Introduction to Digital Twins for Supporting Quantitative Cybersecurity Risk Assessment

Antonio Manzi1, Matteo Iaiani1, Alessandro Tugnoli1,\*, Giacomo Antonioni1, 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: a.tugnoli@unibo.it

1. Introduction

With the increasing digitalization of the chemical, process, Oil&Gas, and energy production industries, cybersecurity has emerged as a critical issue (Center for Chemical Process Safety, 2022). This is particularly evident in scenarios where cyber attackers gain access to and manipulate Operational Technology (OT) systems, including the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS). In fact, historical evidence demonstrates that such malicious interferences can initiate events with consequences comparable to scenarios arising from conventional equipment failures (Iaiani et al., 2023a).

A key phase in quantitative cybersecurity risk assessment (QCRA) involves understanding and modeling the dynamics of plants when BPCS and SIS are maliciously manipulated through cyber-attacks, alongside evaluating the response performance of the adopted protection strategies (e.g., inherent/passive safeguards such as pressure safety valves, and procedural/active safeguards such as shutdown procedures), to identify vulnerabilities, quantify potential consequences, and prioritize mitigation measures.

In this regard, the present study investigates the use of digital twins—digital replicas of physical plants implemented in dynamic process simulation environments—as a tool to support the quantitative assessment of cybersecurity risks. The conditioning section of a green hydrogen production plant was taken as case study.

2. Method

The method employed in this study is outlined in Figure 1.



Figure 1. Method adopted in the present study.

Firstly, the digital twin of the plant section analyzed was created using aspen HYSIS software in dynamic mode. Then, the cybersecurity scenarios to be simulated (e.g., those relevant in the context of quantitative cyber risk assessment) were identified

 using POROS 2.0 (Process Operability analysis of Remote manipulations through the cOntrol System) methodology, developed by the authors in a previous study (Iaiani et al., 2023b). The methodology provides the sequence of manipulations of BPCS and SIS components that can initiate process-related critical events such as major events or operation outages.

The identified scenarios were individually simulated using the developed digital twin, and the resulting data—including pressure, temperature, level, and flow plots—were analysed to extract information relevant to quantitative risk assessment, such as response times and the capability of the installed pressure safety valves in managing the pressurization induced by the scenario.

3. Case Study

3.1 Description

Figure 2 shows Process Flow Diagram (PFD) of the plant section analysed in the case study. The section represents one of the parallel conditioning lines in a green hydrogen production plant utilizing AEL electrolysers. Specifically, the produced hydrogen is first dehydrated in V-100 after being cooled in HE-100, where water condenses. Subsequently, the small amount of oxygen present in the stream is converted into water within the deoxidizer (CRV-100). This water is then separated in V-101, and the hydrogen is compressed to meet transport specifications.



Figure 2. Process Flow Diagram (PFD) of the section analysed (green H2 conditioning)

3.2 Results and discussion

The digital twin corresponding to the plant section depicted in Figure 2 was developed using Aspen HYSYS in dynamic mode. This process involved designing all equipment and valves, as well as implementing the necessary control loops.

POROS 2.0 was subsequently applied to identify relevant cybersecurity scenarios. For the sake of brevity, the results are presented for a single scenario: the simultaneous opening of the bypass stream between the conditioning line under assessment and the adjacent line (via manipulation of the BPCS controller managing valve VLV-102) and the closure of the gas outlet stream from V-100 (via manipulation of the pressure controller managing VLV-100). This scenario is designed to over-pressurize the dryer V-100, potentially causing a breach and the subsequent release of hydrogen (highly flammable gas). It was then simulated using the digital twin to assess the adequacy of the PSV installed on V-100, which was designed for a closed outlet configuration, and to evaluate the system’s response time.

Figure 3 illustrates the pressure response within the separator V-100 under the simulated cybersecurity scenario. The pressure exceeds the Maximum Allowable Accumulated Pressure (35 bar), reaching a peak of 40 bar (black curve) after 17 s after the second manipulation (pressurization time to be used in QCRA). This highlights that the PSV installed on V-100, with an orifice area of 29 mm², is unable to provide adequate relief for the overpressure induced by the described manipulations. As previously stated, this scenario is critical, as the excessive pressure could compromise the structural integrity of the separator and lead to a potential release of hydrogen, warranting consideration within cybersecurity risk assessment.

To address this criticality, the installation of a type D PSV (orifice area of 70.97 mm2), as specified in API standard 526, is proposed to enhance the system's overpressure protection capabilities against this cybersecurity scenario.



Figure 3. Pressure trend in dryer V-100 obtained with Aspen HYSYS simulation.

4. Conclusions

The present study investigates the role of digital twins in supporting quantitative cybersecurity risk assessment (QCRA). The dynamic Aspen HYSYS-based digital twin of the conditioning section of a green hydrogen production plant, considered as a case study, demonstrated the effectiveness of digital twins in checking the adequacy of passive safeguards (such as PSVs) in preventing or mitigating the cyber malicious interference with the BPCS and SIS and in evaluating the system’s response time, information required in QCRA. Future developments will explore the use of digital twins to simulate more complex scenarios and to assess whether the order of manipulations affects the extent of consequences.

Acknowledgments

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

References

Center for Chemical Process Safety (CCPS), 2022. Managing Cybersecurity in the Process Industries - A Risk-based Approach. Wiley.

Iaiani, M., Tugnoli, A., & Cozzani, V., 2023a. Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry. Proc Saf Env Prot. 172, 69–82. https://doi.org/10.1016/j.psep.2023.01.078

Iaiani, M., Tugnoli, A., & Cozzani, V., 2023b. 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