change. 	10	Warning	20	topology change detected.
Integrity check error: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Program operating mode change (run, stop, init, ...). 	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.
(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
Major changes in the system: <ul style="list-style-type: none"> 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: Unity Pro specific events not described in previous table are defined in the **Security Editor** user profile (see *Unity Pro, Operating Modes*) 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 Unity Pro for all devices, DTMs, and Unity Pro.

The event logging function, server address, and port number are configured in Unity Pro 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 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
Unity Pro	If a communication error with the syslog server occurs, the detected error is recorded in the event viewer.
BME NOC 03•1 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	
BME CXM 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
 - Unity Pro
- 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 Unity Pro Application, Section, Data Storage, and Firmware Password

In Unity Pro, passwords apply to the following (depending on the CPU):

- **Application**

Unity Pro and CPU application protection by a password prevents unwanted application modification, download, or opening (.STU and .STA files). More details are provided in the topic on Application Protection (*see Unity Pro, 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 topic on Section and Subroutine Protection (*see Unity Pro, 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 topic on Data Storage Protection. (*see Unity Pro, Operating Modes*)

- **Firmware**

Firmware download protection by a password prevents download of a malicious firmware inside the CPU.

Control Authorizations

Unity Pro Security Editor

A security configuration tool is used to define software users and their respective authorizations. Unity Pro access security concerns the terminal on which the software is installed and not the project, which has its own protection system.

More details on the security editor are provided in the section on Access security management (see *Unity Pro, Operating Modes*).

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 Unity Pro, select: **Tools** → **Options...** → **Connection** → **Default connection mode**.

More details on those modes are provided in the topic on Services in Online Mode (see *Unity Pro, Operating Modes*).

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 topic on Section and Subroutine Protection (see *Unity Pro, Operating Modes*).

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

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.

The memory protection is activated as follows:

- Modicon M340 CPU: Input bit. More details in the section on Configuration of Modicon M340 processors (see *Unity Pro, Operating Modes*).
- Modicon M580 CPU: Input bit. More details in the section on Managing Run/Stop Input (see *Modicon M580, Hardware, Reference Manual*).
- Modicon Quantum CPU: Physical key switch on the CPU module, either for low end (see *Quantum with Unity Pro, Hardware, Reference Manual*) or high end (see *Quantum with Unity Pro, Hardware, Reference Manual*) CPU.

- Modicon Premium CPU: Input bit. More details in the section on Configuration of Premium processors (see *Unity Pro, Operating Modes*).
- Modicon MC80 CPU: Input bit. More details in Modicon MC80 CPU manual.

CPU Remote Run/Stop Access

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 section on *Managing Run/Stop Input* for CPU configuration options that help prevent remote commands from accessing the Run/Stop modes (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 section on *Configuration of Modicon M340 Processors* (see *Unity Pro, 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 section on *Configuration of Premium/Atrium Processors* (see *Unity Pro, 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 section on **Configuration of Modicon MC80 Processors** in MC80 user manual.

CPU Variables Access

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

- Use unlocated data.
- Configure Unity Pro 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 Unity Pro on an authorized PC to help prevent Unity Pro files and software from being changed via a virus / malware through the Internet.

Perform an Integrity Check

Unity Pro automatically performs an integrity check **only** when you first launch Unity Pro. The PAC firmware integrity check is done automatically after a new firmware upload or restart of the PAC. To perform a manual integrity check in Unity Pro, follow these steps:

Step	Action
1	Click Help → About Unity Pro XXX .
2	<p>In the Integrity check field, click Perform self-test.</p> <p>Result: The integrity check runs in the background and does not impact your application performance. Unity Pro 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.</p> <p>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.</p>

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 Unity Pro help.

What Is in This Chapter?

