YRKESHÖGSKOLAN
NOVIA

Implement NIS2 directive on the automation projects

Strengthening ABB's Cybersecurity Framework with Device Hardening

Janaka Meda Gedara

Degree Thesis

Thesis for a Master of Engineering (UAS) degree

Automation Technology

Vaasa 2025

DEGREE THESIS

Author: Janaka Meda Gedara

Degree Programme and place of study: Automation Technology, Vaasa

Specialization: Intelligent Systems

Supervisor(s): Jan Berglund, Maarit Mäntylä (ABB)

Title: Implement NIS2 directive on the automation projects

Date: 10.2.2025 Number of pages: 44 Appendices: 3

Abstract

This master's thesis is part of the Automation Technology program at Novia University of Applied Sciences, carried out in partnership with ABB Oy, Distribution Solutions. With a rich history spanning 140 years, ABB is recognized as a global leader in process automation and electrification, prioritizing sustainability and innovation in emerging technologies. The Distribution Solutions division is crucial in improving electric power quality and grid resilience by offering tailored solutions for utilities, industries, and infrastructure. Through the optimization of medium-voltage connections, ABB ensures dependable energy distribution while promoting digital advancements within power systems.

This study aims to establish a security measurement guideline specifically for Linux-based automation systems, focusing on the evaluation of ABB's cybersecurity guidelines and the NIS2 Directive. Recognizing that cybersecurity is a constantly changing field, this thesis prioritizes the development of practical security solutions that align with industry standards. The research is limited to automation solutions within ABB's Distribution Solutions division, specifically addressing security measures linked to Zenon SCADA. It will cover essential firewalls and network devices for traffic management, while deliberately omitting aspects related to network topology design and segmentation.

This research greatly enhances secure automation solutions, ensuring compliance with industry standards and protecting critical infrastructure and digital systems.

Language: English

Key Words: three to five keywords

1 Table of Contents

Acknowledgment

This thesis was conducted for ABB Distribution Solution, Vaasa, and I would like to extend my sincere gratitude to all individuals who supported me throughout this journey.

First and foremost, I wish to express my heartfelt appreciation to Maarit Mäntylä and Petri Tuomio from ABB for their invaluable guidance, expertise, and encouragement. Their insights and support have been instrumental in shaping this work.

I would also like to thank Jan Berglund and Ray Pörn from Novia UAS for their continuous mentorship and constructive feedback. Their academic expertise and dedication have significantly contributed to the successful completion of this thesis.

Finally, I am deeply grateful to all those who made this research possible, providing assistance, knowledge, and motivation along the way.

1 Introduction

This master's thesis is part of the master's degree course in Automation Technology at Novia University of Applied Sciences. The client for this thesis is ABB Oy, Distribution Solutions.

ABB Oy has a strong 140-year history and has become a pioneer in the technology industry. More than 105,000 workers work under ABB internationally to achieve one aim: safeguarding the sustainability and resources of future technologies in process automation and electrification areas (About ABB—ABB Group, n.d.).

The Distribution Solutions division delivers efficient and dependable distribution, protection, and energy administration by enhancing electric power quality while boosting the grid's resilience. The division offers segment-specific products and solutions that predominantly serve utilities, industry, and infrastructure, typically providing the needed medium-voltage connection between high-voltage transmission networks and low-voltage customers. (Distribution Solutions (ELDS), n.d.)

Distribution Solutions provides creative, forward-thinking client solutions for improved power distribution across utility, industrial, data center, and infrastructure industries. ABB professionals provide tailor-made digital solutions for electrification processes. Our global client base demonstrates our significant position in the digital systems sector. (Digital Systems - Packaging and Solutions | Packaging and Solutions | ABB, n.d.)

1.1 The purpose of the study

This study aims to suggest a security measuring guideline for Linux-based automation systems by assessing the NIS 2 directive and ABB guidelines. Cybersecurity is a vast area, and this study will cover only a small part of it.

1.1.1 Goals of study

- Evaluate the existing ABB cybersecurity guidelines and the NIS2 Directive.
- Develop security measures guidelines for Linux-based Automation SCADA projects.
- Identify required resources and tools for implementing the security measure guideline.

- Practice the developed suggestions accepted procedure on a Linux-based system.

1.1.2 Scope and Limitations

Cybersecurity is a vast technical area continuously updating and connecting every industry and every sector. This thesis only focuses on the NIS2 directive, which was imposed on the nations' law in EU countries, and ABB guidelines related to automation solutions provided by the ABB distribution solutions team. Also, this thesis work will consider specific devices practically used with the Zenon SCADA project, such as firewalls and switches, to handle the network traffic and accomplish the project tasks. Network topology planning and segmentations would be regarded as not involving the thesis work, but other practical steps that make automation solutions secure and hardened.

1.2 Research Questions

There are two research questions in this study. The first research question provides a comparison of the ABB existing guidelines vs the NIS2 directive components, and it will be covered with the first two goals. The second research question describes the procedure, practical tools, resources, and best practices, which will be covered in the last two goals.

1. What is NIS2, and how does it differ from ABB Cyber Security guidelines for Automation projects?
2. How has the NIS2 Directive influenced cybersecurity practices in industrial automation projects? What are the best practices to secure automation systems?

1.3 NIS

The Network and Information Systems Directive (NIS) was adopted in 2016 as the first European law on cybersecurity. Its principal purpose was to strengthen the cyber resilience of EU Member States by identifying key service operators in the Union and implementing cybersecurity measures, with incident reporting being a fundamental requirement. It became transparent that Member States had significant disparities in their implementations of the Directive. This inconsistency resulted in a fragmented system where certain industries and organizations were classified as essential in some countries,

yet not in others. To tackle some of the challenges related to the NIS, such as the unclear identification of covered entities and their specific needs, NIS2 was revised in 2021.

2 Theory

This chapter encompasses the theoretical framework of the thesis. It starts with cybersecurity and discusses automation systems, Zenon soft PLC, network devices used to develop a system, and device hardening strategies used to secure the system. The aim is to focus on ABB's existing guidelines and NIS2 directives and compare them.

2.1 Cybersecurity

Cybersecurity involves safeguarding systems, networks, and programs from digital assaults. These assaults often target acquiring, altering, or destroying sensitive information, extorting funds from users via ransomware, or disrupting standard corporate operations. (*What Is Cybersecurity? - Cisco*, n.d.)

Implementing Ethernet and TCP/IP-based communications makes systems more interoperable and opens the way for trojans, worms, viruses, and Internet-based attacks. However, security considerations aside, the answer is not to block technological improvements, which, from a reliability aspect, will continue to increase the total power system performance considerably. Overall, the demand for cybersecurity, both from a technological and procedural aspect, will increase. Cybersecurity will become critical in products, systems, solutions, and processes as industry standards are created and regulations are implemented as law. (ABB, n.d.)

Adopting secure cybersecurity best practices is essential for people and companies of all sizes. Employing robust passwords, regularly upgrading software, exercising caution before clicking on dubious links, and enabling multi-factor authentication are the fundamentals of "cyber hygiene" and will significantly enhance online security. These fundamental principles of cybersecurity apply to both people and businesses. (*Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA*, n.d.)

Cybersecurity has continually grabbed attention and significance for automation and control systems in the electric industry over the past few years. While cybersecurity was not considered a concern or even a nice-to-have in the past, it has increasingly become a must-have, and its significance continues to increase. The level of attention and the

incentives for cybersecurity differ throughout the globe. The most considerable emphasis on cybersecurity is provided by North America, with Europe being a fast follower. Focus is progressively expanding to South America, the Middle East, and Asia. It may be anticipated that a comparable degree of worldwide attention will be attained shortly. (ABB, n.d.)

Jeremy Jurgens from the World Economic Forum notes the rising complexity of cyberspace, which is driven by fast technical improvements, the increased sophistication of cybercriminals, and interwoven supply networks. He stresses the relevance of the Global Cybersecurity Outlook in providing leaders with essential insights to negotiate these difficulties and build cyber resilience. (*Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities > Press Releases | World Economic Forum*, n.d.)

Overall, a rise in the need for cyber security, both from a technical and procedural standpoint, will be evident soon. When industry standards are formed and rules are enacted as law, cybersecurity will be a fundamental requirement in goods, systems, solutions, and processes (ABB, n.d.).

2.1.1 Cybersecurity threats in the EU

With more than 10 terabytes of data compromised monthly, threats to availability and ransomware are the most significant cyber threats in the EU, with phishing currently accepted as among the most prominent beginning vectors of such assaults. Distributed Denial of Service (DDoS) attacks are also rated among the top dangers. (*Top Cyber Threats in the EU - Consilium*, n.d.)

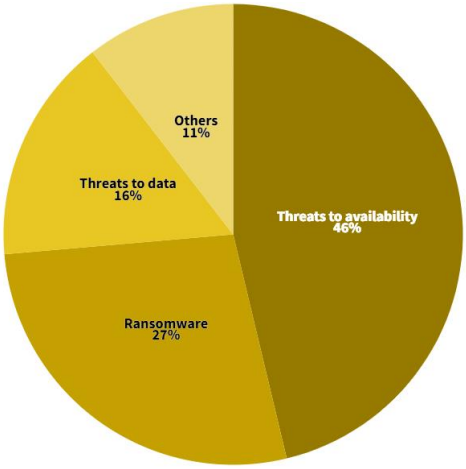

Figure 01: **Cybersecurity threats in the EU** (*What Are the Top Cyber Threats in the EU? - Consilium*, n.d.)

DDoS attack: A distributed denial-of-service (DDoS) attack makes an artificial internet traffic jam of a targeted server, service, or network. (DDoS Attack? | Cloudflare, n.d.) It differs from DoS attacks because DDoS attacks utilize thousands/ millions of connected devices by installing malware as a botnet to attack a target that the attacker can control. Amazon Web Services (AWS) and GitHub were the largest victims of DDoS attacks, respectively, in 2020 and 2018. (DDoS Attack? | Fortinet, n.d.)

