

# Cybersecurity consideration for intelligent electrical systems



Markus Wünsche  
Frank Sanjay

*1st edition*

**EATON**

*Powering Business Worldwide*

# Cybersecurity considerations for intelligent electrical systems

## Table of contents

### Cybersecurity considerations for intelligent electrical systems

#### Purpose

Introduction.....	3
Connectivity – why do we need to address cybersecurity for industrial control systems (ICS)? .....	3
Cybersecurity threat vectors .....	4
The typical industrial network.....	4
Defence in depth.....	5
Addressing threat vectors via layers of defense in depth.....	6
Policies, procedures, standards and guidelines .....	6
Continuous assessment and security training .....	6
Physical security .....	6
Network security .....	6
Endpoint protection.....	7
Demilitarized zones (DMZ).....	7
Intrusion detection and prevention systems (IDPS).....	7
Host security .....	7
ICS Hardening .....	7
Application security.....	8
Understanding an ICS network.....	8
Log and event management.....	9
Patch management planning and procedures.....	9
Vulnerability disclosure.....	9
Secure decommissioning / zeroization.....	10
Security right from the start – Eaton’s cybersecurity approach .....	10
Organizational cybersecurity measures .....	10
Risk analysis and design.....	10
Implementation .....	10
Verification and validation.....	10
Cybersecurity measures during operation and maintenance .....	11
Cybersecurity according to international standards .....	11
Internationally strong: ul 2900 and iec 62443.....	12
Secure products with certificate.....	12
Conclusion.....	13
Terms and definitions.....	14
Acronyms .....	14
References.....	14

## Author:



**Markus Wünsche**

**B.Sc.**

Engineering Manager  
Processes Methods  
Tools, Functional Safety  
and Cybersecurity

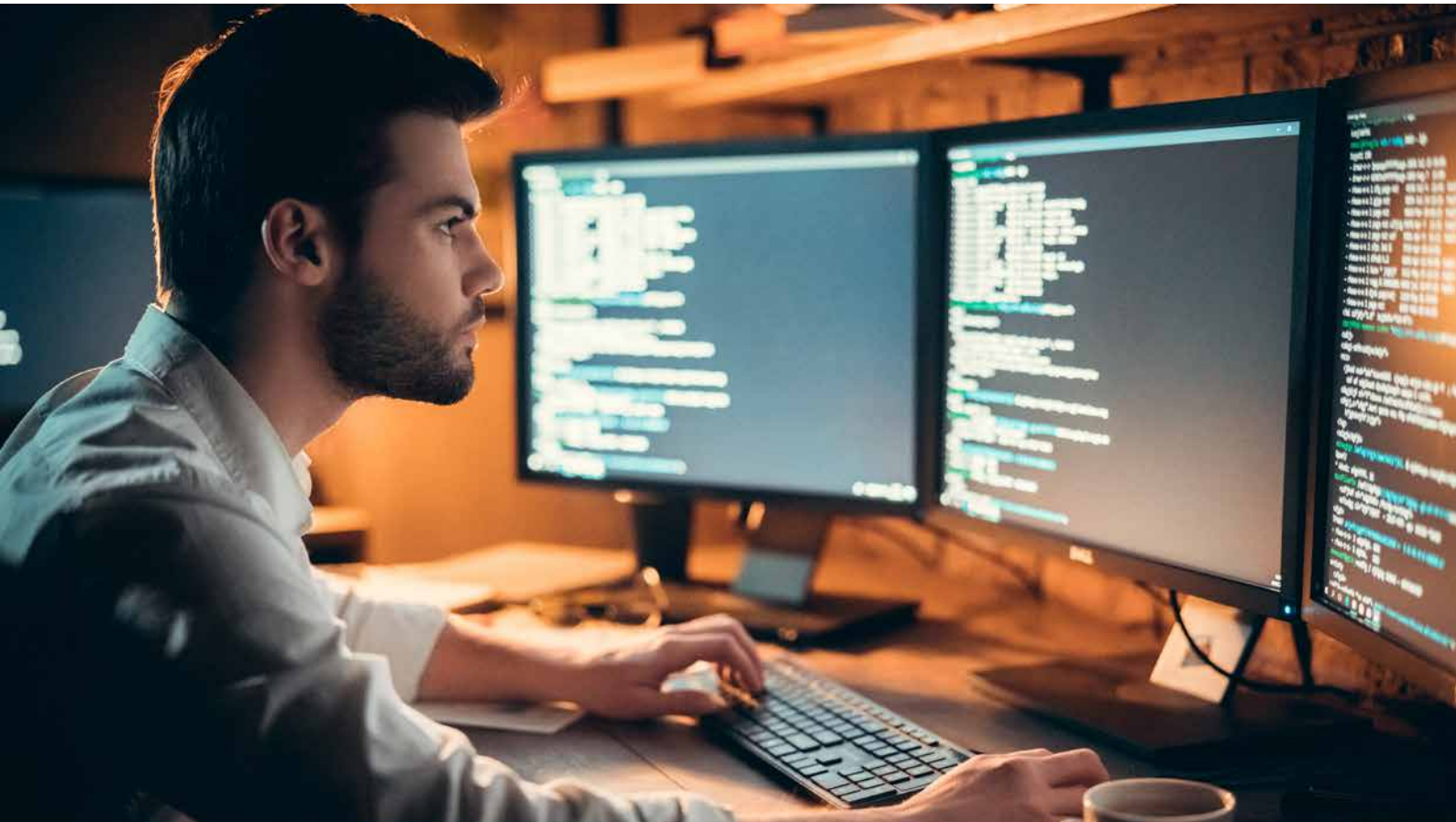
Industrial Controls  
& Protection Division  
Eaton Industries GmbH



**Frank Sanjay**

**M.Sc (FS), GREM,  
EnCE, ITIL v3**

Manager,  
Product Cybersecurity  
Center of Excellence



## Introduction

Cyberattacks on companies, energy suppliers and public authorities are today part of everyday life. Whether it is a matter of stealing intellectual property or blocking operations, the tools and techniques used for unauthorized network access are becoming increasingly sophisticated. Critical infrastructures and industrial systems are now as much affected by cyber threats as office networks. Hackers exploit weak points in the design and thus put entire industrial plants out of operation or, in the worst case, even endanger the nationwide energy supply. IBM X-Force data indicates that in 2019 Operational technology (OT) targeting increased 2000 percent year over year. In fact, the number of attacks on Industrial Control Systems (ICS) and OT infrastructure was greater than any of the prior three years.<sup>1)</sup>

In order to protect ICS and OT from these attacks, a holistic approach is required. A high level of cybersecurity can only be achieved if both the company's own processes are secure and the products used in the plants have a high level of security. This also requires secure processes in development, production and sales of the products used. The whitepaper describes the necessary steps within the company as well as the measures required by the manufacturer of the electronic components used. The latter is based on Eaton's proven comprehensive approach to protecting its products and solutions throughout the entire product development lifecycle.

### Connectivity – why do we need to address cybersecurity for industrial control systems (ICS)?

There is increasing concern regarding cybersecurity across industries, where companies are steadily integrating field devices into enterprise-wide information systems. Cyber-crime occurs in discrete manufacturing and industrial process environments, a wide range of general and specific purpose commercial buildings and even utility networks. Traditionally,

electrical systems were controlled through serial devices connected to computers via dedicated transceivers with proprietary protocols. In contrast, control systems today are increasingly connected to more extensive enterprise networks, which can expose these systems to similar vulnerabilities that are typically found in computers systems.

