A framework for Seveso-compliant cyber-physical security testing in sensitive industrial plants

A Framework for Seveso-compliant Cyber-Physical Security Testing in Sensitive Industrial Plants

Luigi Coppolino[a], Salvatore D'Antonio[a], Vincenzo Giuliano[a], Giovanni Mazzeo[a,*], Luigi Romano[a]

[a] *University of Naples 'Parthenope'*
Centro Direzionale, Isola C4, 80133 Napoli

Abstract

The InfraStress-EU framework was defined in the context of the H2020 project *InfraStress*, to provide operators of sensitive industrial sites – i.e., industrial plants where dangerous substances are handled and are thus subject to the Seveso III Directive (2012/18/EU) – with a technically sound approach and an accompanying simulation tool for the prevention of accidents. The framework enables reliable and effective cybersecurity testing of industrial infrastructures, with the ultimate goal of improving the resilience of critical processes to cyber-physical attacks. It takes a cue from the TIBER-EU initiative, of which it extends the core penetration testing phases to "hybrid"—meaning consisting of a mix of real and simulated components—setups. By doing so, it relieves operators from their main concern, i.e., the risk of compromising the normal functioning of control systems when performing key security testing activities, such as gathering information on cyber-threats and/or trying out alternative response strategies. InfraStress-EU was implemented and evaluated in close cooperation with five operators, who contributed the requirements of real setups in their respective industrial sectors.

Keywords: Seveso, Sensitive Industrial Plants, Industrial Control Systems, Security Testing, Simulation

1. Introduction

The Seveso Directives are the main EU legislation [1] dealing with the control of major accident hazards involving dangerous substances to protect human health and the environment. Specifically, Seveso Directives oblige member countries to ensure that operators of Sensitive Industrial Plants (SIPS) adopt well-defined procedures to prevent major accidents. While the directives provide clear strategies for ensuring infrastructure reliability when hardware or software faults occur, they lack well-defined approaches for protecting service continuity against cyber attacks [2]. SIPS are quite attractive targets – due to factors such as the availability of large quantities of hazardous materials, and the possible presence of chemicals which may be used to manufacture Improvised Explosive Devices (IEDs) [3] – as well as an easier and easier one, as a consequence of the increasing use of automated controls and ICT-based instrumentation, which expose systems to cyber attacks. In such an increasingly threatening technology landscape, the deeper and the more extensive security testing procedures, the higher the chance of succeeding in surviving attacks, since security testing is the only discipline that actually enables organizations to identify where systems are vulnerable, to take proper corrective actions, and – ultimately – to make the cyber-physical world of SIPS compliant with Seveso. The inherent complexity of security testing is exacerbated in Seveso infrastructures, where the testing activity may adversely impact the normal operation of industrial systems supporting critical processes, possibly violating the directive. It is worth emphasizing that security breaches may well result in safety cases, since the misuse of critical systems might go far beyond service interruption or data loss, and include destruction of expensive machinery, harm to people, or damage to the environment [4][5][6].

In the literature, there are plenty of works, proposing: i) methodologies for risk management [7][8][9][10][11]; ii) supporting tools and solutions for security evaluation [12][13][14][15][16]; iii) approaches and guidelines for planning and performing security testing campaigns [17][18][19][20]. However, some of these techniques are only applicable to a specific of Industrial Control System (ICS) context [10][15][11], some cover a limited set of industrial technologies [19][20][17][16], some produce simulation-based evaluations but fail to provide details on how the simulation approach they propose can be integrated in a real infrastructure [9][8][12][7]. To the best of our knowledge, there is no previous work featuring a complete security testing procedure — compliant with legislation — that copes with operators' concerns about conducting live testing on their infrastructures.

