IT Vulnerability Analysis of Industrial Network and Robotic Systems - Cybersecurity Challenges and Protection Strategies in Industrial IT Systems

Zoltán Nyikes

Milton Fiedman University, Budapest, Hungary, nyikes.zoltan@uni-milton.hu

László Tóth

Obuda University, Banki Donat Faculty of Mechanical and Safety Engineering, Budapest, Hungary, toth.laszlo@bgk.uni-obuda.hu

Tünde Anna Kovács

Obuda University, Banki Donat Faculty of Mechanical and Safety Engineering, Budapest, Hungary, kovacs.tunde@bgk.uni-obuda.hu

Abstract: In recent years, the convergence of industrial automation and information technology has significantly increased the complexity and vulnerability of industrial control systems (ICS). This study provides a comprehensive analysis of the cybersecurity vulnerabilities inherent in industrial IT elements, with a particular focus on network infrastructure and robotic systems. Through real-world case studies and technical assessments, the paper identifies key threat vectors, including remote access misconfigurations, outdated firmware, unencrypted protocols, and social engineering attacks. It further explores systematic methods of vulnerability assessment, such as passive and active network analysis, physical and logical security audits, and automated vulnerability scanning tools. The study also emphasizes the role of international standards and regulations—such as IEC 62443, ISO/IEC 27001, and the NIS2 Directive—in strengthening industrial cybersecurity. Additionally, it presents effective defensive strategies, including network segmentation, multi-factor authentication, SIEM integration, and the application of ITIL-based governance frameworks. The findings highlight the urgent need for continuous monitoring, targeted training, and proactive security architecture to ensure the resilience and operational continuity of industrial environments in the face of evolving cyber threats.

Keywords: Industrial Cybersecurity; Vulnerability Assessment; SCADA and ICS Security; Robot Systems; Critical Infrastructure Protection

1 Introduction

Along with the digitalisation of industrial systems[1], vulnerabilities in industrial IT infrastructure[2] have increased dramatically. Automated production lines[3], robotics systems[4], and SCADA-based control systems[5] are being increasingly closely integrated into classic IT and network environments[6], bringing with them new types of threats[7]. The widening of attack surfaces[8] –such as remote access[9], inadequately updated firmware[10], social engineering methods[11], and unencrypted industrial protocols[12]– makes these critical systems particularly vulnerable.

Industrial cyber security[13] is therefore not only an IT task, but also a strategic issue that affects the continuity of production[14], personal safety[15] and economic competitiveness[16]. The logical security audit[17] and related defense strategies[18] are not in themselves, but international standards (ISO/IEC 27001[19], IEC 62443[20]), IT service management (ITIL[21]), IT management models (COBIT[22]), as well as the current legal environment – especially the NIS2 directive[23] and its Hungarian implementation, LXIX of 2024[24]. can be interpreted in the light of law.

This study aims to provide a comprehensive picture of security risks[25] in industrial IT systems and to present the methodological and practical tools[26] that can be used to mitigate these risks. Special attention will be paid to network segmentation[27], regular software updates[28], Zero Trust-based access management[29], physical protection[30] and the development of incident response capabilities[31]. The purpose of the material is to provide a practice-oriented guide[32] to increasing industrial cyber resilience[33] that is useful for technical and managerial decision-makers[34].

2 Main vulnerabilities in industrial IT components

2.1 Vulnerabilities in robotic systems

Modern industrial robots are becoming more and more complex and are being used in more and more areas to automate production processes. However, because these systems operate over network connections, they provide a variety of attack surfaces for cybercriminals. The most common vulnerabilities include exploitation of remote access options, outdated software and firmware, physical vulnerabilities, weaknesses in communication protocols, and malicious firmware updates.

2.1.1 Remote access and control

A significant number of industrial robots are connected to control centres and other industrial systems via Ethernet or Wi-Fi networks. If the security settings for these

connections are incorrect, then attackers may be able to remotely control the robots, modify their operation, or even shut down the production line altogether.
Example. In 2010, a computer worm named Stuxnet[35] attacked a uranium enrichment facility in Natanz, Iran. The attackers wrote the malware specifically for industrial Siemens PLC controllers, which manipulated the operation of centrifuges. The attack destroyed thousands of centrifuges without the facility staff immediately noticing the problem. This attack was the first known instance of a cyberweapon causing physical industrial damage.

2.1.2 Outdated software and firmware

Industrial robots and their control units often operate unchanged for many years and can pose serious security risks over time due to a lack of updates. An old or unupdated firmware can contain known vulnerabilities that can be easily exploited by attackers.
Example. In 2021, a security research team discovered that several KUKA industrial robots continued to run outdated firmware, which allowed attackers to remotely manipulate robots. A penetration test succeeded in taking remote control of a robot operating on a production line, which could have created dangerous situations in a real-world industrial environment[36].

2.1.3 Physical vulnerabilities

One of the things people sometimes overlook is just how much damage someone can do simply by getting close to a robot. You don’t always need a sophisticated hacking toolkit — just plugging in a USB drive and dropping the right kind of malicious code can mess things up pretty badly.
Example: Take what happened at Tesla’s Fremont plant back in 2018. One of their employees got hold of the robots’ control system and deliberately sabotaged it by sneaking in some harmful code. Nobody noticed right away, but the sabotage caused all kinds of production problems that only came to light later when an internal audit dug into it. Once they figured out what was going on, the worker was fired immediately. After that, the company took extra steps to lock things down physically and make sure it couldn’t happen again[37].

1.1.4 DDoS (Distributed Denial of Service) attacks

Here’s another weak spot you don’t really think about until it happens: DDoS attacks. These things don’t even touch your control systems directly — they just bury your network in so much junk traffic that everything freezes.

Example: That’s exactly what happened in 2022 at a water treatment plant in the USA. Hackers pointed a botnet at the plant’s SCADA system and sent a storm of requests, millions at once, until the whole operation ground to a halt. The water supply was cut off for hours, and people in the area were left high and dry. Not a great day for anyone.

Stories like these are a good reminder: it doesn’t take much to cause a lot of damage when there are gaps in security. Keeping a close eye on systems, updating them regularly, and having solid defences in place isn’t optional — it’s what keeps everything running[38].

2.2 Network infrastructure vulnerabilities

If you think about it, the network is really what keeps an industrial plant alive. It connects everything — the machines, the control systems, the people monitoring the whole thing. But the truth is, these networks are often not as secure as you’d expect. When something slips through, it can throw the whole operation off balance. Here’s what that tends to look like in the real world.