This chapter contains the following topics:

Topic	Page
Cyber Security Services	42
Modicon M340 Security Services	47
Modicon M580 Security Services	48
Modicon Quantum Security Services	49
Modicon X80 Security Services	51
Modicon Premium/Atrium Security Services	52

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:

- Unity Pro (see page 42) software.
- Modicon M340 (see page 43) CPU.
- Modicon M580 (see page 43) CPU.
- Modicon Momentum (cyber security services are not implemented).
- Modicon Quantum (see page 44) CPU and communication modules.
- Modicon X80 (see page 45) modules.
- Modicon Premium/Atrium (see page 46) CPU and communication modules.

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

- Disable unused services (see page 17)
- Access control (see page 18)
- Secured communication (see page 20)
- Event logging (see page 25)
- Authentication (see page 33)
- Authorizations (see page 36)
- Integrity checks (see page 39)

Cyber Security Services in Unity Pro Software

Cyber security services availability in Unity Pro software:

Software		Cyber security services						
Reference	Version	Disable unused services	Access control	Secured com	Event logging	Authenti-cation	Authori-zations	Integrity checks
Unity Pro	8.1	–	N.A.	–	–	X	X	X
Unity Pro	10.0	–	N.A.	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. firm ware	Disable unused services	Access control	Secured com	Event logging	Authenti-cation	Authori-zations	Integrity checks
BMX P34 1000	2.60	–	–	–	–	X	X	–
BMX P34 2000	2.60	–	–	–	–	X	X	–
BMX P34 2010	2.60	–	–	–	–	X	X	–
BMX P34 20102	2.60	–	–	–	–	X	X	–
BMX P34 2020	2.60	X	X	–	–	X	X	–
BMX P34 2030	2.60	X	X	–	–	X	X	–
BMX P34 20302	2.60	X	X	–	–	X	X	–
X Available, at least one service is implemented. – Not available								

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. firm ware	Disable unused services	Access control	Secured com	Event logging	Authenti-cation	Authori-zations	Integrity checks
BME P58 1020	1.00	X	X	–	X	X	X	X
BME P58 2020	1.00	X	X	–	X	X	X	X
BME P58 2040	1.00	X	X	–	X	X	X	X
BME P58 3020	1.00	X	X	–	X	X	X	X
BME P58 3040	1.00	X	X	–	X	X	X	X
BME P58 4020	1.00	X	X	–	X	X	X	X
BME P58 4040	1.00	X	X	–	X	X	X	X
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. firm ware	Disable unused services	Access control	Secured com	Event logging	Authen-tication	Authori-zations	Integrity checks
140 CPU 311 10	3.20	–	–	–	–	X	X	–
140 CPU 434 12•	3.20	–	–	–	–	X	X	–
140 CPU 534 14•	3.20	–	–	–	–	X	X	–
140 CPU 651 •0	3.20	X	X	–	–	X	X	–
140 CPU 652 60	3.20	X	X	–	–	X	X	–
140 CPU 658 60	3.20	X	X	–	–	X	X	–
140 CPU 670 60	3.20	X	X	–	–	X	X	–
140 CPU 671 60	3.20	X	X	–	–	X	X	–
140 CPU 672 6•	3.20	X	X	–	–	X	X	–
140 CPU 678 61	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. firm ware	Disable unused services	Access control	Secured com	Event logging	Authen-tication	Authori-zations	Integrity checks
140 NOC 771 0•	1.00	–	X	–	–	X	–	–
140 NOC 780 00	2.00	X	X	–	–	X	–	–
140 NOC 781 00	2.00	X	X	–	–	X	–	–
140 NOE 771 ••	X	X	–	–	–	X	–	–
140 NWM 100 00	–	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. firm ware	Disable unused services	Access control	Secured com	Event logging	Authen-tication	Authori-zations	Integrity checks
BME CXM 0100	1.01	X	X	–	X	–	–	X
BME NOC 0301	1.01	X	X	X	X	X	–	X
BME NOC 0311	1.01	X	X	X	X	X	–	X
BMX NOC 0401.2	2.05	X	X	–	–	–	–	–
BMX NOE 0100.2	2.90	X	X	–	–	–	–	–
BMX NOE 0110.2	6.00	X	X	–	–	–	–	–
BMX PRA 0100	2.60	X	X	–	–	X	–	–
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. firm ware	Disable unused services	Access control	Secured com	Event logging	Authen-tication	Authori-zations	Integrity checks
TSX H57 •4M	3.10	–	–	–	–	X	X	–
TSX P57 0244M	3.10	–	–	–	–	X	X	–
TSX P57 •04M	3.10	–	–	–	–	X	X	–
TSX P57 •54M	3.10	–	–	–	–	X	X	–
TSX P57 1634M TSX P57 2634M TSX P57 3634M (through ETY port)	3.10	X	X	–	–	X	X	–
TSX P57 4634M TSX P57 5634M TSX P57 6634M (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. firm ware	Disable unused services	Access control	Secured com	Event logging	Authen-tication	Authori-zations	Integrity checks
TSX ETC 101.2	2.04	X	X	–	–	–	–	–
TSX ETY 4103	5.70	X	X	–	–	–	–	–
TSX ETY 5103	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 section on *Security (see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Access control: Refer to section on *Messaging Configuration Parameters (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 section on *Security (Enable / Disable HTTP, FTP, and TFTP)* (see *Modicon Quantum with Unity, Ethernet Network Modules, User Manual*).