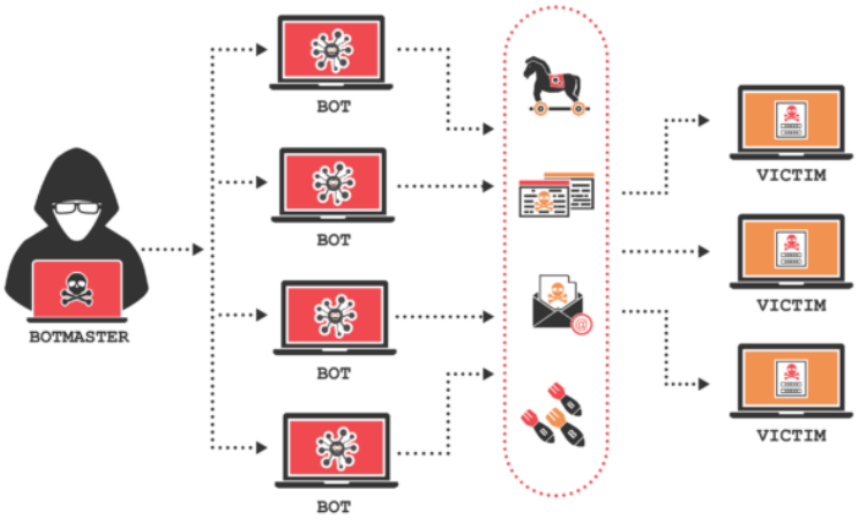

Figure 02: DDoS Attack (DDOS Attacks, n.d.)

Ransomware attack: The attacker controls the target asset and demands a ransom to restore it. Some popular Ransomware vectors, such as malware, email attachments, web pages, pop-up windows, instant messages, text messages, and social engineering, can be prevented. (Top 7 Most Common Ransomware Attack Vectors, n.d.).

Figure 03: Ransomware (Just What Is a Ransomware Attack, n.d.)

Social Engineering: Social engineering is the term used in the security industry to describe the use of psychology and sociology to deceive victims into disclosing important information, such as passwords. Disgruntled workers may divulge passwords to their bosses to do damage to the company. A hacker may contact someone on the phone pretending to be from a credit card business, an Internet provider, or someone with a genuine interest in accounts or computer equipment. The purpose of the masquerade is to fool victims into disclosing their passwords, usernames, and other vital data. (*What Are the 7 Most Critical Cyber Threat Types*, n.d.)

Phishing: Phishing is another common approach have probably seen before, second only to malware. This cyber threat involves fraudsters posing as respectable individuals or organizations and reaching out to targets by text, phone, email, or social media**.** ((*What Are the 7 Most Critical Cyber Threat Types*, n.d.)

Drive-bys: The drive-by attack is one additional method. It lures the user into accessing a malicious website that starts programs that infect victims with malware when viewed in a browser. Typically, the infection grants hackers access, enabling them to carry out their harmful operations. Drive-bys usually take place on questionable sites meant to lure in the unwary. They typically offer too-good-to-be-true weight reduction methods, compromising images of celebrities, or costly tax advice**.** (*What Are the 7 Most Critical Cyber Threat Types*, n.d.)

OnPath: Cybercriminals take immense pleasure in exploiting any technological weakness they encounter. One widely used technique is the OnPath attack, a "man-in-the-middle" or MITM assault. In an OnPath attack, malware is used by a hacker to steal a user's financial and personal information without the user's knowledge by intercepting a two-party transaction, often over an unencrypted public Wi-Fi network. As these attacks frequently target individuals using free Wi-Fi, their prevalence has increased with the growing availability of Wi-Fi to the general public. (*What Are the 7 Most Critical Cyber Threat Types*, n.d.)

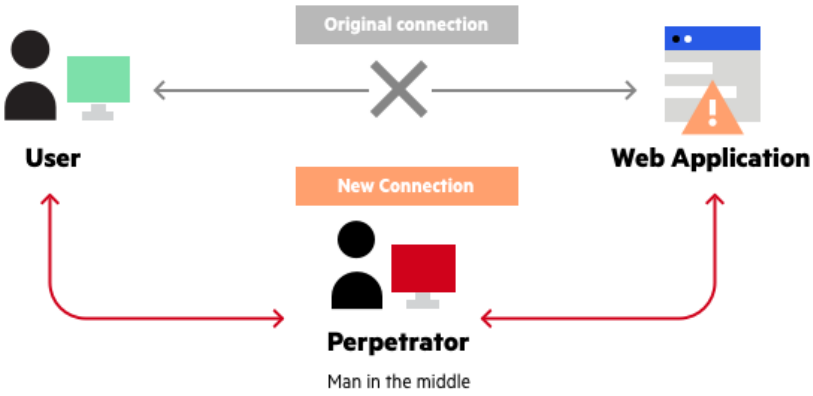

Figure 04: man-in-the-middle (What Is MITM | Imperva, n.d.)

2.2 Automation Systems

Automation systems refer to a system that monitors, controls, and manages the tangible or non-tangible miscellaneous aspects of any environment such as energy generation management, access control, data and information management, remote monitoring and controlling, and process management. It is a kind of collective work between sensors, actuators, TCP network applications, cybersecurity, and software applications that use predefined rules and automated tasks to achieve the specified goal. However, nowadays automation systems are continuously getting more complex due to the increase in expectations and requirements. Also, due to the surge in cybercrimes, all automation systems need to be focused on cybersecurity. (Sallans et al., 2006)

The automation systems related to the energy sector, such as generation, transmission, and distribution, need to be competently monitored and controlled because of their importance. Data acquisition and supervision are contiguous with various devices such as measuring and protection devices to provide high-reliable control according to the particular instance. The SCADA system is chosen for executing the essential activities that synchronize the production, distribution, and consumption of generated energy. The design of the automation system has supervisory elements that enable unattended operation while also managing the heterogeneity of the subsystems.(Ramjanee & Shah, 2024)

2.2.1 SCADA

SCADA refers to supervisory control and data acquisition, a word that outlines the core tasks of a SCADA system. Companies utilize SCADA systems to control devices throughout their facilities and to collect and record data about their operations. Companies may utilize SCADA systems to control their industrial processes both locally and remotely, enabling direct contact with apparatus like motors, pumps, and sensors from a single point of control. These systems may occasionally automatically regulate equipment depending on incoming data. Furthermore, SCADA systems allow enterprises to monitor and report their activities in real time, as well as preserve data for later analysis and review. SCADA systems are a combination of software and hardware components, including programmable logic controllers (PLCs) and remote terminal units (RTUs). Data collection begins with PLCs and RTUs, which interface with process floor infrastructure comprising industrial gear and sensors. The data acquired from this equipment is then sent to a higher level, such as a control room, where operators may monitor the PLC and RTU controls via human-machine interfaces (HMIs). HMIs, displays used by operators to connect with the SCADA system, are a significant part of these systems**. (***What Is SCADA? | SCADA Control | COPA-DATA, n.d.)*

2.2.2 ZENON Soft PLC

Zenon is a software platform meant to facilitate the engineering and automated functioning of industrial and infrastructure equipment. Zenon assures that equipment functions reliably, flexibly, and efficiently. Decision makers, engineers, and operators in manufacturing businesses and energy distribution industries employ this complete software platform to connect all essential areas, from project design to maintenance. Consequently, the total effectiveness of the devices may be enhanced. Centralized operational data storage is supported by Zenon, which regularly collects, analyzes, and distributes data to other systems when necessary. A wide library of drivers and open interfaces is supplied, providing for straightforward integration and expansion of diverse hardware landscapes. Zenon methodically collects and analyzes data from multiple sources, organizes and saves it for convenient access, and offers clear and uncomplicated interfaces for monitoring and managing operations. Extensive reports are prepared, and data is evaluated to gain critical insights. Additionally, the engineering and maintenance of applications are optimized utilizing sophisticated tools, and Information Technology (IT)

and Operational Technology (OT) systems are seamlessly connected to promote cooperation and productivity. ((*Zenon Software Platform for Industrial Automation & Energy Automation | COPA-DATA*, n.d.)

A well-structured backup management strategy and the capacity to recover projects are specified by NIS 2. Zenon projects may be backed up and restored at any point. User management, secure password security, and measures against unwanted access are provided as integrated functional components in Zenon. Designed with a unified user interface, these components are straightforward to set up. Additionally, permission levels that regulate access privileges and approved user behaviors are also readily adaptable, thus boosting the overall security of operations. ((*Industrial Cybersecurity with Zenon | COPA-DATA*, n.d.)

2.2.3 Network Devices used in automation projects

Switches and firewalls are often used in automation projects as key components for handling network traffic. Both switches and firewalls can be utilized to ensure the security of the automation system. Additionally, redundant and secure networks and network components act as the backbone of the automation system; thus, components should be kept up to date, which covers high-risk exploits.

2.2.3.1 Network Switches

Switches allow incoming network traffic to be broadcasted to connected devices. By sending the necessary packets to their appropriate destinations through VLANs, switches effectively manage each communication link in the system for automation tasks. Generally, switches offer smarter functionality than hubs. Switches are multi-port devices that enhance network efficiency and are commonly utilized to interconnect Local Area Network (LAN) segments. They possess the capability to interpret the hardware addresses of incoming packets, directing them to their appropriate destinations. By establishing virtual circuits, switches demonstrate superior performance compared to hubs and routers in terms of network efficiency. Furthermore, they can enhance network security by rendering these virtual circuits less detectable to network analyzers. In essence, switches amalgamate the beneficial features of both routers and hubs. Within the Open Systems Interconnection

(OSI) model, a switch functions at the Data Link layer or the Network layer. A multilayer switch, which functions at both layers, acts as both a switch and a router, utilizing the same routing protocols as routers. To protect against malicious traffic such as Distributed Denial of Service (DDoS) attacks, switches are equipped with flood guards. It is vital to secure the following switches through port security measures: disable any unnecessary ports using MAC address filtering, ARP inspection, and DHCP snooping. **(**(Eswar & S, 2021).