2.2.1 Firewalls that don’t do their job

You’d think a firewall would protect you, right? Well, not if it’s old, poorly set up, or just ignored. In lots of plants, firewalls are running with bad configurations or outdated rules that let all kinds of traffic through. And that can mean attackers walking right in and getting straight to the sensitive systems without much effort.
Example: A good example of this happened in 2019 at a car factory in Germany. The attackers simply found an open port that no one had bothered to block. They slipped in, shut down a few production lines, and the plant lost an entire shift before anyone could stop it. That single mistake cost them millions[39].

2.2.2 Weak or unprotected communication

Here’s another problem: the way the machines talk to each other. A lot of plants still use old communication protocols like Modbus or DNP3 that don’t encrypt anything. No passwords, no scrambling, nothing. So anyone listening in on the line can see what’s being sent — or worse, send their own fake commands back.
Example: In 2021, a British water company learned this the hard way. Hackers noticed their SCADA system was using plain old Modbus, with nothing to hide the commands. They stepped in, messed with the water pressure readings, and before long one of the facilities had minor flooding. A headache they didn’t see coming[40].

2.2.3 Outdated SCADA and control systems

And then there’s SCADA — the brain of the whole operation. The problem is, a lot of these systems are ancient by today’s standards. They don’t get patched much, and they can’t handle modern attacks. Which, of course, makes them an easy target.
Example: That’s exactly what happened in 2022 at a U.S. chemical company. Hackers got into their network, locked up the entire control system with ransomware, and

demanded five million dollars. The company refused to pay and rolled everything back from backups, but it still took days to recover and cost them plenty[41].

When you see how easy it is for these things to go wrong, it's clear that keeping the network secure has to be a priority. Without good firewalls, encrypted communication, and systems that are actually up to date, you're basically leaving the door wide open.

2.2.4 Vulnerability to social engineering attacks

Sometimes the biggest weak spot in an industrial company isn't the technology — it's the people running it. Hackers know this all too well, and they take advantage of it by sending out convincing emails, making fake phone calls, or using other tricks to get someone to give up information they shouldn't.

Example: At a steel plant in France, for example, a senior engineer got what looked like a normal email one morning. It told him he needed to log in to an "update portal" to keep his account active. It all looked official enough, so he went ahead and logged in. Only later did they realise the site was fake, and his password had been stolen. With that, the attackers got into the plant's control system from the outside and messed with the production lines. After cleaning up the mess, the company decided everyone needed proper security training, so this wouldn't happen again[42].

2.2.5 Exploiting zero-day vulnerabilities

Then there are attacks no one really sees coming — what they call zero-day vulnerabilities. These are bugs or flaws in the system that no one knows about yet, not even the companies that made the software. There's no fix ready, no warning, and nothing much you can do once it's being used against you.

Example: That's exactly what happened to a big electronics manufacturer in Asia at the start of 2023. Hackers discovered a flaw in Windows on the company's industrial control machines that no one even knew existed. They used it to bring production to a standstill. It took the company's tech team quite a while to figure out what went wrong and patch things up before they could get the lines running again[43].

2.2.6 DDoS (Distributed Denial of Service) attacks

Most industrial networks really aren't ready for what happens when someone floods them with fake traffic. Everything just clogs up. The whole thing slows down, then stops. People usually don't even see it coming — by the time they figure out what's happening; it's already too late.

One case: In 2022, an energy company in Europe got hit. It shut down their dispatch centre for hours and left parts of several cities in the dark. Not just a random hacker either. Investigators said it probably came from a group supported by a government, with the goal of throwing critical infrastructure into chaos.

This is exactly why keeping networks in good shape is so important[44]. Updates, regular checks, and making sure people know what to watch for. Skipping that? Sooner or later, it bites you.

2.3 Other real-world stories

A few years ago, at Tesla's Fremont plant, back in 2018, they had an insider problem. One of their own employees went in and messed with the robots. He slipped malicious code into the control system, and production went haywire. Cars came off the line with all kinds of defects. They didn't catch it right away. It showed up later when the company ran a routine check. He was out the door immediately[45].

In 2020, Nissan's factory in Sunderland had its turn. Hackers spotted an open port and walked right into the SCADA system running the painting robots. Nobody noticed until thousands of cars were already painted wrong. Fixing that must've been a nightmare[46].

And at a German security conference in 2021, ethical hackers showed just how easy it still is to take over industrial robots. They picked a KUKA model, guessed the password — which was laughably weak — and took full control. They made the robot move in ways that could have been dangerous if this weren't just a demo. All because the firmware hadn't been updated[47].

3 Methods for testing vulnerabilities

3.1 Passive and active network testing

When it comes to figuring out how secure an industrial system really is, there are basically two ways to look at the network: passively or actively. Both have the same goal — spotting weaknesses and possible ways an attacker could get in — but they go about it differently. And the key here is to get that information without messing up the way the system is running.

3.1.1 Passive analysis

Passive analysis is pretty much what it sounds like. You watch and record what's already happening on the network without actually touching or changing anything. The idea is to look for anything odd in the data traffic — something that could hint at an attack or some kind of vulnerability waiting to be exploited. This kind of approach makes a lot of sense for industrial setups because those systems tend to handle really sensitive control signals and data, and you don't want to risk interfering with them.

So what’s good about it? Well, the big plus is that it doesn’t disrupt anything. You can quietly collect a lot of useful information about how the network normally behaves and pick up on strange patterns over time. And if you let it run long enough, you might even see clear signs of attack strategies starting to emerge.

But it’s not perfect. Since you’re only watching and not poking at anything, you’re limited to what shows up in the regular traffic. If an attacker is smart and manages to blend in with normal operations, there’s a chance passive monitoring won’t catch it in time. So while it’s a useful tool, it’s not the full picture.

3.1.2 Passive network analysis techniques

Passive techniques leave the system untouched. Traffic is just observed as it moves. This makes it possible to notice problems without changing anything. Packets can be saved during transmission. Later, they are checked to see what is inside — the data itself, what kind of protocols, how the messages are put together. Wireshark is usually used for this because it works well. It’s also common to notice patterns that don’t seem normal. A network usually behaves in a predictable way. If more traffic than usual is seen, or connections to unexpected places show up, this suggests something is off. Monitoring tools are often set up to handle this automatically. These tools watch for strange activity and warn when they find something unusual. Some compare to known attack examples, others just watch for anything outside the norm. Sometimes changes happen slowly and are only visible if traffic is watched over time. For example, a device that always talked only to local servers might suddenly start connecting to unknown servers outside the network. That usually needs to be checked.

