Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment

User Guide

Original instructions

08/2021

EIO0000004242.00

www.se.com

Legal Information

Table of Contents

Safety Information

Important Information

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please Note

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

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

About the Book

Document Scope

The Cybersecurity Guidelines define the 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 cybersecurity topics.

Validity Note

This document has been created for the release of EcoStruxure™ Machine Expert V2.0.

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

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

Related Documents

Document title	Reference
Schneider Electric Cybersecurity Best Practices	CS-Best-Practices-2019-340
How Can I Reduce Vulnerability to Cyber Attacks	STN+v2
Cybersecurity Assessment – The Most Critical Step to Secure an Industrial Control System	998-20298472
Effective Implementation of Cybersecurity Countermeasures in Industrial Control Systems	998-20304108_GMA-US
EcoStruxure Machine Expert, Programming Guide	EIO0000002854 (ENG); EIO0000002855 (FRE); EIO0000002856 (GER); EIO0000002857 (ITA); EIO0000002858 (SPA); EIO0000002859 (CHS)
Modicon M251 Logic Controller, Programming Guide	EIO0000001462 (ENG); EIO0000001463 (FRE); EIO0000001464 (GER); EIO0000001465 (SPA); EIO0000001466 (ITA); EIO0000001467 (CHS)
Modicon M241 Logic Controller, Programming Guide	EIO0000001432 (ENG); EIO0000001433 (FRE); EIO0000001434 (GER); EIO0000001435 (SPA);

Document title	Reference
	EIO0000001436 (ITA); EIO0000001437 (CHS)
Modicon M62 Logic/Motion Controller, Programming Guide	EIO0000003651 (ENG); EIO0000003652 (FRE); EIO0000003653 (GER); EIO0000003654 (SPA); EIO0000003655 (ITA); EIO0000003656 (CHS)
PacDrive Logic Motion Controller - LMC Eco, Hardware Guide	EIO0000001501 (ENG); EIO0000001502 (GER)
PacDrive Logic Motion Controller - LMC Pro/ Pro2, Hardware Guide	EIO0000001503 (ENG); EIO0000001504 (GER)
How to Configure the Firewall for PacDrive LMC Controllers, User Guide	EIO0000004198 (ENG); EIO0000004199 (GER)

Product Related Information

⚠WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop, power outage and restart.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Observe all accident prevention regulations and local safety guidelines.[1]
- Each implementation of this equipment must be individually and thoroughly tested for proper operation before being placed into service.

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

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

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

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

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

For reasons of Internet security, TCP/IP forwarding is disabled by default. Therefore, you must manually enable TCP/IP forwarding. However, doing so may expose your network to possible cyberattacks if you do not take additional measures to protect your enterprise. In addition, you may be subject to laws and regulations concerning cybersecurity.

⚠WARNING

UNAUTHENTICATED ACCESS AND SUBSEQUENT NETWORK INTRUSION

- Observe and respect any and all pertinent national, regional and local cybersecurity and/or personal data laws and regulations when enabling TCP/IP forwarding on an industrial network.
- Isolate your industrial network from other networks inside your company.
- Protect any network against unintended access by using firewalls, VPN, or other, proven security measures.

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

Terminology Derived from Standards

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

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

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2015	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2013	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2015	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2016	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

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

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

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

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

General Information

General Information for Cybersecurity

Overview

This document is intended to describe cybersecurity risks and abatement strategies in control and automation, and to provide a quick introduction to a more robust and secure system. It is not intended to replace any specific product documentation, nor any of your own design documentation. On the contrary, it offers supplemental information to any product documentation on the installation, configuration and implementation of your system.

Of course, your specific application requirements may be different and will require additional and/or different components. In this case, you will have to adapt the information provided in the present document to your particular needs. To do so, you will need to consult the specific product documentation of the components that you are substituting in your application. However, you must be aware of the consequences of component substitutions as they may impair the compatibility and interoperability of software and hardware.

⚠CAUTION

EQUIPMENT INCOMPATIBILITY OR INOPERABLE EQUIPMENT

Read and thoroughly understand all hardware and software documentation before attempting any component substitutions.

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

Pay particular attention in conforming to any safety information, different electrical requirements and normative standards that would apply to your adaptation.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

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

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

Cybersecurity in the Industrial Market

Overview

The present document helps you to understand what constitutes cybersecurity in the industrial market and secure Modicon controllers, PacDrive controllers and associated equipment by applying the proposed hardening configuration. It allows you to become more familiar with the methods of malicious network penetration, the risks caused by system vulnerabilities, and Schneider Electric's propositions to mitigate those risks. It provides a common, readily understandable reference point for end users, system integrators, OEMs, salespeople, business support, and other parties.

What is Cybersecurity?

- Cybersecurity is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions.
- The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.
- Cybersecurity is an ongoing process that encompasses procedures, policies, software, and hardware.

Why is Security Important in Industrial Control Today?

The content of this section is derived from content available on the US-CERT Industrial Control Systems Emergency Response Team web page (see Related Documents section of the present document). The intent is to summarize and otherwise clarify that information by presenting it here. However, you should review all the material available there to gain a more thorough understanding of control system vulnerabilities and potential threats.

Cybersecurity is no longer a secondary requirement in the world of industrial controls. It is as important as safety or high availability.

Industrial control systems based on computer technology and industrial-grade networks have been in use for decades. Earlier control system architectures were developed with proprietary technology and were isolated from the outside world. In many cases, physical perimeter security was deemed adequate and cybersecurity was not a primary concern.

Today many control systems use open or otherwise well known technologies, such as standard operating systems and Ethernet TCP/IP, to reduce costs and improve performance. Many systems also employ direct communications between control and business systems to improve operational efficiency and manage production assets more cost-effectively.

This technical evolution exposes control systems to vulnerabilities previously thought to affect only office and business computers. Control systems are now vulnerable to cyber attacks from both inside and outside of the industrial control system network.

Security challenges for the control environment include:

- Diverse physical and logical boundaries.
- Multiple sites and large geographic spans.
- Adverse effects of security implementation on process availability.
- Increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open.
- Increased exposure to malicious software from USB devices, vendor and service technician laptops, and from the enterprise network.
- Direct impact of control systems on physical and mechanical systems.

No longer are fences and security guards adequate to protect industrial assets. Companies must be diligent in the steps they take to help secure their systems. A successful cyber attack can, among other things, result in lost production, damaged company image, environmental disaster, or even loss of life. The controls industry and its customers must apply cybersecurity lessons learned from the IT world.

Cyber Threat Profile

Overview

Cyber threats are deliberate actions or accidents that can disrupt the normal operations of computer systems and networks. These actions can be initiated

from within the physical facility or from an external location. Experts estimate that nearly half of all cyber incidences occur from within the enterprise. With the proliferation of e-mail phishing schemes and ransomware attacks. This number is likely to rise.

A cybersecurity plan needs to account for various potential sources of cyber attacks and accidents, including:

- Internal:
  - Misconfiguration
  - Forbidden tools (remote tools)
  - Inappropriate employee or contractor behavior
  - Disgruntled employee or contractor
  - Opening an e-mail or attachment from an unknown or spoofed sender
  - Inadvertently launching a virus by downloading a file or font
  - External devices connected on the network
- External opportunistic (non-directed):
  - Script kiddies (slang term for hackers who use malicious scripts written by others without necessarily possessing a comprehensive understanding how the script works or its potential impact on a system)
  - Recreational hackers
  - Virus writers
- External deliberate (directed):
  - Criminal groups
  - Activists
  - Terrorists
  - Agencies of foreign states
- Accidents

A deliberate cyber attack on a control system may be launched to achieve a variety of malicious objectives, including:

- Disrupt the production process by blocking or delaying the flow of information
- Damage, disable, or shut down equipment to negatively impact production or the environment
- Modify or disable safety systems to cause intentional harm
- Theft of intellectual property or confidential business and/or production data

Accidental Events

Overview

Experts attribute more than 75% of network-related system outages to accidental events. Causes of these accidents can include poor network design, programming errors, improperly functioning network devices, non-compliance with procedures, or human error such as accidentally connecting network cables to incorrect ports. Many of the security features and processes discussed in this document can also mitigate accidental events.

In many cases, contractors contribute directly to system design, commissioning, or maintenance. Operational procedures should be refined so that contractors cannot introduce malware or vulnerabilities into the control network. For instance, automatically scan contractor equipment for malware infection before allowing access to any equipment. USB keys are another common source of malware infection and should be carefully screened before permitting their use.

Individuals who inadvertently connect a network cable into an incorrect port on a multi-port switch can create outages or broadcast storms that could disable the network or severely affect its performance.

In general, the cause might be accidental; but, the features, practices, and procedures used for cybersecurity work equally well against accidental system outages.

Incident recovery methods should be developed and tested so that recovery from an outage or other events can be quickly and reliably managed. High availability and redundant architectures play a role in this area when even short system outages cannot be tolerated.

Schneider Electric Cybersecurity Services

Overview

Schneider Electric offers cybersecurity vulnerability services including:

- Risk Assessment
- Security Plan (guidelines, consultancy services)
- Training
- Ethernet/Cybersecurity Network Audit

For more information on these services refer to http://software.schneider-electric.com/services/security-and-compliance-services/cyber-security-services/.

Schneider Electric and our Collaborative Automation Partner Program (CAPP) partners provide specific cybersecurity offerings that include the following:

- ConneXium firewall offerings (Industrial Firewall and Tofino Firewall)
- Network Access Control system (Cisco/Extreme Networks/Hirschmann)
- Security Information and Event Management (SIEM) partnership with McAfee®
- 802.1X certificate services
- VPN capabilities

Schneider Electric Defense in Depth

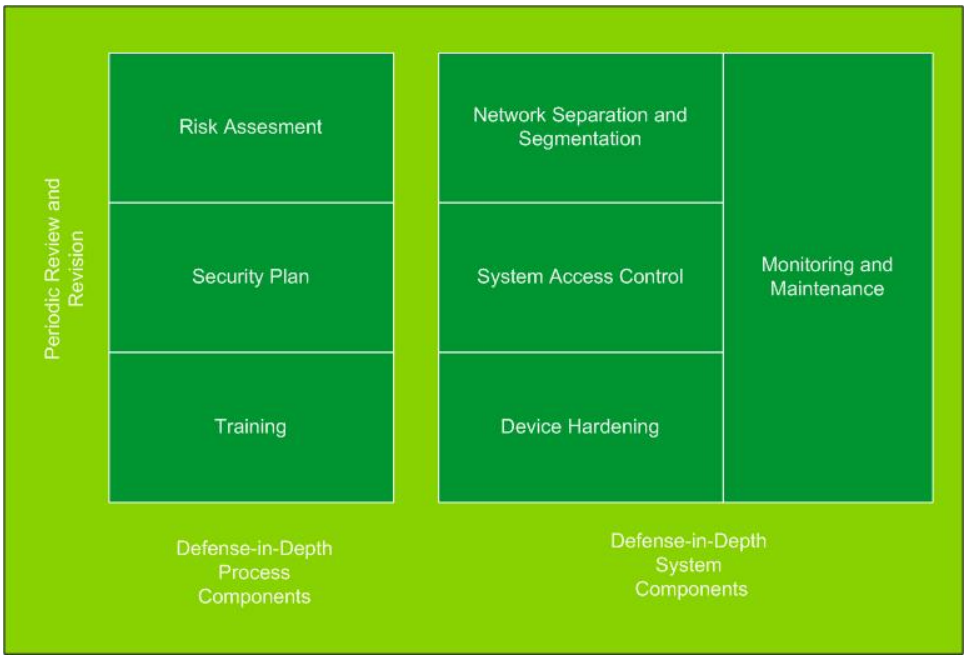
Schneider Electric Defense in Depth

Introduction

Schneider Electric supports a defense-in-depth approach to cybersecurity. No single approach is adequate. The defense-in-depth approach layers the network with security features, appliances, and processes.

Network Defense-in-Depth Process Components

As shown in the graphic below, this defense-in-depth approach integrates a set of related process and systems components to provide higher levels of security in an EcoStruxure network.



The basic components of the Schneider Electric defense-in-depth approach are:

1. Risk assessment
   - A systematic security analysis of the EcoStruxure environment and related systems
   - A security plan built on the results of the risk assessment
   - A multi-phase training campaign
2. Network separation and segmentation
   - Physical separation of the control network from other networks using a demilitarized zone (DMZ)
   - Division of the control network itself into segments and security zones
3. System Access Control
   - Controlling logical and physical access to the system with firewalls, authentication, authorization, VPN, and antivirus software
   - This effort also includes traditional physical security measures such as video surveillance, fences, locked doors and gates, and locked equipment cabinets.
4. Device hardening
   - The process of configuring a device against communication-based threats

- Device hardening measures include disabling unused network ports, password management, access control, and the disabling of all unnecessary protocols and services.

5. Network monitoring and maintenance

   An effective defense-in-depth campaign requires continual monitoring and system maintenance to meet the challenge of new threats as they develop.

Supported Defense-in-Depth Devices

Schneider Electric supports defense-in-depth with a wide selection of devices:

- ConneXium industrial firewalls to help provide a high level of control network perimeter security and support components such as VPN and DMZ.
- ConneXium Tofino firewall to help secure communication zones within the control network using basic firewall rules, stateful packet inspection, and deep packet inspection.
- ConneXium Tofino infrastructure devices to limit internal access to areas of responsibility and act as a second line of defense in the event of a firewall breech.
- Logic controllers, Motion controllers, Drives, SCADA, HMI devices, and Ethernet communication equipment hardened with password protection, access control, and the ability to disable unneeded services.