Two types of switches are available,

1. Managed switches
2 . Unmanaged switches

Aspect	Managed Switch	Unmanaged Switch
Configuration	Open to configuration	Can not configuration
Technical Skill	Required	Not required
Features & Capabilities	STP, QoS, Port monitoring	Only the MAC address table
Security	Strong	Basic

Table 01: Managed Switch vs Unmanaged Switch

(Managed vs Unmanaged Switch, n.d.)

2.2.3.2 Network Firewall

A network firewall systematically evaluates and filters both incoming and outgoing data streams in compliance with established protocols to protect the internal network. Its principal function is to serve as a barrier between a secure internal network and an unreliable external network. The firewall can be configured to prevent unauthorized access, assess potentially harmful data, and prevent intrusion attempts, all governed by specific rules.Firewalls may be deployed as either hardware or software solutions. Threats can arise from both external and internal sources. External threats include viruses, backdoors, phishing emails, and denial-of-service (DoS) attacks, while internal threats stem from malicious actors or risky applications. The present cybersecurity landscape demands a holistic approach. While firewalls are essential for netw3ork security, advanced attacks

call for further protective measures. As cloud computing and hybrid work arrangements continue to grow, it's becoming more important than ever to have solid security solutions in place. Next-generation firewall technologies, combined with AI-driven services, are making network security even more effective. By blending the strengths of traditional technologies with the cutting-edge features of modern solutions, today's firewall providers are helping organizations protect themselves against the increasingly sophisticated tactics of cyber attackers. Next-Generation Firewalls provide organizations with protection against escalating cyber threats, incorporating the best aspects of previous firewall technology along with the enhanced capabilities needed to tackle current challenges. (*What Is a Firewall? Definition and Types of Firewall | Fortinet*, n.d.)

Deep Packet Inspection (DPI): Also referred to as packet sniffing, this technique involves looking at data packets' contents as they go by a network checkpoint. An administrator or an internet service provider (ISP) may preconfigure specific rules that DPI employs to examine the contents of data packets. It then ascertains the appropriate response to the identified hazards. Intrusion Prevention (IPS): Intrusion prevention systems require network security technology that continually evaluates network data to detect threats. A widespread deployment for an IPS security service is "in-line," meaning that it resides in the direct communication path between the source and the destination. This enables it to examine every network traffic flow in real time and take immediate preventive action.

Data Loss Prevention: A cybersecurity technology called Data Loss Prevention discovers and prevents data breaches. Corporations adopt it for regulatory compliance and internal security, as it prevents sensitive data from being accessed. The possibility of data breaches—situations in which an unauthorized person acquires, accesses, or reads protected information—has grown drastically as the world has become more digitally linked. DLP is a key tool for firms looking to secure sensitive information.(*What Is Deep Packet Inspection (DPI)? | Fortinet*, n.d.)

2.3 Device Hardening Techniques

2.3.1 Concept and importance of hardening devices.

Device hardening involves enhancing a device's security against cyber-attacks by identifying and mitigating vulnerabilities that could be exploited. By decreasing the likelihood of breaches, device hardening significantly contributes to a secure system, safeguarding sensitive information and ensuring critical data stays protected. ((*Device Hardening Explained: Strengthening Cybersecurity Foundations*, n.d.-a)

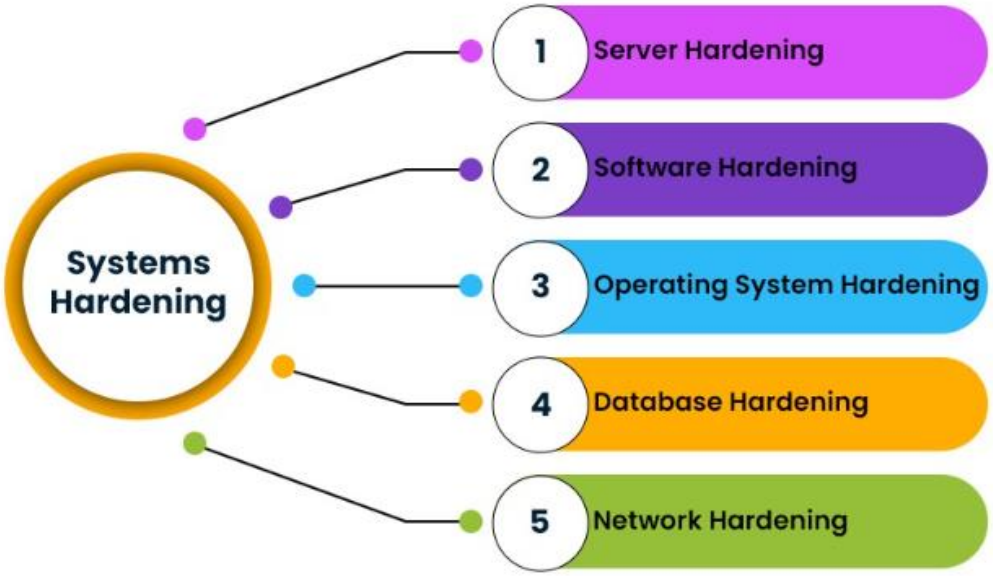

Figure 05: Type of Device Hardening

(*What Is Device Hardening and Its Different Types?*, n.d.)

2.3.1.1 Server Hardening

Server hardening involves securing ports, data, role-based permissions, and server functions. Some common security practices for server hardening are using strong passwords, locking user accounts after multiple failed login attempts, implementing multi-factor authentication, disabling USB ports, and closing unnecessary network ports. (*What Is Device Hardening and Its Different Types?*, n.d.)

2.3.1.2 Software Hardening

Application hardening focuses on securing the software installed on a device. Common methods include using antivirus, adware, and malware protection solutions, along with systems designed to detect intrusions. The advantages of application hardening encompass masking and integrity checks to ensure that applications remain unchanged. Furthermore, runtime application self-protection (RASP) is utilized to identify compromised devices, enabling appropriate actions to safeguard the applications. (*What Is Device Hardening? | Baeldung on Computer Science*, n.d.)

2.3.1.3 Operating System Hardening

Operating system hardening aims to protect the device's operating system. Common strategies include restricting access, limiting user account installations, and removing unnecessary device drivers that could expose the system to cyberattacks. Additional methods involve regularly applying OS updates through service packs and security patches, along with encrypting the storage that contains the operating system. (*What Is Device Hardening? | Baeldung on Computer Science*, n.d.)

2.3.1.4 Database Hardening

This includes three key elements essential for secure data storage. The first element is about managing user access and permissions. The second emphasizes the encryption of data sets and the removal of unnecessary functions. Finally, the third element involves monitoring database activities. Moreover, to ensure a secure database, it is vital to regularly update passwords, configure firewalls, and establish proper backup and recovery protocols. (*What Is Device Hardening and Its Different Types?*, n.d.)

Network Hardening

Network hardening techniques explain how to enhance security between two network ports and the data packets traveling through the network. Implementing encryption and configuring firewalls are effective practices for improving network security. (*What Is Device Hardening? | Baeldung on Computer Science*, n.d.)

2.3.2 Practical methods

Many hackers succeed in gaining access to servers or workstations due to outdated software and services. They continuously exploit vulnerabilities in older software and hardware. Thus, the primary defensive measure should be to regularly update both software and hardware. Keeping the operating system, BIOS, and firmware up to date are considered best practices.

One effective strategy is to strengthen the network by configuring the firewall to minimize the risk of network-based attacks. Set up configurations to block and filter unnecessary IP addresses or MAC addresses that don’t engage with the system. Furthermore, control inbound and outbound network traffic through established rules.

By implementing precise access controls and role-based permissions, organizations can mitigate the risks of internal threats and unauthorized access, thereby protecting the integrity of their digital systems. Eliminate or deactivate unnecessary services, protocols, and features that are not in use, as each active service poses a potential entry point for attackers.

When creating passwords, incorporate a mix of letters, numbers, and special characters at specific lengths. The adoption of multifactor authentication enhances security levels significantly, ensuring that one password isn't reused across various websites or services. Password phrases should exceed 12 characters and be structured in a way that makes them difficult to read. A random sequence of characters or patterns is preferable to using repeated phrases. Using a code sent to a mobile phone provides extra protection against unauthorized access. Additionally, multifactor authentication includes various verification methods such as biometric recognition and third-party authentication apps, which help secure the connection with the user.

Backing up and restoring data is a key practice to secure information, preventing complications during security incidents or data loss. Incremental backups and cloud storage offer the most promise for efficient backups and restorations.

2.3.3 Challenges with the device hardening process

Device hardening has numerous challenges in a real situation. It involves a lengthy and complicated process that requires more IT knowledge and awareness of various technical stuff, especially for Linux systems. Hardening requires regular software or firmware upgrades, or hardware upgrades due to emerging danger or hardware evaluation. Some steps or services, like multifactor authentication, can be annoying for users.

To generate an impact analysis report that delineates the effects of policy on production, it is imperative to establish a test environment. The challenge arises from the diversity of infrastructure's environments, machines, and applications. Older systems may lack compatibility with contemporary security measures, resulting in substantial difficulties in fortifying these systems. This scenario can pose significant challenges in safeguarding older devices against emerging threats. The threat landscape keeps changing, with new vulnerabilities and attack methods emerging regularly. Hardening practices need to be adjusted in response to these emerging threats.(*Device Hardening Explained: Strengthening Cybersecurity Foundations*, n.d.-b)

2.4 ABB Existing Cybersecurity Guidelines

ABB adheres to rigorous guidelines for the cybersecurity of project deployment. Most of these guidelines are derived from IEC 62443 international standards, NIST, and internal cybersecurity protocols, with an emphasis on system security and industrial networks. This discussion focuses solely on the essential policies pertinent to the project deployment of Distribution Solutions.