An example happened in Germany, in 2020. A steel plant noticed one controller connecting to strange addresses. It was found that a former employee had tried to get in through VPN. After that, rules for VPN were made stricter, firewalls updated, and better monitoring added. These methods are better when combined. Passive checks alone are not enough. It is usual to also run active checks and audits as well[48].

3.1.3 Active scans

Active scans are different. Here the system is tested directly. Weak points are found before anyone else can find them. Usually these are done by trained staff or hired testers. These tests often find mistakes that passive watching misses. Things like ports left open, software not updated, bad settings. But they have risks too. If they are done wrong, they can break normal work. And they need to be approved, otherwise they can cause other problems. That’s why they are planned carefully.

3.1.4 Methods used in active testing

Several methods are applied when active testing is carried out. Each serves to uncover specific weaknesses by interacting with the system directly. One method is port scanning. Tools such as Nmap are used to check which ports are open, what services are running behind them, and even the version numbers of those services.

Vulnerability scanning is another approach. Automated programs like Nessus, OpenVAS, or Qualys run a broad analysis of the system. They compare its state against databases of known vulnerabilities and produce a report that lists potential risks.

Penetration testing is also performed. In this case, trained ethical hackers try to break into the system by hand. They use a variety of attack techniques. These often include attempts to crack weak passwords, inject malicious SQL queries, or take advantage of mistakes in how access permissions are set up.

Exploit testing goes one step further. Here the vulnerabilities that have been identified are actively exploited, though in a controlled setting. Frameworks such as Metasploit are often used to carry out these tests.

Manipulating network traffic can also reveal weaknesses. Attacks such as ARP spoofing or man-in-the-middle interception are sometimes simulated to show how communication between devices could be eavesdropped on or altered.

One example comes from 2022. At an American pharmaceutical company, a penetration test was carried out on the manufacturing network[49]. The test found that the administrator account for a SCADA system still used its default password and could be reached from outside the company. If this had been exploited, it could have allowed an attacker to change manufacturing processes and compromise the quality or safety of products. After this discovery, the company enforced stronger password policies and began regular vulnerability reviews.

4 Physical and logical security audits

Industrial IT security covers more than just defending against software and network attacks. Physical access and logical protection also need to be considered. Audits are done to find weak points and recommend actions to lower risks.

4.1 Physical security audit

A physical audit checks if critical equipment and control systems are protected against unauthorised access. This includes looking at access control, where sensitive infrastructure is placed, video surveillance, and other protective measures.
Audits are usually based on standards and legal rules. Common ones are:

- ISO/IEC 27001, for information security management, including physical aspects.
- NIST SP 800-53, from the US, also covering physical safeguards.

- IEC 62443, focused on industrial automation and control cybersecurity.
- NIS2 Directive, the EU’s updated rules, requiring physical protection in critical sectors.
- In Hungary, Act LXIX of 2024, which implements NIS2 and sets national requirements for physical security in industrial systems.

4.1 Physical security audit steps

4.1.1 Access point analysis

In a physical audit, access points are checked. This means entrances, gates, locks, and other barriers. Critical areas — like control rooms, server rooms, production lines — are tested to see if access is really limited to authorised staff. Sometimes fake ID or unauthorised entry is attempted to observe how security responds.

Access control systems are reviewed separately. RFID cards, PIN locks, and biometric systems are tested. Weaknesses are noted. For example, cards that can be copied, weak passwords, or poor log review. Logs are examined for suspicious patterns.

Cameras and surveillance are checked too. Placement and coverage are reviewed. Footage storage is checked to see if it can be changed or deleted. Networked cameras are tested to see if they are protected from unauthorised remote access.

Attention is also given to critical infrastructure. This includes control rooms, data centres, network switches. Physical access to robots, control panels, and energy systems is checked to see how well they are protected from tampering or sabotage.

An audit in 2021 at a Japanese electronics factory showed several open control panels[50]. Anyone could plug in a USB stick and interfere. After this was found, stricter access rules were set and better storage for critical equipment was added.

4.2 Logical security audit

The purpose of a logical security audit is to review the configuration and operation of IT systems in order to identify potential security vulnerabilities. This includes software access rights management, password security, data protection, and compliance with applicable security protocols.

User privilege analysis: The audit assesses which users have which privileges and whether these are appropriately restricted. A common problem is that some employees have unnecessarily high levels of access, which increases the risk of abuse.

Password management policies: The audit checks whether the company has appropriate password management policies in place, such as multi-factor authentication (MFA) or mandatory regular password changes.

Software updates and patch management: The audit examines whether the software and operating systems in the system are kept up to date and whether the necessary security updates are applied.

Data protection and encryption: They check whether sensitive data is stored and transmitted with appropriate encryption. The protection of industrial control systems and customer data is particularly important.

4.3 Logical security audit and the legal environment

Logical security audit and the application of the NIS2 Directive and Act LXIX of 2024 The NIS2 Directive (EU 2022/2555) is the European Union's new cybersecurity regulation, which was transposed into Hungarian law by Act LXIX of 2024. The aim of the regulation is to establish uniform requirements for the protection of network and information systems, with particular regard to the security of critical infrastructures, such as industrial systems. During industrial logical audits, the application of NIS2 and its domestic implementation becomes essential to ensure legal compliance and cyber resilience.

4.3.1 Main guidelines of NIS2 and Act LXIX of 2024

Audits also check compliance with the key requirements set out in NIS2 and the Hungarian Act LXIX of 2024. One area is mandatory security measures. The audit looks at whether technical and organisational protections are in place. This includes logging of activity, proper network segmentation, managed access rights, and systems to detect incidents. A risk-based approach must also be verified. The law requires a documented risk analysis and clear action plans based on the risks found. The audit checks if these documents exist and if they are kept up to date. Incident handling is another point. Major security incidents must be reported to the Regulatory Activities Supervisory Authority (SZTFH) within 24 hours. The audit examines whether the company has clear procedures and practices to meet this obligation.

Finally, management responsibility is reviewed. The law expects senior managers to play an active role in cybersecurity. The audit checks if they are involved enough and if they understand the security processes properly.