Thus, when considering cybersecurity for ICS, both IT (Information Technology) from the perspective of the company networks, and OT (Operational Technology) from the perspective of the field devices must be considered. IT has its roots in the classic business environment and describes the management of information. This includes different types of servers (e. g. web and mail servers) as well as management systems, client systems and also mobile devices including the application software and the related network infrastructure. The highest protection goals in IT usually are confidentiality and authenticity.

In contrast, OT gives top priority to the availability and integrity of the system when protecting against cyberattacks. This is because OT manages and influences physical processes, examples for OT systems as part of industrial control systems, are PLCs, sensors and actors like a drive or robotic arm. The protection of the OT is intended to prevent negative impact on the related physical processes up to a production stop and at the same time ensure safe operation.

IT and OT also show a big difference in the life cycle of the hardware used: The life cycle of IT hardware is about three years - OT devices, on the other hand, are used for up to 30 years and more.

With the increasing connectivity related to industrial processes and the growing implementation of the Industry 4.0 concept, IT and OT are growing even closer together. The Cyber-Physical Systems realized in smart factories are combining information and software-related systems with mechanical and electronic

<sup>1)</sup> IBM X-Force Threat Intelligence Index 2020

components. To a large extent, OT devices are connected to each other, to critical IT-related systems and even directly to external networks.

To ensure that such networked systems are protected against cyberattacks, organizational and process-related measures must be combined with technical protection measures. This is the only way to protect networks and industrial control systems against malicious attacks.

Threats and measures are organized in relation to the security objectives and must be seen in the context of the type and purpose of the system as also the environment.

- The most important security objectives for industrial control systems are usually **availability, integrity and authenticity**.
- The focus of an IT network is to ensure the **confidentiality** and the **integrity** of the data using rigorous access control and data encryption.
- Enterprise security protects the data residing in the servers from attack.
- Control system security protects the ability of the facility to safely and securely operate, regardless of what may occur across the rest of the network.

**Cybersecurity threat vectors**

Cybersecurity threat vectors are paths or tools that an adversary can use to maliciously gain access to a device or control network in order to deliver a malicious attack. Figure 1 below shows examples of attack vectors on a network that might otherwise seem secure and the types of paths that could be used to attack the network are listed below:

- External users accessing the network through the internet.
- Infected laptops elsewhere that can access the network behind the firewall.
- Infected USB keys and PLC logic programs.
- Compromised supply chains, where adversaries can introduce backdoors through malicious firmware and configurations.

- Internal users with inadequate knowledge, training of cyber threats.
- Internal users who have been compromised through social engineering.

As the achievement of a high level of cybersecurity in the automation context requires a holistic approach in the following will be given some background knowledge regarding industrial networks also there will be described which aspects the operators of ICS have to consider to secure the own environment. Then there will be a description of the Eaton secure development lifecycle to achieve a high level of product cybersecurity under consideration of world leading ICS related cybersecurity standards.

**The typical industrial network**

The basis of any defense strategy for ICS is an understanding of the basic structure of industrial networks.

In the past, ICS were physically decoupled from other IT systems and networks (air gap) and thus protected from external attacks.

Therefore, IT security was of secondary importance in the selection and development of mostly proprietary software and protocols.

Industrial networks can be roughly divided into three layers or levels: The consideration starts right at the top with the company-wide operational organization. This includes ERP systems (Enterprise Resource Planning) and office workstations. This layer is followed by the upper control level, which includes the plant-related IT systems. The components located here take over the functions of plant or operational management - this is where the Manufacturing Execution Systems are located, for example. Finally, the lowest layer consists of the IT and OT systems, which have a direct influence on the execution and control of the physical process as they are controlling and monitoring the various automated functions at field level. This includes the components directly involved in the industrial process (e. g. PLCs, limit switches,

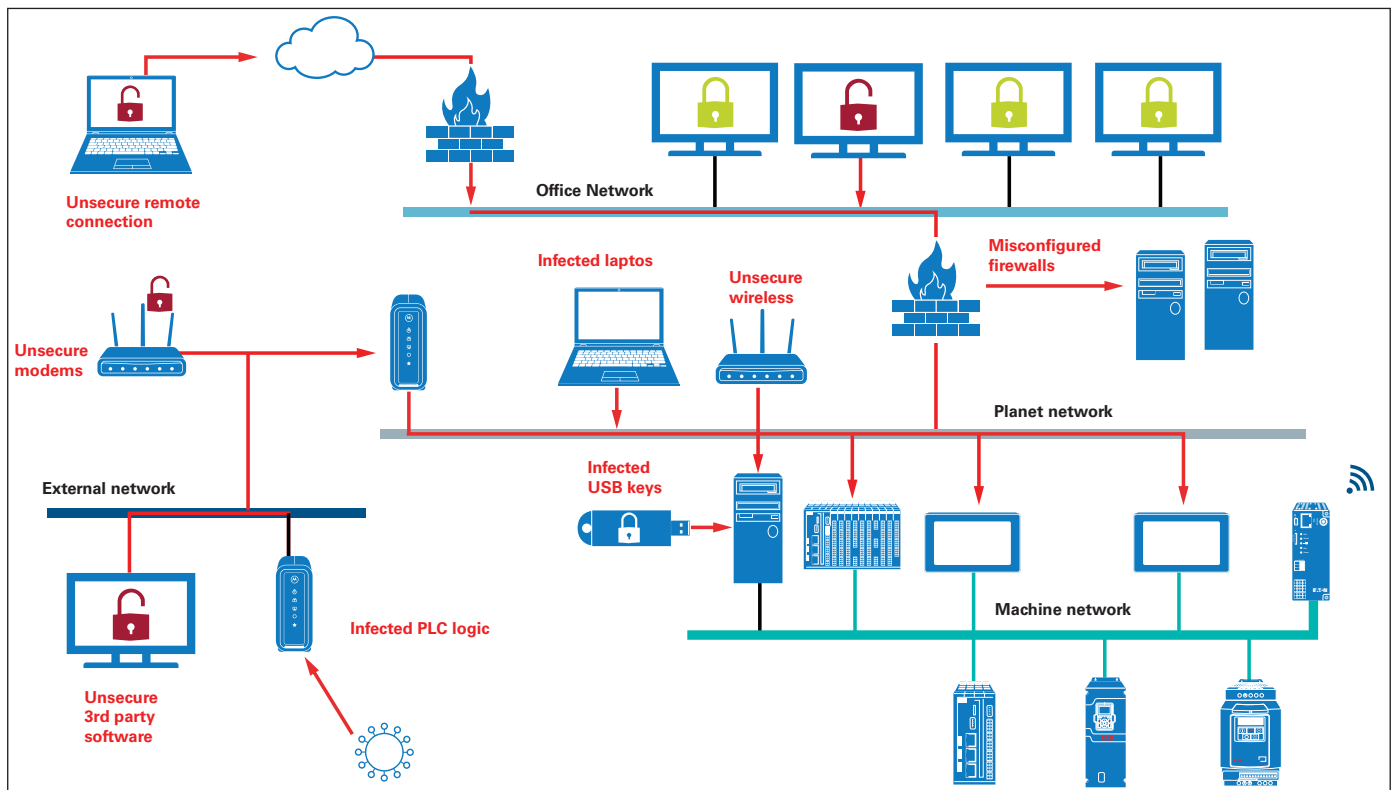


Figure 1: Paths to the control Network

transducers, valves, actuators and motors).