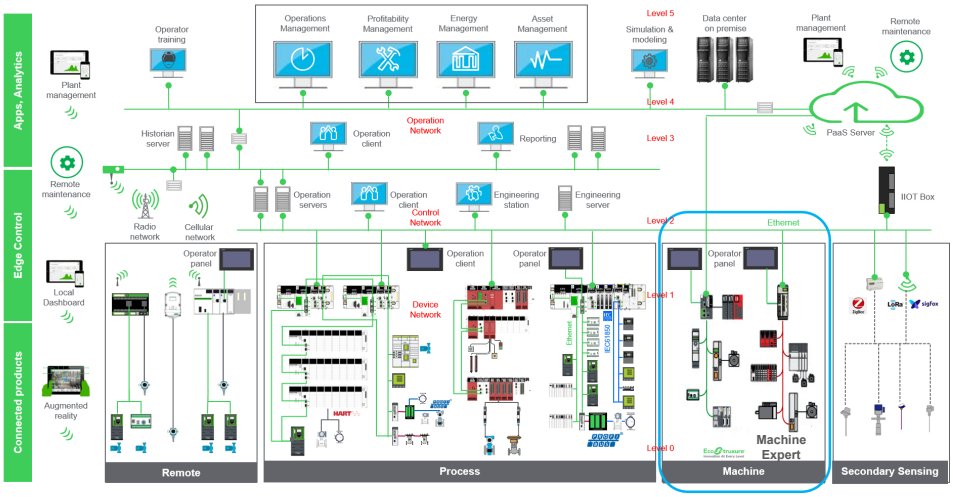
For more information of the Schneider Electric defense-in-depth approach, refer to How Can I Reduce Vulnerability to Cyber Attacks.

Machine Solutions Architecture

Machine Solutions Architecture

Overview

The Machine Solutions architecture recommendations in this section are limited to single-site communications with no plant-to-plant or external to plant communications. This hardening guideline describes general security settings for devices in the Machine Solutions security architecture encircled below.



Device Hardening

Password Management

Overview

Password management is one of the fundamental tools of device hardening. Passwords are often neglected in industrial control systems. Policies and procedures on password management are often inadequate or missing entirely.

Password Management Guidelines

- Enable password authentication on e-mail and Web servers, controllers, Ethernet interface modules, and embedded Web servers
- Change the default logins/passwords or set new login/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
- Grant passwords only to people who need access. Prohibit password sharing.
- Passwords should be hidden, and not displayed during password entry:
  - Require passwords that are difficult to guess or easily obtained
  - Enforce passwords that contain at least 8 characters, combining upper and lowercase letters, digits, and non-alpha/numeric characters when permitted
  - Remove employee access account when employment has terminated or the access is not needed anymore
  - Require use of different passwords for different accounts, systems, and applications
  - Maintain a secure master list of administrator account passwords so that they can quickly be accessed in the event of an emergency
  - Implement password management in a way that does not interfere with the ability of an operator to respond to an event such as an emergency shutdown
  - Passwords should not be transmitted via e-mail or in any other way over the insecure Internet

EcoStruxure Machine Expert

Overview

EcoStruxure Machine Expert is used to program Modicon M258 Logic Controller/ Modicon LMC058 Motion Controller (requires Machine Expert version 1.2.x), Modicon M241 Logic Controller, Modicon M251 Logic Controller, Modicon M262 Logic/Motion Controller, PacDrive LMC Eco and PacDrive LMC Pro/Pro2 controllers. Using this software, you can configure cybersecurity settings of the controllers:

- Integrity check, page 19
- Network configuration, page 19
- User rights, page 20

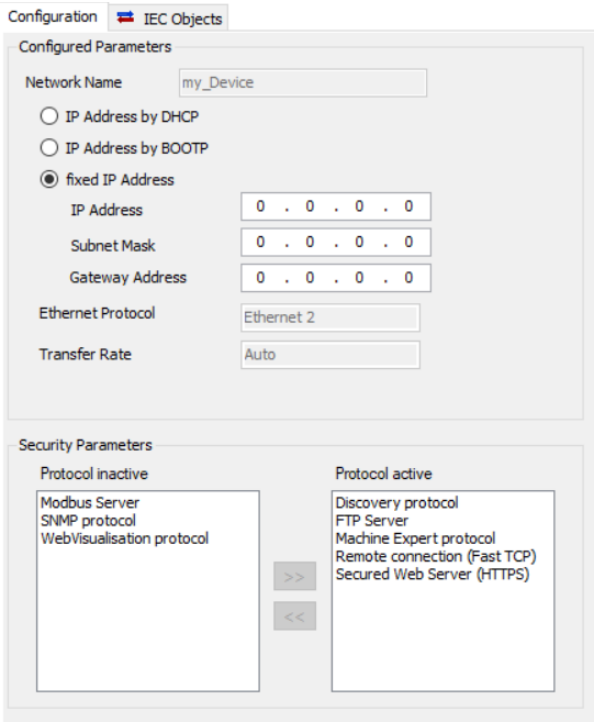
- Secure settings, page 21 (secure communications, certificates)

Integrity Check

During startup of EcoStruxure Machine Expert, an integrity check is performed on the loaded libraries. You are notified when an integrity issue has been detected.

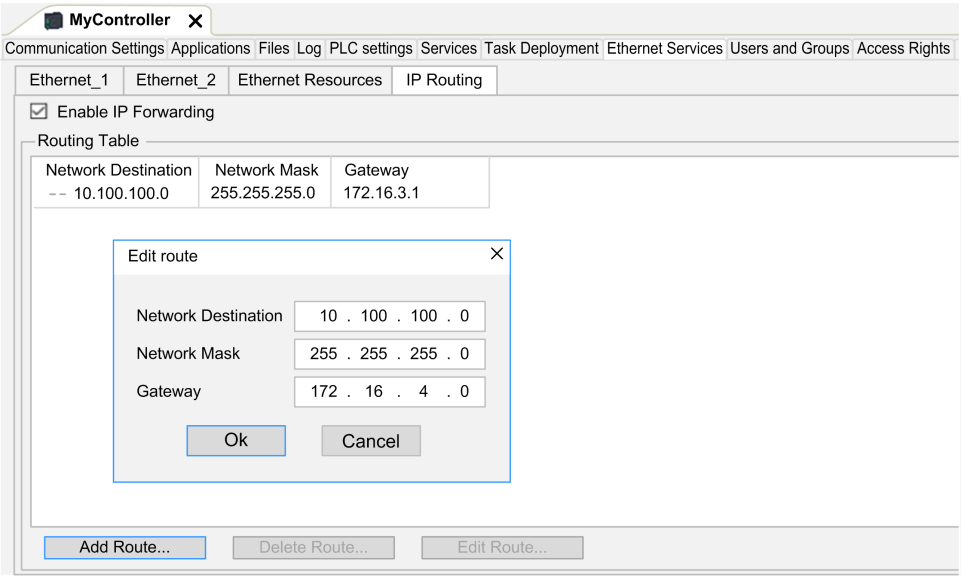
Network Configuration

EcoStruxure Machine Expert allows you to configure the network and active protocols. The **IP Address** can be set either manually or automatically via DHCP configuration, for example.



Additionally, also enable or disable routing packets on Ethernet interface to ensure network separation. **IP Forwarding** can be disabled on the **IP Routing** tab on the **Ethernet Services**.

NOTE: For PacDrive controllers this setting is done through the firewall configuration. For more information refer to *How to Configure the Firewall for PacDrive LMC Controllers* in the EcoStruxure Machine Expert online help.



NOTE: On Modicon M241 Logic Controller, the **IP Forwarding** is configured in the Ethernet security parameters of the TM4ES4. On M251MESE, it is configured in the Ethernet security parameters for ETH1.

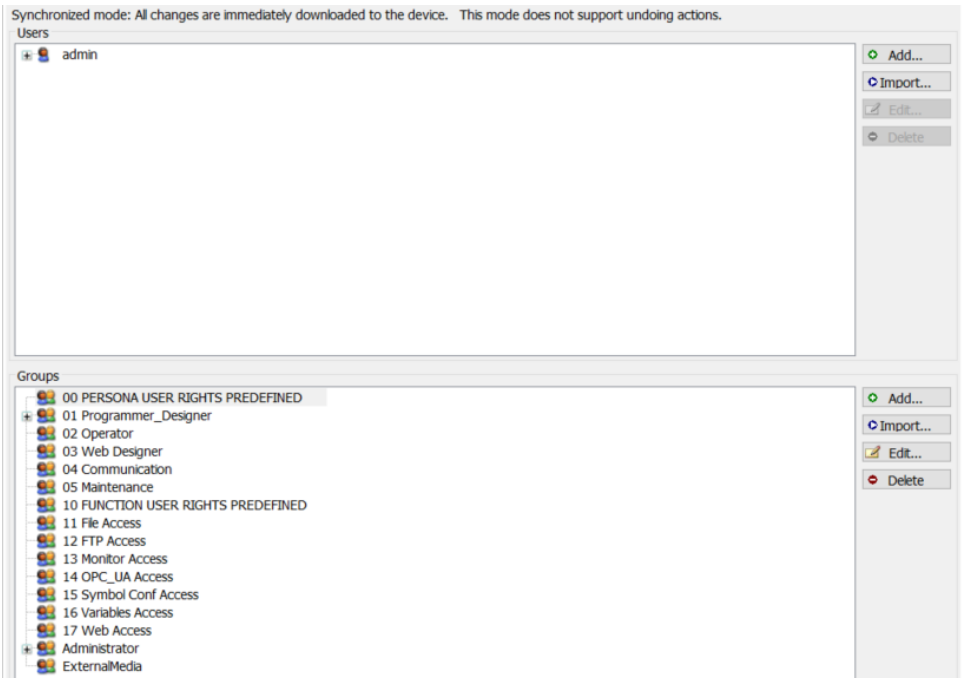
User Rights Management

EcoStruxure Machine Expert user rights management is by default activated for the following Schneider Electric controllers:

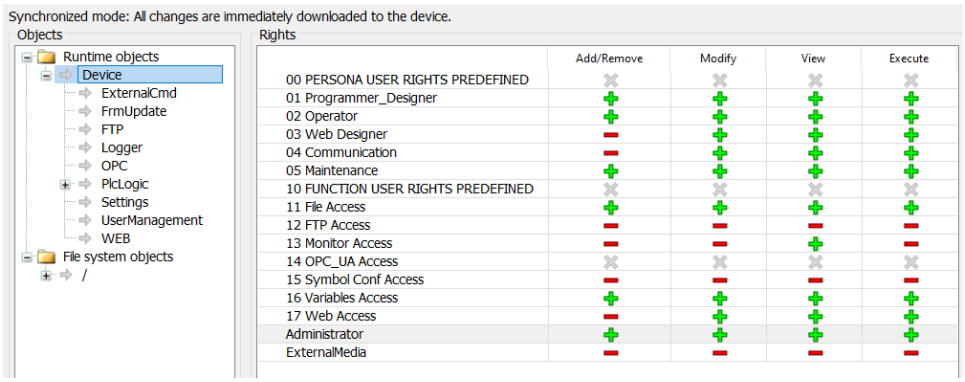
- Modicon LMC058 Motion Controller
- Modicon M241 Logic Controller
- Modicon M251 Logic Controller
- Modicon M258 Logic Controller
- Modicon M262 Logic/Motion Controller
- PacDrive LMC Eco
- PacDrive LMC Pro/Pro2

For the above-mentioned controllers, you are requested to configure an administrator account with user name and password. Moreover, a role-based access control mechanism is provided by EcoStruxure Machine Expert which lets you configure user accounts and groups with different privileges and customized access rights to services provided by the controllers.

The following graphic shows the **Users** and **Groups**:



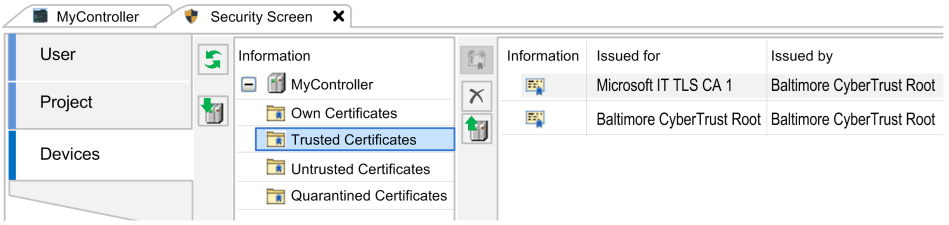
The following graphic shows the access rights:



For information on device user management, refer to Users and Groups Management in the EcoStruxure Machine Expert Programming Guide.

Enhanced Security Settings

EcoStruxure Machine Expert also provides a dedicated **Security Screen** to configure more advanced cybersecurity parameters for encrypted communication related to the user, to the project and to the controller.



Tab	Description
User	Allows you to configure security-related parameters for the logged-in user: • Certificates required for secured communication • Digital signature of the user
Project	Allows to secure the project by activating project encryption.
Devices	Allows you to configure secured TCP communication to the connected controller by managing certificates.

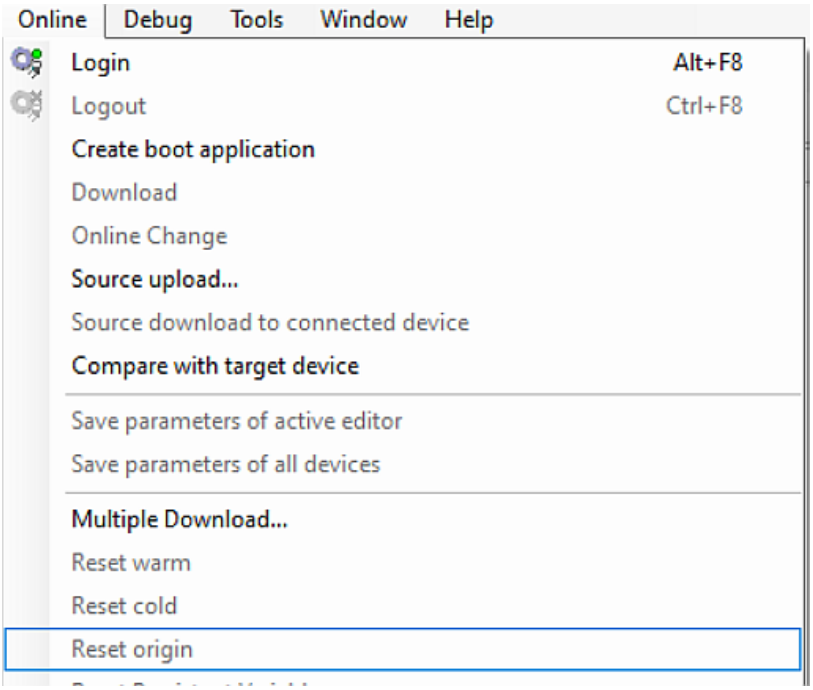
By default, encrypted communication is automatically enabled whenever the controllers provide encryption capabilities. Refer to the EcoStruxure Machine Expert Menu Commands Online Help for details on the **Security Screen**.