4.3.2 NIS2 and the audit relationship of Act LXIX of 2024

During the logical security audit of industrial systems, NIS2 and Hungarian legal compliance can be interpreted as follows:

Documentation of legal compliance: The audit must examine whether the organisation fulfils the obligations specified by law. Non-compliance may result in significant fines and operations that jeopardise the security of supply.

Examination of reactive and proactive controls: The audit assesses not only existing security measures, but also their functionality, effectiveness, and speed of response to incidents.

Mapping critical services and dependencies: Under the law, all organisations are required to identify their critical services and their technological dependencies. These mappings and records must also be checked during the audit.

Example: During a 2024 logical security audit of a Hungarian water utility provider, an investigation conducted in accordance with the NIS2 Directive and Act LXIX of 2024 revealed deficiencies in the incident reporting procedure and management awareness. Following the audit, the organisation appointed a dedicated cybersecurity officer, introduced automatic log analysis, and updated its access rights management system.

4.4 Logical security audit and ITIL principles

Logical audits check IT system configurations. User access rights and security processes are reviewed. The ITIL framework helps make IT security and service management more consistent.

4.4.1 ITIL support areas

Incident management. This is for dealing with security incidents in industrial systems quickly and efficiently. Using ITIL principles makes sure that every incident is properly documented and analysed, so systems can be restored quickly after an attack.

Problem management. This is for investigating and eliminating recurring errors and vulnerabilities in industrial systems. The ITIL methodology enables Root Cause Analysis (RCA), which helps to increase the reliability of systems in the long term.

Change management. This ensures the controlled introduction of changes to industrial infrastructure. This is particularly important for industrial control systems (ICS) and SCADA networks, where any change can potentially pose a serious security risk.

Configuration and asset management. Ensures continuous monitoring of industrial networks and systems, guaranteeing that systems operate in a precisely documented state and that security settings are updated in a timely manner.

3.4.2 ITIL and auditing

When logical audits are done on industrial systems, ITIL principles help improve several areas. Security processes become more transparent. ITIL gives a structured way to handle incidents and apply audits consistently. Incident management and reporting are automated. Detected vulnerabilities or attacks are logged and addressed faster. Risk and change are managed better. Changes in IT systems follow formal steps, which lowers the chance of new weaknesses.

Example: In 2023, a European car manufacturer audit showed recurring software errors in SCADA networks. Downtime was caused by faulty commands. After ITIL-based processes were introduced, problem management improved stability and reduced downtime[51].

4.5 Areas of COBIT support

Aligning corporate goals and IT goals. Industrial systems security is effective when IT processes are directly aligned with business strategic objectives. COBIT helps to ensure that technical measures are evaluated from a business perspective during security audits.

Responsibility matrix (RACI): COBIT clearly defines which actors are responsible, approve, consult or inform in the secure operation and audit of industrial systems. This is particularly important in the area of access to critical systems and incident management.

Process maturity and performance measurement. The COBIT framework allows the maturity level of logical security processes to be measured. This means that industrial audits can reveal not only compliance but also opportunities for improvement.

Establishment of a regulated control environment. In line with COBIT's control objectives, the rules and controls introduced for industrial IT systems can be examined in a structured manner, so that audits are not isolated activities but an integral part of organisational management.

3.5.1 The relationship between COBIT and auditing

When conducting logical security audits of industrial systems, the use of COBIT allows the audit to focus not only on technical errors, but also to evaluate the entire IT management and operating environment:

The relationship between management objectives and compliance controls. COBIT helps us to evaluate the fulfilment of the organisation's strategic objectives during security audits, not just regulatory compliance.

Transparent process and accountability system. The audit clarifies which actors are responsible for preventing, managing, documenting, and reporting security incidents.

Assessment of process maturity. The COBIT model helps determine the maturity level of industrial IT security processes and what improvements are needed to achieve higher reliability.

Example. During a logical security audit in 2022, IT management practices at an Eastern European chemical company were analysed in a structured manner based on the COBIT framework[52]. The audit revealed that change management and incident management documentation were incomplete, which hindered the effective handling of security incidents. The new responsibility matrix and audit log system introduced based on COBIT increased accountability and made it possible to trace recurring problems back to their root causes.

4.6 Areas supported by ISO/IEC 27001

Risk-based approach. Through risk assessment, which forms the basis of industrial system security, ISO/IEC 27001 enables organisations to identify, evaluate, and manage relevant threats and vulnerabilities.

System of security controls. Based on the ISO/IEC 27002 control catalogue associated with the standard, the implementation of specific measures (e.g., encryption, access management, incident management) becomes mandatory, which significantly strengthens the protection of industrial systems.

Documentation and compliance. Detailed policies, process descriptions, and logging requirements are introduced within the ISMS to ensure continuous auditability.

Continuous improvement (PDCA cycle). The Plan-Do-Check-Act cycle required by the standard ensures that the security of industrial systems is continuously improved in line with the changing technological and threat environment.

4.6.1 The relationship between ISO/IEC 27001 and auditing

When auditing the logical security of industrial systems, the application of ISO/IEC 27001 allows the audit to be conducted according to objective, standards-based requirements:

Development of an auditable control system. The controls specified in the standard enable formal examination of IT operations and security measures.

Compliance and certification. ISO/IEC 27001 certification confirms that the company meets international expectations, which can be an advantage during supplier or government audits.

A full life cycle approach. ISMS not only examines current operations, but also integrates risk prevention, incident management, and post-incident analysis into the security system.

Example. During a logical security audit in 2023, a Hungarian food manufacturer was able to manage network access control and supplier risks in a more structured manner after implementing an ISMS in accordance with the ISO/IEC 27001 standard. The audit showed that standardised incident management procedures and regular risk assessments reduced the possibility of unauthorised access to critical production data and improved the organisation's response time to security incidents.

The application of ISO/IEC 27001 during industrial logical security audits provides a structured, verifiable, and internationally recognised basis for cybersecurity compliance. Standardised controls, documentation, and continuous improvement requirements help organisations develop their security measures in a strategically and operationally sound manner. It is particularly important for industrial players to integrate the principles of ISO/IEC 27001 into their IT management, as this strengthens business continuity and cyber resilience in the long term.

Physical and logical security audits play a key role in protecting industrial systems, as they help identify risks of unauthorised access, configuration errors, and data security issues. It is essential for industrial companies to conduct these audits regularly and continuously update their security measures in order to prevent potential threats and attacks.