With the integration of IT systems from the office environment and the increasing connectivity in ICS even beyond network boundaries (e.g. into a corporate network), the classic layers of an industrial network are increasingly merging - or even disappearing completely. As a result, these systems are now exposed to similar threats as systems from classic corporate IT. This convergence of IT and OT is accelerated even further by the increasing use of cloud-based technologies. First applications already allow a direct connection of cloud-based systems to OT technologies in the field, for example via mobile communication technologies. As a result, company or plant-network-related security measures will have less or no effect. Suddenly, systems which were considered highly protected become exposed due to the addition of such a system to the OT network. To reduce this risk, the OT devices connected to the cloud must additionally meet high cybersecurity requirements.

An effective defense strategy protects Critical Infrastructures against attacks that are ever evolving in sophistication. It is required to have a strategy that can counter the attacks effectively. This enables the products to be able to defend themselves against such attacks for a longer time. Simple approaches which are tactical in nature might render the defenses useless in a short time and might expose such Critical Infrastructure to malicious actors. This paper discusses some approaches that enable comprehensive protection.

**Defense in depth**

‘Defense in depth’ is a strategy of integrating technology, people and operations capabilities and counter-measures for mitigating risks, in a layered or stepwise manner. Defense in depth is responsibility of product supplier, system integrator and customer in terms of achieving a secure environment for installation, operation and maintenance. The diagram below visualizes a layered approach.

While there are differences between traditional IT systems and ICS, the fundamental concept of ‘defense in depth’ is applicable to both.

The different layers in defense in depth are policy and procedures, physical security, network security, host security and application security. The aforementioned five layers when followed ensure secure operations of a system or a device.

To understand it better, take an example of an Engineering Work Station (EWS) in a supervisory control center of an industrial facility –

- Policies and procedures will define rules and procedures for secure usage.
- Physical security will prevent unauthorized persons from accessing the EWS.
- Network security will limit access on the network only to authorized individual.
- Host security will ensure attack surface reduction via application whitelisting and protection agents to highlight and protect from malicious activity.
- Application and data Security as it also mentioned in the diagram will ensure the installed application is secure and free from any known vulnerabilities

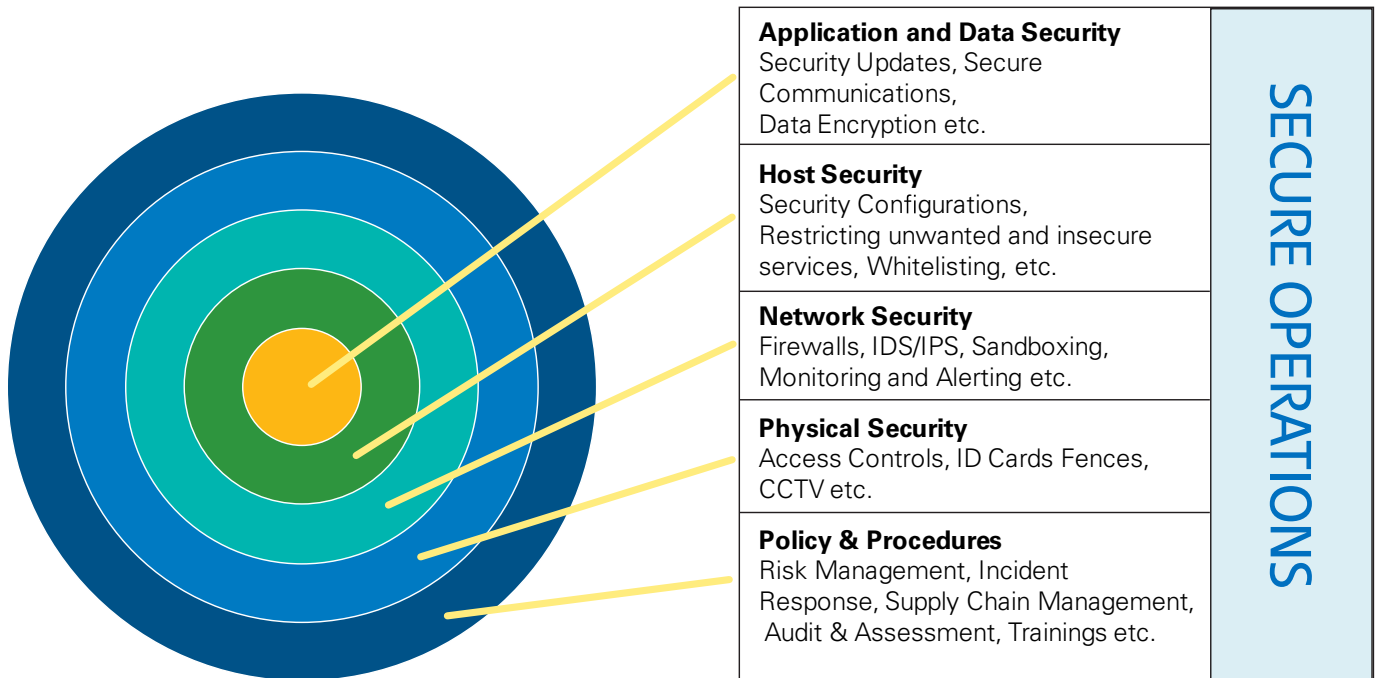


Figure 2: Defense in Depth – Secure Operations

## Addressing threat vectors via layers of defense in depth

### Policies, procedures, standards and guidelines

For the defense in depth strategy to succeed, there must be well-documented and continuously reviewed policies, procedures, standards and guidelines.

- **Policies** provide procedures or actions that must be carried out to meet objectives, and address the who, what and why
- **Procedures** provide detailed steps to follow for operations and address the how, where and when
- **Standards** typically refer to specific hardware and software, and specify uniform use and implementation of specific technologies or parameters.
- **Guidelines** provide recommendations on a method to implement the policies, procedures and standards.

It is important to identify “Asset owners,” and develop policies and procedures for a cybersecurity program. These policies need to be practical and enforceable in order to be effective. Policies should also address access related issues, such as physical access, contractors, and vendors.

Existing (traditional) IT standards and policies may not apply (or have not been considered) for control systems. A gap analysis should be performed to determine which components are not covered (or not adequately covered) by existing policy. Relationships with existing policies and standards should be explicitly identified and new or supporting policies developed. It's important that industrial control system administrators have proper authorizations and full support of their management to implement policies that will help secure the ICS network.

Policies and procedures tie up the whole security management system. They address risk management, supply chain management, audits, training etc. It also helps organizations to comply with various Federal, State, and Industry regulations. Organizations should customize policies to suit their specific environment. Policies should be easy to understand and inform employees about their duties and expected actions.

It helps to educate employees about their importance in protection and proper usage of organization's sensitive data. It can start from choosing the right passwords, to providing guidelines for file transfers and data storage, which increases employee's overall awareness of security and how it can be strengthened.

Policies and procedures help in addressing multiple threats vectors like Compliance violation with various Federal, State, and Industry regulations, Improper usage, Unintentional errors, Phishing scams etc.

Following are some recommended cybersecurity policies but should not be limited to –

- **Password policy** to help and inform employees about using strong passwords.
- **Virus and malware protection policy** to detect, remove and repairs the side effects of viruses and malwares risks by using signatures.
- **Firewall policy** to block unauthorized users from accessing the systems and networks that connect to the internet and to remove the unwanted sources of network traffic.
- **Intrusion detection/prevention policy** to detect and block the network attacks and browser attacks. It also protects applications from vulnerabilities.
- **Patch management policy** to manage and implement patches in a timely fashion based on organizations security profile.
- **BCP/DR policy** to manage any unexpected security events.
- **Audit log policy** to record all events and actions performed in chronological order. This facilitates active monitoring and incident analysis.

## Continuous Assessment and Security Training

Proper training of the individuals administering and operating an industrial control systems network is critical to the security and safety of the ICS facility and the people working.