Software and Firmware Updates

EcoStruxure Machine Expert notifies you when a new software component or firmware is available. Install software and firmware updates proposed by EcoStruxure Machine Expert. In addition, implement processes to ensure that software and firmware updates for Schneider Electric products are installed once they are available.

Reset Controllers

To remove sensitive data from your controller, execute the command **Reset origin**.



EcoStruxure Machine Expert - Basic

Overview

EcoStruxure Machine Expert - Basic is used to program Modicon controllers M100/M200/M221.

Integrity Checks

Integrity checks of the libraries are performed during the startup of the software. When an integrity issue has been detected you are notified.

Network Configuration

You can configure the TCP/IP connection to the logic controller by configuring the Ethernet network.

- The Ethernet establishes a local area network (LAN) between the logic controller and other devices.
- The Ethernet configuration provides you the ability to configure the IP address of the network device.

You can obtain the IP address automatically via DHCP protocol or configure it manually by specifying:

- IP address
- Subnet mask
- Gateway address

NOTE: Schneider Electric adheres to industry best practices in the development and implementation of control systems. This includes a defense-in-depth approach to secure an industrial control system. This approach places the controllers behind one or more firewalls to restrict access to authorized personnel and protocols only.

⚠WARNING

UNAUTHENTICATED ACCESS AND SUBSEQUENT UNAUTHORIZED MACHINE OPERATION

- Evaluate whether your environment or your machines are connected to your critical infrastructure and, if so, take appropriate steps in terms of prevention, based on Defense-in-Depth, before connecting the automation system to any network.
- Limit the number of devices connected to a network to the minimum necessary.
- Isolate your industrial network from other networks inside your company.
- Protect any network against unintended access by using firewalls, VPN, or other, proven security measures.
- Monitor activities within your systems.
- Prevent subject devices from direct access or direct link by unauthorized parties or unauthenticated actions.
- Prepare a recovery plan including backup of your system and process information.

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

For more information on organizational measures and rules covering access to infrastructures, refer to ISO/IEC 27000 series, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, IEC 62351, ISA/IEC 62443, NIST Cybersecurity Framework, Information Security Forum - Standard of Good Practice for Information Security.

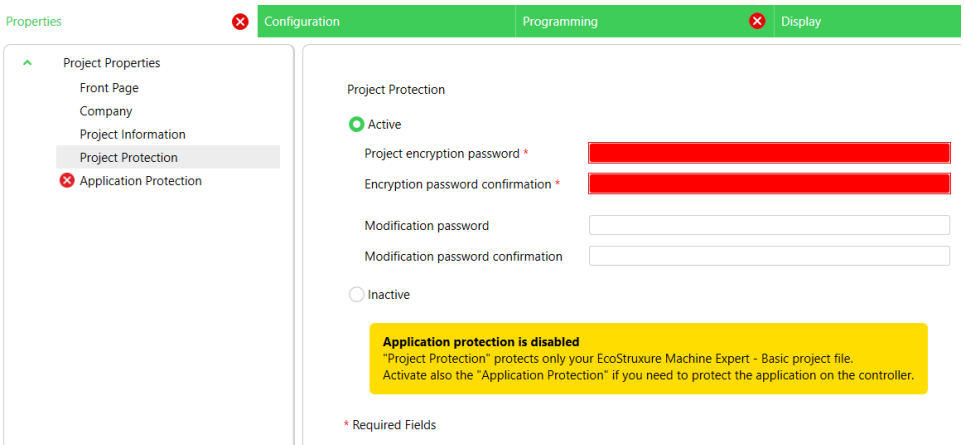
For more information on network configuration, refer to the EcoStruxure Machine Expert - Basic, Operating Guide.

Enhanced Security Settings

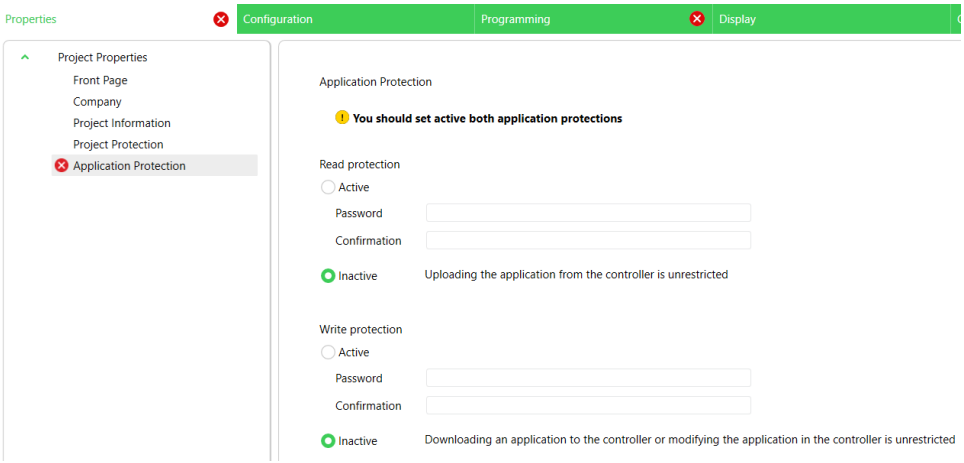
Within EcoStruxure Machine Expert - Basic, you can enhance the cybersecurity of the projects and applications by configuring password protection.

When creating a project, set a password for **Project Protection** and **Application Protection**.

The graphic shows the EcoStruxure Machine Expert - Basic **Project Protection**:

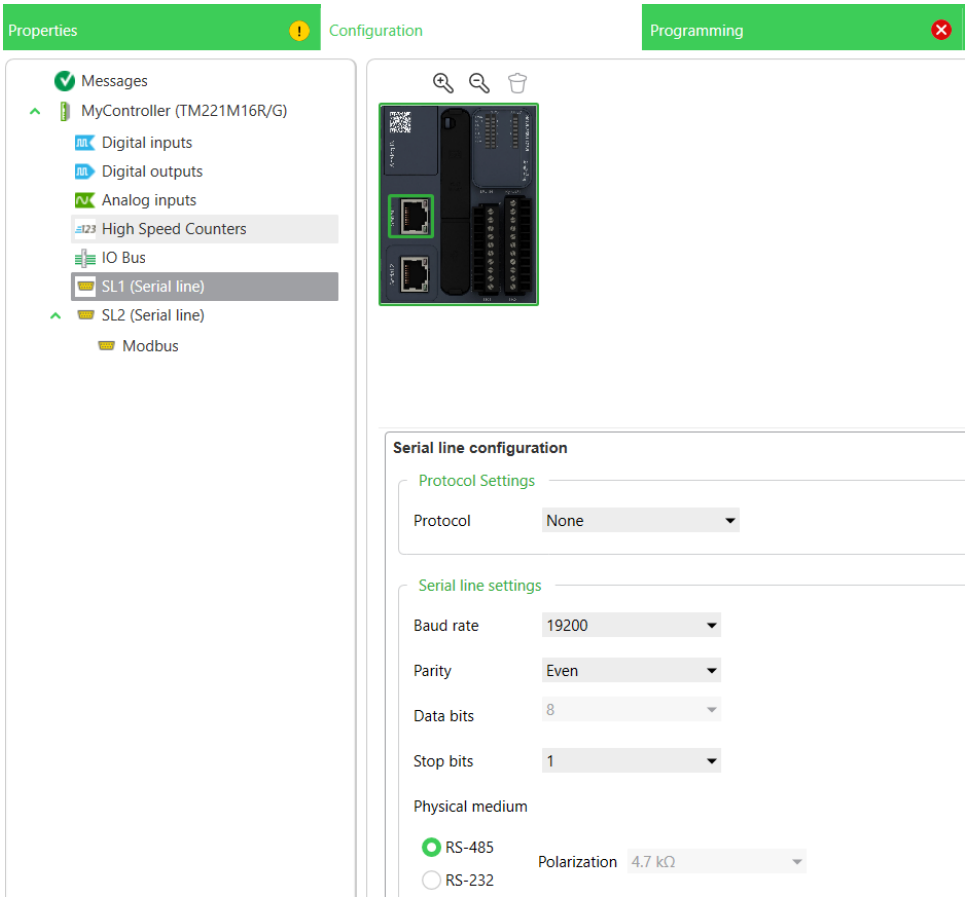


The graphic shows the EcoStruxure Machine Expert - Basic **Application Protection**:



EcoStruxure Machine Expert - Basic also requests you to configure necessary protocols to be used with the controllers.

The graphic shows the EcoStruxure Machine Expert - Basic protocol configuration:



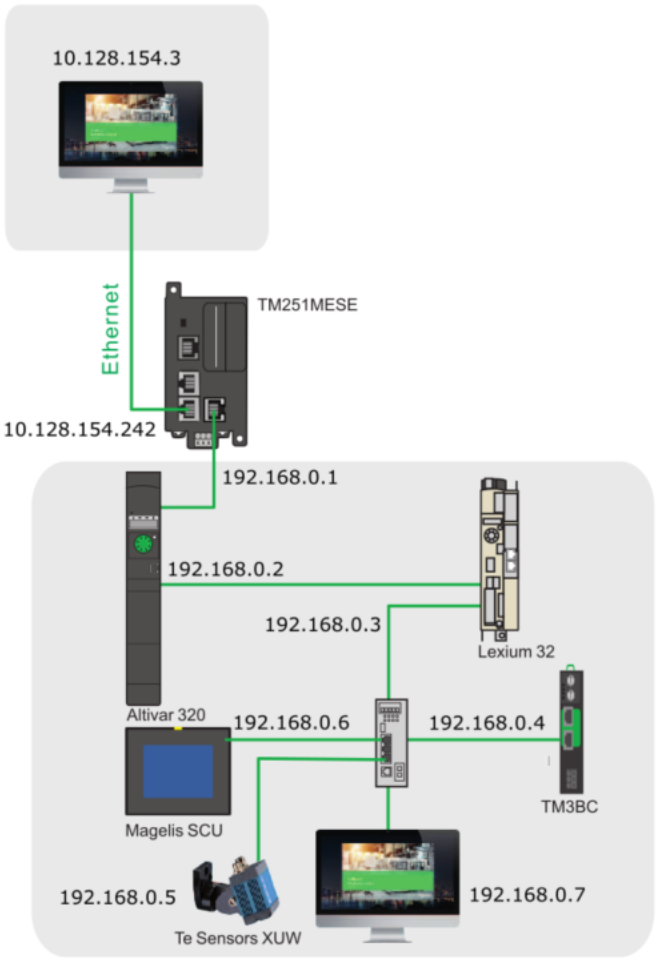
Software and Firmware Updates

EcoStruxure Machine Expert - Basic notifies you when a new software or a new firmware is available and when updates are required.

Hardening: Modicon M251 Logic Controller

Overview

The graphic shows an example Modicon M251 Logic Controller architecture:



The following sections describe the typical architecture where a Modicon M251 Logic Controller is usually integrated. The architecture shows, that the Modicon M251 Logic Controller is able to communicate with different networks. One for machine control and one for device control.

Modicon M251 Logic Controller Security

To meet cybersecurity requirements, the Modicon M251 Logic Controller has been designed in accordance with the standard IEC 62443. As this standard constantly evolves, the Modicon M241 Logic Controller and the Modicon M251 Logic Controller are compliant with a part of the 2019 standard.

In addition, the Modicon M251 Logic Controller has achieved an Achilles Level 1 certification. Within the Modicon M251 Logic Controller platform you can enhance cybersecurity by the following methods:

- Configure user rights
- Disable unused services (for example FTP, HTTP)
- Disable IP forwarding
- Use network separation
- Filter ports and IP through the embedded firewall
- Use secure communication to connect to the web server
- Clone user rights settings

Network Configuration

The Modicon M251 Logic Controller architecture presents a machine control architecture with Ethernet based fieldbus.

The architecture consists of:

- Modicon M251 Logic Controller
- Magelis HMI
- TM3 Bus coupler module
- XUW vision sensor (refer to https://www.se.com/vn/en/product-range/62038-vision-sensors/)
- Altivar 32 variable speed drive
- Lexium 32M servo drive

The machine is controlled by a Modicon controller TM251MESE. This controller provides two separated Ethernet networks. Each one gets its own and unique IP and MAC address. The Ethernet settings for the controller interfaces in this architecture are:

Interface	Parameter	Description
Ethernet 1	Address mode: fixed IP address IP address: 10.128.154.242 MAC address: 00:80:f4:0C:01:02 Subnet mask: 255.255.255.0	Ethernet 1 consists of two switched Ethernet ports dedicated to communication between machines or with the control network.
Ethernet 2	Address mode: fixed IP address IP address: 192.168.0.1 MAC address: 00:80:f4:0A:01:01 Subnet mask: 255.255.255.0	Ethernet 2 consists of one Ethernet port dedicated to the device network and supporting industrial Ethernet connections.

Control Network

In the sample architecture, the Ethernet 1 network of the controller is used for maintenance purposes only.

Therefore, if you establish an Ethernet connection to the machine, you connect to the Ethernet 1 network of the controller. This is considered for the firewall configuration of the controller. The TM251MESE controller supports IP forwarding between Ethernet 1 and Ethernet 2 networks. It is possible to access the Ethernet 2 network through the connection to the Ethernet 1 network of the controller. In order to reach devices on the Ethernet 2 network from Ethernet 1 network, the following preconditions needs to be fulfilled.

- The PC connected to Ethernet 1 must be configured in a way that all traffic dedicated to Ethernet 2 is sent to the IP address of the controllers Ethernet 1 interface. This can be achieved by the configuration of the correct gateway address (in most cases, you will have to create a route on this PC).
- The checkbox **Enable IP forwarding** can be activated (disabled by default) under the Security Parameters of Ethernet 1 interface of the Modicon M251 Logic Controller in EcoStruxure Machine Expert.
- The gateway address parameter of all devices in the Ethernet 2 network must be set to the IP address (Ethernet 2) of the Modicon M251 Logic Controller.

Device Network

The device network is used for the communication between the Ethernet devices inside the machine.

