Safety meets security

How to set up your machines safely

The progressive digitalization and networking of machines and systems is leading to an increasing fusion of safety and security. In addition, crime on the Internet is becoming an ever-increasing threat potential for companies. A large number of companies have already registered cyberattacks with production downtimes. Cybercrime is therefore considered to be one of the biggest business risks. "Triton" is the first prominent case that has overcome security-related mechanisms in an automation system through a cyberattack.

Regulatory developments in the European Union are currently being pursued to address this threat potential. In particular, the new Machinery Regulation (MVO), the Cyber Resilience Act, and the NIS2 are worth mentioning here.

The Machinery Regulation, which will be applied from January 20, 2027, onwards, specifies EU-wide protection objectives for the design and construction of machinery. It takes new risks into consideration and adapts the security specifications to the current state of technological progress. The Cyber Resilience Act, on the other hand, protects consumers and companies that purchase or use digital products and software. As part of this, binding cybersecurity standards have been defined for manufacturers and dealers, and a CE marking has been specified for cybersecure products that are made available in the European Economic Area.

In this context, it is important to recognize that safety and security can no longer be considered in isolation. They are complementary aspects of machine and system security. The security of machines and systems depends both on physical protective measures (safety) and on measures to prevent cyberthreats (security). A holistic approach that takes both aspects into consideration and uses synergies is promoted by the new Machinery Regulation and the Cyber Resilience Act.

This document describes such a holistic approach in broad terms and is intended to serve as an initial orientation.

Contents

Machinery Regulation

In particular, Annex III - 1.1.9 of the new MVO, which comes into force on January 20, 2027, deals specifically with protection against corruption. This section specifies that no dangerous situations may arise as a result of the connection or communication with “another device”.

In practice, this means that machines and systems must be designed and constructed such that they can communicate with other devices and networks without this causing any security risks. This includes both physical connections (e.g., via cable) and wireless connections (e.g., via WLAN or Bluetooth).

The software for operating the machine or system must also be designed to protect it against manipulation. This can be achieved through various measures, such as the use of encryption technologies and the implementation of security protocols. This also includes regular updates of the software to counter already known security vulnerabilities.

It is important to note that these requirements do not only apply to manufacturers of machines and safety components. They also apply to the operators who are responsible for maintaining and updating the systems.

Cyber Resilience Act

The Cyber Resilience Act (CRA) is a significant piece of legislation that establishes cybersecurity regulations for manufacturers of products with “digital components”. It therefore applies to all products that are directly or indirectly connected to another device or network. This includes both hardware and software. However, some exceptions must be taken into consideration, such as open source software and services that are already covered by existing regulations.

The protection must extend throughout the entire product lifecycle – from planning, through design and development, right through to product maintenance. These obligations apply to all stages of the value-added chain.