5 Automated vulnerability testing

Automated testing is used to find security gaps in industrial systems. Quick, efficient. Networks, control units, and other components are scanned without manual effort. Regular use reduces human mistakes. Gives a clear picture of security status.

5.1 Vulnerability testing tools

Automated scanners: Nessus, OpenVAS, Metasploit. Find known vulnerabilities. Classify severity (CVSS). Produce reports with fixes.

Works well in large plants. Many devices are checked at once. SCADA, PLC, HMI. Example: 2021, French food plant. OpenVAS audit found outdated SCADA firmware[53]. Vulnerabilities public. Systems updated. Network defences improved.

5.2 Manufacturer-specific security tests

Systems used in industrial environments often use proprietary manufacturer protocols and unique configurations that differ from those used in general IT systems. Special industrial security testing tools are used to test these unique systems, taking into account the specific operating characteristics, protocols (e.g., Profinet, Modbus, EtherCAT), and topologies of the industry in question (e.g., automotive, energy, pharmaceutical).

Example: In 2020, internal security tests conducted by a German automotive company revealed that the Siemens control system they were using contained a previously undocumented security vulnerability that would have allowed attackers to send unauthorised commands to robots[54]. As a result of the test, the company began working more closely with the manufacturer to improve the security of the system.

5.3 Fuzzing testing

Fuzzing sends random or incorrect data to system inputs. The goal is to find weaknesses an attacker might use. Works well on industrial protocols and hardware. Can expose unexpected errors or buffer overflows.

Example: 2019, American energy company. Fuzzing test showed critical protocols failed on specially formatted data. A crafted packet could shut down a control server. Company responded with software updates and new protection measures[55].

5.4 Red Team and Blue Team exercises

Red Team (attacker) and Blue Team (defender) exercises are used more often in industrial security. Red Team tries to break into the system like a real attacker. Blue Team defends and improves protection. These tests show technical gaps, human errors, and how staff react.

Example: 2022, American chemical company. Red Team found a weak spot in the manufacturing network. Attackers could have changed chemical dosing[56]. Blue Team responded with new firewall rules and closer monitoring of access attempts.

Case study: 2021, American pharmaceutical company. Ethical hackers tested the control system. Default passwords were still in use. Attackers could have changed production[57]. Afterward, the company improved password policies and made audits of networks regular.

5.5 Network segmentation and security protocols

VLANs and zoning in industrial networks. Network segmentation allows different systems, such as production, administration, and maintenance segments, to operate separately, thereby reducing the chance of lateral attacks spreading. The use of virtual LANs (VLANs) and DMZs enables stricter access control and allows industrial automation networks (e.g., SCADA, DCS) to be separated from office IT systems.

Example. An Italian automotive supplier in 2022 segmented its production line PLCs from the administrative network by introducing VLANs [58]. After this step, during a simulated internal attack, the attackers were unable to access the control technology devices and only reached the office system.

5.6 VPN and encrypted communication

VPN is needed for remote access to industrial systems. Encrypted connections stop sensitive data from being intercepted or changed. Secure protocol versions (like TLS, DTLS) should also be used. Applies to industrial protocols such as Modbus/TCP and OPC UA. Helps prevent attacks.

Example: 2023, energy industry audit. Maintenance staff were still using unencrypted remote access. VPN was made mandatory. Logging improved. Data security increased[59].

Network segmentation and encrypted protocols are key defences. Together they support Zero Trust setups. Every connection is treated as untrusted by default.

5.7 Regular software and firmware updates

In industrial systems, it is generally required that software and firmware updates are applied regularly. But in reality, this is not always done as it should be. Updates can be delayed for weeks, or even skipped entirely, which leaves the systems exposed to vulnerabilities for longer. For this reason, automatic update systems are often chosen instead. These are set up so that updates from a trusted source are downloaded and installed at specific times. Once installed, these mechanisms do not require much additional work from staff.

Before each update is actually installed, some checking is done. Version numbers are compared, and compatibility tests are carried out as well. If something goes wrong after the update, the system can usually be rolled back to the earlier state, which is important because downtime can otherwise be quite damaging.

Example: A company in Finland that produces logistics automation equipment set up a central control system to keep their production line controllers updated. The system checked for firmware changes and installed them automatically[60]. This reduced the risk of hackers exploiting old software, and over time they also saw fewer operating errors.

5.8 Developing patch management strategies

For patching, it is usually suggested to start with a full list of the devices and systems in place. Then all weaknesses are divided into four levels: critical, high, medium, and low. This way, the most serious ones can be handled first.

When a patch is available, it is first tested in a separate, closed test environment, often called a sandbox. This testing is done before anything is changed on the real system. Then a timetable is set up, and all steps are planned so that staff are told what will happen, and when. After the patch is applied, feedback from users and operators is collected and added to improve the process next time.

Example: During an audit in Spain in 2022, it was found that PLC devices were still using old firmware. After this, the company put in place a central system to track firmware versions and send warnings when updates were ready[61]. They also decided to do a weekly check to make sure patches were applied. This lowered the risk of zero-day attacks and made the systems run more reliably.

5.9 Multi-factor authentication and access management strategies

The Zero Trust security model is based on the idea that no user or device on the network is trusted by default. Every access request is checked and controlled. This applies even when the request comes from inside the network. In industrial environments this is especially important. Unauthorised access, such as from an uncertified workstation or maintenance laptop, can directly affect physical processes. As part of Zero Trust, systems are segmented. Authorisation is given based on access level. Continuous authentication is also used.

Example: At a Belgian chemical plant in 2023 the Zero Trust model was implemented. VPN use was required for all access. Multi-factor authentication was also added, together with device fingerprinting. After this, the number of unauthorised access attempts went down. The resilience of IT systems was improved as well[62].

5.10 Role-based access control (RBAC) and privilege minimisation

The RBAC model ensures users only have access to what they need for their specific role. During audits, it is often seen that rights are too broad. This happens especially with long-term employees or staff who have changed roles. The aim of privilege minimisation is to follow the least privilege principle.

Example: In 2022 an audit was carried out at a Hungarian food company. It was discovered that production managers had full administrator rights on the SCADA system. After the audit, RBAC was introduced. Jobs were matched to clear privilege levels. After changes were applied, security improved. Fewer accidental configuration errors were also reported[63]. Combining multi-factor authentication and role-based access management is now a standard element in industrial security. It increases protection against cyber threats. It also improves transparency, compliance, and how incidents are handled.

