CHEMICAL ENGINEERING TRANSACTIONS
VOL. 116, 2025
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Bruno Fabiano, Valerio Cozzani

ISBN 979-12-81206-18-2; **ISSN** 2283-9216
DOI: 10.3303/CET25116008

Cyber Security in the Process Industry: the Role of SEVESO Inspections in the Control of the Safety Management System

Vitantonio Colucci[a,*], Romualdo Marrazzo[b], Valerio Galasso[c], Maria Giovanna De Santis[a], Emanuela Laterza[a], Vincenzo Campanaro[a]

[a]ARPA Puglia, Corso Trieste 27-70126 Bari, Italia
[b]ISPRA, via V. Brancati, 48 - 00144 Roma, Italia
[c]INAIL, Via Plinio ang. Via Salinella – 74121 Taranto, Italia
v.colucci.arpa@gmail.com

The digitalization of HSE management in the process industry through integrating the best technologies is a valid support for improving process management and safety in working and environmental contexts. Advanced technologies allow constant monitoring of operating conditions, timely identification of risks, and prevention of potential accidents through predictive analysis. This digitalization can be useful to the well-established and regulated Seveso Directive to prevent major accidents that could affect people and the environment. Industrial Cyber Security fits into this digitalized context, aimed to control systems such as PLC, SCADA, and HMI immune from attacks. These devices deserve attention as they are the fulcrum of production processes and Industry 4.0. A cyber threat can bring disastrous consequences, leading to possible major accidents in the process industry. Thanks to the advancement of such technologies in the process industry and cybersecurity, Seveso inspections play a crucial role in acquiring more detailed information on how the industry is managing this issue, with particular attention to industrial equipment, identifying critical points, and assessing the adequacy of worker safety management and training.

1. Introduction

Cybersecurity is the protection of confidentiality, integrity, and cyberspace (ISO/IEC, 2023). Cyberspace is a complex environment resulting from interacting with people, software, and internet services through technological devices and connected networks. The increasing digitalization of industrial automation systems, their interconnection with the internet, and the use of digital mobile devices (PCs, USB drives, laptops, etc.) for both operational control and local and/or remote maintenance activities make process plants vulnerable to potential internal and/or external cyber-attacks (IEC, 2018), whether intentional or accidental. Process plants, such as those in the industrial, chemical, energy, and manufacturing sectors, are vulnerable to various types of cyberattacks, both internal and external (Cozzani V. et al.,2005). These threats can be intentional (targeted attacks) or accidental (human errors, technical problems, etc.). The primary vulnerabilities are unauthorized access, non-segregated IT-OT networks, outdated software, unprotected devices, human errors, and physical attacks (Leith et al., 2013). Process plants often use Industrial Control Systems (ICS) or SCADA (Supervisory Control and Data Acquisition) systems, which, if not adequately protected, can be accessed by malicious actors (Iaiani, 2023). Attacks can exploit weak or compromised credentials. Additionally, the lack of segregation between operational (OT) and traditional IT networks may allow attackers to access critical systems (Landucci et al.,2015). This interconnection exposes plants to malware and ransomware originating from attacks on the IT network. Outdated or unpatched systems may also present known vulnerabilities that attackers can exploit. Poorly configured IoT devices or endpoints can serve as entry points for attacks. These attacks can lead to severe consequences such as service interruptions, theft of sensitive data, and manipulation of industrial systems.

The risk analysis for industrial sites under the Seveso III directive (Directive 2012/18/EU), aimed at the prevention of major accidents, cannot overlook the actions of company technicians. Operators may accidentally