Ongoing vulnerability assessments are critical to identify issues and understand the effectiveness of other defensive network elements. Assessments should include testing and validating the following:

- Monitoring capabilities: are alerts triggered and responded to as expected.
- Device configuration of services and applications & their inventory.
- Expected connectivity within and between zones.
- Existence of previously unknown vulnerabilities in the environment.
- Effectiveness of patching.

A program should be established for performing assessments. The actual assessment should be performed by a qualified resource, which can be an in-house or third-party organization. Regardless of who performs the assessments, in-house resources need to be involved in the planning, scoping, and supporting assessment activities and must be appropriately trained to do so.

Assessments should be conducted according to a methodology that is clearly defined to address:

- Physical security
- People and processes
- Network security
- Host security
- Applications security (both internally developed and commercially off-the-shelf (COTS))
- Device security.

### Physical security

Physical protection can be a major concern for assets like PLCs, controllers, other industrial devices, storage devices, hard drives, engineering work stations, organization's machines, and laptops and servers. Such equipment often gets overlooked in terms of cybersecurity, but it is equally important. A crude example could be a SCADA setup which is geographically distributed (e.g. Power Grids, Oil & Gas etc.). These distributed setups have stations (e.g. electrical substations) in remote locations. These remote stations should have a very strong physical security for protection (e.g. electric fences), detections (e.g. motion sensors) and monitoring (e.g. CCTV) otherwise a software firewall cannot protect an attacker in walking away with hardware such as a storage device from a station.

Physical security protection helps in addressing threats such as unauthorized access, theft, vandalism, natural disasters like fire and flood etc. Physical security requires physical controls such as locks, CCTV, protective barriers, rooms and cabinets with access control mechanisms, uninterrupted power supply, and or security personnel for protecting hardware and software assets.

### Network security

Network security is a practice to protect confidentiality, usability and integrity of your network and data, preventing and protecting against unauthorized intrusion into an organization's networks. Network security includes both hardware and software technologies. It blocks malicious actors from accessing and traversing a network.

Network security helps in addressing threats like data leakage,

data spoofing, DoS, DDoS, MiTM, unauthorized remote access, DNS spoofing, HTTPS spoofing, IP spoofing and many others.

Network security can start with a simple authentication technique of single-factor username and password. Still, it can go forward to multifactor authentication to complex hardware and software technologies depending on the risk profile of an organization. Few of the technologies used in network security are discussed below.

### Endpoint protection

Endpoint protection for example firewall devices provide the capability to add stringent and multifaceted rules for communication between various network segments and zones in an ICS network. They can be configured to block data from certain segments, while allowing the relevant and necessary data through. A thorough understanding of the devices, applications and services that are in a network will guide the appropriate deployment and configuration of firewalls in a network. Typical types of firewalls that can be deployed in a network include:

- **Packet filter or boundary firewalls that work on the network layer**
- **Host firewalls**
- **Application-level proxy firewalls**
- **Stateful inspections firewalls**
- **SCADA hardware firewalls**

### Demilitarized zones (DMZ)

Network segmentation is a key consideration in establishing secure control networks. Firewalls should be used to create DMZ by grouping critical components and isolating them from the traditional business IT network. A three-tier architecture should be employed at a minimum, with a DMZ between the organization's core network and an isolated control systems network as shown in Figure 2 below.

In Figure 2, the control networks are divided into layers or zones based on control functions, which are then connected by conduits (connections between the zones) that provide security controls to:

- Control access to zones.
- Resist denial of services (DOS) attacks or the transfer of malware
- Shield other network systems
- Protect the integrity and confidentiality of network traffic

Beyond network segmentation, access control (both physical and logical) should be defined and implemented.

The key consideration when designing access control is defining the required interactions both within a given zone and between zones. These interactions should be mapped out clearly and prioritized based on need. It is essential to realize that every hole poked in a firewall potentially increases exposure to attacks. Non-essential functionality that provides access or creates additional connectivity potentially increases exposure. A system then becomes only as secure as the devices connecting to it.

If mapped correctly, the potential adverse impact on controlling system reliability and functionality should be negligible. However, this element does introduce additional cost (in terms of firewall and other network infrastructure) and complexity to the environment.

### Intrusion detection and prevention systems (IDPS)

These are systems that are focused primarily on identifying

possible incidents in an ICS network, logging the information about them, attempting to stop them, and reporting them to ICS security administrators. Since these systems are critical in an ICS network, they are regular targets for attacks and securing them is extremely important.

The type of IDPS technology deployed will vary with the type of events that need to be monitored. There are four classes of IDPS technology:

- Network-based IDPS monitors network traffic for particular ICS network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.
- Wireless IDPS monitors wireless network traffic and analyzes it to identify suspicious activity involving the ICS wireless network protocol.
- Network behavior analysis IDPS examines ICS network traffic to identify threats that generate unusual traffic flows such as DOS attacks.
- Host based IDPS that focus on monitoring the characteristics of a single ICS network host and the events occurring within that host for suspicious activity.

### Host security

A host can be defined as hardware within an organization network capable of running software. In industrial control systems a host can be level 1 devices like PLCs, controllers, PACs, HMIs, EWS, Historians, servers etc. Strong host security addresses the key aspects of your hosts, including hardware, software, server and storage components. It ensures you are equipped to defend yourself against, and appropriately respond to, cyberattacks when they occur.

A strict host security may include strong access controls, restrictive privileges based on principle of least privilege, no account sharing, session management, audit policies etc. In case a host permits Host based IDS, antivirus solutions can also be used to secure hosts.

### ICS Hardening

The goal for system hardening is to reduce as many security risks as possible by securely configuring ICS systems. The idea is to establish configurations based on what is required and eliminate unnecessary services and applications, which could potentially provide another possible entry point to an intruder.

Minimum security baselines should be established for the various platforms and products deployed (operating system, application, and infrastructure elements such as drives, meters, HMI devices). The following actions should be implemented where applicable:

- Disable unnecessary services
- Disable Anonymous FTP
- Do not use clear text protocols (e.g. use SSH v2 instead of Telnet)
- Install only required packages/applications/features
- Deploy antivirus solutions (where possible)
- Disable or otherwise control use of USB devices
- Establish a warning banner
- Change default passwords (e.g. SNMP).

It may be easier to implement these actions on devices for which you control the base operating system platform. However, several of the items listed above can be configured from the product -specific configuration options.

Changes such as these could potentially impact the functionality of a control system device. Extensive testing needs to be conducted before deployment to minimize this impact.

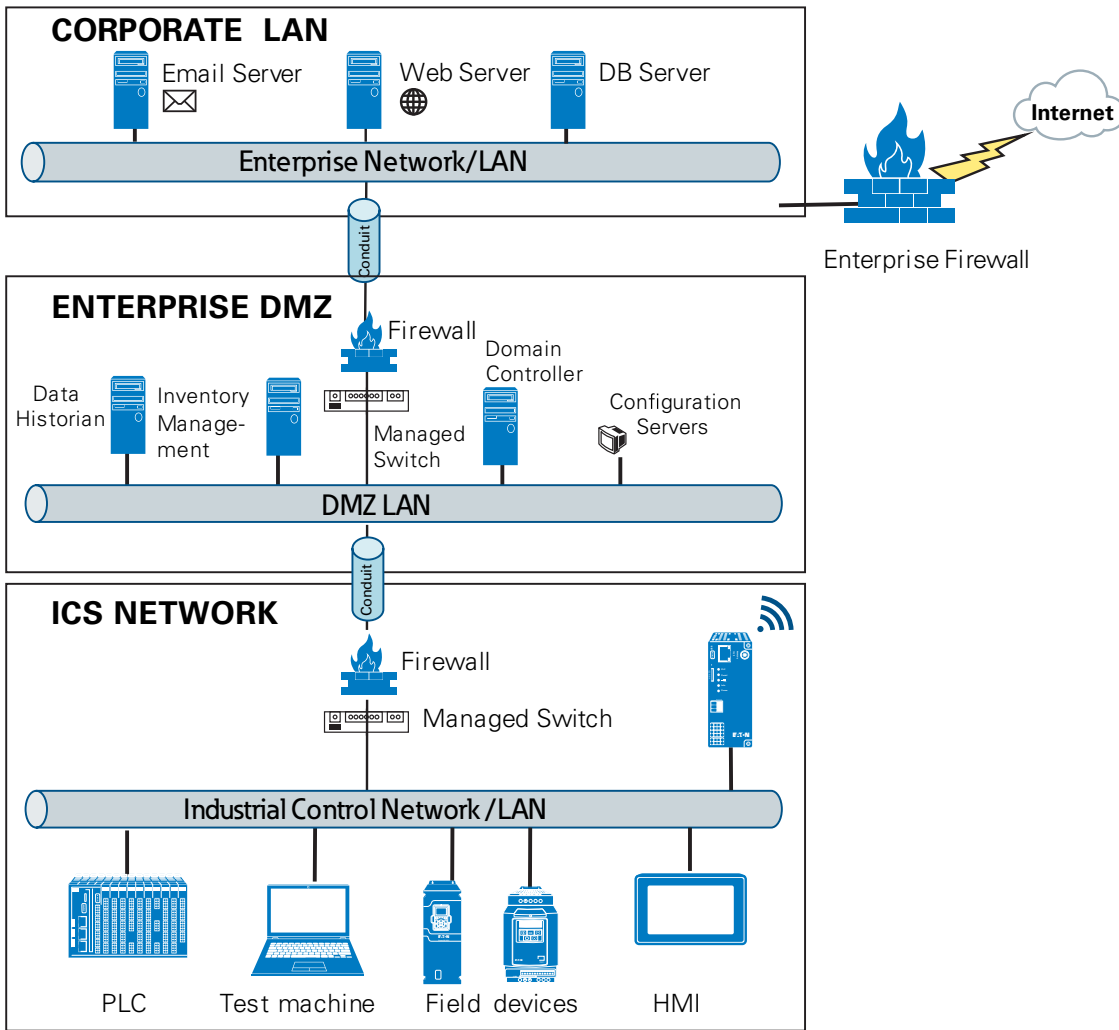


Figure 3: High level example of an industrial Network also showing zones and conduits

**Application security**

Application security is vital as applications are most actively used and exposed interfaces in a device. This makes applications prime target to attackers. It is recommended to observe best practices for secure system development when an application is developed and on the device:

- Privacy and security by design: the application should take security and privacy into consideration from the outset, including at the stage of defining requirements and assessing the associated risks.
- Communication protection: if the application communicates over the network, it is recommended to encrypt the communications in accordance with the applicable level described by the fips 140-2 standard.
- Access enforcement: the application should provide the ability to enforce access controls to protect the application against unauthorized access and to protect accounts against unauthorized authentication attempts (for example, through account lockout).
- Least privilege: any application developed should not run with root account privileges. The root account has full control over and access to the operating system. Therefore, if an application that requires root privileges has any security vulnerability, it endangers the entire system.
- Input checking: all input to the application should be sanitized before storing and processing by the application to protect against malicious code injection.

- Output Handling: Data output by the application for user consumption, including error messages, should be appropriately handled to avoid revealing important information about the application and the underlying system.
- Password management: the application should securely store and transmit credentials (for example, encrypting authentication traffic, and salting and hashing passwords in transit and at rest). Password complexity should be implemented, and password should be masked when entered on-screen.
- Secure coding practices: follow secure coding practice while developing applications for the device (for example, implementing multiple security layers, verifying authorization for all requests, conducting code reviews, etc.).
- Administration interface: the interface for administering the application should be separated from the end-user interface.
- Session controls: all application sessions should be encrypted, logged and monitored.
- Event log generation: the application should have the capability to log security-related events at a minimum, including the time, date, and user.

**Understanding an ICS network**

Creating an inventory of all the devices, applications and services that are hosted in a network can establish an initial baseline for what to monitor. Once those components are identified and understood, control, ownership and operational consideration can be developed.

### Log and event management

It is essential to understand what is happening within the network from both a performance and security perspective. This is especially true in a control systems environment.

This entails monitoring infrastructure components such as routers, firewalls and IDS/IPS as well as host assets. Security Information and Event Management (SIEM) systems can collect events from various sources and provide correlation and alerting.

Generating and collecting events, or even implementing a SIEM is not by itself sufficient. Many organizations have SIEM solutions, but alerts go unwatched or unnoticed.

Monitoring includes both the capability to monitor environments and the capacity to perform the monitoring. Capability relates to the design and architecture of the environment. Has it been built in a manner that takes into consideration the ability to monitor? Capacity speaks to the resources (personnel, tools, expertise) needed to perform a meaningful interpretation of the information and initiate timely and appropriate action.

Through monitoring, the organization can identify issues such as suspicious or malicious activities. Awareness can be raised when new (potentially unauthorized) devices appear in the environment. Careful consideration should be taken into account to ensure that log and event management should not adversely impact the functionality or reliability of the control system devices.

### Patch management planning and procedures

A patching and vulnerability management process should be established based on the timely awareness of issues and appropriate action based. This process should take all the elements that make up the control system environment into consideration.

Information resources should be identified for vulnerability and advisory information for the various components in the

environment. These should include vendor-specific sources as well as other public or commercial services that provide vulnerability advisory information. For example, the National Vulnerability Database (NVD) provides information related to vulnerabilities identified in general IT components. At the same time, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) publishes advisories specific to control systems.

A regular patch deployment schedule should be established for each component in the environment. Depending on the component, this could range from a monthly schedule to as needed deployment, depending on the historical frequency of patch or vulnerability related issues for the component or vendor. Additionally, out-of-band or emergency patch management needs to be considered, and qualifications defined.

Vulnerability information and advisories should be reviewed regularly, and assessments should be performed to determine the relative severity and urgency of issues.

Elements of the process should also include the preparation, scheduling and change controls; testing and rollback procedures; and pre-deployment notification to stakeholders that includes scope, expectations and reporting. Testing is a significant element, as the effect of the patch application needs to be clearly understood; unintended or unexpected impacts to a control system component influence the decision to deploy a patch. In the event it is determined that a patch cannot be safely deployed, but the severity of the issue represents a significant concern, compensating controls should be investigated.

### Vulnerability disclosure

It is recommended to report all cybersecurity incident and vulnerabilities to regulatory authorities as mandated by local laws. Product suppliers should also be notified of any vulnerabilities or cybersecurity incidents experienced in their product.

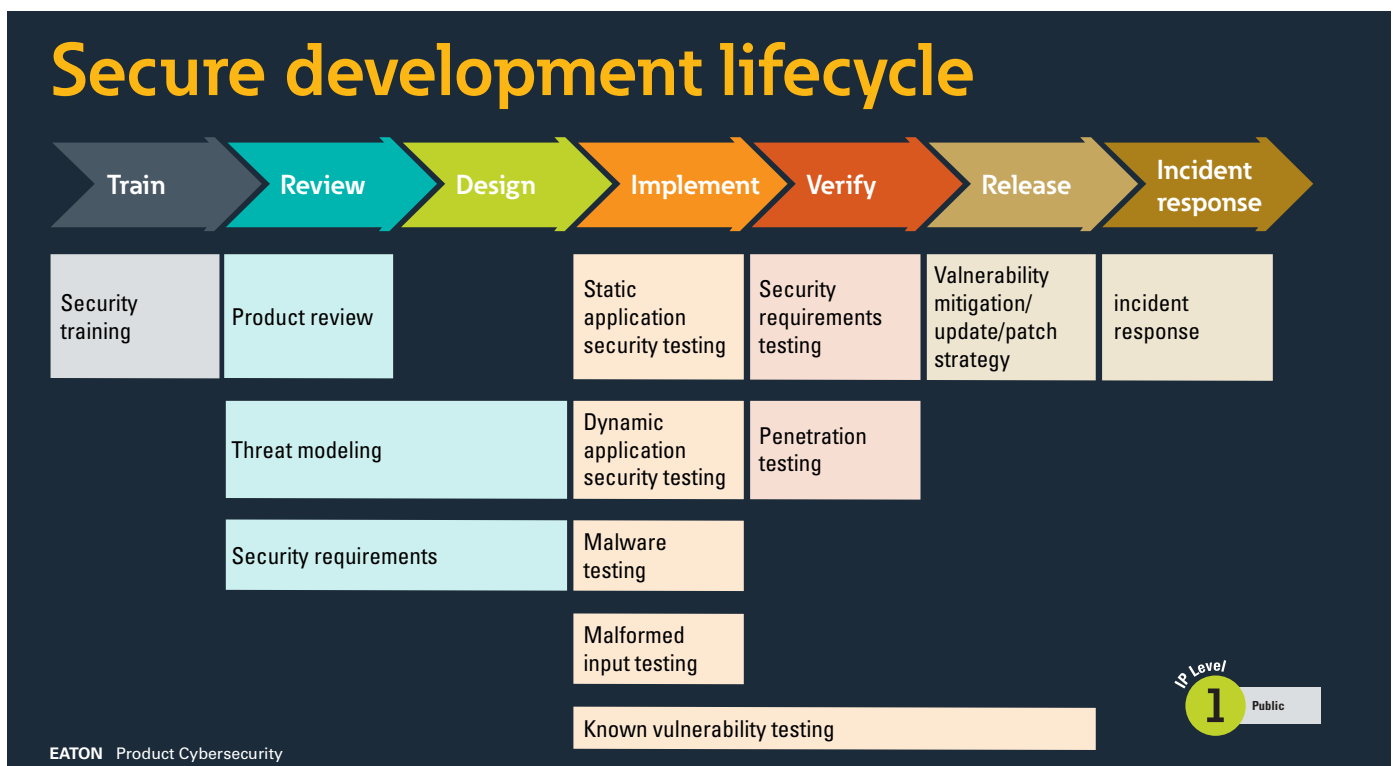


Figure 4: Eaton secure development lifecycle

Link below should be used for reporting cybersecurity incident and vulnerabilities in Eaton products –

<https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/vulnerabilitydisclosure.html>

## Secure decommissioning/zeroization

It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88r1 [6]. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.

- Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory.
- **Clear:** if supported by the device, reset the state to original factory settings.
- **Purge:** if the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the circuit board that contained the flash memory. Otherwise, the whole board should be destroyed.
- **Destroy:** shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator.

## Security right from the start - Eaton's cybersecurity approach

Eaton takes a comprehensive approach to protect its products and solutions. So cybersecurity is an integral aspect of Eaton, with rigorous procedures for people, processes and technology within the secure development lifecycle process (SDLC). This program ensures that cybersecurity is considered at every stage of product development. It extends from design to deployment and maintenance, ensuring that a high grade of cybersecurity is provided at every stage of the product lifecycle.

## Organizational cybersecurity measures

A fundamental organizational measure is the training. All employees receive mandatory training on cybersecurity. This creates a fundamental understanding of the challenges of protecting against cyberattacks - the basis for developing secure products and solutions for customers. Developers, testers and managers who are involved in the development of products which are critical to cybersecurity like components of IACS or software and firmware solutions in general have to complete additional security training courses. Specific topics such as threat modeling, security requirements, secure coding or testing are covered here.

Another important aspect of cybersecurity is the ability to react quickly when a cybersecurity incident occurs or is discovered: Eaton's cybersecurity strategy, therefore, includes a detailed procedure for handling security incidents (Incident Response Plan). If previously unknown security gaps are discovered in the products, they are immediately published on Eaton's cybersecurity website. Customers can log in here so that they can receive appropriate notifications securely - and can also report security vulnerabilities themselves. Of course, Eaton does not stop at appropriate notifications, but also provides appropriate patches for new threats as fast as possible.

## Risk analysis and design

Security procedures and recommendations are defined beginning from the initial phase of a new product. These include a data flow diagram that depicts the entire data flow in the product and an analysis of the product architecture to determine which components are particularly critical with regard to cybersecurity. In addition, the extent to which

sensitive and personal data is processed is analyzed to ensure compliance with applicable data protection regulations. Also threat modeling is performed which involves assessing the risks associated with the components and environment identified in the architecture analysis and prioritizing the corresponding security requirements. Finally, the cybersecurity requirements are defined based on relevant industry standards such as UL 2900 or IEC 62443. This allows the development of products that are compliant with multiple security standards.

The early identification of cybersecurity requirements in the design phase enables a product design that eliminates or reduces vulnerabilities from the outset and reduces the risk of costly adjustments to eliminate errors in later phases.

## Implementation

During the implementation phase, the product is also continuously developed to take cybersecurity into account. In doing so, it runs through a series of automated test series. These help to identify weak points as early as possible.

These include static application security testing (SAST), which automatically detects security vulnerabilities in the source code and/or in compiled versions of the code. In this way, cybersecurity-relevant potential errors in the code can be detected and eliminated at an early stage. Software applications like Web applications and mobile applications are then subjected to automated dynamic application security testing (DAST). The analysis looks for security vulnerabilities such as cross-site scripting, SQL injection, command injection, path traversal and insecure configurations.

Fuzz tests or "malformed input tests" are another test procedure that a product undergoes during the implementation phase at Eaton: In these tests, weak points are discovered by testing the product with sometimes random, thoroughly inappropriate queries. These assessments go far beyond the typical tests that developers perform for all foreseeable attacks, because in contrast to classic penetration investigations, fuzz tests attempt to provoke malfunctions. They can also identify unexpected behaviour such as a system crash or hang, denial of service (DoS) and memory leaks - errors that are generally not detected during code reviews.

If third-party code is used in the products, it is checked for known vulnerabilities (Common Vulnerabilities and Exposures, CVEs). If vulnerabilities are identified, they can be tested and minimized before release.

## Verification and validation

In the phase of verification and validation of the design, further manual tests are performed. They are based on the security requirements applicable to each product individually and are required to confirm conformity with the relevant industry standard.

The final validation is done by penetration tests. These tests use means and methods that would be used by an attacker to penetrate the system without authorisation. Priority is given to external interfaces through which potential attackers could penetrate the product system. In this way, configuration errors and unresolved weaknesses can be identified. The penetration tests ensure that the product meets the defined security requirements before it is released into production. They also offer the opportunity to identify and investigate other ways that could be exploited for an attack.

Before a product is released for market launch, a strategy is defined in order to close future vulnerabilities through patches. Therefore, it determines how often updates are carried out. It also contains an incident response plan (IRP), which determines how to react to newly discovered vulnerabilities and attack-scenarios.

**Cybersecurity measures during operation and maintenance**

Eaton delivers its products and equipment with the security features enabled. This means, for example, that all ports with a higher risk are closed at delivery and that all protective measures are activated. For instance, the secure communication protocol “https” is activated by default for Internet access, which is used to transmit encrypted data. Customers can switch it off, for example if the compatibility with a system in use is not given. But in doing so they are taking a higher cybersecurity risk. Corresponding information is contained in the so-called “Hardening Documentation”, which is enclosed with every Eaton product. Here users receive detailed information on how they should set up the network or the respective device in order to achieve the intended grade of cybersecurity.

Eaton also has a product related certificate infrastructure which is used to digitally sign the firmware of a product. That enables the device by cryptographic methods in case of an update to verify if the firmware update package was created by Eaton and also was not modified. Only if this verification is successful, the device will accept the firmware.

The cybersecurity process at Eaton not only applies to new developed products, also the established products are continuously checked for their vulnerability to cyberattacks. Among other things, this is done by so-called MOL assessments (Maintenance of Line). Eaton monitors all supported devices and in addition Eaton experts are monitoring whether new forms of attack could pose a risk to existing systems or devices already on the market. For this purpose, newly discovered vulnerabilities are mapped with a list of the components used in Eaton devices.

If a newly discovered vulnerability endangers a component, an assessment is performed to determine the actual risk for the use of the device. If necessary, measures are taken in close cooperation with the respective product team to remedy the newly created vulnerability. For the products which are developed in collaboration with third-party suppliers, there is a contractual assurance that the supplier will remedy discovered weaknesses in its components within a specified period.

In order to keep abreast of current threats, Eaton works closely with various researchers, intelligence security agencies or the ICS-CERT. ICS-CERT is part of the United States Computer Emergency Readiness Team (US-CERT), which is subordinate to the Department of Homeland Security and is specifically responsible for the security of industrial control systems. Eaton also incorporates reports from customers and field staff on newly discovered vulnerabilities and risks into its device monitoring.

**Cybersecurity according to international standards**

Currently, various security standards for automation solutions are being further developed. Standards such as UL 2900 and IEC 62443 are becoming increasingly important. However, product-related standards like IEC 60947 are also being adapted to incorporate cybersecurity aspects. In order to always be capable of implementing the current status of cybersecurity standards in its products, Eaton works closely with the relevant standardization organizations worldwide like UL and IEC, but also with national or regional institutions such as the German DKE or the European CENELEC. Through its participation in the various standardization committees, Eaton takes part at the appropriate integration of cybersecurity aspects into several industry related standards.

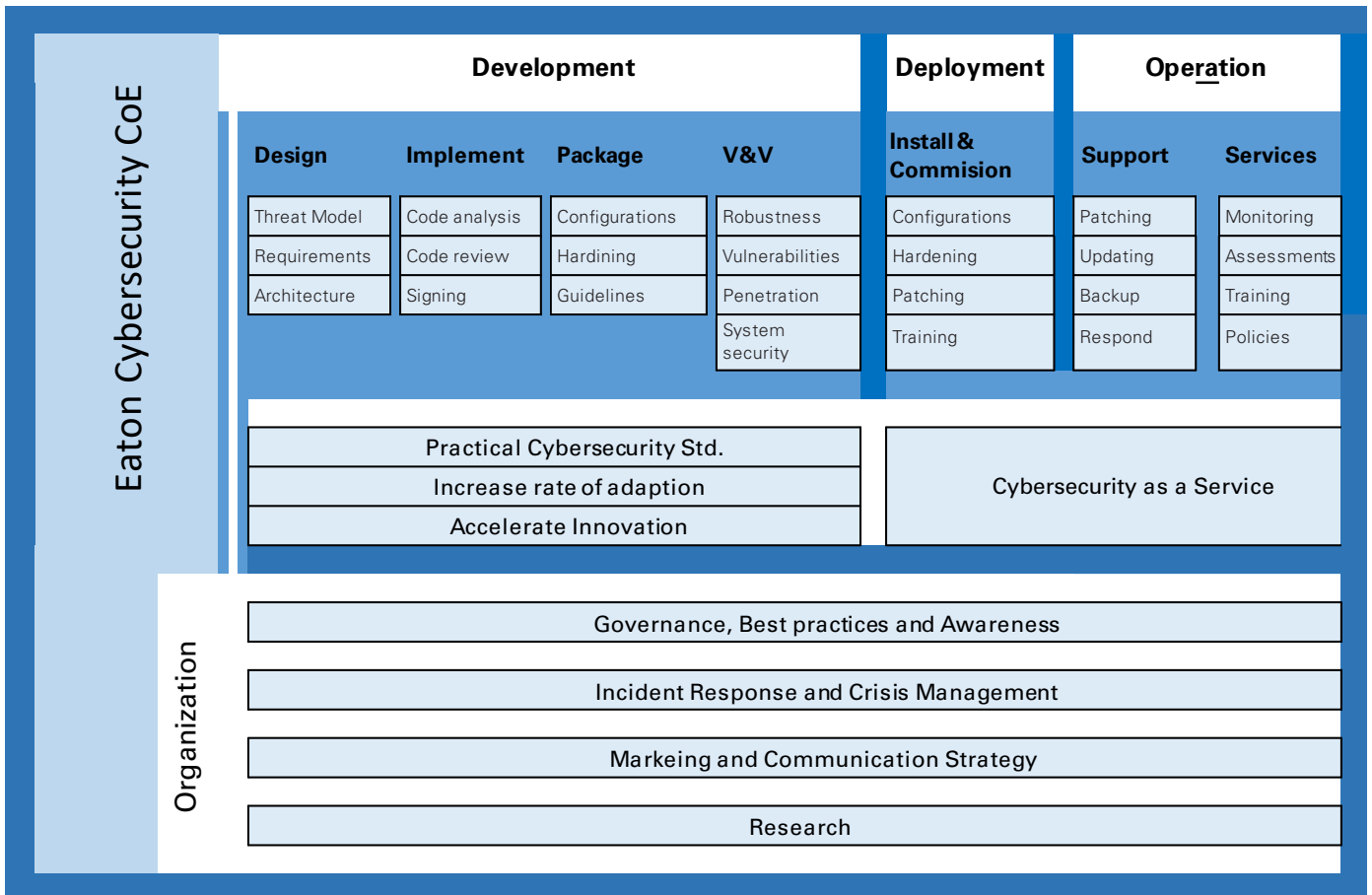


Figure 5: Overview of Eaton’s comprehensive cybersecurity-strategy (not all aspects are described in the whitepaper)

### Internationally strong: UL 2900 and IEC 62443

In general, Eaton’s cybersecurity concept is based on the internationally recognized industry standards UL 2900 and IEC 62443. The company and its secure development lifecycle Process is designed in a way that the developed and produced devices can be certified according to UL 2900 and IEC 62443. Eaton is the first company in the world to have the processes assessed and certified under both UL 2900-1 and IEC 62443-4-1. This fact is underling the leading position of Eaton in regards of cybersecurity.

UL 2900, which is primarily relevant for the North American market, is a more practical standard, while IEC 62443, which is geared to the European market, is a comprehensive standard with a high level of detail that takes a holistic approach for operators, integrators and manufacturers. Although the two standards are different, they may well complement each other. The IEC 62443 series of standards is specifically dedicated to industrial automation and control systems (IACS). It specifies several criteria and requirements for IT-security in such networks, systems and the related components. In addition, UL has developed UL 2900-2-2 for Industrial Control Systems (ICS) with a focus on requirements and test procedures. It allows the cybersecurity of industrial control systems to be evaluated and certified by an independent organisation through customized product tests.

Eaton operates two research and testing facilities (in Pittsburgh, USA and Pune, India) that are approved for participation in the UL Data Acceptance Program (DAP) for cybersecurity. These accredited laboratories test Eaton products with intelligence or embedded logic not only against key aspects of UL 2900-1, but also against IEC 62443 criteria. Common to both standards is the requirement for mandatory test protocols regarding vulnerabilities and software weaknesses.

Overall, this ensures that every product developed or sold by Eaton goes through the secure development lifecycle, even if no cybersecurity certification is required for it at all. This also includes third-party suppliers. Eaton - and the company’s products - are thus well prepared for future changes in standardization, because the highest requirements are already being met today.

### Secure products with certificate

Eaton’s first power management product to be certified to the UL 2900-2-2 standard for cybersecurity in industrial control systems was the Power Xpert Dashboard. With this user portal to Eaton’s switchgear, customers can monitor, diagnose and control devices from outside the arc fault zone. Another example is the SMP IO-2230 utility automation system, the first UL 2900-2-2 certified substation automation system. The technology is designed to help users around the world monitor and control intelligent electronic devices in the power grid and microgrid applications.



Figure 6: The Power Xpert Dashboard Processor paired with Power Xpert Dashboard HMI for visualization to enable secure remote control and management of Eaton Switchgear outside the arc fault boundary.



Figure 7: Eaton’s substation-grade SMP distributed I/O platforms are specially designed to meet the requirement for distributed I/O in modern utility substation automation systems.

Depending on application requirements Eaton also certifies products according to IEC 62443-4-2 today. In contrast to Part 4-1, which describes the necessary organizational and development process related requirements, Part 4-2 defines the technical requirements for products. Examples of Eaton products certified in accordance with IEC 62443-4-2 are the Gigabit Network Card and the Industrial Gateway Card: Both have cybersecurity certificates in accordance with IEC 62443-4-2. The products also meet cybersecurity standards in accordance with UL 2900-1 to ensure and demonstrate a high grade of security for networked UPS devices (uninterruptible power supply). Both Eaton products allow easy networking of single- and three-phase UPS systems in data centres, commercial buildings and industrial facilities. This ensures a constant power supply protected against cyber-attacks. With these products, Eaton was the first in the industry to achieve double certification in accordance with the strict guidelines of IEC and UL.

## Conclusion

Cybersecurity is not a goal in itself and should not be seen as a burden. Because strong cybersecurity for products, applications and companies represents a value: In large networks, cybersecurity-certified components and devices protect against major failures and high financial losses. In smaller networks, the integration of cybersecurity-certified devices is worthwhile, because it is often more cost-effective to increase protection against cyberattacks with a few secure automation components than to equip the entire network with firewalls and complex electronic protective measures. Even if such protective measures are already in place, secure devices provide another valuable line of defence. With the increasing connectivity of individual systems and devices to the Cloud or through individual channels directly to the OT level (e.g. for remote maintenance or for new business models such as pay-per-use), it is also imperative to integrate cybersecurity directly in the corresponding devices because a secure network can only help to a limited extent in such instances.

To protect important assets, all organizations must take cybersecurity threats seriously and meet them proactively with a system-wide defensive approach by applying defense in depth techniques specific to organizational needs.

Cybersecurity standards are gaining importance at all levels. In addition to cross-device standards, cybersecurity is also becoming an increasingly important aspect of device-related standards such as IEC 60947 series for low voltage switchgear. Anyone who installs cybersecurity-certified components in their systems today is thus well equipped to meet the requirements of the future. And even if customers

already expect a certain level of cybersecurity today, a machine and system manufacturer can still secure an important competitive advantage by installing components with a high level of cybersecurity.

There is no protection method that is completely secure. A defense mechanism that is effective today may not be effective tomorrow – as the ways and means of cyberattacks constantly change. It is critical ICS administrators remain aware of changes in cybersecurity and continue to work to prevent any potential vulnerabilities in the systems they manage.

And similar to functional safety, there is a parallel to cybersecurity: To achieve security in an application, it is not sufficient to implement cybersecurity-certified devices. The complete application and all associated systems must be evaluated, and the organizational environment (including procedures and guidelines) also have to be considered.

As a manufacturer of automation equipment and energy management technologies, Eaton's main focus is naturally on product and manufacturer-related standards, but Eaton also supports its customers with its cybersecurity know-how at system and application level. The experts at Eaton's Cybersecurity Center of Excellence provide users with a wide range of cybersecurity services. They help users to examine applications for cybersecurity vulnerabilities and evaluate how cyberattacks could affect other, more sensitive systems. Eaton's cybersecurity services help customers to design, update and maintain their networks and processes. Also Eaton's cybersecurity experts provide employee training at customer sites to ensure that cyber-criminals are kept at bay.

## Terms and definitions

<b>DMZ</b>	A demilitarized zone is a logical or physical sub network that interfaces an organization's external services to a larger, untrusted network and providing an additional layer of security.
<b>Encryption</b>	The process of transforming plain or clear text using an algorithm to make it unreadable to anyone except those possessing special knowledge.
<b>ICS</b>	A device or set of devices that manage, command, direct, or regulate the behavior of other devices or systems.
<b>Protocol</b>	A set of standard rules for data representation, signaling, authentication, and error detection required to send information over a communications channel.

## Acronyms

AAA	Authentication, Authorization, and Accounting
BCP/DR	Business Continuity Planning/ Disaster Recovery
CCTV	Close-circuit Television
COTS	Commercially Off-The-Shelf
DMZ	Demilitarized Zone
DNS	Domain Naming System
DOS	Denial of Service
DDoS	Distributed Denial of Service
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control Systems
IACS	Industrial Automation and Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IT	Internet Protocol
MiTM	Man in the Middle
NVD	National Vulnerability Database
OSI	Open System Interconnection
PAC	Process Automation Controller
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SIEM	Security Information and Event Management
USB	Universal Serial Bus

## References

1. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense- In-Depth Strategies, October 2009  
[https://us-cert.cisa.gov/sites/default/files/recommended\\_practices/NCCIC\\_ICS-CERT\\_Defense\\_in\\_Depth\\_2016\\_S508C.pdf](https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf)
2. NIST.SP.800-82-82r2 Guide to Industrial Control Systems (ICS) Security, May 2015  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
3. NIST.SP.800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), Feb 2007  
<http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>
4. Common Cybersecurity Vulnerabilities in Industrial Control Systems, May 2011  
[http://ics-cert.us-cert.gov/sites/default/files/recommended\\_practices/DHS\\_Common\\_Cybersecurity\\_Vulnerabilities\\_ICS\\_2010.pdf](http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf)
5. The Tao of Network Security Monitoring, 2005 Richard Bejtlich
6. Guidelines for Media Sanitization  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

This page is intentionally left blank

We implement what really matters.\*

\*We at Eaton believe that energy is an essential part of everything people do. Technology, transport, energy, and infrastructure—these are all things the world relies on every day. At Eaton, we are committed to helping our customers find new ways to manage electrical, hydraulic, and mechanical energy more efficiently, safely, and sustainably. We do this to improve people's lives, the communities in which we live and work, and the planet on which future generations depend. Because that is what really counts. And we are here to make sure it gets implemented.



**Eaton**  
**Eaton Industries GmbH**  
Hein-Moeller-Str. 7-11  
D-53115 Bonn / Germany

© 2021 Eaton  
All Rights Reserved  
Publication No. WP182004EN  
May 2021

Eaton is a registered trademark  
of Eaton Corporation.

All other trademarks are property  
of their respective owners

Follow us on social media to get the  
latest product and support information.