6 Implementation of physical security measures

6.1 Physical isolation of critical systems

In industrial settings, critical systems are usually kept apart from others. This means control stations, SCADA servers, also data collection devices. They are separated from normal workstations and from rooms that can be accessed freely. For this, closed server rooms are created. Access is kept limited. Cabinets or even safes are used for sensitive equipment. The goal here is to make sure even someone inside the company but without permission cannot reach these systems. This lowers the chance of direct tampering or someone leaking data.

Example: At a Polish chemical plant in 2023, it was seen during an audit that SCADA terminals were left out in the open, in the factory hall. Anyone walking by could have used them. To fix this, separate containers were put next to the production line. These containers had locks[64]. Only technicians who were authorised could get inside. After this was done, the risk from insiders was much lower.

6.2 Use of biometric and card access control systems

Modern ID systems are used to keep critical rooms secure. Fingerprint readers and face recognition are often used. RFID cards are also common. These systems make sure only people with permission can enter. Logs are kept, showing who entered, when, and how long they stayed. This can help prevent problems and also figure out what happened later if something goes wrong.

Example: In 2022, a German automation company added a biometric access system for its control rooms. The system used hand geometry scans. After it was added, staff followed rules better. Fewer people tried to enter without permission[65].

It is clear that good physical security is an important part of protecting industrial systems. These extra layers make it harder for attackers to get in by just walking up to the equipment instead of hacking.

6.3 Continuous monitoring and incident management plan development

6.3.1 Use of SIEM systems to detect real-time threats.

Security Information and Event Management (SIEM) systems play a key role in industrial environment security, as they are capable of collecting, analysing, and correlating security logs from various sources (e.g., firewalls, endpoint protection systems, SCADA logs) in real time. SIEM systems generate automated alerts when they detect a suspicious event, thereby significantly reducing the time between detection and response (reducing MTTD/MTTR metrics).

Example: In 2023, a Dutch pharmaceutical company installed a SIEM system between its ICS and corporate IT systems. A wave of failed login attempts was immediately detected by the SIEM correlation rules, allowing the IT department to block the affected IP address ranges before the attack escalated[66].

6.3.2 Establishment of an Incident Response Team (IRT) and rapid response protocols

An Incident Response Team, or IRT, is usually set up when incidents need to be handled properly. The team is supposed to work based on written protocols, which are prepared before anything happens. These protocols usually say how incidents are classified and also who is responsible for what. They also describe first actions to take and which communication channels to use. A post-incident check is also part of the process. In industrial systems, this setup is very important because it helps keep production running and protects data at the same time.

Example: In 2022, one SCADA station at a Hungarian electronics company was hit by ransomware. The IRT followed the written protocol and first isolated the network, which they did in three steps. Then they restarted the backup. Later, when forensic work was finished, access policies were updated too. Because the response was fast, no serious production loss was reported[66].

Monitoring and incident response are not just useful for reacting quickly. They also help the organisation to learn from each event and also get better prepared next time, which is why resilience can improve over time.

Conclusions

Industrial systems have changed a lot in recent years. More parts are connected now. Robotics, control units, networks. All tied together. This makes production faster and more efficient. But it also opens up more risks. Weaknesses that were not there before are now part of the system. Attackers have more ways in. Problems can hurt production, cause delays, damage equipment. Even put people in danger.

This study looked at these risks. There were examples of what went wrong. Outdated firmware. Bad passwords. No network segmentation. Not enough monitoring. Insider sabotage. Ransomware. Phishing. Many different problems. Not just technical. People make mistakes too. Organisations don’t always follow rules.

What can be done? Many things. Systems need checking often. Both passive watching and active testing help. Physical audits are important. Logical audits too. Automated scanners can find problems fast. Segmentation helps. Zero Trust helps. RBAC and

MFA should be used. SIEM systems can watch for attacks. Software and firmware must be kept up to date.

But it is not just about tools. Security needs to be part of how the company works. Managers must care about it. Staff must know what to do. Standards help. ISO/IEC 27001. NIS2. ITIL. Training helps. Planning helps.

Security is never finished. New threats keep coming. Only by combining technology, rules, and good management can companies stay safe. It takes regular work. Learning from mistakes. Fixing weak spots. This is how resilience is built. Step by step. Over time.

References

[1] Yongjiang Shi, Yibo Gao, Yining Luo, Jialun Hu: Fusions of industrialisation and digitalisation (FID) in the digital economy: Industrial system digitalisation, digital technology industrialisation, and beyond, Journal of Digital Economy, vol. 1, no. 1, 2022, pp. 73-88, ISSN 2773-0670, https://doi.org/10.1016/j.jdec.2022.08.005., https://www.sciencedirect.com/science/article/pii/S2773067022000061

[2] A. Shaji George, T. Baskar, and P. Balaji Srikaanth: Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors, Partners Universal International Innovation Journal, vol. 2, no. 1, 2024, pp. 51–75,

[3] F.M. Bono, L. Radicioni, S. Cinquemani: A novel approach for quality control of automated production lines working under highly inconsistent conditions, Engineering Applications of Artificial Intelligence, vol. 122, 2023, 106149, ISSN 0952-1976, https://doi.org/10.1016/j.engappai.2023.106149. https://www.sciencedirect.com/science/article/pii/S0952197623003330

[4] Rosen, J., Hannaford, B., & Satava, R. M. (Eds.): Surgical robotics: systems applications and visions. Springer Science & Business Media, 2011.

[5] S. V. B. Rakas, M. D. Stojanović and J. D. Marković-Petrović: A Review of Research Work on Network-Based SCADA Intrusion Detection Systems, in IEEE Access, vol. 8, pp. 93083-93108, 2020, doi: 10.1109/ACCESS.2020.2994961.

[6] Shui-Yuan Huang, Wan-Jia An, De-Shun Zhang, Nan-Run Zhou: Image classification and adversarial robustness analysis based on hybrid quantum–classical convolutional neural network, Optics Communications, vol. 533, 2023, 129287, ISSN 0030-4018, https://doi.org/10.1016/j.optcom.2023.129287. https://www.sciencedirect.com/science/article/pii/S0030401823000329

[7] L. Gitelman, E. Magaril, M. Kozhevnikov: Energy Security: New Threats and Solutions. Energies, 16(6), 2023, 2869. https://doi.org/10.3390/en16062869

[8] M. Bradbury, C. Maple, H. Yuan, U. I. Atmaca and S. Cannizzaro: Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures, 2020 IEEE Aerospace Conference, Big Sky, MT, USA, 2020, pp. 1-20, doi: 10.1109/AERO47225.2020.9172785.

