Use of digital twins to assess malicious manipulations of BPCS and SIS in green energy production systems

Antonio Manzi[a], Matteo Iaiani[a,*], Alessandro Tugnoli[a], Giacomo Antonioni[a], Valerio Cozzani[a]

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

*E-mail: matteo.iaiani@unibo.it

With the increasing digitalization of the chemical, process, Oil&Gas, and energy production industries, cybersecurity has emerged as a critical issue. 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).

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. This phase includes evaluating the performance of existing protection strategies, both passive safeguards (e.g., pressure safety valves) and active/procedural measures (e.g., automated, process shutdown procedures) to detect vulnerabilities, quantify potential consequences, and support the prioritization of mitigation actions.

To support this type of analysis, digital twins represent a valuable tool. A digital twin is a dynamic, model-based representation of a physical system, capable of simulating real-time responses of a plant under both normal and abnormal operating conditions. Since it is grounded in actual plant data and configurations, it enables realistic reproduction of system behaviour, including responses to cyber-physical attacks.

The present study focuses on the development and application of a digital twin of a green hydrogen production facility, with the electrolyzer section defined as the battery limit. The model is implemented in Aspen HYSYS using the dynamic simulation environment. Potential cyber-attack scenarios were generated using the POROS 2.0 methodology, a systematic approach designed to identify sequences of manipulations on BPCS and SIS components that could trigger high-consequence events, such as operational disruptions or safety-critical failures (e.g., major events).

The most critical scenarios identified through POROS 2.0 were simulated using the digital twin to assess their impact on the process. The results provided detailed insights into the system's vulnerability to cyber threats, highlighting which equipment is most susceptible to targeted manipulation and under what conditions existing safeguards might fail. These findings serve as a foundation for developing and validating more robust mitigation strategies to improve the cyber resilience of the facility and reduce the risk of successful cyber-attacks.

Keywords: *Quantitative risk assessment , Digital twin , Green Hydrogen*