The table lists the devices linked to the device network:

Device	IP address	MAC address	Description
Modicon M251 Logic Controller	192.168.0.1	00:80:f4:0A:01:01	ModbusTCP and EtherNet/IP Master Master DHCP server FDR server
Altivar 32 variable speed drive	192.168.0.2	00:80:f4:0B:01:02	EtherNet/IP slave DHCP client FDR client
Lexium 32M servo drive	192.168.0.3	00:80:f4:0B:01:03	
TM3 Bus Coupler module	192.168.0.4	00:80:f4:0B:01:04	Modbus TCP slave DHCP client
XUW vision sensor	192.168.0.5	00:80:f4:0B:01:05	EtherNet/IP slave DHCP client
Magelis HMI STU	192.168.0.10	00:80:f4:0B:01:06	Read and write access to data provided by the controller (EcoStruxure Machine Expert protocol)

In the sample architecture described herein, the device network is a private network. Everyone who is connected to the network can access the devices directly. Therefore, physical access to the network needs to be limited by appropriate measures.

These measures are, for example:

- Avoid free access to active Ethernet ports
- Use lockable electrical cabinets

External access to the device network is only provided from the control network using the Modicon M251 Logic Controller as a gateway with a configured firewall.

Modicon M251 Logic Controller

Beside providing the monitoring and control functions for the machine, the Modicon M251 Logic Controller represents the gateway between the control and the device network. To restrict access to the controller and to the device network, the following protective measures are implemented into the controller:

- Firewall configuration, page 28
- User management, page 29
- Disabling of unused functions
- Limited access rights to published variables

Services Configuration

EcoStruxure Machine Expert allows you to configure the protocols which need to be activated and to disable unused protocols. This configuration can be done on each Ethernet interface by activating or deactivating protocols for this interface.

The table describes the different security parameters settings of the Modicon M251 Logic Controller and their default settings:

Security Parameters	Description	Default settings
Discovery protocol	This parameter deactivates discovery protocol. If the **Discovery protocol** is deactivated, the discovery requests are ignored.	Active
FTP Server	This parameter deactivates the FTP Server of the controller. When deactivated, FTP requests are ignored.	Active
Machine Expert protocol	This parameter deactivates the Machine Expert protocol on Ethernet interfaces.	Active

Security Parameters	Description	Default settings
	When deactivated, every EcoStruxure Machine Expert request from every device is rejected, including those from the UDP or TCP connection. Therefore, no connection is possible on Ethernet from a PC with EcoStruxure Machine Expert, from an HMI target that tries to exchange variables with this controller, from an OPC server, or from Controller Assistant.	
Modbus Server	This parameter deactivates the Modbus server of the controller. If the Modbus Server is deactivated, every Modbus request to the controller is ignored.	Inactive
SNMP protocol	This parameter deactivates the SNMP server of the controller. If the SNMP protocol is deactivated, SNMP requests are ignored.	Inactive
Secured Web Server (HTTPS)	This parameter deactivates the Secured Web Server of the controller.	Active
WebVisualisation protocol	This parameter deactivates the Web visualization pages of the controller. You are prompted to enter login and password to access the web visualization.	Inactive

You should disable the unused services and use secure protocols as a priority.

Firewall Configuration

The firewall on the controller is configured to help protect the controller and the device network by allowing only packets from authorized sources. Unauthorized packets are rejected. For the sample architecture described herein a static firewall is used for the controller to allow all packets related to the system communication. In addition, a dynamic configuration of the controller firewall is provided in order to allow temporary access to the controller from a dedicated IP address.

For details on firewall configuration refer to the Modicon M251 Logic Controller programming guide.

Static Firewall

The firewall of the controller must be configured with the use of a firewall script file located on the file system of the controller. The default firewall is configured during each boot-up of the controller.

The default firewall of the controller has the following requirements:

- The firewall is configured as an allowlist. Only known packets identified by IP address, MAC address, or port number are allowed.
- Ethernet 1 interface: all packets are rejected by default
- Ethernet 2 interface: all packets related to system communication, for example EtherNet/IP or DHCP, are allowed

For the sample application the script file for the default firewall configuration contains the entries as listed in the code.

```
;Enable firewall.
Firewall Enable;
;Reject all traffic on eth1
Firewall Eth1 Default Reject;
;Allow traffic for MAC on Eth1
Firewall Eth1 Allow MAC 00:80:f4:0C:01:03;
;Allow traffic discovery
Firewall Eth1 Allow udp ports 27126 to 27127;
;Reject all traffic on eth2
Firewall Eth2 Default Reject;
;Allow traffic for all MAC slaves on Eth2
Firewall Eth2 Allow MAC 00:80:f4:0B:01:02;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:03;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:04;
```

```
Firewall Eth2 Allow MAC 00:80:f4:0B:01:05;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:06;
;Allow traffic for all EtherNet/IP slaves
Firewall Eth2 Allow IPs 192.168.0.2 to 192.168.0.6 on TCP
port 2222;
;Allow ethernet IP udp on eth2
Firewall Eth2 Allow IPs 192.168.0.2 to 192.168.0.6 on UDP
port 44818;
;Allow traffic for HMI
Firewall Eth2 Allow IP 192.168.0.6 on UDP ports 1740 to
1743;
;Allow traffic for DHCP
Firewall Eth2 Allow UDP port 67;
```

Dynamic Firewall

For maintenance purposes, temporary access to the controller and the device network via Ethernet 1 interface of the controller is provided in the sample architecture. This temporary access is realized with a dynamic firewall configuration from the controller application.

The dynamic firewall configuration of the controller has the following requirements:

- On Ethernet 1 interface: all packets are rejected, unless the packets are sent from a dedicated IP address (maintenance PC)
- On Ethernet 2 interface: the same settings as for the default firewall configuration must be applied
- After a reboot of the controller or a preconfigured time, the default firewall configuration must be activated again

Apart form the script file for the default firewall, an additional script file for the temporary firewall configuration is created and stored on the controller file system.

Example of entries:

```
;Enable firewall. All frames are rejected
Firewall enable;
;Reject all traffic on eth1
Firewall Eth1 Default Reject;
;Allow traffic for MAC on Eth1
Firewall Eth1 Allow MAC 00:80:f4:0C:01:03;
;Allow traffic with Maintenance PC on eth1 on port 11740
Firewall Eth1 Allow IP 10.128.154.03 on TCP port 11740;
;Reject all traffic on eth2
Firewall Eth2 Default Reject;
;Allow traffic for all MAC slaves on Eth2
Firewall Eth2 Allow MAC 00:80:f4:0B:01:07;
;Allow traffic with Maintenance PC on eth2 on port 11740
Firewall Eth2 Allow IP 192.168.0.7 on TCP port 11740;
```

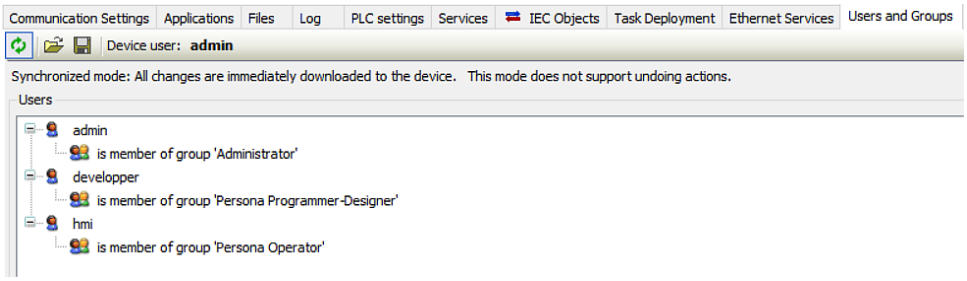
User Management

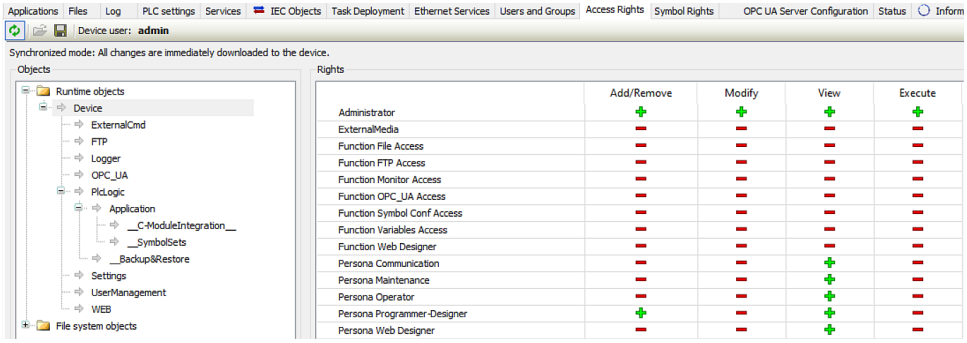
By default, user rights are activated on the controller. During first login, configure the user name and a password account which will have administrator privileges.

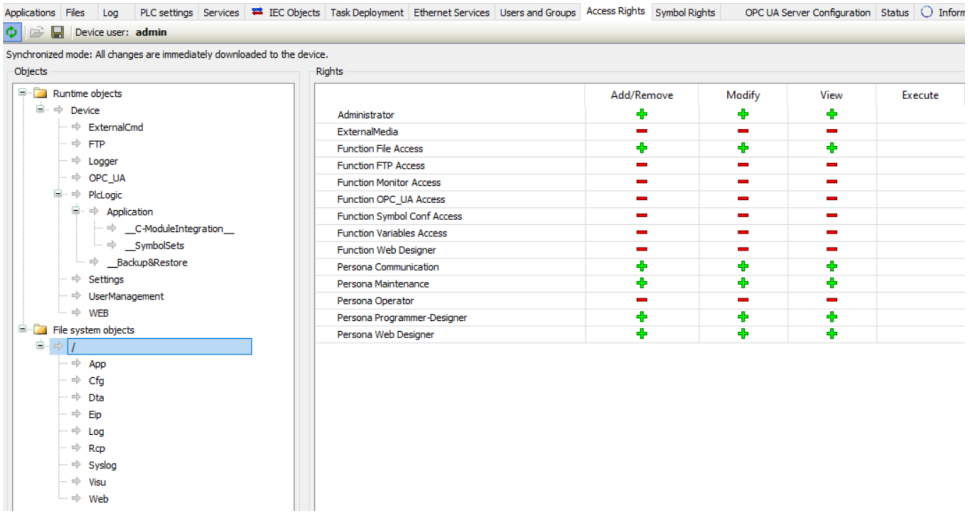
The Modicon M251 Logic Controller supports an online user management. The user management is used to manage user accounts and user access rights groups and the associated permissions. This allows you to control the access to the EcoStruxure Machine Expert project and the controller in online mode.

In EcoStruxure Machine Expert, on the **Users** and **Groups** tab of the device editor of the controller, you can configure the user management for your EcoStruxure Machine Expert project and the contained controllers.

In the user account settings like user name and password, you need to assign the **Access Rights** for each user. By default, a number of access rights groups are predefined for the single Access Types. The default access rights groups cannot be changed but you can create your own access right groups.







Cloning the User Rights

Modicon M251 Logic Controller also offers a mechanism to duplicate the user right settings from one controller to another Modicon M251 Logic Controller. This can be achieved by using cloning mechanism which consists to duplicate the user rights and application of one controller on an SD card and copy the configuration to another controller.

In order to execute the cloning feature, you first need to login on the Modicon M251 Logic Controller web server and enable the option to allow the copy of the user rights.

Symbol Configuration - Access Rights

The symbol configuration functionality allows you to create symbol descriptions. The symbols and the variables they represent can then be accessed by external applications, such as Vijeo Designer or OPC server.

The previously configured protective measures like user management and firewall configuration already restrict the access to the data which are published with the symbol configuration.

An additional measure regarding cybersecurity is the configuration of the appropriate access rights for each published symbol. Each symbol represents a variable in your application and in the symbol configuration you can select

between read-only, write-only, or read and write access rights for each variable. By default, each symbol is equipped with read and write access rights.

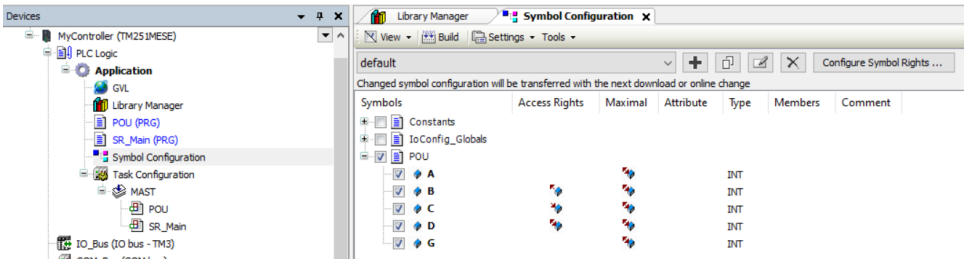
From the cybersecurity point of view, the approach secure by default is preferred. This can be achieved with the use of pragma `{Attribute 'symbol'}` within the variable declaration.

For the architecture, in the very first line of each variable declaration editor the pragma `{Attribute 'symbol' := 'none'}` has been added. In consequence, the variables declared below are published as soon as a **Symbol Configuration** is added but without access rights.

In order to provide the appropriate access rights to a variable, an additional pragma must be added in front of each single variable declaration.