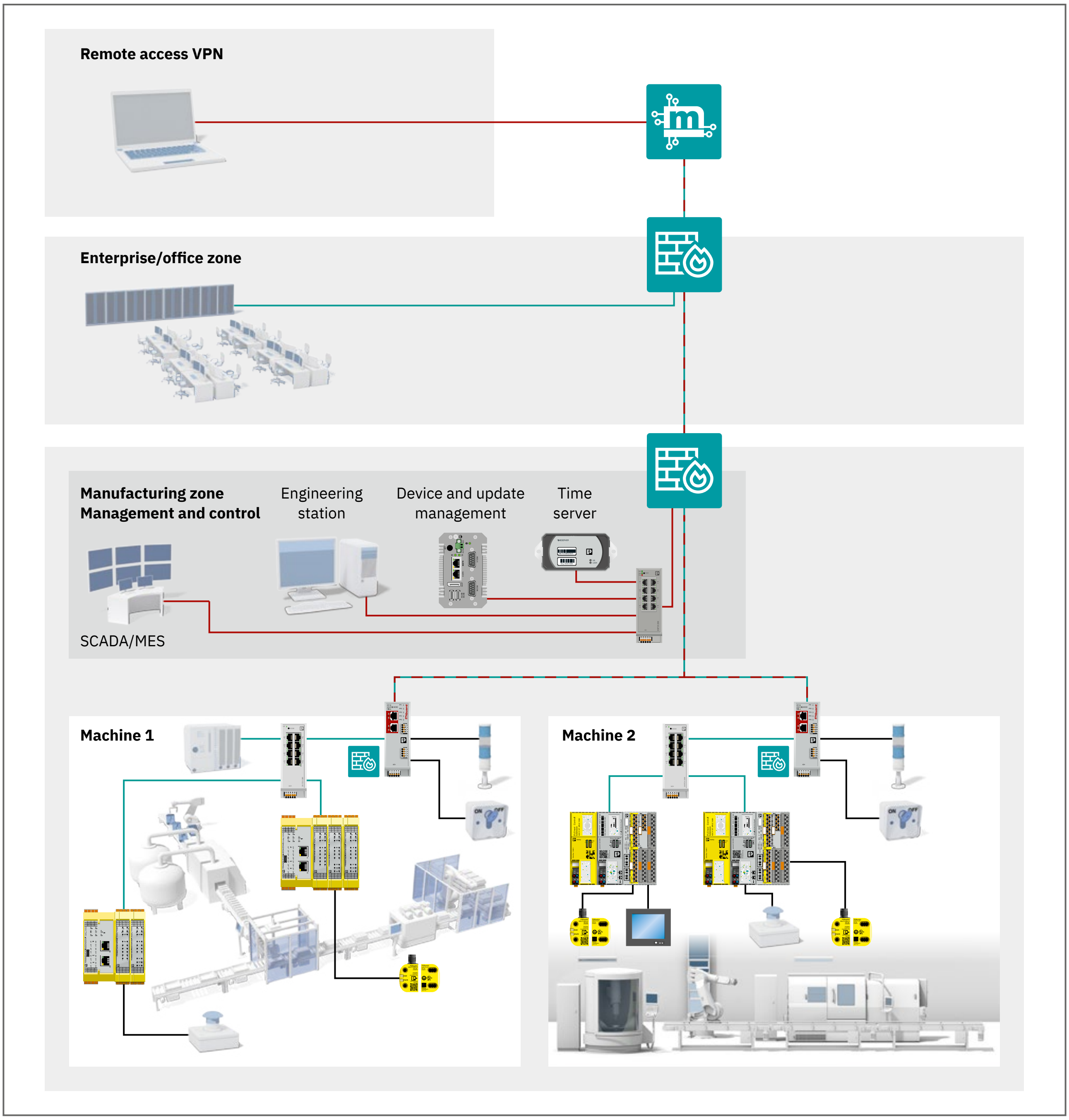
The CRA affects a wide range of products. As of the entry into force of the CRA, these products must indicate through the CE marking that they comply with the protection objectives of this legislation. This then enables the users of the products to derive further measures to improve cybersecurity.

The regulation was announced in the EU Cybersecurity Strategy 2020 and supplements other legal provisions in this area, in particular the NIS2 framework. At present, it can be assumed that the CRA will be applied in the course of 2027.

Reference architecture “Safety meets security”

In the following example, a reference architecture from the point of view of an operator describes how a safety application can be created to be “secure”.

The reference architecture shown in the figure is based on the defense-in-depth concept with various security levels and corresponding transitions (zones/conduits). The blue and green connections represent security mechanisms for



Safe setup of safety applications in a reference architecture

Ethernet TCP/IP communication (e.g., TLS/HTTPS). Red connections represent virtual private network connections (VPNs). The various zones of the reference architecture are described in more detail below.

Perimeter security – the external zone (remote access VPN)

The external zone regulates access protection for the company network by means of the following measures:

- Physical isolation
- Digital isolation through network segmentation
- Logic-driven access controls
- Use of specially configured firewalls
- VPN or other security measures for remote access
- Documentation of all remote access points

Network security – (enterprise/office zone)

In the enterprise/office zone, the focus is on protecting the plant network. This takes into account both the corporate network zone and the service management zone, which is considered a demilitarized zone (DMZ).

Potential security measures include:

- Identification of all network devices and hosts
- Analysis of protocols/data traffic
- Checking wireless communication/data traffic
- Analysis of switch/router configurations

Measures in the DMZ:

- Operating-system check for vulnerabilities
- Operating-system patch management
- Preventing the use of USB and removable media
- Restriction of connection of unknown devices

System integrity – (manufacturing zone)

Potential measures for SCADA applications in the manufacturing zone include:

- Monitoring the network for plain text transmission and the use of encryption
- Ensuring the use of individual user accounts
- Restricted access to the desktop

In addition, a record of data traffic for Ethernet connections should be provided for subnetworks at the control level of machines and production lines.