Paper Received: 5 December 2024; Revised: 18 January 2025; Accepted: 21 April 2025
Please cite this article as: Colucci V., Marrazzo R., Galasso V., De Santis M.G., Laterza E., Campanaro V., 2025, Cyber Security in the Process Industry: the Role of Seveso Inspections in the Control of the Safety Management System, Chemical Engineering Transactions, 116, 43-48 DOI:10.3303/CET25116008

introduce malware (*e.g.*, via infected USB devices), misconfigurations, or a lack of awareness regarding security, which can facilitate cyber-attacks. Sometimes, intentional physical attacks may already be underway within the process plant. An internal attacker might gain physical access to systems, introducing vulnerabilities or tampering with critical devices. The number of incidents in process plants and critical infrastructures continues to rise, making it difficult to manage cyber risks beyond what is outlined in the ISO/IEC 27000 standard (Information Security Management Systems) and also by IEC 62443 (Security for Automation and Control Systems). This standard is derived from ISA99 (Industrial Automation and Control Systems Security). The growing number of incidents in process plants and critical infrastructures is a global concern, reflecting the increasing complexity of threats and the rise in digital interconnections. This trend is also evident in Italy. According to the 2024 Clusit Report, 2779 serious attacks were recorded worldwide in 2023, marking a 12% increase compared to the previous year (Clusit, 2024). This represents an average of 232 attacks per month, with peaks of up to 270 attacks. In Italy, serious attacks increased by 65%, representing 11% of the total attacks. This highlights how the country is increasingly targeted by cybercriminals, with 56% of incidents having a critical or severe impact. Globally, approximately 81% of attacks were of high or critical severity, causing damage that included service interruptions, theft of sensitive data, and manipulation of industrial systems. Globally, sectors such as healthcare, government, and finance are among the most affected, while in Italy, manufacturing and critical infrastructures show significant vulnerabilities. The growing interconnection of industrial systems (IoT) and low digital awareness are major contributing factors. Additionally, evolving attack techniques, such as ransomware and malware, make protecting these systems increasingly challenging. The rise in cyberattacks targeting critical infrastructures and process plants stems from technological, geopolitical, and security management factors. Key targets include electrical grids and gas pipelines for their strategic national roles, hospitals and healthcare infrastructures facing ransomware attacks that endanger lives, and manufacturing plants (e.g., steelworks), which are disrupted to halt supply chains. Contributing factors include (Iaiani et al., 2023):

1. **Increased interconnection and IoT:** Connected industrial technologies expand the attack surface. IoT devices and SCADA systems often lack adequate security standards. The convergence of OT (Operational Technology) and IT exposes industrial networks to corporate-level risks (Cozzani et al., 2006).
2. **Advanced attack techniques:** Often state-sponsored or part of criminal organizations, attackers use sophisticated malware like Triton (targeting industrial safety systems) and Industroyer (disrupting energy networks). Ransomware remains prevalent, impacting critical operations and demanding multimillion-dollar pay-outs (Iaiani et al., 2023).
3. **Legacy system vulnerabilities:** Many plants rely on outdated software and hardware no longer receive security updates, making them easy targets.
4. **The process industry's significant issue is the lack of culture and skills in cybersecurity.** This underscores the urgent need for comprehensive training programs and a shift in organizational culture toward prioritizing cybersecurity. Investing in human resources is crucial in addressing this issue.
5. **Geopolitical tensions:** During geopolitical instability, international conflicts drive state-sponsored attacks aimed at sabotage or industrial espionage, particularly in critical sectors like energy and healthcare.

To mitigate these risks, it is essential to improve cybersecurity resilience through stricter regulations like the NIS2 Directive, mandatory incident reporting, and fostering a strong digital security culture at all organizational levels. Investments in resilience for Seveso process plants can be enhanced by implementing network segmentation to separate OT and IT systems, adopting advanced technologies like intrusion detection systems and AI to identify anomalies, and promoting international collaboration to share threat intelligence between governments and businesses. The aging of components in chemical plants, particularly in Industrial Control Systems (ICS), is a critical concern that impacts operational reliability and cybersecurity. Aging components, whether through physical wear or obsolescence, can lead to vulnerabilities, especially as manufacturers discontinue support or spare parts. This issue is compounded by the complexity of maintaining compatibility between old and new systems, often resulting in "black box" solutions that are difficult to maintain or secure. Maintenance and timely upgrades are crucial to mitigate outdated hardware and software risks. Aging components exacerbate cybersecurity challenges, as legacy systems often lack compatibility with modern security protocols and are more susceptible to attacks. Integrating IT and OT systems introduces additional risks, as older systems are more vulnerable to malware and ransomware. Effective strategies, such as implementing proactive maintenance, network segmentation, advanced detection technologies, and cybersecurity awareness, are essential to enhancing chemical plant's resilience and protection against operational failures and cyber threats.