Access control: Refer to section on *Modicon Quantum with Unity Ethernet Controller Messaging Configuration* (see *Modicon Quantum with Unity, 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 section on *Security (Enable / Disable HTTP, FTP, and TFTP)* (see *Modicon Quantum with Unity, Ethernet Network Modules, User Manual*).

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

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

Access control: Refer to section on *Configuring Access Control* (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 section on *Security (Enable / Disable HTTP, FTP, and TFTP)* (see *Modicon Quantum with Unity, Ethernet Network Modules, User Manual*), the section on *Security* (see *Modicon Quantum with Unity, Ethernet Network Modules, User Manual*), and the section on *Establishing HTTP and Write Passwords* (see *Modicon Quantum with Unity, 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 section on *Security (Enable / Disable HTTP, FTP, and TFTP)*
(see *Modicon Quantum with Unity, 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.

BME CXM 0100 Module

Description of communication parameters related to cyber security is provided in the chapter on Optional Configuration (see *Modicon M580, BME CXM CANopen Modules, User Manual*).

BME NOC 03•1 Module

Description of communication parameters related to cyber security is provided in the section on Configuring Security Services (see *Modicon M580, BME NOC 03•1 Ethernet Communications Module, Installation and Configuration Guide*).

BMX NOC 0401.2 Module

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

Ethernet communication: Refer to section on *Security* (see *Modicon M340 for Ethernet, Communications Modules and Processors, User Manual*).

Access control: Refer to section on *Configuring Access Control* (see *Modicon M340, BMX NOC 0401 Ethernet Communication Module, User Manual*).

BMX NOE 0100.2 and BMX NOE 0110.2 Module

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

Ethernet communication: Refer to section on *Security* (see *Modicon M340 for Ethernet, Communications Modules and Processors, User Manual*).

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

BMX PRA 0100 Module

The BMX PRA 0100 is configured as a Modicon M340 CPU. Description of communication parameters related to cyber security is provided in the listed topics:

Ethernet communication: Refer to section on *Security* (see *Modicon M340 for Ethernet, Communications Modules and Processors, User Manual*).

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

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 section on *Security Service Configuration Parameters* (see *Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual*).

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

Access control: Refer to section on *Configuration of TCP/IP Messaging* (see *Premium and Atrium Using Unity Pro, 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 section on *Security* (see *Premium, TSX ETC 101 Ethernet Communication Module, User Manual*).

Access control: Refer to section on *Configuring Access Control* (see *Premium, 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 section on *Security Service Configuration Parameters* (see *Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual*).

Access control: Refer to section on *Configuration of TCP/IP Messaging* (see *Premium and Atrium Using Unity Pro, Ethernet Network Modules, User Manual*).