In this paper, we propose a framework — namely, InfraStress-EU — for safe security testing of Seveso infrastructures. Safety is achieved by executing potentially invasive tests on the simulated parts of a hybrid (meaning combining real and simulated components) testbed. This approach ensures accuracy of the results, while enabling live testing on critical processes subjected to the Seveso directive. Our work takes a cue from the TIBER-EU project [21], i.e., the EU framework developed for intelligence-driven testing of critical live production systems, whose objective is to improve the

[*] Corresponding author

Email addresses: `luigi.coppolino@uniparthenope.it` (Luigi Coppolino), `salvatore.dantonio@uniparthenope.it` (Salvatore D'Antonio), `vincenzo.giuliano@studenti.uniparthenope.it` (Vincenzo Giuliano), `giovanni.mazzeo@uniparthenope.it` (Giovanni Mazzeo), `luigi.romano@uniparthenope.it` (Luigi Romano)

cyber resilience of financial institutions, standardize the way tests are performed, and share results across the EU. In the context of the *InfraStress* project [22] , we extended and adapted the three core phases of the TIBER-EU framework to meet the requirements of Seveso operators. We defined the processes and the rules to perform penetration testing on the infrastructure, thus evaluating the capacity of detection and response of operators against cyber-physical threats. Our work is the result of a thorough requirements elicitation process conducted with five sensitive industrial production and storage plants belonging to the *InfraStress* project. More precisely, we collected the needs of: (a) an oil refinery managed by the motor oil company [23]; (b) a medical manufacturing industry managed by DePuy Synthes [24]; (c) a chemical storage site managed by the *Attilio Carmagnani "AC" S.p.A.* company [25]; (d) a chemical plant managed by the Municipality of Barreiro [26]; and (e) an oil storage site managed by the petrol company [27]. One important end goal of the requirement engineering phase was that the framework must support testing procedures on target systems with an increasing degree of criticality, and that there should be no interference on systems with the highest Safety Integrity Level (i.e., SIL4). Our hybrid security testing approach meets the needs of operators while also ensuring an accurate testing process. The framework is composed by three core phases, which were validated in the chemical storage case study managed by *Attilio Carmagnani "AC" S.p.A.*: *i*) Preparation, where internal and external teams are defined, critical processes are identified, and supporting tools are selected; *ii*) Testing, where threat intelligence operations are performed and attack scenarios are executed; *iii*) Closing, where reports are drawn, results are shared, and possible remediation plans are defined. In order to provide a self-contained solution, the framework comes with a reference implementation of a simulator for industrial infrastructures. Also importantly, the paper features a best of breed selection of available technologies, which can be used for extending the simulator and/or to build an alternative implementation of it.

The remainder of this work is organized as follows. Section 2 provides a background on both Seveso directives and on the TIBER-EU framework. Section 3 presents the related work. Section 4 reviews the requirements elicitation phase conducted in cooperation with the five aforementioned Seveso operators. Section 5 identifies the current problems and outlines the goals of the study. Section 6 presents the proposed testing framework. Section 7 discusses the architecture of a reference simulator that can be used to support the testing activity and provides pointers to available technologies for possibly extending it. Section 8 deals with a use case of the framework with respect to a chemical storage infrastructure. Finally, Section 9 discusses the main achievements of this study and its future directions.

2. Background

2.1. Seveso Directive

The Seveso III Directive [1] is an European Parliament directive relating to the control of major accident hazards involving dangerous substances. The Directive establishes rules and measures for the prevention of major accidents whose consequences may have an impact on human health and the environment, with the aim of achieving an improvement in the level of protection throughout the European Union. The final recipients of the Directive are European industrial establishments whose activities concern dangerous substances; lower-tier and upper-tier establishments are distinguished according to the quantity of hazardous substances present in the plant. The operators, i.e., the natural/legal persons who manage and control the establishments, are obliged to take all the necessary measures to prevent major accidents, and limit and mitigate their consequences. Member States designate the national competent authority responsible for the implementation and performance of the tasks set out in the Directive.

Member States shall ensure that the operator submits the following report to the authority:

- *Notification (art.7):* it contains a general description of the establishment, information on hazardous substances, main plant activities, the surrounding environment and factors that can cause a major accident.
- *Major accident prevention policy—MAPP (art.8):* it describes the operator's overall aims and principles of action in terms of accident prevention, role and responsibility management, the commitment to continuously improve the control of major accident hazards and ensure a high level of protection. The MAPP must be proportionate to the complexity of the organization and activities of the plant and must be implemented by a safety management system.
- *Emergency Plan (art.12):* it is a requirement for upper-tier establishments and establishes the procedures to control or contain the effects of a major accident, the measures necessary for the protection of the human health and the environment from the effects of major accidents as well as for the restoration and clean-up of the environment following a major accident.
- *Safety Report (art.10):* it is a requirement for upper-tier establishments and serves to demonstrate the implementation of the MAPP and the safety management system, the development of internal emergency plans, the identification of possible major accident scenarios and the communication to the competent authority of all information related to the preparation of external emergency plans and the location of new plants around the establishment.