Chemical and process industry plants must prioritize safety instrumented systems (SIS) maintenance and security. These systems, including automatic alarms and shutdown mechanisms, are critical to industrial safety management. They are designed to prevent or mitigate incidents that could harm people, property, or the environment. The SIS (Safety Instrumented System) performs specific safety functions, such as continuously

monitoring critical processes and executing automatic actions when abnormal conditions are detected. The main components of a SIS include sensors, which provide real-time data to detect risk conditions; the logic control system (Safety Integrity Level, SIL) or central processing unit (e.g., PLC), which analyses sensor data against predefined thresholds; actuators, which carry out necessary actions to mitigate risks; and Human-Machine Interfaces (HMI), which enable operators to monitor system status and receive alarm notifications. These systems adhere to international standards such as IEC 61508 (guidelines for electrical, electronic, and programmable safety systems), IEC 61511 (specific to safety systems in the industrial process sector), and API 2350. Cybersecurity risk assessments for SIS are essential to safeguard these systems from cyber and physical threats. Given their role in ensuring the safety of critical processes, SIS are strategic targets for malicious attacks, which could significantly harm individuals, the environment, and industrial infrastructure. Figure 1 shows the connection between the level of the infected IACS network structure (IT and OT System) and the impacts in selected entries of the industry database, considering that the final hacking is the last part of the cyber-attack, through which the impacts on the assets of the affected facility are originated (Iaiani et al., 2022).

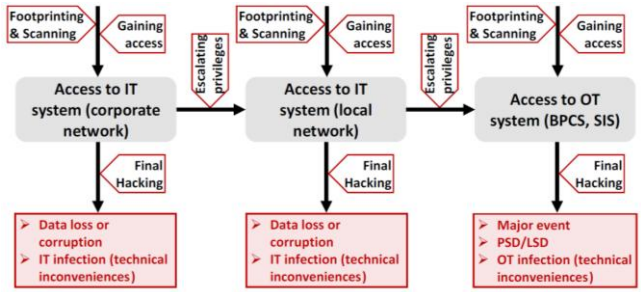

Figure 1: The general steps of a cyber-attack to the typical IT and OT System network structure present in a chemical and process facility.

Another focal aspect is the adoption of a chemical plant's Security Level (SL). Security Levels (SL), defined in standards such as IEC 62443, represent the level of protection required to address specific cyber threats. The level of security adopted for a SIS depends on the risk identified.

2. Methodology: Seveso Inspections on Cybersecurity in Process Plants

The inspections provided for the Seveso III directive are a cornerstone in preventing risks related to major industrial accidents on facilities handling hazardous substances. In recent years, technological advancements and the integration of digital and control systems are beginning to elevate cybersecurity as a critical component of these inspections. Industrial Control Systems (ICS) and Operational Technologies (OT) used in production processes are increasingly vulnerable to cyberattacks, which could escalate into widespread environmental or social crises.