Example for a variable declaration with pragmas:

```
{attribute 'symbol':='none'}
VAR_GLOBAL
   A:INT;// variable will be published without access-rights
   {attribute 'symbol':='read'}
   B:INT;// variable will be published with read-only access
   {attribute 'symbol':='write'}
   C:INT;// variable will be published with write-only
access
   {attribute 'symbol':='readwrite'}
   D:INT;// variable will be published with read+write
access
   G:INT;// variable will be published without access-rights
END_VAR
```

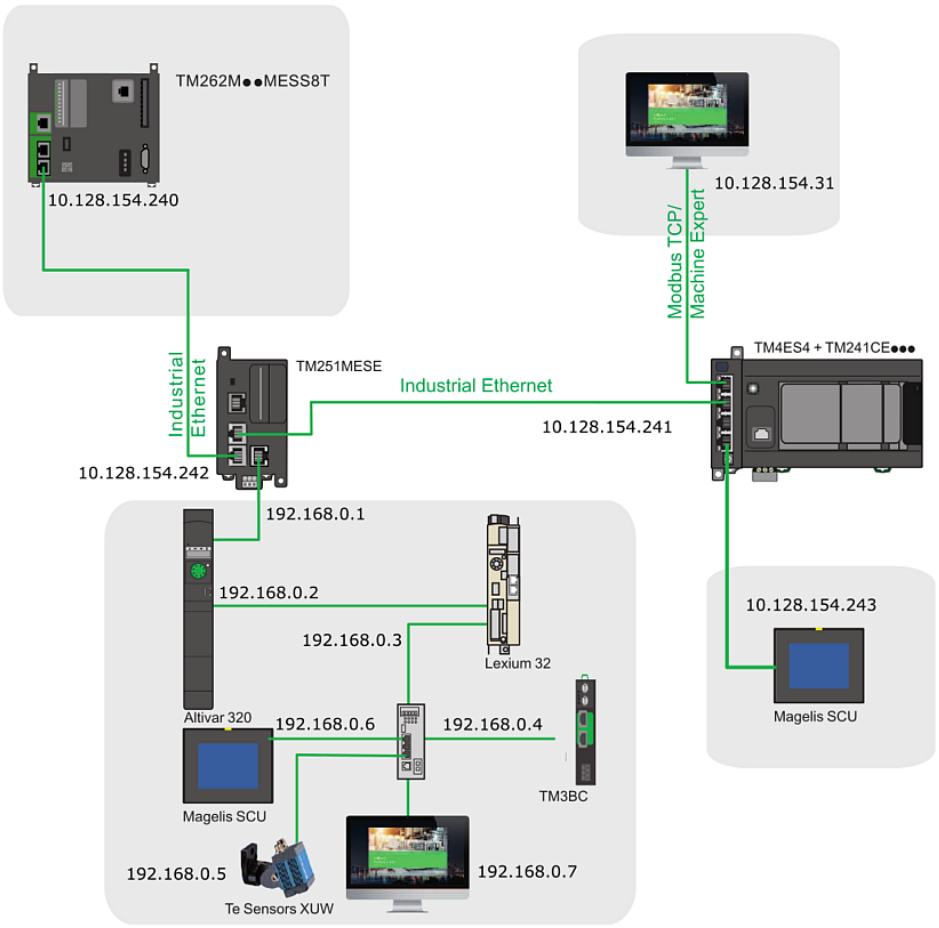


For details on **Symbol Configuration** access rights, refer to the EcoStruxure Machine Expert Programming Guide.

Hardening: Modicon M241 Logic Controller

Overview

The graphic shows the typical Modicon M241 Logic Controller architecture:



The following sections describe where a Modicon M241 Logic Controller is usually integrated.

Modicon M241 Logic Controller Security

In order to meet cybersecurity requirements, the Modicon M241 Logic Controller has been designed in accordance with the standard IEC 62443. As this standard constantly evolves, the Modicon M241 Logic Controller is compliant with a part of the 2019 standard.

In addition, the Modicon M241 Logic Controller has achieved an Achilles Level 1 certification. Within the Modicon M241 Logic Controller platform you can enhance cybersecurity using the following methods:

- Configure the user rights
- Disable unused services (for example FTP, HTTP)
- Disable IP forwarding
- Apply network separation
- Filter ports and IP through the embedded firewall
- Use secure communication to connect to the web server
- Clone user rights settings

Network Configuration

The following table lists the Ethernet devices linked to the control network:

Controller	IP address	MAC address	Description
TM251MESE	Ethernet 1 10.128.154.242	00:80:f4:0C:01:02	EtherNet/IP slave on Ethernet 1 interface.
TM4ES4	10.128.154.241	00:80:f4:0D:01:01	EtherNet/IP slave
TM241CEC24T/U			
TM262M●	Ethernet 2 10.128.154.240	00:80:f4:0E:01:02	EtherNet/IP master on Ethernet 2 interface.
HMI SCU (connected to Modicon M241 Logic Controller)	10.128.154.243	00:80:f4:0D:01:03	Read and write access to data provided by the controller.
Maintenance PC	10.128.154.31	00:80:f4:0D:01:04	—

For more information refer to the Device Network, page 26 of the Modicon M251 Logic Controller.

In the sample architecture, the control network is used for the data exchange between the controllers. The exchanged data include actual status information and commands required to synchronize the operation of the separated machine modules. Furthermore, the HMI touch panel linked to Modicon M241 Logic Controller and PC for maintenance purposes are linked to the control network.

The communication inside the control network is not encrypted and therefore the physical access to the network needs to be limited by appropriate measures.

These measures can be for example:

- Avoid free access to active Ethernet ports
- Use lockable electrical cabinets

Services Configuration

EcoStruxure Machine Expert allows you to configure the protocols which need to be activated, and to disable unused protocols. This configuration can be done on each Ethernet interface by activating or deactivating protocols for this interface.

The table describes the different security parameters settings of the Modicon M241 Logic Controller and their default settings:

Security Parameters	Description	Default settings
Discovery protocol	This parameter deactivates the discovery protocol. When deactivated, discovery requests are ignored.	Active
FTP Server	This parameter deactivates the FTP Server of the controller. When deactivated, FTP requests are ignored. FTPS is by default activated.	Active
Machine Expert protocol	This parameter deactivates the EcoStruxure Machine Expert protocol on Ethernet interfaces. When deactivated, every EcoStruxure Machine Expert request from every device is rejected, including those from the UDP or TCP connection. Therefore, no connection is possible on Ethernet from a PC with EcoStruxure Machine Expert, from an HMI target that tries to exchange variables with this controller, from an OPC server, or from Controller Assistant.	Active
Modbus Server	This parameter deactivates the Modbus server of the controller. When deactivated, every Modbus request to the controller is ignored.	Inactive
SNMP protocol	This parameter deactivates the SNMP server of the controller. When deactivated, SNMP requests are ignored.	Inactive

Security Parameters	Description	Default settings
Secured Web Server (HTTPS)	This parameter deactivates the Secured Web Server of the controller. When deactivated, HTTPS requests to the controller Secured Web Server are ignored.	Active
WebVisualisation protocol	This parameter deactivates the Web visualization pages of the controller. When deactivated, HTTP requests to the logic controller WebVisualisation protocol are ignored. You are prompted to enter login and password to access the web visualization.	Inactive

NOTE:

- You should disable all unused services and use in priority secure protocols. Unused services should be disabled for security reasons to remove attack opportunities if not needed.
- Use secure protocols as a priority.

Firewall Configuration

For each controller, a firewall configuration has been done to protect the controller itself and the machine modules. The firewall configuration allows packets only from authorized sources. All unauthorized packets are rejected.

For each of the three controllers in this sample architecture a static configuration is provided. Like already described in the previous example the dynamic firewall configuration is provided in order to allow temporary access to the controller from a dedicated IP address. In this case, the IP address belongs to the maintenance PC.

In the following, the entries for the single firewall script files are illustrated together with a short explanation.

Static firewall Modicon M251 Logic Controller

The firewall configuration for the controller from the previous example must be expanded in order to allow continuous access from the line controller via the EtherNet/IP protocol.

For the sample application the script file for the default firewall configuration of Modicon M251 Logic Controllercontains the entries as listed below:

```
;Enable firewall.
Firewall Enable;
;Reject all traffic on eth1
Firewall Eth1 Default Reject;
;Allow traffic for MAC on Eth1
Firewall Eth1 Allow MAC 00:80:f4:0C:01:03;
Firewall Eth1 Allow MAC 00:80:f4:0E:01:02;
;Allow traffic discovery
Firewall Eth1 Allow udp ports 27126 to 27127;
;Reject all traffic on eth2
Firewall Eth2 Default Reject;
;Allow traffic for all MAC slaves on Eth2
Firewall Eth2 Allow MAC 00:80:f4:0B:01:02;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:03;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:04;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:05;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:06;
;Allow traffic for all EtherNet/IP slaves
Firewall Eth2 Allow IPs 192.168.0.2 to 192.168.0.6 on TCP
port 2222;
;Allow ethernet IP udp on eth2
Firewall Eth2 Allow IPs 192.168.0.2 to 192.168.0.6 on UDP
port 44818;
;Allow traffic for HMI
```

```
Firewall Eth2 Allow IP 192.168.0.6 on UDP ports 1740 to
1743;
;Allow traffic for DHCP
Firewall Eth2 Allow UDP port 67;
;Allow traffic for EtherNet/IP master
Firewall Eth1 Allow IP 10.128.154.240 on UDP port 2222;
;Allow traffic for EtherNet/IP master
Firewall Eth1 Allow IP 10.128.154.240 on UDP port 44818;
```

Static firewall Modicon M241 Logic Controller

The firewall configuration for the Modicon M241 Logic Controller must provide continuous access from the HMI touch panel and the line controller via the EtherNet/IP protocol.

For the sample application, the script file for the default firewall configuration of Modicon M241 Logic Controller contains the entries as listed below.

```
;Enable firewall.
Firewall Enable;
;Reject all traffic on eth1
Firewall Eth1 Default Reject;
;Allow traffic for MAC on Eth1
Firewall Eth1 Allow MAC 00:80:f4:0E:01:02;
Firewall Eth1 Allow MAC 00:80:f4:0D:01:03;
;Allow traffic for HMI
Firewall Eth1 Allow IP 10.128.154.243 on UDP ports 1740 to
1743;
;Allow traffic for EtherNet/IP master
Firewall Eth1 Allow IP 10.128.154.240 on udp port 2222;
;Allow traffic for EtherNet/IP master
Firewall Eth1 Allow IP 10.128.154.240 on tcp port 44818;
```

Static firewall Modicon M262 Logic/Motion Controller

The firewall configuration for the Modicon M262 Logic/Motion Controller must provide continuous access from machine controllers Modicon M241 Logic Controller and Modicon M251 Logic Controller via the EtherNet/IP protocol on Ethernet 2 interface. In the sample application all traffic on Ethernet 1 interface is rejected.

```
;Enable firewall. All frames are rejected
Firewall Enable;
;Reject all traffic on eth1
Firewall Eth1 Default Reject;
;Reject all traffic on eth2
Firewall Eth2 Default Reject;
;Allow traffic for MAC on Eth2
Firewall Eth2 Allow MAC 00:80:f4:0C:01:02;
Firewall Eth2 Allow MAC 00:80:f4:0D:01:01;
;Allow traffic for EtherNet/IP slaves
Firewall Eth2 Allow IPs 10.128.154.241 to 10.128.154.242 on
udp port 2222;
;Allow traffic for EtherNet/IP slaves
Firewall Eth2 Allow IPs 10.128.154.241 to 10.128.154.242 on
tcp port 44818;
```

Dynamic Firewall Modicon M251 Logic Controller

For maintenance purposes temporary access through Ethernet 1 interface of the controller is provided for a dedicated IP address which belongs to maintenance PC.

For the sample application the script file for the dynamic firewall configuration of Modicon M251 Logic Controller contains the entries as listed below.

```
;Enable firewall.
Firewall Enable;
;Reject all traffic on eth1
Firewall Eth1 Default Reject;
;Allow traffic for MAC on Eth1
Firewall Eth1 Allow MAC 00:80:f4:0C:01:03;
Firewall Eth1 Allow MAC 00:80:f4:0E:01:02;
```

```
Firewall Eth1 Allow MAC 00:80:f4:0D:01:04;
;Allow traffic discovery
Firewall Eth1 Allow udp ports 27126 to 27127;
;Reject all traffic on eth2
Firewall Eth2 Default Reject;
;Allow traffic for all MAC slaves on Eth2
Firewall Eth2 Allow MAC 00:80:f4:0B:01:02;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:03;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:04;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:05;
Firewall Eth2 Allow MAC 00:80:f4:0B:01:06;
;Allow traffic for all EtherNet/IP slaves
Firewall Eth2 Allow IPs 192.168.0.2 to 192.168.0.6 on TCP
port 2222;
;Allow ethernet IP udp on eth2
Firewall Eth2 Allow IPs 192.168.0.2 to 192.168.0.6 on UDP
port 44818;
;Allow traffic for HMI
Firewall Eth2 Allow IP 192.168.0.6 on UDP ports 1740 to
1743;
;Allow traffic for DHCP
Firewall Eth2 Allow UDP port 67;

;Allow traffic for EtherNet/IP master
Firewall Eth1 Allow IP 10.128.154.240 on UDP port 2222;
;Allow traffic for EtherNet/IP master
Firewall Eth1 Allow IP 10.128.154.240 on UDP port 44818;
;Allow packets from maintenance PC via Ethernet 1
Firewall Eth1 Allow IP 10.128.154.31 on TCP port 11740;
```

Dynamic Firewall Modicon M241 Logic Controller

For maintenance purposes, temporary access through Ethernet 1 interface of the controller is provided for a dedicated IP address which belongs to maintenance PC.

For the sample application the script file for the dynamic firewall configuration of Modicon M241 Logic Controller contains the entries as listed below.

```
;Enable firewall. All frames are rejected
Firewall enable;
;Allow traffic for all Ethernet slaves
Firewall Eth2 Allow IPs 192.168.0.2 to 192.168.0.5;
;Allow traffic for HMI
Firewall Eth2 Allow IP 192.168.0.10;
;Allow traffic for DHCP
Firewall Eth2 Allow udp port 67;
;Allow traffic for EtherNet/IP master (line controller)
Firewall Eth1 Allow IP 10.128.154.240 on udp port 2222;
;Allow traffic for EtherNet/IP master (line controller)
Firewall Eth1 Allow IP 10.128.154.240 on tcp port 44818;
;Allow packets from maintenance PC via Ethernet 1
Firewall Eth1 Allow IP 10.128.154.31;
```

Dynamic Firewall Modicon M262 Logic/Motion Controller

For maintenance purposes, temporary access through Ethernet 2 interface of the controller is provided for a dedicated IP address which belongs to maintenance PC.

For the sample application, the script file for the dynamic firewall configuration of Modicon M262 Logic/Motion Controller contains the entries as listed below.

```
;Enable firewall. All frames are rejected
Firewall Enable;
;Reject all traffic on eth1
Firewall Eth1 Default Reject;
;Reject all traffic on eth2
Firewall Eth2 Default Reject;
;Allow traffic for MAC on Eth2
Firewall Eth2 Allow MAC 00:80:f4:0C:01:02;
Firewall Eth2 Allow MAC 00:80:f4:0D:01:01;
```

```
Firewall Eth1 Allow MAC 00:80:f4:0D:01:04;
;Allow traffic for EtherNet/IP slaves
Firewall Eth2 Allow IPs 10.128.154.241 to 10.128.154.242 on
udp port 2222;
;Allow traffic for EtherNet/IP slaves
Firewall Eth2 Allow IPs 10.128.154.241 to 10.128.154.242 on
tcp port 44818;
;Allow packets from maintenance PC via Ethernet 1
Firewall Eth2 Allow IP 10.128.154.31 on TCP port 11740;
```

User Management

Out of the box it is requested to set login and password with administrator privileges. The same configuration as the Modicon M251 Logic Controller can be applied.

