Introduction of quantitative approaches supporting cybersecurity risk assessment in the chemical and process industry

Matteo Iaiani\*, Alessandro Tugnoli, Valerio Cozzani

LISES - Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum - Università di Bologna, via Terracini n.28, 40131 Bologna (Italy)

\*matteo.iaiani@unibo.it

1. Introduction

Cyber-attacks to Industrial Automation and Control Systems (IACS) such as the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) in chemical and petrochemical facilities are of major concern due to the potential severity of consequences on humans, property, and the surrounding environment, which are comparable to those of the major accident scenarios caused by safety-related causes (Iaiani et al., 2021). The ISA/IEC 62443 series of standards offer a systematic and practical framework to address cybersecurity challenges in IACS. Implementing this framework requires identifying all potential impacts of deliberate malicious attacks on the BPCS and SIS, evaluating the consequences on the physical plant, and assessing their likelihood. However, the standards do not provide specific methods or guidelines to support these activities, highlighting a critical research gap that demands further investigation.

2. Proposed approaches supporting cyber-risk assessment

The proposed set of tools supporting cyber-risk assessment (e.g., ISA/IEC 62443) is graphically represented in Figure 1. In particular, the contribution covers:

* *Identification of critical events*. This step focuses on determining major events (release of hazardous materials, fire, explosion, etc.) or production outages that could be initiated by cyber-attacks targeting the BPCS and SIS. The POROS 2.0 (Process Opera­bility Analysis of Remote manipulations through the cOntrol System) methodology developed by the authors is suggested for this purpose. Details can be found in Iaiani et al. (2023a), together with an example of application.
* *Identification of cyber-attacks*. This step focuses on determining potential attack pathways within the IT (Information Technology) – OT (Operational Technology) system that adversaries might exploit to access the target elements of BPCS and SIS. The new tool called Cyber – Adversary Sequence Diagram (Cyber-ASD) is suggested for this purpose. It consists in a schematic representation of the IT-OT network structure (e.g., cyber areas such as IT intranet, BPCS, SIS, and cyber path elements such as firewalls and switches) through which it is possible to systematically identify all cyber pathways to access a certain target element. The formal conceptualization of the cyber-ASD is part of future work; however, application of the ASD in the context of the physical security of chemical and process plants can be found in Iaiani et al. (2023b). Moreover, this step requires identification of the specific set of manipulations of the BPCS and SIS target elements (e.g., PID controllers, PLCs) to initiate the critical events identified in the previous step. This can be systematically performed through the application of POROS 2.0 methodology.
* *Evaluation of consequences*. In this step, the consequences of identified critical events are quantified in terms of their impact on people, assets, the environment, and reputation. The score-based approach provided in the POROS 2.0 methodology is suggested for this purpose
* *Evaluation of likelihood*. This step requires the evaluation of the probability of success of the identified cyber-attacks. This is given by the product of the probability of attempted attack and the conditional probability of successful execution given the attempt. While quantification of the first contribution requires expertise of intelligent and socio-political analysists, the evaluation of the second term falls within the background of risk analysts. To this purpose, a Bayesian Network (BN)-based approach, leveraging the Estimate of Adversary Sequence Interruption (EASI) model developed by the Sandia National Laboratory in the context of nuclear security, is proposed. The formal conceptualization of the method is part of future work; however, an application in the context of physical security of offshore Oil&Gas platform is provided in Iaiani et al. (2023b).



Figure 1. Tools proposed to support different steps of the quantitative cyber-risk assessment.

3. Conclusions

A set of novel approaches is proposed to enhance the identification of critical cybersecurity events and cyber-attack pathways, the evaluation of potential consequences, and the assessment of attack likelihood. These approaches aim to improve the reproducibility and accuracy of cyber-risk assessments in chemical and process facilities.

Acknowledgments

This work was supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

References

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021. Analysis of Cybersecurity-related Incidents in the Process Industry. Reliab Eng Syst Saf. 209, 107485. https://doi.org/10.1016/j.ress.2021.107485

Iaiani, M., Tugnoli, A., Cozzani, V., 2023a. Process hazard and operability analysis of BPCS and SIS malicious manipulations by POROS 2.0. Proc Saf Env Prot. 176, 226–237. https://doi.org/10.1016/j.psep.2023.06.024

Iaiani, M., Tugnoli, A., Cozzani, V., Reniers, G., Yang, M., 2023b. A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities. Ocean Eng. 273, 114010. https://doi.org/10.1016/J.OCEANENG.2023.114010