2.1 The Role of Cybersecurity in Seveso Inspections

Although the Seveso III directive primarily focuses on preventing physical and chemical risks, it has evolved to address cyber threats as an integral part of operational risk. Inspections now evaluate compliance with legal provisions and the effectiveness of defense systems against cyber threats. The goal is to ensure that cyberattacks do not compromise essential systems, leading to the release of hazardous substances or interruptions to critical processes. Seveso inspections' evolution highlights cybersecurity's growing role in evaluating risks associated with industrial control systems. Challenges in implementing adequate security measures include a lack of specialized expertise, limited resources for small and medium-sized enterprises, and the rapid evolution of cyber threats (Cozzani, V. et al., 2014). The SMS (Safety Management System) inspections for the prevention of Major Accident Hazards (MAHs) assess the adequacy of Safety Integrity Levels for Safety Instrumented Systems, such as automatic alarms and shutdown mechanisms, by IEC 61511 (Functional Safety - Safety Instrumented Systems for the Process Industry Sector). The 2016 revision of IEC 61511 introduced specific requirements for cybersecurity within SIS, outlined in clauses 8.2.4 and 11.2.12. Clause 8.2.4 mandates a cybersecurity risk assessment for the SIS and its components, while clause 11.2.12 requires that the SIS be designed to withstand identified cybersecurity risks.
Process and chemical plants must perform cybersecurity risk assessments for SIS and adopt the necessary Security Levels in compliance with IEC 62443-3. SEVESO inspectors verify whether operators have conducted these risk assessments and implemented the required SLs. Maintaining the effectiveness of safety systems is

also a key inspection criterion. Operators must demonstrate periodic testing (e.g., Proof Tests), implement predictive or preventive maintenance strategies, and validate Safety Integrity Level requirements.

2.2 Key Aspects of Inspections

- *Assessment of Industrial Control Systems (ICS):* Inspectors analyze Operational Technologies security levels used to control and manage facilities. Systems like SCADA or PLC often exhibit vulnerabilities due to outdated software or poorly secured networks.
- *Cybersecurity Plans:* Facilities must include cybersecurity risk assessment and mitigation measures in their safety reports. These measures may involve access controls, firewalls, network segmentation, and incident response plans.
- *Integration with Physical Security***:** Cybersecurity is evaluated alongside physical security. For example, a cyberattack could turn off fire detection systems or emergency alarms, exacerbating public and environmental risks.
- *Compliance with Standards and Regulations:* Inspectors ensure facilities adhere to international standards such as IEC 62443 for OT security, the NIST CSF framework, and European regulations like the NIS2 Directive, which strengthens critical infrastructure protections.

A prominent case highlighting the necessity of incorporating cybersecurity was the 2017 cyberattack on Saudi industrial systems, known as Triton. This malware, designed to target industrial safety systems, demonstrated how a cyberattack could have catastrophic consequences for chemical and petrochemical plants. Seveso inspections increasingly account for similar scenarios in Europe to prevent cyber vulnerabilities from endangering populations or the environment.

This work focuses on the procedure for an SMS audit of a petrochemical plant. Given the complexity of the processes and the potential catastrophic consequences of a cyber-attack, protecting security instrumented systems against cybersecurity risks requires a particularly rigorous approach. The main objectives are to ensure that SISs continue to perform their security functions even in the event of a threat and to minimize attack surfaces.

3. Case study

During a Seveso inspection on the Safety Management System, cybersecurity checks play an increasingly important role, as a cyber-attack could compromise industrial control systems (ICS) or SCADA systems and cause major accidents, making them “credible events” as resulting from the risk analysis. The objectives of the checks of a Seveso inspection are to ensure that the safety-critical systems of the plant are protected against cyber threats, preventing attacks that could lead to major accidents, and safeguard public health, the environment, and the integrity of the infrastructure. The latest Seveso inspections are starting to adopt a new methodology for the checks to be carried out for a chemical and process plant to prevent cybersecurity risks. These checks are summarised in the following steps:

Step 1. Cybersecurity Management Assessment

It comprises a “*Cyber Risk Management Plan*” and “*Defined Responsibilities*”.

The inspection commission verifies that the plant has conducted a cyber risk assessment and adopted a specific plan to mitigate the identified risks. This is possible because the company has appointed a cybersecurity manager and fully involved IT and ICS personnel in the risk management plans.

Step 2. SCADA/ICS System Protection

The second step is defined by three main points: “Network Segmentation”, “Controlled Access”, and “Patches and Updates”. In this second step, the role of the inspection commission has a less incisive provision on the chemical plant because, to possible safety improvements for the prevention of major accidents, it asks the Plant Manager if the critical systems (SCADA, ICS) are isolated from the company network and the Internet, if there is an implementation of security zones through the use of a separate network for the control systems, if strong credentials and multifactor authentication (MFA) are used to access the critical systems and if access to the network is only authorized and tracked. Where possible and following a critical event, the inspection commission can verify that the control systems' software and firmware are updated with the latest security patches by establishing procedures to test the updates before implementing them.