For more information, refer to User Management, page 29.

Cloning the User Rights

Modicon M241 Logic Controller also offers a mechanism to duplicate the user right settings from one controller to another Modicon M241 Logic Controller. This can be achieved by using cloning mechanism which consists to duplicate the user rights and application of one controller on an SD-Card and copy the configuration to another controller.

In order to execute the cloning feature, you first need to login on the Modicon M241 Logic Controller webserver, and enable the option to allow the copy of the user rights.

Symbol Configuration - Access Rights

Refer to Symbol Configuration - Access Rights, page 30.

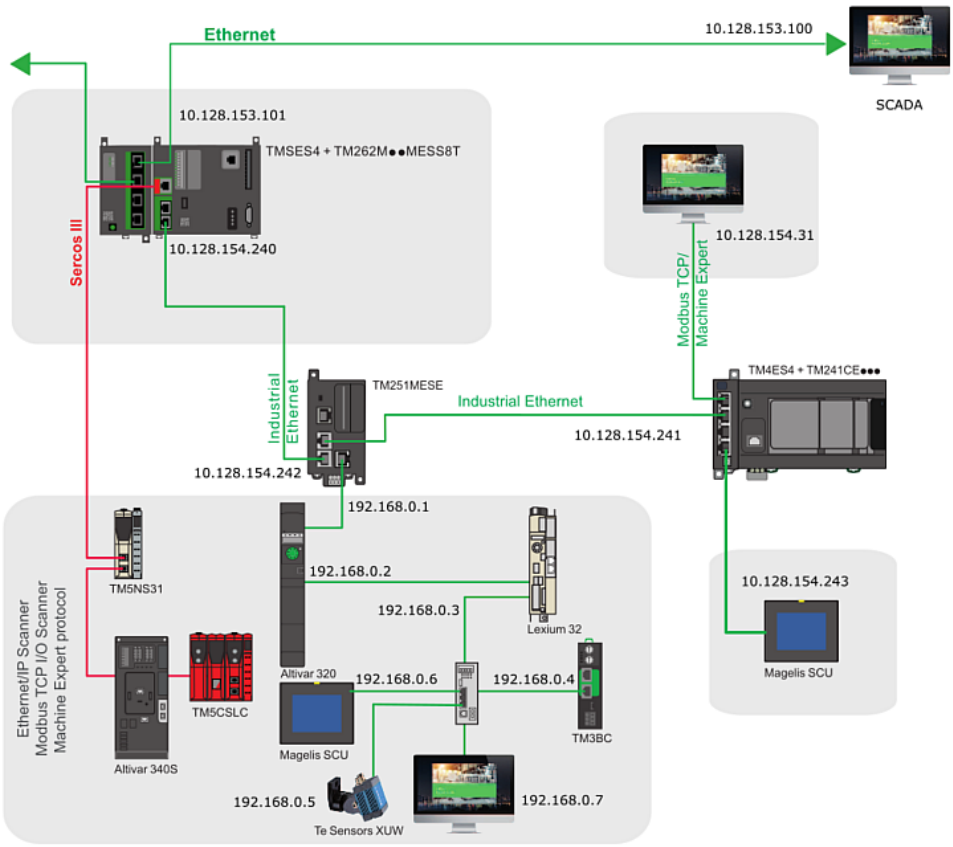
Hardening: Modicon M262 Logic/Motion Controller and TMSES4

Overview

The following sections describe the typical architecture where a Modicon M262 Logic/Motion Controller and the TMS expansion modules, which fits onto the left side of the controller, are usually integrated.

TMSES4 is a switch providing additional Ethernet ports to the Modicon M262 Logic/Motion Controller.

The graphic illustrates, that the Modicon M262 Logic/Motion Controller is able to communicate using Ethernet and Sercos communications channels. In this architecture a SCADA system has been connected to Modicon M262 Logic/Motion Controller as well.



Modicon M262 Logic/Motion Controller Security

In order to meet cybersecurity requirements, the Modicon M262 Logic/Motion Controller has been designed in accordance with the standard IEC 62443. As this standard constantly evolves, the Modicon M262 Logic/Motion Controller is compliant with a part of the 2019 standard.

In addition, the Modicon M262 Logic/Motion Controller has achieved an Achilles Level 2 certification. Within the Modicon M262 Logic/Motion Controller platform, you can enhance cybersecurity by the following methods:

- Configure the user rights
- Disable IP forwarding
- Apply network separation
- Filter ports and IP through the embedded firewall
- Use secure communication to connect to the web server
- Apply traceability of system events via syslog
- Clone user rights settings
- Use OPC-UA secure server

Network Configuration

In the graphic of the typical Modicon M262 Logic/Motion Controller architecture, the SCADA system and the Modicon M262 Logic/Motion Controller are connected to the control network. The following table lists the Ethernet devices linked to this network:

Controller	IP address	Description
TM262M●	Ethernet 1 10.128.153.101	Real data provider for the OPC server.
SCADA	10.128.153.100	OPC client and SCADA system,

The control network where the communication between the SCADA system and the machine takes place is separated from the machine network. This control network is also used for other communication purposes and therefore it provides access to an increased number of users. Thus, the requirements for cybersecurity are likewise increased.

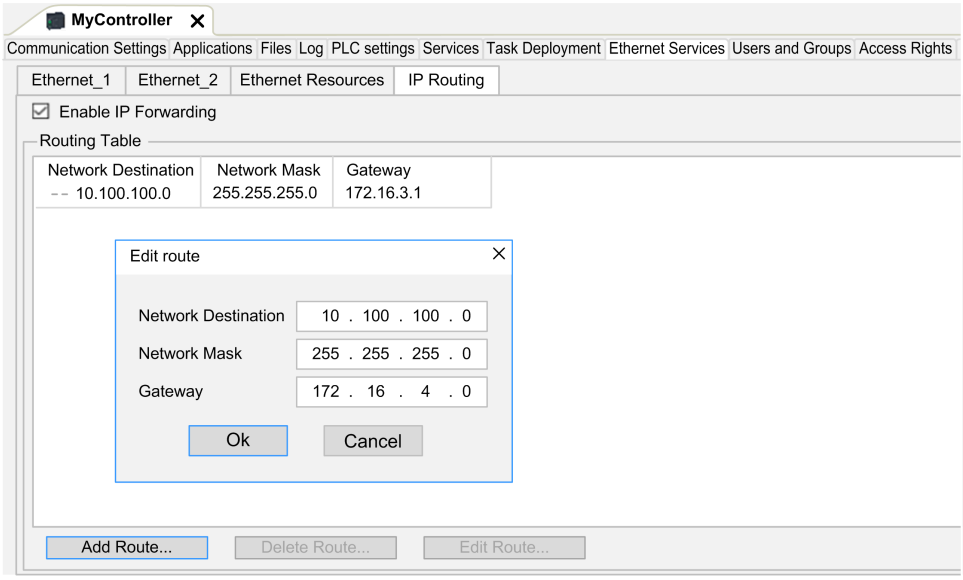
To help prevent the unintended access from the control network to the controller and the provided process data, the internal firewall configuration and the access control through the user management of the controller have been applied.

Apart form the monitoring and control functions of the machine modules, the Modicon M262 Logic/Motion Controller line controller represents the interface between the machine and the SCADA system. To help prevent the unintended access from the control network, the following protective measures have been applied on the controller:

- Firewall configuration, page 40
- User management, page 41
- Limited access rights to published variables

In a typical Modicon M262 Logic/Motion Controller architecture, the Modicon M262 Logic/Motion Controller is using Sercos protocol to communicate with devices.

In order to separate control network from devices connected through Sercos channel, disable **IP Forwarding** mechanism on the **IP Routing** tab. By default, **Enable IP Forwarding** is disabled, but can be enabled.



Once the network configuration is done and active protocols are set on the Modicon M262 Logic/Motion Controller and TMSES4 module(s), you can enhance cybersecurity by configuring the firewall.

Services Configuration

EcoStruxure Machine Expert allows you to configure the protocols which need to be activated, and to disable unused protocols. This configuration can be done on each Ethernet interface by activating or deactivating protocols for this interface.

The table describes the different security parameters settings of the Modicon M262 Logic/Motion Controller and their default settings:

Security Parameters	Description	Default settings
Discovery protocol	This parameter deactivates the discovery protocol. When deactivated, discovery requests are ignored.	Active
FTP Server	This parameter deactivates the FTP Server of the controller.	Active

Security Parameters	Description	Default settings
	When deactivated, FTP requests are ignored. FTPS is by default activated.	
Machine Expert protocol	This parameter deactivates the EcoStruxure Machine Expert protocol on Ethernet interfaces. When deactivated, every EcoStruxure Machine Expert request from every device is rejected. Therefore, no connection is possible on Ethernet from a PC with EcoStruxure Machine Expert, from an HMI target that tries to exchange variables with this controller, from an OPC server, or from Controller Assistant.	Active
Modbus Server	This parameter deactivates the Modbus server of the controller. When deactivated, every Modbus request to the controller is ignored.	Inactive
Remote connection (Fast TCP)	This parameter deactivates the remote connection. When deactivated, fast TCPs requests are ignored.	Active
Secured Web Server (HTTPS)	This parameter deactivates the Secured Web Server of the controller. When deactivated, HTTPS requests to the controller Secured Web Server are ignored.	Active
SNMP protocol	This parameter deactivates the SNMP server of the controller. When deactivated, SNMP requests are ignored.	Inactive
WebVisualisation protocol	This parameter deactivates the Web visualization pages of the controller. When deactivated, HTTP requests to the logic controller WebVisualisation protocol are ignored. You are prompted to enter login and password to access the web visualization.	Inactive

NOTE:

- You should disable all unused services and use in priority secure protocols. Unused services should be disabled for security reasons to remove attack opportunities if not needed.
- Use secure protocols as a priority.

Firewall Configuration

Once the network and Ethernet services are configured, the Modicon M262 Logic/Motion Controller embedded firewall must be configured to reject all unauthorized packets.

For the controller in this example architecture a static firewall configuration is provided. The only change for the firewall configuration is the addition of an exception rule which allows the access through the SCADA system on Ethernet 1 interface of the controller.

Static firewall

For the example application, the script file for the default firewall configuration of a Modicon M262 Logic/Motion Controller contains the entries as listed below.

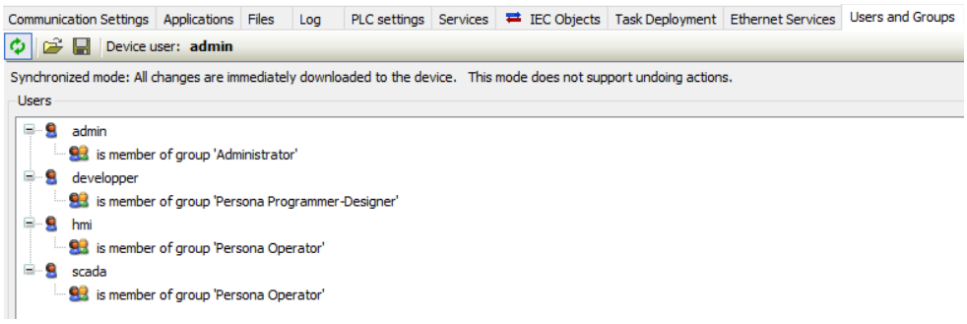
```
;Enable firewall. All frames are rejected
Firewall enable;
;Reject all traffic by default on M262
Firewall Eth1 Default Reject;
Firewall Eth2 Default Reject;
;Reject all traffic by default on TMSES4
Firewall Eth3 Default Reject;
;Allow traffic for ntp
Firewall Eth1 Allow UDP port 123;
Firewall Eth2 Allow UDP port 123;
;Allow OPC-UA traffic with SCADA on TMSES4
Firewall Eth3 Allow IP 10.128.153.100 on tcp port 4080;
```

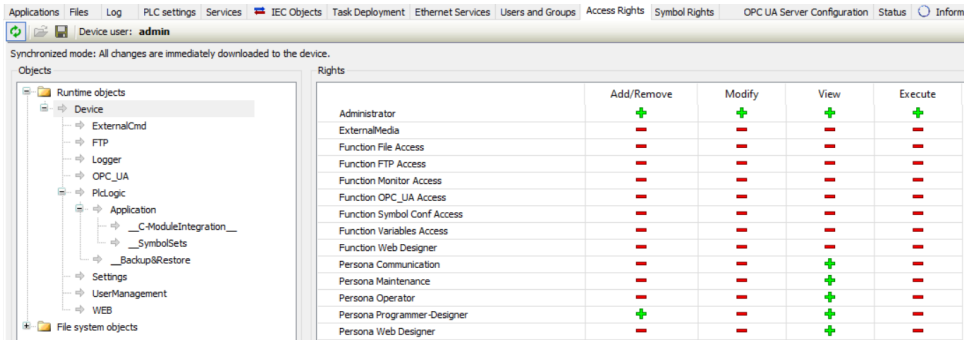
```
;Allow traffic for EtherNet/IP slaves (machine controllers)
Firewall Eth2 Allow IPs 10.128.154.241 to 10.128.154.242 on
udp port 2222;
;Allow traffic for EtherNet/IP slaves (machine controllers)
Firewall Eth2 Allow IPs 10.128.154.241 to 10.128.154.242 on
tcp port 44818;
;Allow traffic for SCADA system for Machine Expert network
protocol
Firewall Eth1 Allow IP 10.128.153.100 on tcp port 11740;
Firewall Eth1 Allow IP 10.128.153.100 on udp ports 1740 to
1743;
```

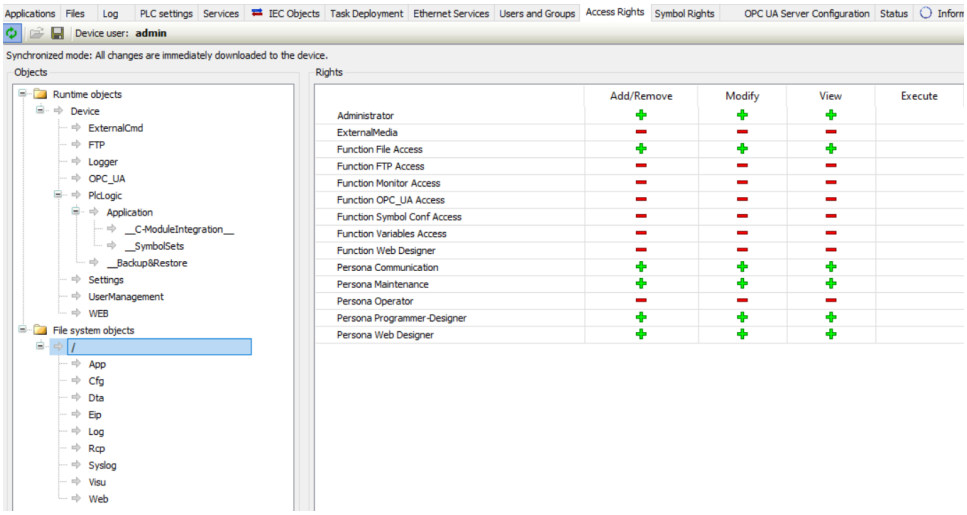
User Management

On the controller, an account with administrator privileges is requested to be created at first use. Create the other user accounts and the corresponding rights according to the requirements of your application and your cybersecurity process definitions. You can then also add in the architecture example for Modicon M262 Logic/Motion Controller, a SCADA user which will only be able to read and write data.