Member states establish or appoint one or more competent authorities to ensure compliance with the requirements of the Directive. The authority is responsible for:

- Developing an *external emergency plan* which specifies the provisions for receiving alarms sent by operators in the event of an accident, implementing off-site mitigation actions and providing information to the public and nearby infrastructures.
- Evaluating the *domino effect* due to an accident, and identifying all the establishments whose geographical position can increase the risk and consequences of an accident.

- Planning *periodic inspections* at the plants with the aim of monitoring the uptake of all preventive measures by the operator.

In the event of a major accident, the operator shall inform the competent authority by providing details about the accident (art.16), while the Member State shall inform the Commission (art.18). The Seveso Directives are made complete through other articles that explain further aspects on the exchange of information among parties, land use, public participation on relevant decisions, sanctions, and specify —through the annexes— the classification of dangerous substances and the essential data to be included in reports. In order to support the Seveso Directives, the Major Accident Hazards Bureau of the Joint Research Centre of the European Commission has created the MINERVA portal to provide access to all information on ongoing activities, relevant publications and control tools of main chemical hazards, with the overall goal of improving the prevention of major accidents and mitigating the potential consequences.

2.2. TIBER-EU

We designed INFRASTRESS-EU starting from TIBER-EU [21] since this is the reference framework adopted by the European Central Bank for developing security testing procedures. TIBER-EU delivers a controlled, bespoke, intelligence-led red team test of critical live production systems. The framework was created for being used on infrastructures and institutions within the financial sector. It cannot be applied *as-is* in the field of Sensitive Industrial Plants since it could threaten their reliability and lead to the violation of Seveso directives. Our work fills this gap.

In TIBER-EU, intelligence-led red teams conduct tests which mimic the tactics, techniques and procedures of real-life threat actors who are perceived as posing a genuine threat on the basis of threat intelligence. Testing aims to evaluate the protection, detection and response capabilities of a given entity by using several techniques to simulate an attack on its critical functions and underlying systems, e.g., people, processes and technologies. Ultimately, the overall objective of the framework is to strengthen the cyber resilience of entities, standardize the way these entities carry out tests across the EU, support cross-border testing, promote mutual assessments carried out using TIBER-EU, as well as the sharing of results and analysis. The framework is adopted by the authorities that decide which entity, under their responsibility, should participate in the test. Even if the entities conduct internal tests with their own red teams, a TIBER test is validated only if it is carried out by external teams, that are expected to provide a new and independent perspective. The TIBER-EU framework is a process consisting of three phases of different duration: preparation, test, and closure.

Several stakeholders are involved throughout the process. The competent authority that decides to implement the framework constitutes a *tiber cyber team*, which provides support and supervision during all activities. The entity creates the *white team*—the only party aware of the test—to establish the scope and objectives to be achieved, collaborate with third-party teams and manage escalations during the attack phase. The institute's staff who is not included in the white team constitutes the *blue team*, who is informed of the test in the closing phase to evaluate the real capability of detection, response to and mitigation of a cyber attack. The external third party providers are the *threat intelligence team* and the *red team*, who perform threat intelligence operations and launch the attack on the entity's live production systems.

3. Related Work

In this section, the research work on ICS security evaluation and assessment has been grouped into the following three categories: i) methodologies for the risk management; ii) supporting tools and solutions for the security evaluation; iii) approaches and guidelines for planning and performing security testing campaigns.