Step 3. Defence measures against attacks

The third step consists of three sub-phases such as “Firewall and perimeter protection”, “Protection against malware”, and “Secure backups”. In this step, the inspection commission, where possible and following a critical

event, verifies the implementation of IDS/IPS intrusion detection and prevention systems, the use of updated antivirus/anti-malware software on all connected systems, the procedures for detecting and removing malicious software and the presence of regular and updated backups of critical data, stored securely and isolated from the main systems.

Step 4. Checking operating procedures
The fourth step is the phase of interest analyzed by the Seveso Commission because it verifies the existence of procedures to manage cyber-attacks, with clear roles and responsibilities, and also through adequate simulations of cyber incidents to test the effectiveness of the methods. The Inspection Commission has an important role because it examines the management of remote connections, particularly whether they are used only for specific operational needs and monitored, and the cybersecurity awareness programs for personnel working in ICS/SCADA systems.

Step 5. Checking communications between systems
Step 5 is based on checking the “Integrity of communications” and the “Activity log.” The Manager of a petrochemical plant must use secure communication protocols (e.g., TLS, HTTPS) and ensure that company data between systems is encrypted to prevent interception. Where possible and following a critical event, Seveso inspectors can ask the Manager for detailed logs to monitor the activities on critical systems during an incident, analyzing the procedures to examine the "logs" and anomalies detected during the critical event (accident as an explosion, a fire, a toxic release, an eco-toxic release, etc.).

Step 6. Follow-up and regular audits
The last step concerns "periodic audits" and "corrective actions." The inspection commission ensures the adoption of regular inspections of cybersecurity systems to identify vulnerabilities or anomalies, the involvement of external experts for independent checks, the monitoring of non-conformities, and the verification of corrective actions implemented.

The cyber security risk case study for a petrochemical plant that can be analyzed in a Seveso inspection involves a targeted attack on a catalytic cracking unit's industrial control system (ICS). A cyberattack targeting the catalytic cracking unit can lead to cascading failures, including environmental and economic damage and social panic. The cracking unit is a critical section of a petrochemical plant because heavy hydrocarbons are broken down into lighter products such as ethylene, propylene, and gasoline. An attacker or terrorist group can use advanced hacking techniques to access the industrial process control systems and manipulate the plant’s operations to cause explosions, fires, or releases of toxic chemicals.
The causes of an attack can arise from a vulnerability in the IT network or an unprotected VPN connection to infiltrate the ICS systems. Specific malware manipulates industrial processes to sabotage critical components such as pumps, valves, or sensors. This can happen through human error; for example, an employee is tricked through social engineering and a download of compromised software. The attacker can then use the stolen credentials to access the SCADA systems, overloading the monitoring and control systems and causing malfunctions. Examples of scenarios can be:
1. Explosion due to overheating of chemical reactions.
2. Release of toxic substances due to interruption of the cooling flow.
3. Economic damages due to defective production out of specification.
Therefore, the consequences of the cyber-attack can concern the following:
a) The safety of employees and the population surrounding the petrochemical plant due to a fire, explosion, or release of toxic chemicals. For the case study, a fire/explosion can be caused by manipulating pressure or temperatures in cracking reactions or through the unauthorized opening or closing of critical valves. *b)* Production interruption due to cracking plant shutdown due to sabotage or through the production of low-quality products by manipulating cracking parameters. *c)* Environmental impacts due to uncontrolled emissions and chemical spills causing damage to soil, air, and water. *d)* Economic consequences including loss of profits and fines/compensation for environmental damage. *e)* Damage to the corporate image with loss of trust of customers and investors.
For this case study, the Seveso Inspection Commission is called by the judicial authorities to verify the mitigations and defense adopted by the Manager by verifying the security of the network, updates on system protection, continuous monitoring of suspicious activities, training of personnel on raising awareness of phishing and social engineering risks, the presence of procedures for updating control systems, conducting security audits and simulating attacks to test the resilience of the petrochemical IT systems.