Ethernet devices should also be subjected to a test for vulnerabilities. This includes replacing the manufacturer's default passwords. Network segmentation between machines is also recommended to restrict unauthorized access as far as possible.

The two safety applications within the manufacturing zone will be taken into consideration in more detail in the following.

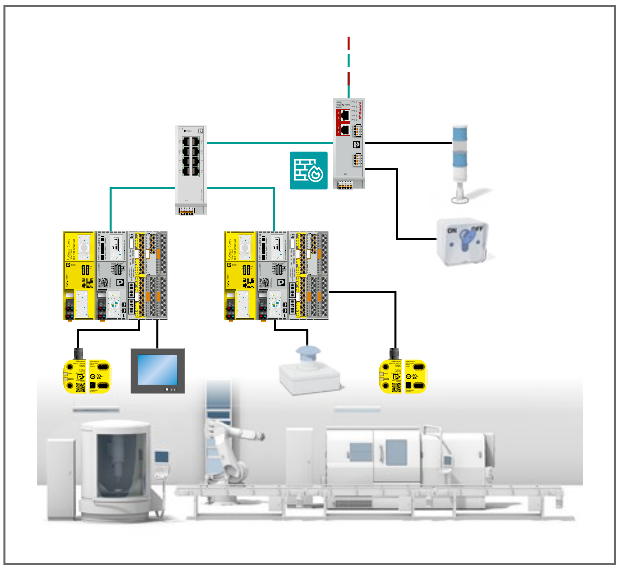
The main approach to overcoming threat potentials lies in the detection and prevention of unauthorized access from outside the "manufacturing zone" so that no safety-critical changes can be made.

Security-related changes may include:

- Not executing emergency stop commands
- Bypassing safety equipment
- Impermissible change of parameters such as watchdog times

Furthermore, network segmentation should prevent unauthorized access from machine 1 to machine 2 (and vice versa).

Example 1: production line with Phoenix Contact SPLC safety controller in conjunction with PLCnext Control and security router (mGuard)



In the example shown, the production line (machine 1) consists of various machine modules that are equipped with one or more safety controllers (SPLC safety controller in conjunction with PLCnext Control).

Within the production line, the safety controllers can communicate with one another in a safety-oriented way. To protect the zone, an "mGuard" is used to monitor the data traffic between the manufacturing zone and the zones above it.

With comprehensive security functions, the mGuard security routers protect against unauthorized access by people or malware. At the same time, the proven mGuard security technology enables the control and safeguarding of communication within the manufacturing zone.

A secure VPN connection can be established to the mGuard security router to allow access to the machine cell from outside. Within this connection, accesses can be restricted by a firewall in the VPN. For full control over the establishment of such a connection, it can be controlled via a key switch that is only accessible to authorized personnel on site.
In addition, the PLCnext Technology platform also provides various security measures at device level (including security logging, boot integrity check, password complexity rules, specialized user roles, zone and denial-of-service protection, etc.)[1]. The following options are available as additional security measures for functional safety:

- Additional user roles (SafetyEngineer and SafetyFirmware updater)
- Protected file system area with special access rights
- PROFINET® / PROFIsafe®

For further information on the mGuard security routers, visit:
phoenixcontact.com/mguard

[1] The security profile must be activated to use PLCnext Technology as an IEC 62443-4-1/4-2-certified component.

In addition, general measures for functional safety are also supported:

