**Identification of cyber-risks due to the malicious manipulation of Industrial Automation and Control Systems in chemical and process facilities**

Matteo Iaiani1\*, Alessandro Tugnoli1, Valerio Cozzani1

*1 LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali,*

*Alma Mater Studiorum – Università di Bologna, via Terracini n.28, 40131 Bologna, Italy*

*\*Corresponding author E-Mail: matteo.iaiani@unibo.it*

**1. Introduction**

Cyber-attacks to Industrial Automation and Control Systems (IACSs) in chemical and process facilities such as the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS), are of major concern due to the potential severity of consequences on humans, assets, and the environment, which are comparable to those caused by safety-related causes [1–3].

The ISA/IEC 62443 series of standards provide a systematic and practical approach to address cybersecurity issues of IACSs. In particular, it requires the evaluation of all the impacts (including those on the physical plant (process equipment, storage equipment, interconnections)) that can result from intentional malicious attacks to the BPCS and SIS in order to evaluate the actual level of cyber-risk of a facility and implementing proper cybersecurity countermeasures for its reduction. However, neither specific methods nor guidelines are provided to conduct the proposed approach. Similarly, also the common methodologies dedicated to process plant Security Vulnerability/Risk Assessment (SVA/SRA) such as the VAM-CF methodology, the CCPS methodology, and the one proposed by API RP 780, consider attacks to the BPCS and the SIS in the evaluation, but no specific procedures for assessment of the link between malicious manipulations and consequences is provided [4].

In the present study a toolbox was developed to fill the gap in the availability of tools aimed at supporting cyber-risk identification in the context of SVA/SRA and cybersecurity risk assessment of ISA/IEC 62443.

**2. Methods**

Two complementary approaches were used. The first approach consisted in the population and analysis using Exploratory Data Analysis (EDA) of a dedicated database of cybersecurity-related incidents that occurred in chemical and process facilities worldwide in the last 50 years. Data was gathered from a broad set of sources (open source databases on industrial accidents/incidents, scientific literature, and the web) using a specific set of keywords translated in different languages (English, Italian, German, French and Spanish).

The second approach consisted in the development and application of two systematic qualitative procedures in order to systematically identify the possible scenarios affecting the operability and system integrity of a chemical process plant, of the malicious manipulations by which they may be initiated, and of the existing inherent/passive and active/procedural safeguards in place (safety/security barriers). Both the methodologies were demonstrated on case studies (upstream onshore Oil&Gas plant for the preliminary treatment of crude oil and offshore Oil&Gas platform for natural gas production).

**3. Results and discussion**

A database of 82 cybersecurity-related incidents was populated (see the structure in Figure 1a). Its analysis using EDA evidenced important differences as regards the geographical distribution, the distribution among the industrial sectors, the impacts of the attacks, the type of attackers and the target system infected. The analysis of a sub-set of more detailed incidents allowed also the identification of the general steps of a cyber-attack, the main hacking techniques used by the attackers and the more common cybersecurity countermeasures. Overall, the results obtained can be used to define generic cybersecurity-related scenarios that can be employed by authorities and practitioners as a reference starting point to undertake a case specific cybersecurity risk assessment (approach very consolidate in the safety management practice).The detailed method used and results obtained are reported in [2].

Two rigorous systematic qualitative procedures for cyber-risk identification were developed, exploiting a reverse-HazOp concept (see the flowchart in Figure 1b): PHAROS (Process Hazard Analysis of Remote manipulations through the cOntrol System) for the analysis of system integrity and POROS (Process Operability analysis of Remote manipulations through the cOntrol System) for the analysis of process operability. Overall, the results from PHAROS and POROS application can be used by a team of experts to perform a case-specific cyber risk identification, to define protection requirements for the safeguards in place (inherent/passive and procedural/active), and to support the design of the network systems (e.g. network segmentation). Detailed information on PHAROS and POROS can be found in [5] and [6] respectively.



**Figure 1.** a) Structure of the developed database (grey boxes: free text fields; orange boxes: itemized fields); b) Flowchart of POROS (red arrows) and PHAROS (blue arrows).

**4. Conclusions**

A synergic toolbox aimed at supporting cyber-risk identification in the context of SVA/SRA methodologies and the cybersecurity risk assessment proposed by ISA/IEC 62443 was developed and tested on case studies that proved the quality of the results that can be achieved. The provided toolbox paves the way to future developments in strategies for a more secure network architecture design and supports quantitative approaches for assessing the probability of success of a cyber-attack aiming at interfering with the operability and/or system integrity of a process plant.

**References**

1. G. Landucci, G. Reniers, Preface to special issue on quantitative security analysis of industrial facilities, Reliab. Eng. Syst. Saf. (2019).
2. M. Iaiani, A. Tugnoli, S. Bonvicini, V. Cozzani, Analysis of Cybersecurity-related Incidents in the Process Industry, Reliab. Eng. Syst. Saf. 209 (2021) 107485.
3. M. Iaiani, V. Casson Moreno, G. Reniers, A. Tugnoli, V. Cozzani, Analysis of events involving the intentional release of hazardous substances from industrial facilities, Reliab. Eng. Syst. Saf. 2012 (2021) 107593
4. A. Matteini, F. Argenti, E. Salzano, V. Cozzani, A comparative analysis of security risk assessment methodologies for the chemical industry, Reliab. Eng. Syst. Saf. 191 (2019) 106083
5. M. Iaiani, A. Tugnoli, S. Bonvicini, V. Cozzani, Major accidents triggered by malicious manipulations of the control system in process facilities, Saf. Sci. 131 (2021) 105043
6. M. Iaiani, A. Tugnoli, P. Macini, V. Cozzani, Outage and asset damage triggered by malicious manipulation of the control system in process plants, Reliab. Eng. Syst. Saf. 213 (2021) 107685