Many researchers proposed ICS modelling frameworks to facilitate the setting up of proper risk management policies. Amin et *al.* [7] presented a framework for assessing security risks in cyber-physical systems, which is designed to benchmark security risks when inter-dependencies of physical and logical components may result in correlated failures. dos Anjos et *al.* [8] leveraged a tool called Ponder to create a policy-based ICS security management model enabling formal policy specification, rule validation, policy distribution and application, as well as conformity check with current standards on information security of critical systems. Hieb et *al.* [9] proposed an ontology framework that allows formal representation of process control systems, together with a fault diagnosis algorithm capable of identifying process faults induced by a cyber intrusion. Langer [10] proposed an approach to risk management based on concepts of robustness, fragility, reliability and maintainability. The author also presented a UML-based solution for creating ICS models and supporting risk management. Castellanos et *al.* [11] proposed a model-based testing methodology to analyse the security of cyber-physical systems such as the ICS. They leveraged a data flow graph to highlight interactions between internal entities throughout the system under test. Moreover, authors proposed an algorithm and an attack diagram to highlight the dependencies between cyber and physical domains, thus enabling the human operator to identify attack vectors, and, most importantly, to identify the dependencies and the related attack propagation.

The second category of related work comprises solutions to automate or facilitate the security evaluation process out of traditional risk management schema. Tools have been designed to meet requirements of specific use cases and to have little or even no operational impact on the real industrial process. Wang et *al.* [12] presented a hybrid testbed for security assessment composed of real control network devices and simulated enterprise network equipment in a *ns-2* network simulator environment. Davis et *al.* [14] proposed a power grid virtual testbed based on PowerWorld and RINSE simulators. Genge et *al.* [13] developed a simulation framework whose goal is to ease simulation of cyber-physical attacks on physical systems. Suthors used Emulab to emulate cyber components, and MATLAB Simulink to simulate the physical processes. Mallouhi et *al.* [15] designed a different type of virtual testbed, which uses simulation technologies such as PowerWorld, Modbus RSim and OPNET to enable safe security testing. Reaves et *al.* [28] implemented a virtual testbed capable of interoperating with (real) physical industrial control systems. Queiroz et *al.* [16]

proposed SCADASim, a solution that uses the discrete event simulator OMNET++ to reproduce real-like ICS components and allow inter-connections with real industrial control system components.

Finally, there are a number of publications providing guidelines and approaches to ICS security assessment. Caselli et *al.* [18] expanded standardized security testing methodologies, such as the Open Source Security Testing Methodology Manual (OSSTMM) [20], NIST SP800-115 [29] and ISSAF [30], by defining a penetration testing approach tailored to ICS. The authors proposed different changes to the security testing flow of these standards. They included an emergency plan in the testing phase that could help in case of accidents. They extended the analysis phase and assigned the ICS operator the task of establishing an overall criticality score to the units, which need to be checked if the system returned to a normal state after being tested. NIST SP 800-82 [19] provides cross-industry guidelines for hardening industrial ICS and identifies procedures for developing and deploying industrial control system security management programmes. The Swedish Emergency Management Agency (SEMA) also released general guidelines for enhancing ICS security [17]. It deals with security at both organizational and operational level. The guidelines propose the adoption of the well-known Demming Cycle (i.e., plan, do, check and adjust) and suggest 15 recommendations for ICS security enhancement.

Different types of limitations affect the aforementioned categories. The majority of articles are either tailored to a particular ICS domain or to a limited set of industry technologies. We noticed that some relevant aspects of security testing procedures enabled by hybrid real-simulation approach are not addressed. The only contribution in this direction is the work of Reaves et *al.* [28], which provides details on how the simulator could be implemented, but no guidelines on how to use it for performing security assessment. Another limitation is related to the guidelines provided by the community. They guarantee that critical parts of the system are tested with caution. However, they contains no clear guidelines on how to manage the operators' concerns about conducting live testing on their infrastructures.

In this paper, we provide a framework for safe security assessment applicable to different ICS contexts, which also comes with a hybrid testing methodology that ensures accurate results and, at the same time, a solution to the problem of live testing. In order to provide a self-contained solution, this work also presents a tool for setting up the simulation of industrial processes and identifies a plethora of technologies to be used for the simulation.