[9] S. Wilson et al.: The Robotarium: Globally Impactful Opportunities, Challenges, and Lessons Learned in Remote-Access, Distributed Control of Multirobot Systems, in IEEE Control Systems Magazine, vol. 40, no. 1, pp. 26-44, Feb. 2020, doi: 10.1109/MCS.2019.2949973.

[10] T. Bakhshi, B. Ghita, I. Kuzminykh: A Review of IoT Firmware Vulnerabilities and Auditing Techniques. Sensors, 24(2), 2024, 708. https://doi.org/10.3390/s24020708

[11] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman and M. A. Ibrahim: Social Engineering Attacks Prevention: A Systematic Literature Review, in IEEE Access, vol. 10, pp. 39325-39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[12] T. Bartman and K. Carson: Securing communications for SCADA and critical industrial systems, 2016 69th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 2016, pp. 1-10, doi: 10.1109/CPRE.2016.7914914.

[13] F. Djebbar and K. Nordström: A Comparative Analysis of Industrial Cybersecurity Standards, in IEEE Access, vol. 11, pp. 85315-85332, 2023, doi: 10.1109/ACCESS.2023.3303205.

[14] A. Eftekhari Ghoshe Kand, A. Usoli: The most important factors affecting the improvement of resilience and continuity of production, transmission and distribution of the gas network. Strategic Defense Studies, 22(95), 2024, pp. 211-232.

[15] T. Lehtonen: Ethics of Security: From Personal Safety to Cyber Security, In M. Taskiran & F. Pinarbaşi (Eds.), Multidisciplinary Approaches to Ethics in the Digital Era, 2021, pp. 44-59, IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-4117-3.ch004

[16] N. Mmango, T. Gundu : Cybersecurity as a Competitive Advantage for Entrepreneurs, In: Gerber, A. (eds) South African Computer Science and Information Systems Research Trends. SAICSIT 2024. Communications in Computer and Information Science, vol. 2159. 2024, Springer, Cham. https://doi.org/10.1007/978-3-031-64881-6_22

[17] E. Soler, R. Villarroel, J. Trujillo, E. Fernandez-Medina and M. Piattini: Representing security and audit rules for data warehouses at the logical level by using the common warehouse metamodel, First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 2006, pp. 8-921, doi: 10.1109/ARES.2006.110.

[18] A. B. Ige, E. Kupa, O. Ilori: Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources.

International Journal of Science and Research Archive, 12(1), 2024, 2978-2995.

[19] M. Malatji: Management of enterprise cyber security: A review of ISO/IEC 27001:2022, 2023 International Conference On Cyber Management And Engineering (CyMaEn), Bangkok, Thailand, 2023, pp. 117-122, doi: 10.1109/CyMaEn57228.2023.10051114.

[20] Björn Leander, Aida Čaušević, and Hans Hansson: Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19), Association for Computing Machinery, New York, NY, USA, Article 101, 2019, pp. 1–8., https://doi.org/10.1145/3339252.3341481

[21] Muhamet Gërvalla, Naim Preniqi, Peter Kopacek, IT Infrastructure Library (ITIL) framework approach to IT Governance, IFAC-PapersOnLine, vol. 51, 30, 2018, pp. 181-185, ISSN 2405-8963, https://doi.org/10.1016/j.ifacol.2018.11.283. https://www.sciencedirect.com/science/article/pii/S2405896318329562

[22] A. Rusman, R. Nadlifatin, A. P. Subriadi: Information System Audit Using COBIT and ITIL Framework: Literature Review. Sinkron : Jurnal Dan Penelitian Teknik Informatika, 6(3), 2022, pp. 799-810. https://doi.org/10.33395/sinkron.v7i3.11476

[23] P. Eckhardt, A. Kotovskaia: The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. Int. Cybersecur. Law Rev. 4, 2023, pp. 147–164, https://doi.org/10.1365/s43439-023-00084-z

[24] Act LXIX of 2024 on Hungary's Cybersecurity, https://njt.hu/jogszabaly/2024-69-00-00

[25] S. B. Yadav, T. Dong: A comprehensive method to assess work system security risk. Communications of the Association for Information Systems, 34(1), 8, 2014.

[26] S. Belouafa, et. al.: Statistical tools and approaches to validate analytical methods: methodology and practical examples. International Journal of Metrology and Quality Engineering, 8, 9, 2017.

[27] Neerja Mhaskar, Mohammed Alabbad, Ridha Khedri: A Formal Approach to Network Segmentation, Computers & Security, Volume 103, 2021, 102162, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102162, https://www.sciencedirect.com/science/article/pii/S0167404820304351

[28] M. Khan, Z. Bi and J. A. Copeland: Software updates as a security metric: Passive identification of update trends and effect on machine infection, MILCOM 2012 - 2012 IEEE Military Communications Conference, Orlando, FL, USA, 2012, pp. 1-6, doi: 10.1109/MILCOM.2012.6415869.

[29] R. Wang, C. Li, K. Zhang, et al.: Zero-trust based dynamic access control for cloud computing. Cybersecurity 8, 12, 2025, https://doi.org/10.1186/s42400-024-00320-x

[30] Hakan Kayan, Matthew Nunes, Omer Rana, Pete Burnap, and Charith Perera: Cybersecurity of Industrial Cyber-Physical Systems: A Review. ACM Comput. Surv. 54, 11s, Article 229, 2022, 35 pages. https://doi.org/10.1145/3510410

[31] H. Naseer, et al.: Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics, European Journal of Information Systems, 33(2), 2023, pp. 200–220. doi: 10.1080/0960085X.2023.2257168.

[32] E. Börger, V. Gervasi: Structures of Computing: A Guide to Practice-Oriented Theory, Springer Nature, 2024.

[33] Thuraya N.I. Alrumaih, Mohammed J.F. Alenazi, Nouf A. AlSowaygh, Abdulmalik A. Humayed, Ibtihal A. Alablani: Cyber resilience in industrial networks: A state of the art, challenges, and future directions, Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 9, 2023, 101781, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2023.101781. https://www.sciencedirect.com/science/article/pii/S131915782300335X

[34] Y. Hasan, A. Shamsuddin, N. Aziati: The impact of management information systems adoption in managerial decision making: A review. The International Scientific Journal of Management Information Systems, 8(4), 2013, 010-017.