2.4.1 IEC 62443 Standards

The International Electrotechnical Commission (IEC) has established ISA/IEC 62443, a series of global cybersecurity standards tailored for industrial automation and control systems (IACS). The IEC 62443 series of standards is derived from the ISO 27000 series and specifically addresses the distinct requirements of Information Technology (IT) and Operational Technology (OT) within the context of industrial communication. This series encompasses components that outline the procedural requirements throughout the life cycle and their implementation for maintenance service providers, as well as suppliers of

industrial automation systems. The IEC 62443 offers a structured framework for addressing these challenges and for executing cybersecurity measures specifically designed for IACS. Furthermore, ISA/IEC 62443 provides a comprehensive methodology for identifying and mitigating vulnerabilities in industrial networks, whilst safeguarding the confidentiality, availability, and integrity of essential systems integrity.(*IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems | Fortinet*, n.d.)

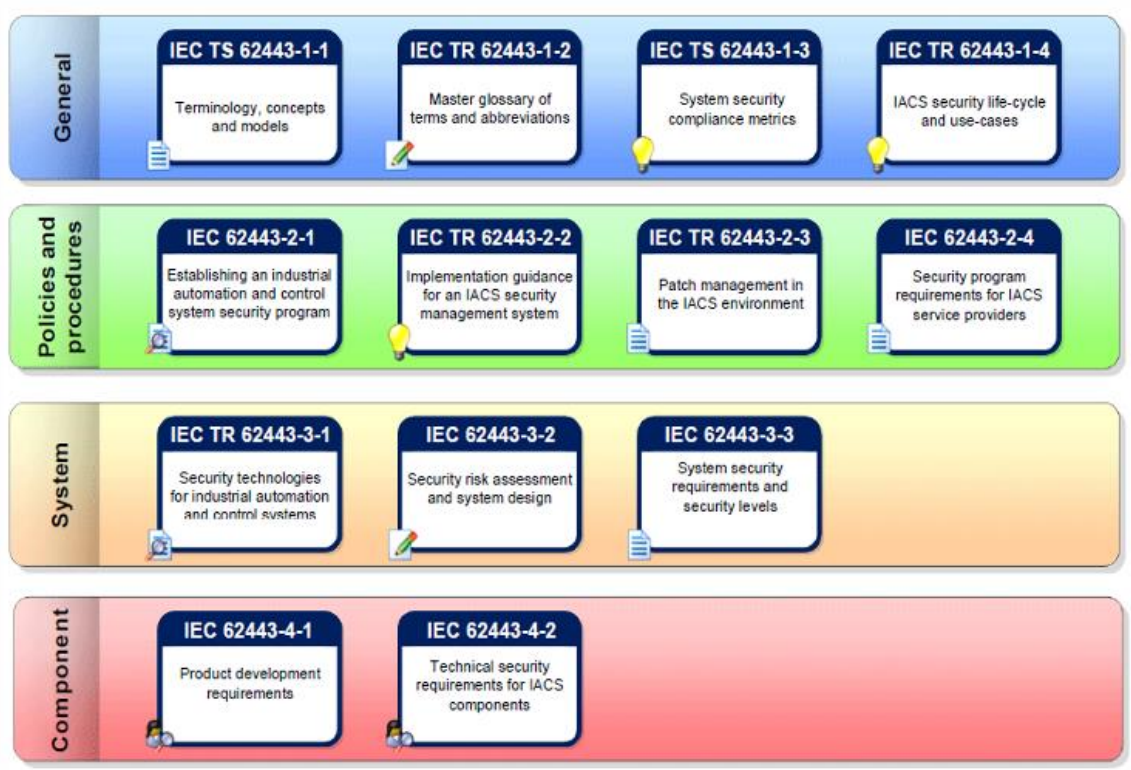

Figure 05: IEC62443 components

General (IEC 62443-1):

Provides an in-depth overview of the IEC 62443 security standard, including definitions, concepts, and models employed in the standard. It contains underlying documentation that facilitates a comprehensive understanding of the entire structure.(*IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems | Fortinet*, n.d.)

Policies and Procedures (IEC 62443-2):

Utilizes established standards, strategic methodologies, and management techniques to guide the development of an effective cybersecurity program within Industrial Automation and Control Systems (IACS). It stipulates that the asset owner or end-user is responsible for creating and implementing security management protocols systems.(*IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems | Fortinet*, n.d.)

System (IEC 62443-3):

Implements and manages a secure IACS by tackling safety issues at the system level. It encompasses system design, risk evaluation, and the deployment of security technologies within Industrial Automation and Control Systems (IACS) settings.(*IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems | Fortinet*, n.d.)

Component (IEC 62443-4):

This document delineates the specifications for the technical functionality, development life cycle, and security of the system's industrial network components. It ensures that, from product creation to deployment, all components comply with security standards.(*IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems | Fortinet*, n.d.)

Cybersecurity threats in industrial automation and control systems are addressed by a set of security levels (SL) under the IEC 62443 framework. Four security levels

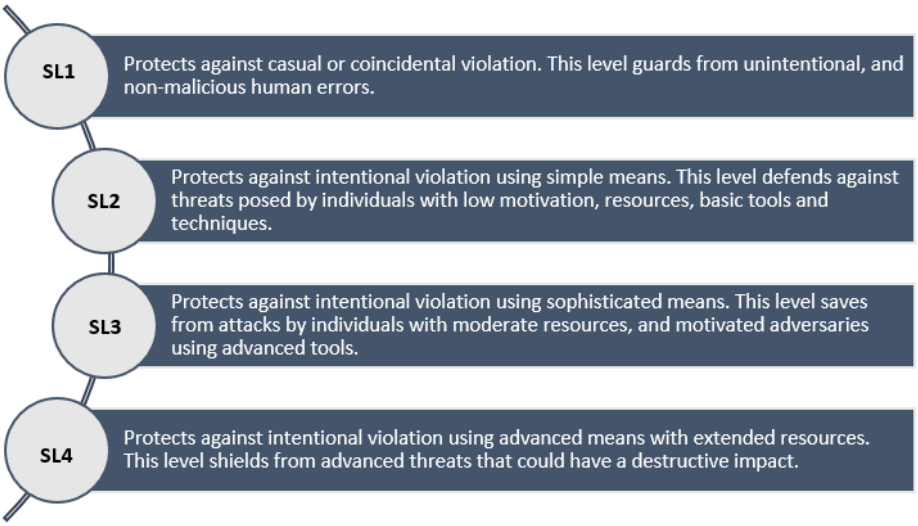

Figure 06: Security levels of IEC62443

Seven fundamental requirements are associated with each IEC 62443 security level to ensure a high level of security.

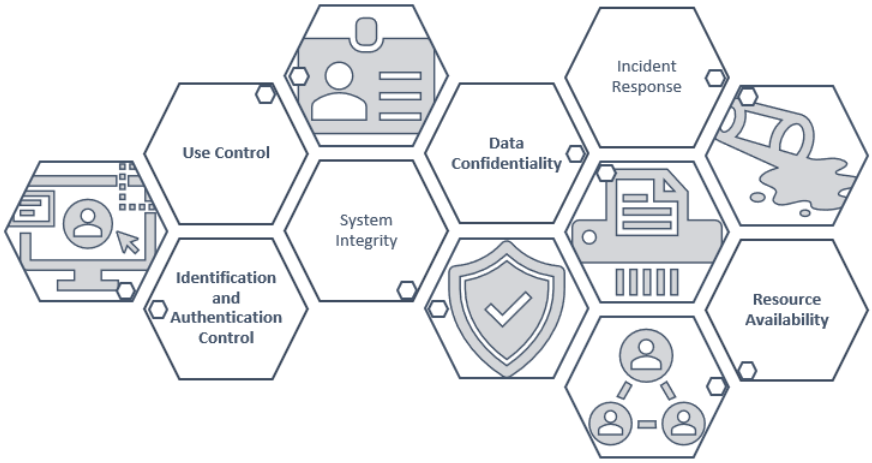

Figure 07: IEC62443 requirements

2.4.2 ABB's cybersecurity guidelines

In this subchapter, the cybersecurity guidelines for automation projects in distribution solutions are discussed. ABB follows international standards and

IEC62443:2018

Distribution solutions in Vaasa comply with IEC62443:2018 secure product development lifecycle requirements.(*IEC 62443 Part 4-1: 2018 Secure Product Development Lifecycle Requirements*, n.d.)

IEC62443-3-2

The risk analysis of the system for establishing zones and conduits represents a vital aspect of the security management process. A comprehensive risk assessment is essential for assigning an appropriate security level to each zone. Furthermore, conducting a risk assessment for the communication conduits is imperative, as this delineates the overall security management framework of the system. The steps are shown as follows.