!

%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.

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 Unity Pro, 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.

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 the subnet.

C**CCOTF**

(*change configuration on the fly*) A feature of Unity Pro 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 the 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 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*) Legacy term for distributed equipment. DRSSs 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 DRSSs, 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 communication server 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 communication 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 in order 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 3 types of devices: a local rack, an X80 EIO drop, and a ConneXium extended dual-ring switch (DRS). Distributed equipment may also participate in an EIO network via connection to DRSs or the service port of X80 EIO adapter 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 **Error 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 communication server service

an embedded communication server service of M580 CPUs (BME P58 1020, BME P58 2020, BME P58 3020, BME P58 4020) that manages distributed equipment only on an M580 device network

Ethernet I/O communication server service

an embedded communication server service of M580 CPUs (BME P58 2040, BME P58 3040, BME P58 4040) that 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**

An event-triggered (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*) A 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 in order 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.

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.

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.

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*) This language is 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*) A 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 communication server service)
- RIO drop (including an Ethernet X80 EIO adapter module)
- DRS switch with a predefined configuraton

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 communication server 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.

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.

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 the 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.

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 Unity Pro and the device DTM.

RIO drop

One of the three types of RIO modules in an Ethernet RIO network (*see **RIO network** for the other two types*). A 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.

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

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 the following major functions (depending on the module type):

- port mirroring: for diagnostic use
- access: for connecting HMI/Unity Pro/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*) 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.

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 communication server 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*) The process of determining the order of events in an industrial system and correlating those events to a real-time clock.

ST

(*structured text*) The structured literal language 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) 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.

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.



A

- access control
 - cyber security, 42
 - security, 18
- accounts
 - cyber security, 33
- ACL
 - security, 18
- architecture, 14
- audit trail
 - security, 25
- authentication
 - cyber security, 42
- authorization
 - security, 36
- authorizations
 - cyber security, 42

C

- communication services
 - disable, 17

- cyber security, 11
 - access control, 42
 - accounts, 33
 - authentication, 42
 - authorizations, 42
 - disable unused services, 42
 - event logging, 42
 - firmware, 42
 - guidelines, 11
 - HTTP, 34
 - integrity checks, 42
 - LANMAN / NTLM, 16
 - literature, 11
 - local area connection, 15
 - M340, 47
 - M580, 48
 - network interface cards, 15
 - passwords, 33
 - Premium/Atrium, 52
 - Quantum, 49
 - remote desktop, 16
 - secured communication, 42
 - services, 42
 - SNMP, 34
 - X80, 51

D

- disable
 - communication services, 17
- disable unused services
 - cyber security, 42

E

- event logging
 - cyber security, 42

F

firmware
 cyber security, 42
 security, 42

H

hardening
 PC, 15
HTTP
 cyber security, 34

I

integrity check
 security, 39
integrity checks
 cyber security, 42

L

LAN
 cyber security, 15
LANMAN / NTLM
 cyber security, 16
literature
 cyber security, 11
logging
 security, 25

M

M340
 cyber security, 47
M580
 cyber security, 48
memory
 protect, 36
memory protection
 security, 39

N

network interface cards
 cyber security, 15

P

password
 Unity Pro, 35
passwords
 cyber security, 33
PC
 hardening, 15
Premium/Atrium
 cyber security, 52
protect
 memory, 36
protection
 section, 36

Q

Quantum
 cyber security, 49

R

remote desktop
 cyber security, 16
run/stop
 security, 37

S

section
 protection, 36
secured communication
 cyber security, 42

security

- access control, 18
- ACL, 18
- audit trail, 25
- authorization, 36
- firmware, 42
- integrity check, 39
- logging, 25
- memory protection, 39
- run/stop, 37
- services, 42
- syslog, 25

services

- cyber security, 42
- security, 42

SNMP

- cyber security, 34

syslog

- security, 25

U**Unity Pro**

- password, 35

X**X80**

- cyber security, 51