Possible user configurations on the Modicon M262 Logic/Motion Controller:







Cloning the User Rights

Modicon M262 Logic/Motion Controllers also offer a mechanism to duplicate the user right settings from one controller to another Modicon M262 Logic/Motion Controller. This can be achieved by using cloning mechanism which duplicates the user rights and application of one controller on an SD card and copy the configuration to another controller.

In order to execute the cloning feature, you need to login on the Modicon M262 Logic/Motion Controller web server, and enable the option to allow the copy of the user rights.

Symbol Configuration — Access Rights

Refer to Symbol Configuration - Access Rights, page 30.

OPC-UA Secure Server

Modicon M262 Logic/Motion Controllers offer the capability to communicate with OPC-UA clients in a secure way. The authentication is done through dedicated account configured through the EcoStruxure Machine Expert **Users and Groups** tab.

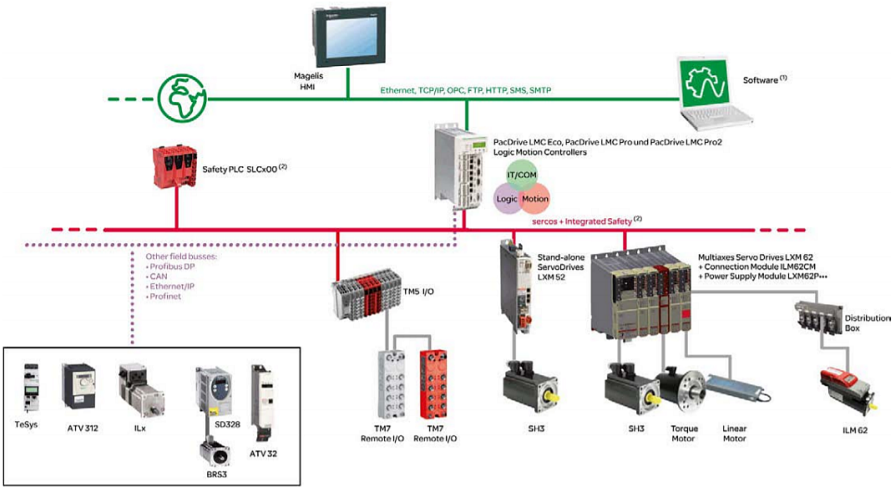
Dedicated OPC-UA plugin is provided through EcoStruxure Machine Expert to configure the OPC-UA security settings.

By default, encrypted OPC-UA communication is enabled and anonymous login is disabled. For more details on the certificate management for OPC-UA, refer to the EcoStruxure Machine Expert – Programming Guide.

Hardening: PacDrive LMC Eco and PacDrive LMC Pro/Pro2

Overview

The following graphic shows the typical architecture for PacDrive LMC Eco and PacDrive LMC Pro/Pro2 controllers.



(1) EcoStruxure Machine Expert software

(2) Safety Logic Controller TM5CSLC•00FS

PacDrive LMC Pro/Pro2 Security

In order to meet cybersecurity requirements, the PacDrive LMC Pro/Pro2 has been designed in accordance with the standard IEC 62443. As this standard

constantly evolves, the PacDrive LMC Pro/Pro2 Logic Controllers are compliant with a part of the 2019 standard.

In addition, the PacDrive LMC Eco and PacDrive LMC Pro/Pro2 Logic Controllers have achieved an Achilles Level 1 certification. Within the LMC Eco and LMC Pro/Pro2 platform, you can enhance cybersecurity by the following methods:

- Configure the user rights
- Disable unused services (for example FTP)
- Apply network separation
- Filter ports and IP through the embedded firewall
- Use secure communication
- Apply traceability of system events via audit logs
- Use OPC-UA server with secure communications

Network Configuration

The network configuration is done in EcoStruxure Machine Expert. The Ethernet port for PacDrive LMC Pro/Pro2 and PacDrive LMC Eco can be configured in the **Ethernet Services** tab (refer to Network Configuration, page 19 in EcoStruxure Machine Expert.

To help prevent the unintended access from the control network to the Sercos network, the following protective measures must be applied on the controller:

- Firewall configuration, page 44
- User management, page 44
- Limited access rights to published variables

To separate control network from devices connected through the Sercos channel, disable the IP forwarding mechanism. IP forwarding is disabled using the PacDrive LMC Pro/Pro2 and PacDrive LMC Eco firewall. For more information, refer to How to Configure the Firewall for PacDrive LMC Controllers – User Guide.

Services Configuration

EcoStruxure Machine Expert allows you to configure the protocols which need to be activated, and to disable unused protocols. This configuration can be done on each Ethernet interface by activating or deactivating protocols for this interface.

The table describes the different security parameters settings of the PacDrive LMC Pro/Pro2 and PacDrive LMC Eco controller and their default settings:

Security Parameters	Description	Default settings
Discovery protocol	This parameter deactivates the discovery protocol. When deactivated, discovery requests are ignored.	Active
FTP Server	This parameter deactivates the FTP Server of the controller. When deactivated, FTP requests are ignored. FTPS is by default activated. FTP is available only after the administrator login and password has been created.	Active

Security Parameters	Description	Default settings
Machine Expert protocol	This parameter deactivates the EcoStruxure Machine Expert protocol on Ethernet interfaces. When deactivated, every EcoStruxure Machine Expert request from every device is rejected, including those from the UDP or TCP connection. Therefore, no connection is possible on Ethernet from a PC with EcoStruxure Machine Expert, from an HMI target that tries to exchange variables with this controller, from an OPC server, or from Controller Assistant.	Active
WebVisualisation protocol	This parameter deactivates the Web visualization pages of the controller. When deactivated, HTTP requests to the logic controller WebVisualisation protocol are ignored. You are prompted to enter login and password to access the web visualization.	Inactive

Firewall Configuration

By default, a firewall is activated on the LMC PacDrive controllers.

- The firewall is configured in a strict way on the general Ethernet interface (CN8 on PacDrive LMC Pro/Pro2 and CN3 on PacDrive LMC Eco).
- Incoming traffic is blocked, with the exception of defined applications / ports.
- Outgoing traffic is not affected by the firewall.
- The firewall can be configured by the customer in two different ways: permanently by editing a configuration file on the memory card or during runtime via *SystemInterface*, *Common Toolbox* library and function blocks.
- By default, IP forwarding is disabled in firewall default rule. As a consequence, Ethernet network and Sercos network cannot communicate.
- In order to enable the IP forwarding mechanism, you need to change the firewall rules. For details on firewall configuration, refer to How to Configure the Firewall for PacDrive LMC Controllers – User Guide.

User Management

Refer to User Management, page 29.

Symbol Configuration

Refer to Symbol Configuration – Access Rights, page 30.

OPC-UA Secure Server

PacDrive LMC Pro/Pro2 and PacDrive LMC Eco controllers allow the communication with OPC-UA clients in a safe way.

For more information refer to OPC-UA Secure Server, page 42.

Hardening: Modicon LMC058 Motion Controller and Modicon M258 Logic Controller

Modicon LMC058 Motion Controller and Modicon M258 Logic Controller Security

Modicon LMC058 Motion Controller and Modicon M258 Logic Controller are running on EcoStruxure Machine Expert version 1.2.x.

Within the Modicon LMC058 Motion Controller and Modicon M258 Logic Controller platform you could enhance cybersecurity by the following methods:

- Configure the user rights
- Disable unused services (for example FTP)
- Apply network separation
- Filter ports and IP through the embedded firewall
- Clone user rights settings

Cybersecurity configuration can be done in the same way as explained in the sections Network Configuration, page 33 and Services Configuration, page 33 for Modicon M241 Logic Controller and Modicon M251 Logic Controller.

Services Configuration

EcoStruxure Machine Expert allows you to configure the protocols which need to be activated, and to disable unused protocols. This configuration can be done on each Ethernet interface by activating or deactivating protocols for this interface.

The table describes the different security parameters settings of the PacDrive LMC Pro/Pro2 and PacDrive LMC Eco controller and their default settings:

Security Parameters	Description	Default settings
Discovery protocol	This parameter deactivates the discovery protocol. When deactivated, discovery requests are ignored.	Active
FTP Server	This parameter deactivates the FTP Server of the controller. When deactivated, FTP requests are ignored.	Inactive
Machine Expert protocol	This parameter deactivates the EcoStruxure Machine Expert protocol on Ethernet interfaces. When deactivated, every EcoStruxure Machine Expert request from every device is rejected, including those from the UDP or TCP connection. Therefore, no connection is possible on Ethernet from a PC with EcoStruxure Machine Expert, from an HMI target that tries to exchange variables with this controller from Controller Assistant.	Active
Modbus Server	This parameter deactivates the Modbus server of the controller. When deactivated, every Modbus request to the controller is ignored.	Inactive
SNMP protocol	This parameter deactivates the SNMP server of the controller. When deactivated, SNMP requests are ignored.	Inactive
Web Server	This parameter deactivates the web server of the controller. When deactivated, HTTP requests to the controller web server are ignored.	Active
WebVisualisation protocol	This parameter deactivates the Web visualization pages of the controller. When deactivated, HTTP requests to the logic controller WebVisualisation protocol are ignored. You are prompted to enter login and password to access the web visualization.	Inactive

User Management

User management is handled in the same way as for Modicon M241 Logic Controllers, Modicon M251 Logic Controllers and Modicon M262 Logic/Motion Controllers.

Cloning the User Rights

This cloning feature for Modicon LMC058 Motion Controller and Modicon M258 Logic Controller is similar to the cloning feature for the Modicon M241 Logic Controller, Modicon M251 Logic Controller and Modicon M262 Logic/Motion

Controller, except the cloning has to be done using USB as opposed to using an SD card.

Hardening: Modicon M218 Logic Controller

M218 Security

The Modicon M218 Logic Controller is programmed in EcoStruxure Machine Expert.

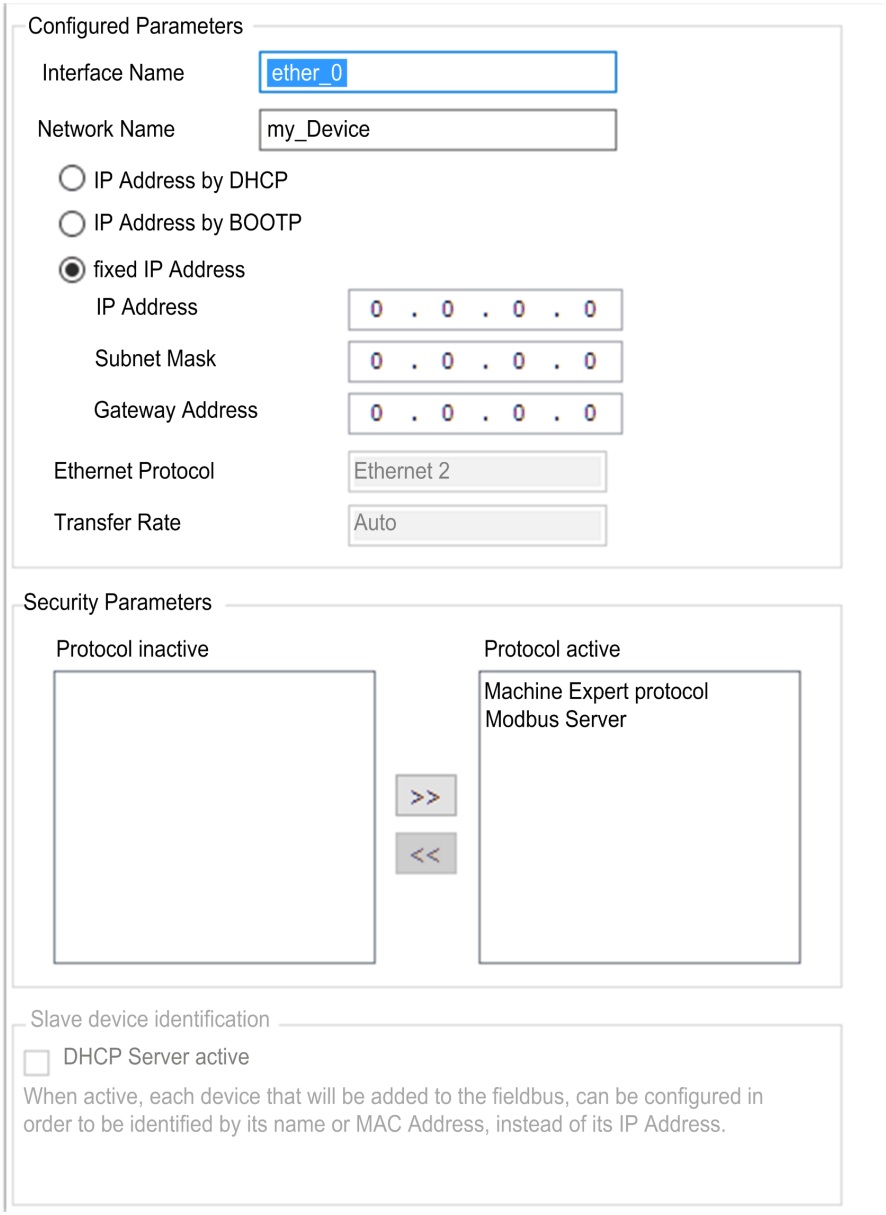
The Modicon M218 Logic Controller platform allows you to enhance cybersecurity by the following methods:

- Disable unused services (for example FTP)
- Network configuration

Network Configuration

The network configuration is done in EcoStruxure Machine Expert in the **Ethernet Services** tab.