- Identification of the system under consideration
- Define Security Requirements
- Define Zones and Conduits
- Detailed risk assessment
- Compare individual risks with tolerable risks
- Design security measures

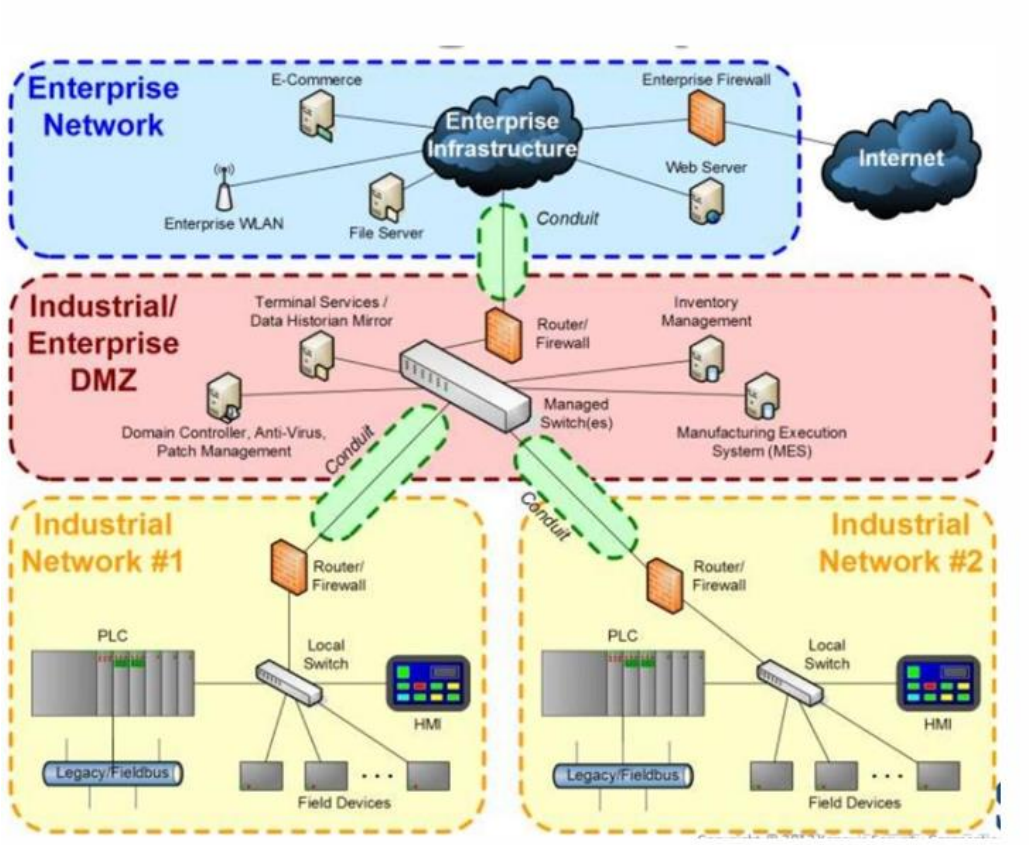

Figure 08: Concept on the system level

IEC62443-2-4 - Requirements for IACS Service providers

IEC62443-2-4 delineates the security features that service providers for IACS integration and maintenance must possess to deliver system integration and automation activities for an automation solution.

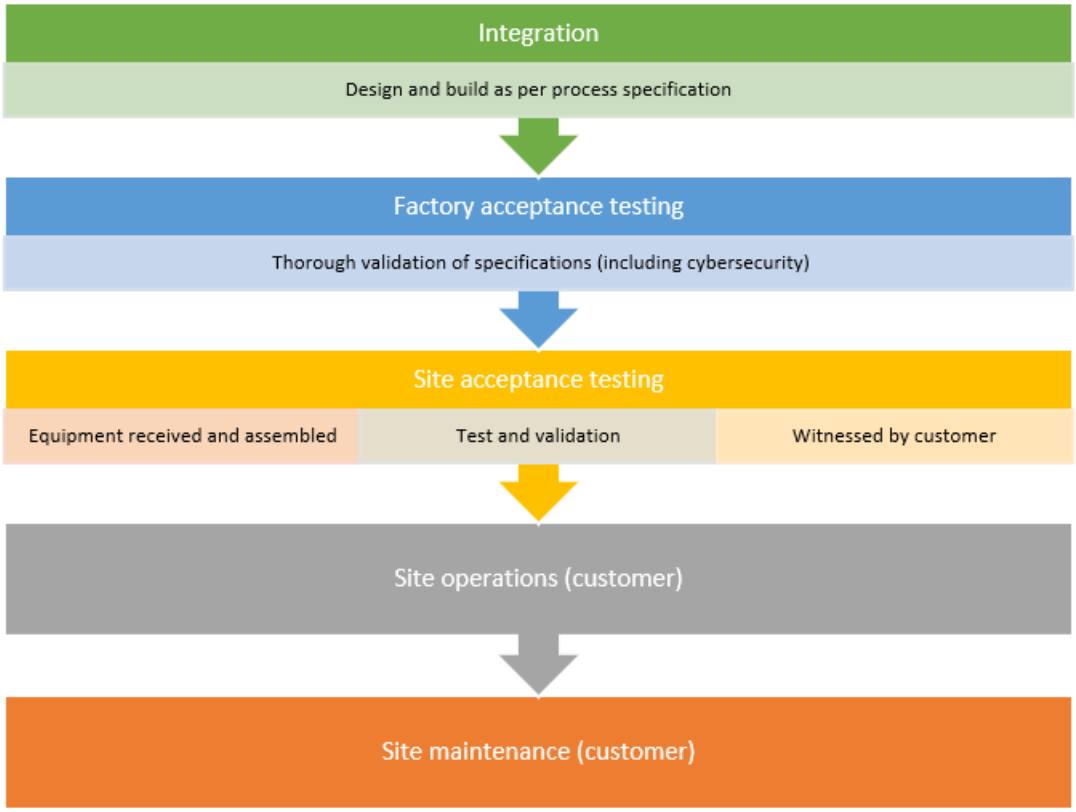

Figure 09: Major areas covered by IEC62443-2-4

ABB Distribution Solutions enforces its cybersecurity guidelines to effectively tackle security concerns and requirements for customer projects. The newly released ABB cybersecurity standards mainly focus on deployment projects and field operations service. (ABB Group Cyber Security Council, n.d.)

Any deployment project pertaining to ABB must conform to the stipulations outlined in Section 2 of this document, particularly when it encompasses activities such as the installation or commissioning of any software-related products or systems, or when there is a requirement for access to or modification of customer software products or systems. All elements of the delivery, in conjunction with ABB's engineering, implementation, and commissioning endeavors, must be in accordance with the directives set forth in Section 2. The clientele includes end-users, system integrators, engineering firms that subcontract with ABB, as well as entities involved in engineering, procurement, and construction (EPC) contractors.(ABB Group Cyber Security Council, n.d.)

RACI Matrix	Operations Organization	Division Cyber Security Officer	Project Manager
Compliance with this standard for every project.	A	C	R
Approval of compliance with this standard for every project.	I	A	R

Table 1: **R** = Responsible, **A** = Accountable, **C** = Consulted, **I** = Informed

Table 02: Role and Responsibilities

ABB Standard	Standard Title	Description	Covering International Standard
ABB-DSP-3	Security expertise	All ABB employees involved in deployment projects from tendering to commissioning shall be adequately trained on cyber security depending on their role.	IEC 62443-2-1 IEC 62443-4-1 ISO 27001
ABB-DSP-4	Project environment security	All ABB IT Assets involved in the establishment of the above-mentioned protection, and specifically segregation, shall be compliant with applicable ABB Information Security Policies and Standards.	ISO/IEC 27001:2022
ABB-DSP-5	Malware propagation protection	This standard outlines key measures to prevent, detect, and mitigate malware threats, including anti-malware software, user training, access controls, and secure change management	ISO/IEC 27002:2022, Control 8.7 ISO/IEC 27001:2022
ABB-DSP-6	Patch management	Up until the transfer of cybersecurity responsibility, any system node or software included in the ABB delivery shall, as technically feasible, be periodically updated with latest available patches, hotfixes, updates, and/or service packs for software.	IEC 62443-2-3 ISO/IEC 27001:2022
ABB-DSP-7	Deployment guidelines	Any product or system feature not to be used by the customer and/or end-user shall be disabled or removed as described in deployment guidelines provided with the product or by the Divisions.	IEC 62443-3-3 ISO/IEC 27001:2022
ABB-DSP-8	Removal of temporary software, configurations, and accounts	Before the delivery handover to the customer, all software, configurations, and accounts that have only been added/set to engineer, test, and/or commission the system and are not required for the operation or maintenance of the delivery shall be removed.	ISO/IEC 62443-3-3
ABB-DSP-9	Product development	Any project-specific or local product development and/or adjustment shall be in accordance with the Security Development Life Cycle Standard, Product Security Standard, and Cloud Offering Security Standard as applicable.	IEC 62443-4-1:2018
ABB-DSP-10	Project documentation	At the delivery handover to the customer, the project documentation on ABB's deliveries shall include as a minimum the following up-to-date information. Inventory of installed software/firmware including their versions where such information is readily available or easily obtainable from the system node. • List of used/required ports and services for each delivered system node including identification of those necessary for external connections. • Used security and hardening product/system deployment guidelines. • Security and hardening settings if applied in addition to what is described in the product/system deployment guidelines. • List of all user and system accounts and a clear written recommendation to change the default accounts and passwords immediately after handover.	IEC 62443-2-4 IEC 62443-3-3 ISO/IEC 27001 ISO/IEC 27002
ABB-DSP-11	Contractual framework	As part of the overall contractual framework with the end-user, appropriate language shall be used to minimize risks associated with cyber security in accordance with the guidelines provided by CF-LI	ISO/IEC 27001/2 NIST Cybersecurity Framework (CSF) IEC 62443-2-4
ABB-DSP-12	Integration and procurement of 3rd-party products	Procurement of any 3rd-party software-related product delivered to, or part of systems delivered to, ABB customers shall be in accordance with the Minimum Cyber Security Requirements for Product Procurement.	ISO/IEC 27036 ISO/IEC 62443-2-4 NIST Cybersecurity Supply Chain Risk Management (C-SCRM)

Table 03: Deployment Project Security Standard

2.5 Introduction to NIS2

After the conclusion of World War II in Europe in 1945, European leaders initiated the establishment of the European Union. To further democracy, safeguard human rights, and uphold the rule of law, 10 Western European nations established the Council of Europe. The European Union Agency for Cybersecurity (ENISA), an EU institution, is dedicated to enhancing the cybersecurity level throughout Europe. ENISA was established in 2004 and provides resources, knowledge, and guidance to the European Union and its member states to strengthen cybersecurity resilience. (Eprs, n.d.)