[35] M. Baezner, P. Robin: Stuxnet (No. 4), ETH Zurich, 2017.

[36] Rogue Robots: Testing the Limits of an Industrial Robot's Security Federico Maggi Trend Micro Forward-Looking Threat Research, https://www.blackhat.com/docs/us-17/thursday/us-17-Quarta-Breaking-The-Laws-Of-Robotics-Attacking-Industrial-Robots-wp.pdf

[37] Neal E. Boudette: Elon Musk Accuses Tesla Employee of Sabotage, The New York Times, June 19, 2018

[38] James: 11 recent cyber attacks on the water and wastewater sector, Wisdiam 13 October 2024 https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/

[39] Eduard Kovacs: German Auto and Defense Firm Rheinmetall Says Malware Hit, Several Plants, SecurtyWeek, September 27, 2019, https://www.securityweek.com/german-auto-and-defense-firm-rheinmetall-says-malware-hit-several-plants/

[40] Ryan Gallagher: UK Water Supplier Hit by 'Extremely Concerning' Cyberattack, Blommberg, August 17, 2022, https://www.bloomberg.com/news/articles/2022-08-17/uk-water-supplier-hit-by-extremely-concerning-cyberattack

[41] Bert Kondruss: Which companies and organizations in the U.S. have been victims of a hacker attack?, KonBriefing Research, https://konbriefing.com/en-topics/cyber-attacks-usa.html

[42] Simon Parker: Understanding The Physical Damage Of Cyber Attacks, Infosecurity-Magazine, 3 Oct 2017, https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks/

[43] Significant Cyber Incidents Center for Strategic & International Studies, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[44] American Institute of Physics: What was behind the 2021-2022 energy crisis within Europe?, ScienceDaily, 2025, www.sciencedaily.com/releases/2024/07/240702135559.htm

[45] Paul A. Eisenstein: Tesla under fire after quality issue allegations and the loss of senior executives, BBC News, March 15, 2018, https://www.nbcnews.com/business/autos/problems-are-piling-tesla-quality-issues-mount-executives-flee-competition-n856946

[46] Ruziev Abdumalik Artikalievich: Issues of Ensuring Information Security in the Digital Economy, Academicia, Vol. 12, Issue 02, 2022, ISSN: 2249-7137, DOI: 10.5958/2249-7137.2022.00108.2

[47] Msomsan: Safety Maintenance Password KR210 L150-2 KC2 ed05, Robotforum, 2019, https://www.robot-forum.com/robotforum/thread/32423-safety-maintenance-password-kr210-l150-2-kc2-ed05

[48] Rajiv Desai: Cybercrime, An Educational Blog, 2020, https://drrajivdesaimd.com/2020/02/18/cybercrime/comment-page-1

[49] Top 5 Pharmaceutical Industry Trends and Predictions for 2022, The Keenfolks, Accessed Aug 17 2022

[50] Japan corporate governance and responsible investment policy, 2024, https://prod-epi.lgim.com/landg-assets/lgim/japan-policy-2024.pdf

[51] Annual report 2023, One Econom, 2023, https://www.econocom.com/ecmedia/fin-ag/econocom-2023-annual-report.pdf

[52] K. AL-Dosari, N. Fetais: Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach, Electronics, 12, 2023, 3629, https://doi.org/10.3390/electronics12173629

[53] Ö. Aslan, S.S. Aktuğ, M. Ozkan-Okay, A.A. Yilmaz, E. Akin: A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions, Electronics, 12, 2023, 1333, https://doi.org/10.3390/electronics12061333

[54] Boosting cybersecurity: Siemens launches new all-in-one security testing suite for industrial networks, Siemens, 2023, https://press.siemens.com/global/en/pressrelease/boosting-cybersecurity-siemens-launches-new-all-one-security-testing-suite-industrial

[55] Zhijie Zhang, Liwei Chen, Haolai Wei, et. al.: Binary-level Directed Symbolic Execution Through Pattern Learning, 2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2022, pp. 50-57, 10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00014

[56] Challenges in red teaming AI systems, Anthropic, 2024, https://www.anthropic.com/news/challenges-in-red-teaming-ai-systems

[57] The 2021 State of Pharmaceuticals and Cybersecurity Report, Fortinet, https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-pharmaceuticals-and-cybersecurity.pdf

[58] A. Alsaleh: Electric and Autonomous Vehicles in Italian Urban Logistics: Sustainable Solutions for Last-Mile Delivery, World Electr, Veh. J. 2025, 16, 338. https://doi.org/10.3390/wevj16070338

[59] Kushtrim Qollakaj, Lukas Einler Larsson: Cybersecurity of remote work migration: A study on the VPN security landscape post covid-19 outbreak, Blekinge Tekniska Högskola, 2023, https://www.diva-portal.org/smash/get/diva2%3A1778036/FULLTEXT03.pdf

[60] Z. Fatima, M.H. Tanveer, et. al.: Production Plant and Warehouse Automation with IoT and Industry 5.0. Appl. Sci. 2022, 12, 2053. https://doi.org/10.3390/app12042053

[61] Mohammed Hussain: Software and firmware compatibility, Siemens, Technical Forum - SiePortal Community, 2023, https://sieportal.siemens.com/en-hu/support/forum/posts/software-and-firmware-compatibility/307690

[62] Anastasiya Novikava: Gartner predicts 2023 to be the year of Zero Trust, NordLayer, 2024, https://nordlayer.com/blog/gartner-predicts-the-year-of-zero-trust

[63] Milton Campoverde-Molina, Sergio Luján-Mora: Cybersecurity in smart agriculture: A systematic literature review, Computers & Security, vol. 150, 2025, 104284, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.104284, https://www.sciencedirect.com/science/article/pii/S016740482400590X

[64] D. Kowal, M. Radzik, L. Domaracká: Assessment of the Level of Digitalization of Polish Enterprises in the Context of the Fourth Industrial Revolution, Sustainability, 16, 2024, 5718. https://doi.org/10.3390/su16135718

[65] Cookey Iyen, Abel Jacob, Ayoola Oluwasegun: Development of Biometric User Identification and Access Control System, European Journal of Applied Science Engineering and Technology, vol. 2(3), 2024, pp.194-204, DOI:10.59324/ejaset.2024.2(3).18

[66] ENISA Threat Landscape 2023, European Union Agency for Cybersecurity, 2023, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf