ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY
A MAGYAR TUDOMÁNY ÜNNEPE
Az MTA programsorozata

Mérnöki Szimpózium a Bánkiban
(ESB 2023)
http://bgk.uni-obuda.hu/esb/

Interconnection between industrial safety and cybersecurity

[1]Kristóf Stölczer, [2]Tamás Szádeczky

[1]*Óbuda University, Doctoral School on Safety and Security Sciences. Budapest, Hungary, stolczerk@icloud.com*
[2]*National University of Public Service. Budapest, Hungary, tamas.szadeczky@uni-nke.hu*

Abstract

It is clear that the continuity of industrial production, which is the key driver of the economy, is a vital priority for our daily lives. It is extremely important that these automated and semi-automated industrial cyberphysical systems operate safely without risk to human life or compromising productivity. Critical infrastructure and critical manufacturing facilities are potentially subject to all types of attackers (state-sponsored cyber attackers and cyber criminals, terrorist groups, hacktivists) who, whether for political, economic, or ideological reasons, select the attacked establishment, thus affecting the global supply chain or even damaging the economic structure of an entire nation.

Keywords: industrial cybersecurity, critical infrastructure's cybersecurity, industrial safety, cybersafety

1. Introduction

When looking at the operation of critical infrastructures or a manufacturing company, it is clear to us that almost all of these sectors and sub-sectors are typically long-standing facilities, often with outdated technology (legacy systems and technologies), multi-generational staffing with fundamentally different mindsets, hazardous manufacturing activities, insufficient cybersecurity control sets, or, in the worst case, none at all (which is probably caused by the result of a general ignorance, a lower preventive maintenance effort for economic reasons, or the decision to minimise the scope of these maintenance actions, solely in order to keep production continuity). The primary lesson from past cybersecurity incidents involving industrial control systems is that security awareness as a line of defence is critical. In the processing of major incidents, it has been found that a key trigger for a cyberattack was an already deficient level of preparedness and awareness. [1] Fortunately, to our knowledge, there have been no cyber-attacks against a company or critical infrastructure performing a dangerous operation that have resulted in mass human casualties. To put my research into context, the cybersecurity of industrial control systems clearly has a major impact on the process safety of manufacturing. Furthermore, I would like to present the current trend of OT/ICS attacks globally and illustrate the importance of addressing cybersecurity and process safety together in many circumstances.

2. Industrial safety and cybersecurity concerns in a hazardous industrial establishments

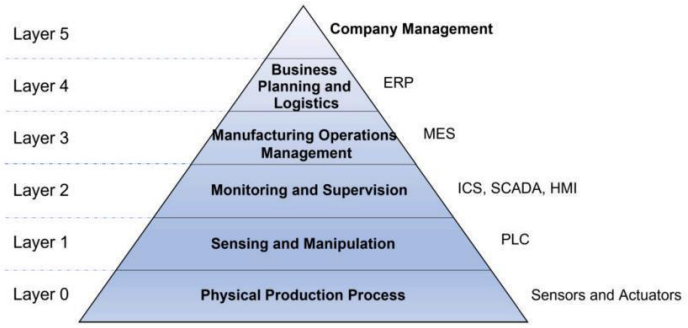

Figure 1. ISA-95 automation pyramid [2]

Typically, an industrial control system has a supervisory control and data acquisition system (SCADA), a remote terminal unit (RTU), programmable logic controllers (PLC), a human-machine interface (HMI) and finally process-related assets on the field. These layers are in semi-direct cooperation with Office IT but in a strictly separated architecture (Layer 4 - Layer 5). Heterogeneous industrial systems are a major safety and security issue. In critical infrastructures, such as power generation units, oil refineries, and natural gas pipelines, these systems must operate at a high level of CIA principles throughout their whole life cycle. An important pillar of its implementation is effective risk management. There is a strong demand for a coherent risk assessment framework, at least for safety and security. Combined safety and security assessments can provide a better and more reliable tool to identify early design defects in a more cost-effective and timely manner. In terms of the dimensions of attacks against OT/ICS, they might typically attack by denial of service to disrupt the continuity of operations, deliberate physical destruction of systems as an attack against assets and property, aggressive attacks against system operators, stealing information about high-value manufacturing processes, or industrial espionage. [2]

2.1 Cybersecurity framework to evaluate the adequate risks

The most common industrial cybersecurity standardized framework is the ISA/IEC 62443 series, which was developed to increase the security of ICS/OT systems throughout their whole lifecycle as vendor product and also from the asset owner perspective.To assess safety and security, an important starting point is the collection of safety and security policies, which in many cases have already taken into account the IEC62443 standard and other sector-specific rules and standards. As part of the evaluation of the documentation, an impact analysis is carried out for many scenarios that could compromise the business-production processes themselves or the equipment and instruments that are considered as assets of the organisation. The impact analysis should identify the OT/ICS systems and which business processes interact with, the identified system should be classificated by security requirements, and the data that flows through it should be identified by security classification as well. [3] In the industrial control system's environment we can use as a cyber-risk assessment method the ISA/IEC 62443-3-2 and 3-3 standard where the main steps are:

- Indentifying cyber threats
- Determine the impacts and consequences

- Determine likelihood
- Determine the security level target and operating model
- Evaluate the existing controls
- Identifying additional controls [4]

2.2 Functional safety approach

Functional safety is a standardized framework to ensure the system functioning approriately and sets out general requirements to achive those specific safety controls which is essential to deliver the safety performance level. This standard is the IEC 61508 standard series as a functional safety benchmark. The standard's approaches and concerns all those hazards which are closely related to the technological, human error and organizational safety risks, where the professional individuals evaluate the causes of possible malfunctions to reach the SIL (Safety Integrity Level). [5]

2.3 Combination of functional safety and cybersecurity assessments

From perspective of engineering, risk and cybersecurity disciplines systematically performed an assessment on the plant hazardous operational processes to determine the possible anomaly in the process (physical properties), the potential root causes of the anomaly (physical properties), the possible deviations from the ICS/OT system's network traffic and the possible consequences of the deviations. The central objective of cybersecurity assessment – supported with process safety aspects - is to evaluate the consequences of cyber incidents on the ICS/OT environment. Cybersecurity-related incidents included either deliberate or inadvertent actions that could lead to interference with the flow of data or information within the control system, which could result in malfunction and damage. [6]

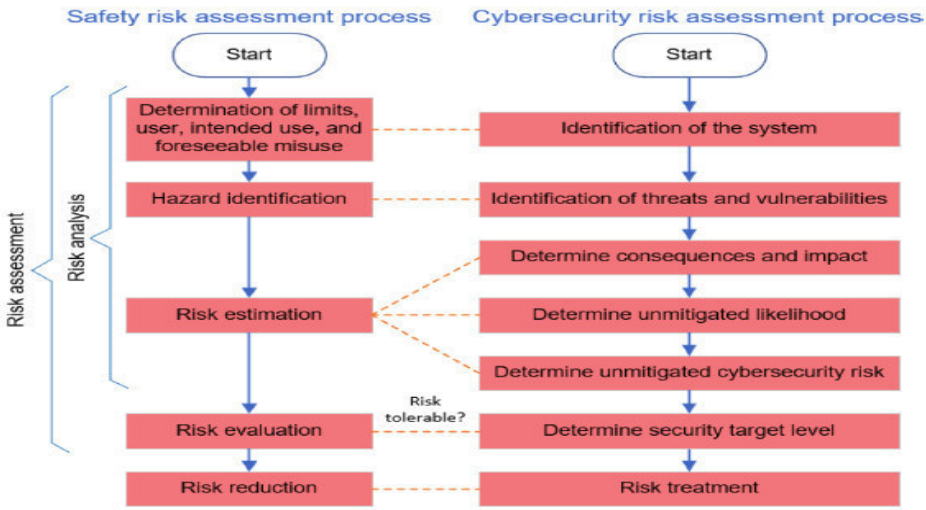

Figure 2. Safety and cybersecurity risk assessment process [7]