The EU Agency for Network and Information Security (ENISA) has released monitoring statistics that show cybercrime has become increasingly lucrative, particularly in large ransomware-based intrusions. Similar to this, the rise of e-commerce and cashless payment methods heightens the risks of cybersecurity breaches and financial crime. Cashless payments have led to a rise in online theft of both money and personal information. An ENISA Threat Landscape 2021 report suggests that cyberattacks have gotten increasingly complicated, concentrated, ubiquitous, and invisible. It also concludes that societies still have a long way to go before they can guarantee a more secure digital environment. Verizon believes that espionage accounted for 10% of breaches in 2019 and financial incentives for 86% of them. Roughly 45% of breaches included hacking, 17% included malware, and 22% involved phishing. This tendency is projected to continue developing in parallel with technology improvements like the proliferation of Internet of Things (IoT)-connected devices. The rising cybersecurity issues in a world where 22.3 billion IoT devices are anticipated to be in use by 2024 have spurred the EU to investigate methods to better defend its companies and people from cyber threats and attacks. (Eprs, n.d.)

Globally, civilizations are seeing an unexpected acceleration in their digital transition due to the coronavirus epidemic. Critical industries, such as transport, energy, health, and finance, have grown more reliant on digital technology to conduct their core operations. While expanding digital connectedness delivers enormous potential, it also exposes economies and society to cyber threats. The number, complexity, and size of cybersecurity events are expanding, as are their economic and societal consequences. However, technology has also made preexisting issues worse, such as the digital divide, and led to an

increase in cybersecurity incidents worldwide. Amid an extraordinary circumstance, Malicious cyber activity has increased in all Member States, according to a recent Europol study. The EU is increasingly facing daily challenges related to cybersecurity. (Eprs, n.d.)

2.5.1 NIS Directive

The European Union's (EU) first cybersecurity law was the Directive on Security of Networks and Information Systems (NIS Directive). Adopted on July 6, 2016, the Directive aims to establish a high level of information and network security for all EU member states. After the Directive went into force in August 2016, EU member states had 21 months to incorporate its provisions into their national legislation and another 6 months to determine which enterprises needed to comply with the NIS Directive. The NIS sets out certain network and information security standards relevant to digital service providers (DSPs) and operators of essential services. The legislation designates companies in the energy, transportation, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure sectors as operators of key services. Every EU Member State is required to create a list of firms it identifies as essential service providers in compliance with the NIS Directive. (What Is the NIS Directive? | Digital Guardian, n.d.)

Key components of NIS directive

- The first key component of the NIS directive is the National Cyber Security Strategy, which reveals each EU member state should develop a national strategy to address cyber security incidents and risks. Which defined roles, responsibilities, and measures for risk management**. (**(*Directive - 2016/1148 - EN - EUR-Lex*, n.d.)
- The cooperation group is the second essential component of the NIS, which pertains to the facilitation of information and strategic plan exchange among member nations**.** ((*Directive - 2016/1148 - EN - EUR-Lex*, n.d.)

- The third objective is to build and strengthen a robust network of Computer Security Incident Response Teams (CSIRTs) across the EU. (*Directive - 2016/1148 - EN - EUR-Lex*, n.d.)
- All operators of essential services and related digital service providers must prioritize the implementation of certain risk management measures and incident reporting protocols**.** ((*Directive - 2016/1148 - EN - EUR-Lex*, n.d.)

Operators of Essential Services (OES) and Digital Service Providers (DSPs) can be classified according to the criticality of the service they provide and the sectors they operate in. Organizations classified as OES play a role in essential services such as energy, transportation, banking, healthcare, water supply, and digital infrastructure. DSP organization's services directly impact the digital economy and functioning under digital infrastructure. For example online markets, cloud computing, and Data centers. (*Operators of Essential Services and the NIS Regulations*, n.d.)

2.5.2 NIS2 Directive

The NIS Directive is the first EU cybersecurity regulation aimed at increasing the resilience of network and information systems in the EU against cybersecurity hazards. Despite its considerable successes, the NIS Directive has exhibited several limits. The digital change in society, compounded by the COVID-19 problem, has extended the danger landscape. Fresh challenges have developed, which demand adaptive and imaginative remedies. Therefore, in December 2020, the Commission proposed a new set of anticipated measures to increase the degree of cyber resilience in the Union concerning the rising hazards brought about by digitalization and connectivity. The co-legislators established a political agreement on May 13, 2022, and the new Directive was legally approved in late November 2022. (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's Digital Future*, n.d.-a)

A single legal framework is established by the NIS2 Directive to protect cybersecurity in 18 vital EU industries. NIS2 expands the scope, clarifies regulations, and fortifies oversight mechanisms to enhance the EU's shared level of ambition on cyber-security. In addition to imposing reporting obligations and risk management measures on companies from more sectors, it mandates that Member States improve their cybersecurity capabilities and establish guidelines for collaboration, information exchange, oversight, and cybersecurity

enforcement**.** (*NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems | Shaping Europe's Digital Future*, n.d.)

Along with the industries already covered by NIS 1, including energy, transportation, healthcare, finance, water management, and digital infrastructure, these regulations also apply to companies that offer public electronic communications services, additional digital services like social media, wastewater, and waste management, the production of essential goods, postal and courier services, and public administration, both locally and nationally. Generally, medium-sized and big organizations in these vital industries will need to implement suitable cybersecurity risk-management strategies and report major occurrences to the appropriate government institutions. (*NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems | Shaping Europe's Digital Future*, n.d.)

Under the directive, each member state is required to establish a national cybersecurity plan that covers supply chain security, vulnerability management, and cybersecurity awareness and education. Member states must also establish and update a list of operators of vital services and ensure that these organizations adhere to the directive's standards. (*NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems | Shaping Europe's Digital Future*, n.d.)

Under the directive, each member state is obligated to produce a national cybersecurity strategy that encompasses supply chain security, vulnerability management, and cybersecurity awareness and education. Member states must also prepare and maintain a list of operators of critical services and ensure that these organizations conform to the directive's criteria. (*NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems | Shaping Europe's Digital Future*, n.d.)

Under the new rules, the EU is better equipped to prevent, manage, and respond to large-scale cybersecurity crises and disasters. By putting in place stronger EU cooperation, rigorous planning, and clearly defined tasks, they accomplish this. NIS2 mandates that Member States establish national authorities responsible for cyber crisis management, utilize national large-scale cybersecurity incident and crisis response plans, and establish the European Cyber Crisis Liaison Organization Network (EU-CYCLONe) to facilitate the coordinated handling of large-scale cybersecurity incidents and crises at the operational

level. This Network was vital in the building of the European Union's cyber crisis management framework as part of the Commission's 2017 Recommendation on Unified Response to Large-Scale Incidents and Crises. (NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems | Shaping Europe's Digital Future, n.d.)

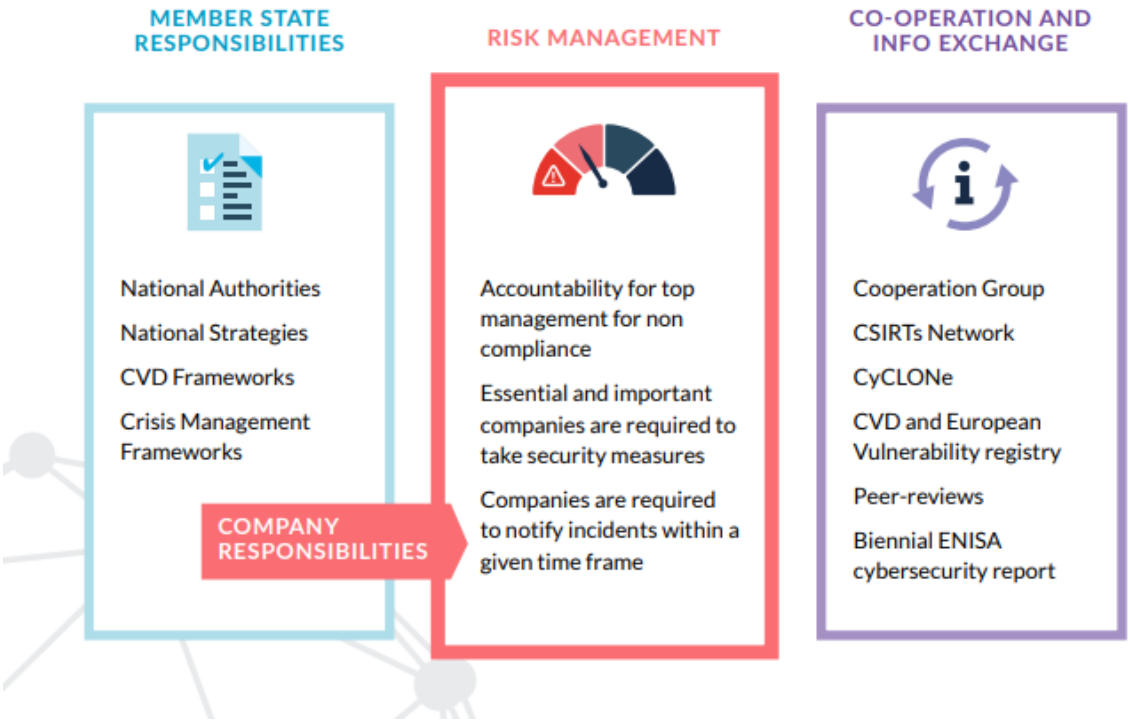

Figure 10: Three Main Pillars of NIS2 (*NIS 2 A Quick Reference Guide*, n.d.)

Requirements of NIS2

The NIS2 Directive establishes essential cybersecurity criteria to enhance organizational resilience and safeguard critical services. It encompasses regulations for risk assessment, the maintenance of secure information systems, and the implementation of comprehensive plans for addressing cyber incidents, to prevent, detect, and respond to such incidents expediently. To enhance their operational resilience, organizations need to create policies related to business continuity and crisis management. Additionally, the directive focuses on supply chain security, which encompasses collaboration with suppliers and service providers, such as data storage, processing services, and managed security services. In addition to acquiring, developing, and sustaining network and information systems, it is imperative to consider security measures aimed at controlling and disclosing

vulnerabilities. Organizations need to establish policies and procedures to evaluate the effectiveness of cybersecurity risk management strategies, such as regular assessments and audits. Finally, the directive stipulates that encryption and cryptography must be utilized to protect sensitive data and communications. (*NIS2 Directive - What Are the NIS2 Requirements? | Conscia*, n.d.)