4. Conclusions

A robust and integrated cybersecurity strategy is essential to protect process plants from internal and external attacks. Prevention and continuous monitoring minimize threats and ensure business continuity. The increase in cyber-incidents in process plants and critical infrastructures poses a growing threat to safety and economic stability. Addressing this issue requires a holistic approach, combining advanced technology, up-to-date regulations, and a strong safety culture at all levels. To ensure resilience against cyber threats, an integrated approach combining technology, regulations, and collaboration is essential. Seveso inspections focusing on cybersecurity are a fundamental step in addressing modern risks in process plants. Integrating cybersecurity into risk management protects plants from digital threats and helps prevent accidents that could devastate the population and the environment. Collaboration between institutions, industry, and professionals is essential to maintaining high safety levels in critical sectors. From the first Seveso experiences in cybersecurity, technicians must be trained to make SMS inspections more effective, cooperation between companies and control bodies must be strengthened, and advanced cybersecurity technologies must be adopted. Chemical and process plant technicians and Seveso inspectors must be continuously updated on new threats and defense techniques. Sharing information on vulnerabilities and attacks between government agencies, companies, and cybersecurity specialists can improve response capacity. AI-based monitoring systems and network segmentation can help quickly identify and isolate threats. However, this study presents some limitations. The rapid evolution of cyber threats requires continuous adaptation, making it challenging to establish a definitive cybersecurity framework in Seveso inspections. Additionally, the variability in industrial processes and digital infrastructures across sites may limit the applicability of standardized solutions. Further legislative implementation may be necessary to address emerging risks, ensuring that regulatory frameworks evolve alongside technological advancements. Future research should focus on refining risk assessment methodologies, integrating cybersecurity measures into existing safety protocols, and evaluating the long-term effectiveness of current regulations in mitigating cyber threats in the process industry.

Acknowledgments

ARPA Puglia, ISPRA, and INAIL collaborated to support this work and adopt a common methodology for analyzing the risks of major accidents caused by cyber security attacks for chemical and process plants on the national territory.

References

Cozzani V., Salzano E.,2005. The assessment of risk caused by the domino effect in quantitative area risk Analysis. Journal of Hazardous Materials, 123(1-3), 1–7.

Cozzani V., Gubinelli G., Salzano E., 2006, Escalation thresholds in the assessment of domino accidental events. Journal of Hazardous Materials, 129, 1–21.

Clusit, 2024, *Italian Association for Information Security Annual Report*. Retrieved from https://clusit.it

Iaiani M., Tugnoli A., Cozzani V., 2022, Chapter Ten - Risk of cascading effects in digitalized process systems. Methods in Chemical Process Safety, Elsevier, Volume 6, 353-388.

Iaiani M., Tugnoli A., Cozzani V.,2023, Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry, Process Safety and Environmental Protection,172,69-82

Iaiani M., Tugnoli A., Cozzani V., Reniers G., Yang M, 2023, Quantitative evaluation of the probability of success of deliberate attacks in the Offshore Oil&Gas Industry, Chemical Engineering Transactions, 99, 121-126.

International Standards ISO/IEC 27032:2023, Cybersecurity — Guidelines for Internet security

Landucci, G. Argenti, F Tugnoli, A Cozzani, V, 2015, Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire, Reliability Engineering & System Safety, 143, 30-43.

Laurent A., Pey A., Gurtel P., Fabiano, B.,2021, A critical perspective on the implementation of the EU Council Seveso Directives in France, Germany, Italy and Spain. Process Safety and Environmental Protection, 148, 47–74.

Leith H.M., Piper, J. W, 2013, Identification and application of security measures for petrochemical industrial control systems, Journal of Loss Prevention in the Process Industries, 26, 982-993