Disable **Modbus communication**, if it is not used.



Services Configuration

The Modicon M218 Logic Controller has limited architecture and is not using the user rights given by EcoStruxure Machine Expert.

Security Parameters	Description	Default settings
Machine Expert protocol	This parameter deactivates the EcoStruxure Machine Expert protocol on Ethernet interfaces. When deactivated, every EcoStruxure Machine Expert request from every device is rejected, including those from the UDP or TCP connection. Therefore, no connection is possible on Ethernet from a PC with EcoStruxure Machine Expert, from a XBT target that tries to exchange variables with this controller from an OPC server or from Controller Assistant.	Active
Modbus Server	This parameter deactivates the Modbus server of the controller. When deactivated, every Modbus request to the controller is ignored.	Active

Refer to the Schneider Electric Cybersecurity Best Practices.

Firewall Configuration

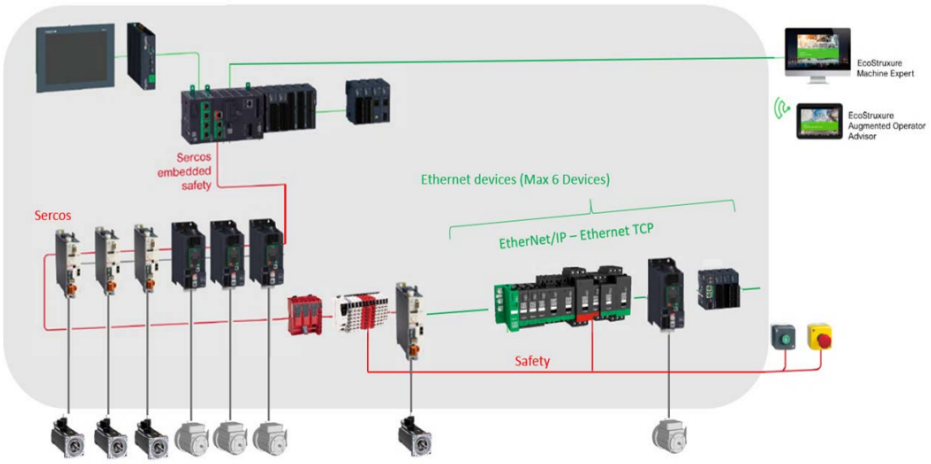
Modicon M218 Logic Controllers do not provide an integrated firewall. Therefore, an external firewall, such as the ConneXium Tofino firewall from Schneider Electric, must be applied.

Hardening: HMISCU

Typical Architecture

HMISCU can be plugged to the controllers and read and access data.

The following graphic shows the typical HMI architecture:



- Software configuration and programming of HMISCU is done in EcoStruxure Machine Expert.
- HMI portion is done using Vijeo Designer.

HMISCU Security

HMISCU security is handled by Vijeo Designer. Vijeo Designer provides user rights configuration and security settings for HMISCU.

EcoStruxure Machine Expert can enhance cybersecurity settings for HMI by configuring symbol configuration access rights for HMI.

Vijeo Designer is the software tool to create the application for the Magelis HMI panels. Vijeo Designer security features protect projects, panels, parts, Data Manager, and other areas from unauthorized users accessing them. Log in with your user name and / or password to access secured areas or to perform secured actions. You can access different areas, depending on your security level.

The table lists the security features which are provided by Vijeo Designer:

Security feature	Protection area
Target Security	Helps prevent an unauthorized user from logging in to a target and from accessing secured panels, popup windows, function keys, and parts on target machines.
Download Security	Helps prevent an unauthorized user from downloading projects to a secured target machine. Secured targets require users to enter in their user name and password in order for download and installation to proceed.
Data Manager Security	Helps prevent an unauthorized user from using the Command Line or the Data Manager to transfer run-time data to and from the target machine.
Web Gate / Web Server Security(1)	Helps prevent an unauthorized user from using Web Gate to access a target machine
Vijeo Design'Air and Vijeo Design'Air Plus Security(1)	Helps prevent unauthorized access to the Vijeo Design'Air server by requiring Vijeo Design'Air client to provide authentication at login.
(1) Security can be enabled only if the feature is enabled for the target at all.	

The configuration of the user management and the security features in Vijeo Designer are performed in three steps:

1. Enable the security features you want to apply for the target
2. Create user groups and assign access rights for each security feature, if enabled, to the single groups.
3. Create users and assign them to the appropriate user group. The user obtains the access rights from the group he is assigned.

The following table lists the security features which have been configured:

Security feature	Configuration
Target Security	**Use Security** has been selected. Further setting for the Target Security like **Security Mode**, **Logout Behavior**, **Secured Object Behavior**, and **Password Management** are available.
Download Security	**Use Security** has been selected. Prevention of unauthorized download using an USB key can be enabled separately.
Data Manager Security	**Deny Access** has been selected. External access to the file system of the target is not provided in the sample application.
Web Gate / Web Server Security(1)	Not configured, because these features are not enabled under the **Remote Access** settings for the target.
Vijeo Design'Air and Vijeo Design'Air Plus Security(1)	
(1) Security can be enabled only if the feature is enabled for the target at all.	

For more details on Vijeo Designer configuration, refer to the online help.

Services Configuration

By default, Vijeo Designer disables all Ethernet or USB protocols at first power-on, while at the same time, presents an advisory message indicating the security risk

presented by using these unsecure communications means. Once you have accepted this safety message, the communication means are available.

Unsecure protocols, for example HTTP, FTP or Modbus, can be enabled again by you if necessary.

Security Mode

After the **Target Security** has been enabled and the **User Groups** have been created, the parameter **Security Level** for panels, popup windows, or parts in your application is available. For each of these items you can select the **Security Level** which is needed to have access to it.

Depending on the **Target Security**, settings for **Security Mode**, the selected **Security Level** for the item allows access also for users from other groups.

In the sample application, the **Security Mode** is set to **Level Based**. By this setting the selected **Security Level** of the item equals the least level needed for access.

Feature	Description
Logout Behavior	Allows to select an inactivity time-out for automatic logout. Allows to select what shall happen on logout, depending on whether the current panel is secured or not.
Secured Object Behavior	Allows to select the display of secured items and you can select what shall happen when trying to access a secured item with insufficient privilege.
Password Management	An activated **Password Management** enables you to: • Configure the validity period of a password • Select the number of maximum attempts to login with an incorrect password before the user account becomes locked • Select parameter which needs to be respected for the creation of a password

NOTE:

- When the security features are enabled you should provide a secured page on the touch panel which provides access to the user management. The access to this user management must require the highest **Security Level**. Only a very limited user group should be equipped with this **Security Level**.
- Do not provide user names to unauthorized or other unqualified personal. This helps to avoid locked user accounts when password management is configured.
- Provide a simple way to log out for the current user. In addition configure an inactivity time-out for automatic log out.
- Provide a clear indication in case a user is logged in, who owns higher privileges than required for normal machine operation.
- Disable unused features or services. Reducing the set of features reduces in consequence also the surface for attacks.

Hardening: HMI using EcoStruxure Operator Terminal Expert

Overview

EcoStruxure Operator Terminal Expert is a configuration software for Harmony ranges supporting gestures and intuitive user interfaces designs.

EcoStruxure Operator Terminal Expert – Security

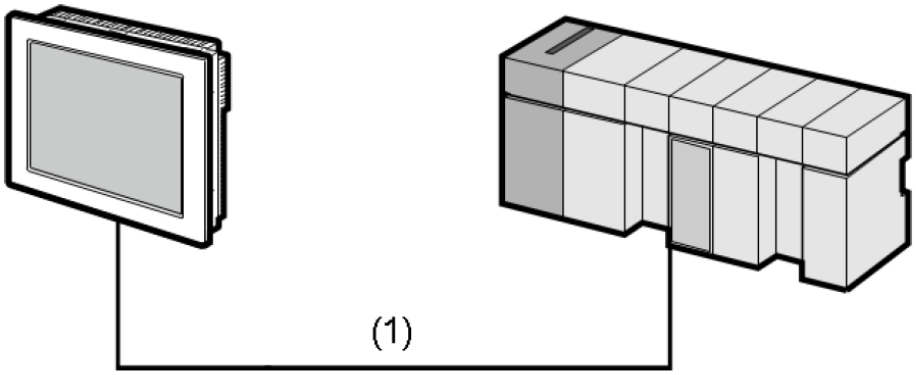
EcoStruxure Operator Terminal Expert provides security feature to secure objects from unauthorized access. Login with a valid user name and password to access secured objects. Auto-logout is supported.

EcoStruxure Operator Terminal Expert enables you to configure Harmony to use user rights and encryption with PacDrive LMC Eco, PacDrive LMC Pro/Pro2 and Modicon M262 Logic/Motion Controllers.

Harmony Configuration with Modicon M262 Logic/Motion Controller, LMC Eco and LMC Pro/Pro2

The HMI can be connected directly with the devices using an Ethernet cable.

The graphic is an example for the connection between Harmony and a controller:



(1) Ethernet cable by Schneider Electric 490 NTC 000

In EcoStruxure Machine Expert define the communication settings for the external equipment:

Step	Action
1	Start EcoStruxure Machine Expert and create a new project.
2	In the **View** menu, select **Navigators** > **Devices Tree**.
3	In the **Devices Tree**, double-click **MyController**.
4	Click **Controller selection**.
5	Right-click the device and select **Change device name**.
6	Enter the **Device name**

NOTE:

- When communicating with EcoStruxure Operator Terminal Expert, set the **Device name** for the external equipment. IP addresses cannot be used for communication.
- When the External Equipment uses the **UserManagement** function like LMC controllers or Modicon M262 Logic/Motion Controllers, the user has to put the login information in **Username** and **Password** under the driver property of EcoStruxure Operator Terminal Expert or hardware configuration for Target.
- When using the encrypted communication, select the **Encrypted communication** check box in either the driver's equipment properties in EcoStruxure Operator Terminal Expert, or in the hardware configuration.

For more details on the EcoStruxure Operator Terminal Expert, refer to the online documentation.

Hardening: Legacy Drives

General Information

In many cases, industrial control systems include legacy devices that are not equipped with sufficient device hardening features. In this case, an external device can be applied in combination with the installed end device to improve the hardening.

An external firewall, such as the ConneXium Tofino firewall from Schneider Electric, can be used to provide these features. Configure the firewall to use the same IP address as the internal device, so the combination of the two units appears as a single end device to the rest of the network.

The single combined unit can also take advantage of the firewall's ability to limit network traffic, restrict access to allow only data requests from specific originating devices and even limit access to specific data register areas or use of specific function codes.

Drives are used behind a controller. In order to enhance protection between the controller and drives, packet routing between controller and drives have been disabled by default. For information on how to activate the packet routing, refer to the programming guide of the respective controller.

Hardening: Modicon M100 Logic Controller, Modicon M200 Logic Controller and Modicon M221 Logic Controller

General Information

The Modicon M100 Logic Controller, Modicon M200 Logic Controller and Modicon M221 Logic Controller are controllers with limited architecture and are programmed using EcoStruxure Machine Expert - Basic. These controllers are using standard Modbus TCP (UMAS) and EIP protocols to communicate. As these protocols are not secured by default, several mitigations can be applied to enhance cybersecurity on these controllers:

- Ensure the network environment has been secured.
- Ensure project encryption and application protection on each project as described in EcoStruxure Machine Expert - Basic chapter (refer to Hardening EcoStruxure Machine Expert - Basic, page 22).
- Observe the Schneider Electric Best Practices (https://www.se.com/us/en/download/document/CS-Best-Practices-2019-340/)

To help maximize security, these controllers must be installed behind a firewall with proper configured access control on the IPs and ports.

Monitoring on the controller is reinforced by the audit log which records issues from the controller.

You can use a Modicon M262 Logic/Motion Controller with an embedded cybersecurity mechanism, and apply the hardening process defined. Refer to Hardening Modicon M262 Logic/Motion Controller and TMSES4, page 37.

Glossary

B

broadcast:

A message sent to all devices in a broadcast domain.

C

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.

D

DMZ:

In computer networking, a De-Militarized Zone (DMZ) is a special local network configuration designed to improve security by segregating computers on each side of a firewall.

F

FDR:

(fast device replacement) A service allows a central device (the FDR server) to store configuration parameters for remote devices on the network. If a remote device requires replacement, the server automatically passes the stored configuration parameters on to a replacement device so that it can operate using the same configuration parameters as the replaced device. The replacement is accomplished without manually configuring the parameters

The FDR service should be used for all on the automation network that support it. It reduces the need for service personnel to keep configuration records on hand, and it reduces the chance of human error in entering the new configuration.
.

forwarding:

Process whereby an Ethernet switch or bridge reads the contents of a packet and passes the packet on to the appropriate attached segment.

G

gateway:

A combination of hardware and software that interconnects otherwise incompatible networks or networking devices. Gateways include packet assembler/disassembler and protocol converters. Gateways operate at layers 5, 6, and 7—the session, presentation, and application layers, respectively—of the OSI model.

P

packet:

A series of bits containing data and control information, formatted for transmission from one node to another. It includes a header with a start frame, the source and destination addresses, control data, the message itself, and a trailer with error control data (called the frame check sequence).

S

SNMP:

(simple network management protocol) Standard Internet protocol used to manage Ethernet network devices such as switches and routers. A 3-part protocol comprising: structure of management information (SMI), management information base (MIB) and the protocol itself. The SMI and MIB define and store the set of managed entities; SNMP itself conveys information to and from these entities.

A TCP/IP host running an SNMP application can query other nodes for network related statistics and detected error conditions. The other hosts, which provide SNMP agents, respond to these queries and allow a single host to gather network statistics from many other network nodes.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

EIO0000004242.00