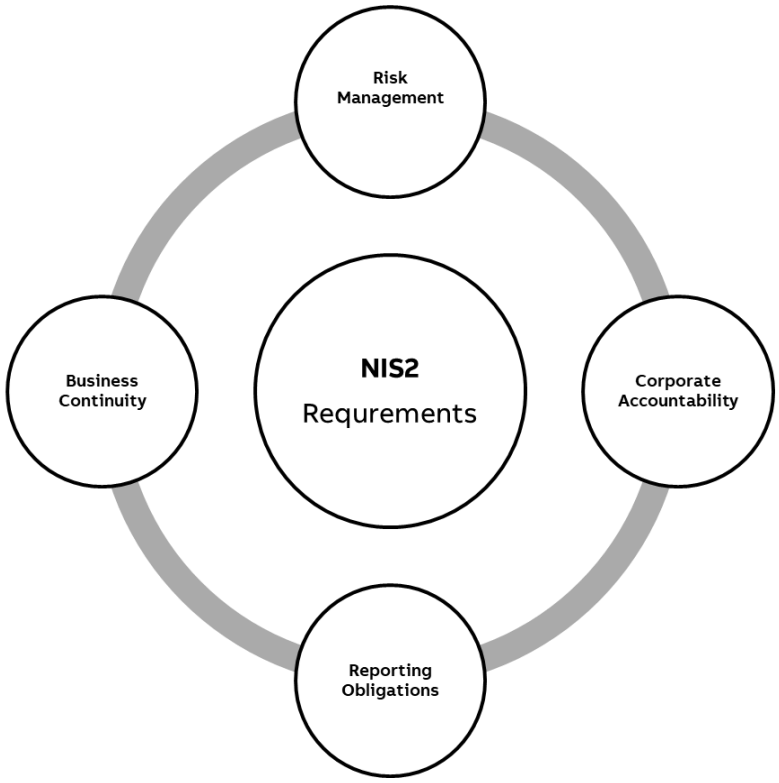

Figure 11: Key Requirements of NIS2

Key elements

The Directive expands the scope of the existing laws by adding additional industries depending on their degree of digitization and interconnection as well as their relevance to the economy and society. This is done by defining a defined size threshold regulation, which implies that all medium- and large-sized enterprises in specified industries will be included in the scope. Nonetheless, it also provides Member States substantial latitude in determining whether to implement the new Directive's provisions on smaller enterprises with a high-security risk profile. The disparity between operators of essential services and digital service providers is erased under the new Directive. Entities are defined according to their significance and are grouped into two categories—essential entities—each subjected to a particular monitoring system. (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's Digital Future*, n.d.-b)

The adoption of a risk management strategy enhances and simplifies security and reporting criteria for enterprises. This strategy includes a minimum list of essential security elements that must be implemented. The new Directive imposes more explicit rules regarding how to report incidents, the content of the reports, and the deadlines. (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's Digital Future*, n.d.-b)

NIS2 tackles the security of supply chains and supplier connections, mandating organizations to manage cybersecurity threats effectively. Additionally, the Directive strengthens cybersecurity measures for essential information and communication technology at the European level. Union-level coordinated security risk assessments of important supply chains may be carried out by Member States, in partnership with the Commission and ENISA, based on the successful methodology employed in the context of the Commission's Recommendation on the Cybersecurity of 5G networks. (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's Digital Future*, n.d.-b)

The role of the cooperation Group in developing strategic policy decisions is reinforced, coupled with improved information exchange and collaboration among Member State institutions. Operational collaboration within the CSIRT network is also reinforced, and the European Cyber Crisis Liaison Organization Network (EU-CyCLONe) is formed to facilitate the coordinated handling of large-scale cybersecurity events and crises. (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's Digital Future*, n.d.-a)

How will the NIS2 Directive be monitored and implemented?

Competent authorities are competent to manage critical and substantial firms. These consist of targeted and regular audits, on- and off-site inspections, information requests, and document or evidence access. In terms of enforcement, Member States have historically been unwilling to impose sanctions on enterprises that omit to report occurrences or install security measures. As a result, entities' cyber resistance may degrade. The new Directive sets a common framework for sanctions throughout the Union to ensure effective enforcement. As a result, it establishes a minimal set of administrative sanctions for breaching the NIS2 Directive's cybersecurity risk management and reporting requirements. Examples of these punishments include administrative fines, required instructions, mandates to implement the conclusions of security audits, and orders to align

security measures with NIS requirements. The new NIS Directive draws a difference between major and critical firms concerning administrative sanctions. Major corporations must pay administrative fines of at least €10,000,000 or 2% of their worldwide annual turnover from the preceding fiscal year, whichever is bigger, according to this regulation. According to NIS2, Member States shall impose a maximum penalty on major firms of at least €7,000,000 or 1.4% of their worldwide annual turnover from the preceding fiscal year, whichever is larger. (*Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's Digital Future*, n.d.-a)

2.5.3 Comparison between NIS and NIS2

Aspect	NIS	NIS 2
Scope	Cover • Digital service providers (DSPs) and fundamental • Services such as electricity and healthcare.	Expanded , • Digital infrastructure, • public administration, and space sectors.
Entity Classification	• operators of essential services (OES) • Digital Service Provider	• Essential • Important
Security requirement	Basic rules for managing risks and dealing with incidents.	More specific security needs include risk management and supply chain security procedures.
Incident Reporting	Lack of guidelines	• Early warning within 24 Hr

		• Detailed report within 72 Hr
Supply chain security	Insufficient attention to supplier relationships.	Increased focus across industries on supply chain security
Penalties	No Penalties across member states	Penalties for non-compliance
Cooperation	Required more collaboration	Enhanced cooperation and established the EU-CyCLONe to manage the cybersecurity crisis.

Table 04: Comparison between NIS vs NIS2

2.6 Comparison Between ABB Guidelines vs NIS2 Guidelines

ABB has initiated aligning its cybersecurity policies with the NIS2 Directive to ensure compliance with the latest EU cybersecurity legislation.

NIS2	ABB
Risk analysis and information system security policies require operators to perform a cybersecurity risk assessment on production systems and identify essential components.	Implementation has occurred. ABB performs IEC 62443-based risk assessments of any production system, irrespective of the ICS vendor. The ABB Cyber Security Risk Assessment teams initially conduct a comprehensive cyber security risk assessment to identify both system-wide and system-specific risks. • **ABB Cyber Security Consulting**

Improved incident handling. Operators must detect cybersecurity compromises and incidents and report these incidents to the asset owner.	ABB provides tools and services to help to detect and respond to incidents through ABB Care. • **24x7 support through an ABB Care Contract** • **ABB Ability™ Cyber Security Event Monitoring with Incident Response** • **ABB Ability™ Cyber Security Workplace**
Improvements in business continuity planning... Operators must define their procedures to ensure prompt restoration of production in case of a cyber incident, starting with the business impact analysis.	ABB helps with contractual commitments of resources with appropriate response times and creating technical recovery plans. • **24x7 support through an ABB Care Contract** • **Consultancy services** • **Backup & Recovery**
Supply chain security, which encompasses security-related elements regarding the connections between each entity and its immediate suppliers or service providers, is essential for fortifying one of the most frequent attack vectors. Operators need to identify information security (IS) requirements for their direct suppliers and implement programs for monitoring and verifying suppliers through audits.	ABB has covered with certifications (ISO/IEC 27001, IEC 62443-2-4) and supplier monitoring. • **ABB's Cyber Security Requirements for Suppliers**
Security in network and information systems encompasses acquisition, development, maintenance, and	ABB's development process is based on industry standards and is certified to these standards.

vulnerability management. Operators must define requirements for the entire information system lifecycle: planning, development, testing, maintenance, and replacement. .	• **ABB's Approach to Software Vulnerability Handling** • **ABB's Alerts and Notifications** • **IEC 62443-4-1 Certified Development Organization** • **IEC 62443-4-2 Certified Components** • **IEC 62443-3-3 Certified Systems**
Policies and procedures for evaluating the effectiveness of cybersecurity risk management strategies must be established. Operators are mandated to develop processes for assessing the efficacy of protective measures implemented in information security.	ABB helps with stay on top of security with solutions and services. • **ABB Ability™ Cyber Security Workplace** • **GAP assessments** • **Consultancy Services incl. Information Security Management System Support**
Fundamental cyber hygiene practices and cybersecurity training are crucial for improving organizational readiness and resilience. Operators must guarantee that only personnel from the service provider are designated to tasks concerning automation solutions.	ABB strengthens team's capacity to recognize and tackle cyber threats. Additionally, a training matrix has been launched for project stakeholders within the distribution system standards guidelines. • **Security Training**
Policies on cryptography and encryption are crucial for enhancing organizational defenses against threats. Operators must create clear definitions and documentation	ABB enables the implementation of cryptographic measures, which include encrypted communication, signed software packages, and secure remote access.

for implementing cryptography, encryption, and digital signatures in information systems.	• Secure Remote Access • IPSec at the HMI level
Implement enhanced human resources security, access control policies, and asset management to foster a culture of cybersecurity awareness. Service providers must maintain an inventory register to ensure their automation solutions support account management effectively.	ABB develop cybersecurity procedures and manage users securely. • **ABB Ability™ Cyber Security Workplace with asset inventory and OTPs for administrative support accounts**
Multi-factor and continuous authentication, secured voice, video, and text communications, and improved emergency systems are essential for protecting networks against emerging threats. Service providers must support multi-factor authentication for automation solution workstations, as required by asset owners.	The industrial cybersecurity experts at ABB will provide assistance in fulfilling the requirements of NIS2 and in implementing Multi-Factor Authentication (MFA) within the Windows environment of Human-Machine Interface (HMI). • **Consultancy services**
Notify within 24 hours of becoming aware of the incident. The notification does not increase liability for the notifying entity.	The initial step involves identifying incidents and ideally blocking the malicious actor from accessing the systems. ABB offers support through our monitoring solutions. • **ABB Ability™ Cyber Security Event Monitoring with Incident Response**

Table 04: NIS2 describes 10 categories of cybersecurity risk-management measures (Let's Get Your Organization Ready for NIS2 - ABB Advanced Digital Services (ABB Industrial Automation Service) AbilityTM Cyber Security | ABB, n.d.)