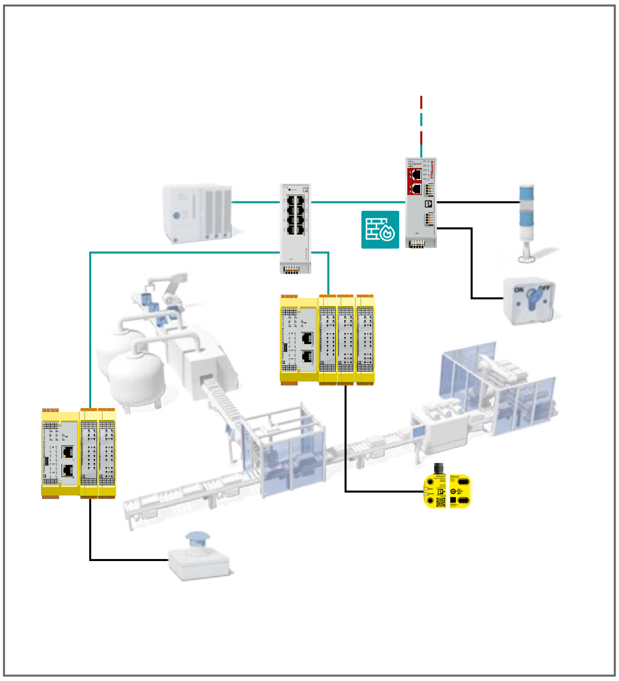
- Left-alignable SPLC 1000 safety-related controller
- Double password protection
- Safety PLC password for access to the safety controller
- Project password for the safety-related processing of the project
- Safety protocols can be accessed via PLCnext Engineer; refer to the PLCnext Engineer online help

For further information, visit the PLCnext Technology Info Center https://security.plcnext.help/se/About/Home.htm

Example 2: production line with configurable PSRmodular and mGuard safety relay module

In the second example, the production line consists of various machine modules with one or more configurable safety devices (PSRmodular).

Within this zone, the configurable safety relay modules can communicate with each other in a non-safety-related way via a higher-level controller. To protect the zone, an mGuard security router is also used here to monitor the data traffic between the manufacturing zone and the zones above it.



Explanation of key terms

The following explains the most important terms and functions in protecting machines and systems as well as the components used in them.

1) Firewall/syslog

A "firewall" is a security solution that protects a network against unwanted data traffic. To do so, a firewall blocks malware, for example, based on preconfigured rules. The basic idea here is to authenticate communication from "insecure" environments before it is forwarded to a protected environment.

Syslog stands for "System Logging Protocol" and describes a standardized message format for communicating with a logging server. These log messages include, for example, a time stamp, IP address, and other event information.

To create the firewall rule sets, the communication relationships between the machine and the production network are determined and documented accordingly.

2) VPN

VPN stands for “Virtual Private Network” and enables secure communication from various end devices that are not physically connected to each other. For this purpose, an encrypted connection is established via the public Internet (“VPN tunnel”).

When using the mGuard, the basic configuration is created via the mGuard Secure Cloud and written to the devices via an SD card.

3) Device management

Device management enables devices to be inventoried, monitored, maintained, and secured. In addition, it can be used to distribute software and operating system updates, to manage configurations, and to enforce security policies. Device management helps to keep a company’s IT infrastructure secure and up-to-date.

4) DMZ

A DMZ (Demilitarized Zone) is a special area of a network that serves as a buffer. This area is located between the internal network of an organization and an insecure external network, such as the Internet.

The DMZ provides an additional protective layer for the internal network. If an attacker is able to compromise a system in the DMZ, they do not yet have access to the internal network. They would have to overcome other security measures, such as an internal firewall, before being able to access sensitive data. In this way, the DMZ contributes to the security of the network.

The DMZ port of the mGuard can be used to implement secure local service access. The service technicians connect to the laptop at the DMZ port and authorize themselves on the mGuard. If authentication is successful, it grants access, for example, and blocks communication to the higher-level network (distribution network).

5) SNMP v3

The SNMPv3 protocol is used to monitor all installed firewalls of the production sites worldwide with a network monitoring tool. Monitoring can be implemented via the internal network.

Since most machines are PROFINET networks, Phoenix Contact recommends using PROFINET switches of Conformance Class B, such as the FL SWITCH 2000 series products. In order to have more diagnostic options on site and via remote access, the switches should support the following functions:

- Port statistics
- Event table
- Syslog
- Snapshot tools
- CRC monitoring
- Port counter
- Port capacity

For more information on the managed switches from Phoenix Contact here:
phoenixcontact.com/industrialethernet

Relevant standards and links

Under "Harmonized Standards", the European Commission's website lists all currently applicable CE directives and regulations related to the MVO and the CRA.

https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en

Further information

Are you looking for a powerful partner for the subject of "Safety meets security"? With products, training courses, and TÜV-certified experts, Phoenix Contact will help you meet the requirements of the new Machinery Regulation and the Cyber Resilience Act. We'll get you fit for the safety of people and machines.

Find out more about our offers for functional safety at:
phoenixcontact.com/functionalsafety

#FitForSafety

phoenixcontact.com

3011819006