3. Cyber-Physical system/Industrial control system's cybersecurity challenges

The triad of confidentiality, integrity, and availability is a fundamental value of the cybersecurity profession, and ensuring these values is central to the cybersecurity mechanisms within an organisation. When the information system of the organisation is augmented with the industrial control systems used in the production environment, the context is completely different. As long as the value of a CIA principle used in an IT environment is compromised, in a "better scenario" we are talking about "only" e.g. a data breach or credentials leakage, and there is no significant impact on human life, but the financial damages and reputational consequences can be significant. [8]

In physical terms, the impact on an industrial cyber-physical system could initiate an irreversible process whereby the cyber-physical system could lose essential functionalities, system degradation could occur, or unauthorised modifications could be inserted into the algorithm created by the manufacturer or the vendor. [9]

We already have relevant experience attacking an industrial facility with hazardous activities. The data clearly demonstrate that the vast majority of incidents have escalated from human error and inattention to physical safety consequences. Typically, a phishing email was used to infiltrate the facility's IT system. A more effective attack generally is the loss of control over programmable logic controllers (PLCs), failure to receive error alerts, falsified sensor data, manipulations of sensor data, making it impossible to perform the critical target operations, e.g., open-close, or the operation is performed in a catastrophic operation phase because of the received false data. [10]

4. Conclusion

The interdependencies and activities of critical infrastructures, as well as the hazardous industrial activities of local and multinational manufacturing companies, and the supply chain itself are exposed to cyber security threats on an unprecedented scale. This is combined with a fragile international security architecture threatened by confrontations arising from geopolitical tensions, cyberterrorism, hacktivism, etc. For the future, it is urgent to establish a complex global, continental, and local industrial safety and cyber security legislation that encourages companies (as the Seveso Directives) to deploy more secure technologies (replacement of legacy systems) and to increase their operational safety and security awareness level.

5. References

[1] René Waslo, Jason Hunt (2023). The connection between cybersecurity and worker safety. www.securitymagazine.com

[2] Roberto Canonico, Giancarlo Sperli (2023). Industrial cyber-phyisical systems protection: A methodological review. Computers & Security Volume 135

[3] Hicham Lalaoui Hassani, Ayoub Bahnasse, Eric Martin, Christian Roland, Omar Bouattane, Mohammed El Mehdi Diouri (2021). Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443. Procedia Computer Science Volume 191, 33-40.

[4] IEC (2020). Quick Start Guide: An overview of ISA/IEC 62443 standards, ISA global cybersecurity alliance.

[5] M. Sliwinski, E. Piesik, J. Piesik (2018). Integrated functional safety and cyber security analysis. IFAC-PapersOnline Volume 51(24), 1263-1270.

[6] Marja Ylönen, Kim Björkman (2023). Integrated management of safety and security (IMSS) in the nuclear industry: – organizational culture perspective. Safety Science, Volume 166.

[7] Jarmo Alanen, Joonas Linnosmaa, Timo Malm, Nikolaos Papakonstantinou, Toni Ahonen, Eetu Heikkila, Risto Tiusanen (2022). Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering and System Safety Volume 2020

[8] Yuchong Li, Qinghui Liu (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports Volume 7, 8176-8186.

[9] Nilufer Tuptuk, Stephen Hailes (2018). Security of smart manufacturing systems. Journal of Manufacturing Systems Volume 47, 93-106.

[10] Nelson H. Carreras Guzman, Igor Kozine, Mary Ann Lundteigen (2021). An integrated safety and security analysis for cyber-physical harm scenarios. Safety Science Volume 144