3 Method

This chapter emphasizes implementing security measures, vital to the NIS2 directive, as most NIS2 goals have already been met. Hardening is a major aspect of these security measures that requires focus. It includes the protocol for building a secure network architecture in automation projects. It aims to clarify hardening guidelines for various components such as managed switches, firewalls, Linux servers, Linux workstations, and process gateways.

3.1 Hardening

This thesis lays out steps that may be taken to improve the security of Linux automation systems used in a variety of projects. The goal is to gain a full understanding of how to harden devices. The main hardware parts that make automation projects possible are switches, firewalls, and servers. This study also talks about ways to limit access, store data, and safeguard passwords. (Device Hardening Explained: Strengthening Cybersecurity Foundations, n.d.-a)

3.1.1 Switches

----------Confidential ----------

3.1.1.1 Hirschmann Switches RSP30

----------Confidential ----------

Step 1. Initial Configuration

----------Confidential ----------

Step 2: Secure Authentication and Access Control

----------Confidential ----------

Step 3: Network Segmentation and Filtering

----------Confidential ----------

Step 04: Hardening Switch Configuration

----------Confidential ----------

3.1.2 Hirschmann Firewall

----------Confidential ----------

Step 1. Initial Configuration

----------Confidential ----------

Step 2: Secure Authentication and Access Control

----------Confidential ----------

Step 3: Network Segmentation and Filtering

----------Confidential ----------

Step 04: Hardening Switch Configuration

----------Confidential ----------

Step 5: Firewall Rule Configuration

----------Confidential ----------

3.1.3 Linux-based server

Step 1: Hardware Hardening

----------Confidential ----------

Step 2: BIOS/UEFI Settings

----------Confidential ----------

Step 3: Firewall configurations

----------Confidential ----------

Step 4: User Management

----------Confidential ----------

Step 5: SSH hardening

----------Confidential ----------

Step 6: NTP (Network Time Protocol) Synchronization or PTP

----------Confidential ----------

Step 7: Removable Media Prevention

----------Confidential ----------

Step 8: Backup and restore

----------Confidential ----------

4 Results

4.1 Case study /example project : ABB customer project for Norway

Objectives :

----------Confidential ----------

Network components:

----------Confidential ----------

Hischmann switch configuration

----------Confidential ----------

Dell PowerEdge XR4520c server

----------Confidential ----------

5 Discussion and Conclusion

The key focus of this thesis was to align the new cybersecurity directive, NIS2, for the ABB distribution project, which is an upgrade from NIS1. The main goal was to create a hardening guideline for the network devices utilized in most automation projects at ABB Distribution Solutions. Chapters 3 and 4 contain confidential information, so Chapters 3 and 4 are attached as an appendix and not published.

In the context of the NIS2 guidelines, hardening devices is vital for minimizing the attack surface of any network-related initiative. This study indicates that the ABB Cybersecurity team has initiated the implementation of most key NIS2 requirements. This thesis explores significant attempts to meet the essential needs set forth by NIS2. ABB Distribution Solutions participates in a range of automation initiatives encompassing switches, firewalls, servers, and ZEE600C devices. Given the project's scope, the results chapter did not include certain aspects of the applied guidelines. The Nessus report on the Dell server indicated that steps have been taken to reduce the server's vulnerability to security threats and attacks, making it more difficult for malicious actors to exploit. Given the extensive nature of cybersecurity, this thesis focused on three standard network devices. Hirschmann switches and a firewall were selected due to their user-friendly interfaces and ease of configuration. Although guidelines for the Hirschmann firewall were developed, testing has not yet been conducted. FortiGate firewalls are frequently employed in projects; however, they present several drawbacks, including the complexity and cost associated with firmware updates and patch management cycles. Consequently, Moxa switches and Moxa firewalls will be considered for future studies.

6 Reference

ABB Group Cyber Security Council. (n.d.). *Deployment Project Security Standard*. Retrieved 22 January 2025, from https://go.insideplus.abb.com/corporate-functions/research-and-development/cyber-security/standards/deployment-project-security-standard

Device Hardening Explained: Strengthening Cybersecurity Foundations. (n.d.-a). Retrieved 24 March 2025, from https://www.forensicit.com.au/post/device-hardening-explained-strengthening-cybersecurity-foundations

Device Hardening Explained: Strengthening Cybersecurity Foundations. (n.d.-b). Retrieved 26 May 2025, from https://www.forensicit.com.au/post/device-hardening-explained-strengthening-cybersecurity-foundations

Directive - 2016/1148 - EN - EUR-Lex. (n.d.). Retrieved 11 March 2025, from https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's digital future. (n.d.-a). Retrieved 12 March 2025, from https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's digital future. (n.d.-b). Retrieved 13 March 2025, from https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Eprs. (n.d.). *BRIEFING EU Legislation in Progress Proposal for a directive on measures for a high common level of cybersecurity across the Union*.

Eswar, M., & S, G. K. (2021). This work is licensed under a Creative Commons Attribution 4.0 International License A Study on Networking Devices. *International Advanced Research Journal in Science, Engineering and Technology*, *8*. https://doi.org/10.17148/IARJSET.2021.86119

Global Cybersecurity Outlook 2025 – Navigating Through Rising Cyber Complexities > Press releases | World Economic Forum. (n.d.). Retrieved 23 January 2025, from https://www.weforum.org/press/2025/01/global-cybersecurity-outlook-2025-navigating-through-rising-cyber-complexities/

IEC 62443 Part 4-1: 2018 Secure product development lifecycle requirements. (n.d.). Retrieved 18 May 2025, from https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A4542

IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems | Fortinet. (n.d.). Retrieved 18 May 2025, from https://www.fortinet.com/lat/resources/cyberglossary/iec-62443

Industrial cybersecurity with zenon | COPA-DATA. (n.d.). Retrieved 17 February 2025, from https://www.copadata.com/en/products/zenon-software-platform-for-industrial-automation-energy-automation/industrial-cybersecurity/#nis+2+directive

Managed vs Unmanaged Switch: What's the Difference? (n.d.). Retrieved 19 February 2025, from https://www.revesoft.com/blog/networking/managed-vs-unmanaged-switch/

NIS 2 A Quick Reference Guide. (n.d.). Retrieved 18 March 2025, from www.ncsc.gov.ie

NIS2 Directive - What are the NIS2 requirements? | Conscia. (n.d.). Retrieved 13 March 2025, from https://conscia.com/whitepaper/nis2-vision-key-objectives-and-tactical-strategies-for-your-organization/

NIS2 Directive: new rules on cybersecurity of network and information systems | Shaping Europe's digital future. (n.d.). Retrieved 11 March 2025, from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Operators of Essential Services and the NIS Regulations. (n.d.). Retrieved 11 March 2025, from https://www.itgovernance.co.uk/nis-regulations-oes-operators-essential-services

Ramjanee, S., & Shah, N. (2024). Towards an Integrated Wide Approach for Sustainable Upstream Field Recovery. *Computer Aided Chemical Engineering*, *53*, 1–6. https://doi.org/10.1016/B978-0-443-28824-1.50001-6

Sallans, B., Bruckner, D., & Russ, G. (2006). Statistical Model-Based Sensor Diagnostics for Automation Systems. *Fieldbus Systems and Their Applications 2005*, 239–246. https://doi.org/10.1016/B978-008045364-4/50073-3

What are the 7 Most Critical Cyber Threat Types. (n.d.). Retrieved 19 February 2025, from https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/threat-intelligence-critical-types-cyberthreats/

What are the top cyber threats in the EU? - Consilium. (n.d.). Retrieved 10 February 2025, from https://www.consilium.europa.eu/en/policies/top-cyber-threats/

What Is a Firewall? Definition and Types of Firewall | Fortinet. (n.d.). Retrieved 24 February 2025, from https://www.fortinet.com/resources/cyberglossary/firewall

What is cybersecurity? - Cisco. (n.d.). Retrieved 22 January 2025, from https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

What Is Deep Packet Inspection (DPI)? | Fortinet. (n.d.). Retrieved 24 February 2025, from https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection?utm_source=blog&utm_campaign=dpi-deep-packet-inspection.html

What Is Device Hardening? | Baeldung on Computer Science. (n.d.). Retrieved 24 March 2025, from https://www.baeldung.com/cs/device-hardening-security

What is Device Hardening and its Different Types? (n.d.). Retrieved 24 March 2025, from https://www.pynetlabs.com/what-is-device-hardening/

What is MITM (Man in the Middle) Attack | Imperva. (n.d.). Retrieved 19 February 2025, from https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

What is SCADA? | *SCADA Control* | *COPA-DATA*. (n.d.). Retrieved 17 February 2025, from https://www.copadata.com/en/products/zenon-software-platform-for-industrial-automation-energy-automation/what-is-scada/#definition

What is the NIS Directive? | *Digital Guardian*. (n.d.). Retrieved 10 March 2025, from https://www.digitalguardian.com/resources/knowledge-base/what-nis-directive-definition-requirements-penalties-best-practices-compliance-and-more

zenon Software Platform for industrial automation & energy automation | *COPA-DATA*. (n.d.). Retrieved 17 February 2025, from https://www.copadata.com/en/products/zenon-software-platform-for-industrial-automation-energy-automation/