4. Consultation with Seveso Operators

The testing framework we describe in this work is the result of a thorough requirements elicitation phase. As a first step, we conducted a stakeholder consultation to gather feedback and insights on the importance of a cyber and physical security testing framework compliant with Seveso directives. Our goal was to identify the limitations perceived by operators in applying a testing framework similar to TIBER-EU. We submitted a questionnaire to five industrial European plants managing critical substances and products:

Motor Oil (Greece) — Petroleum Refinery. Motor Oil Hellas (MOH) is located close to the city of Corinth and around 60 km west of Athens. MOH owns and operates one of the largest refineries in South-Eastern Europe with a high complexity rating (Nelson Complexity Index of 11,54). The Refinery, along with its ancillary plants and off-site facilities, forms the largest privately held industrial complex in Greece. Due to its versatility, it can process crude oils of various characteristics and produce a full range of petroleum products. MOH has an installed storage capacity of 2.5 million cubic meters (crude oil & products) and its own private sea terminal which can accommodate vessels up to the size of a Ultra Large Crude Carrer, making it one of the few ports in the Meditarranean that can accommodate such a capacity. The refinery comprises several capabilities such as: (a) Fuels Production: Crude Oil is processed to produce LPG, Naphtha, Kerosene, Diesel and Fuel Oil; (b) Gasoline Production: Naphtha is treated here to produce gasoline of a high octane number, thus eliminating the need for adding lead in gasoline; (c) A Hydrocracking Complex: to produce the new clean fuels with low sulphur; (d) A Fluid Catalytic Cracking Complex: Atmospheric Fuel Oil is fed to the FCC complex to produce LPG, gasoline, diesel, and Fuel Oil; and (e) Lubes Production: Atmospheric Fuel Oil is also fed to the Lubes Vacuum Unit.

DePuy Synthes (Ireland) — Medical Device Manufacturing. DePuy Synthes is based at the medical device manufacturing site in Ringaskiddy on the shores of Cork Harbour, just outside Cork city, on the south coast of Ireland. The site covers a total of 23.5 ha across two buildings as shown in the following picture. The two marked blue buildings occupy a total area of 47,380 m², of which 31,401 m² is manufacturing space. The site houses approximately 1,000 employees and runs 24-7, manufacturing orthopedic implants for knee, hip and shoulder replacements, which are a cornerstone in the orthopedic supply chain for Johnson & Johnson. Building 2 is also physically adjacent to a pharmaceutical plant (pharma ingredients) and operated by Hovione Ltd, with the physical boundary marked by a red line. The site has a large perimeter area, some of which is open to the sea, and is located near a number of other pharmaceutical plants, all within a 3 km radius.

Attilio Carmagnani "AC" S.p.A. (Italy) — Coastal chemical storage terminal. The terminal covers an area of about $30,000m^2$ and includes a set of 31 semi-buried or underground tanks with a total capacity of 26,840 cubic meters, distributed as follows: five tanks of 3,000 cubic meters, four tanks of 1,000 cubic meters, six tanks of 700 cubic meters, two tanks of 400 cubic meters, six tanks of 300 cubic meters, eight tanks of 130 cubic meters. The tanks normally contain Aromatic Hydrocarbons, Aliphatic Solvents, Acetates, Alcohols and Ethylene Glycols. The terminal is connected to Porto Petroli via three stainless-steel pipelines and is equipped with trucks and rail loading platforms connected to the main road, highway and railway, allowing for the easy transportation of goods towards national and international main commercial hubs. The plant is in a densely populated area, and for this reason, the relationship with the public entities and local communities is very important.

Fisipe (Portugal) — Special acrylic fibres producer. Located in Barreiro, Fisipe is a company that produces standard textile fiber,

	Question	Response Semantic	Result
1	Cyber-security is important for the infrastructure security.	Likert	Strongly agree: 85.7% Mostly agree: 14.3% Neither agree nor disagree: 0% Mostly disagree: 0% Completely disagree: 0%
2	Physical security is important for the infrastructure security.	Likert	Strongly agree: 87.1% Mostly agree: 12.9% Neither agree nor disagree: 0% Mostly disagree: 0% Completely disagree: 0%
3	Have you ever executed a Penetration Test on Cyber Systems?	Differential	Yes: 42.9% No: 57.1%
4	Did you include cyber-security in the Seveso Safety Report?	Differential	Yes: 14.3% No: 85.7%
5	Did you include cyber-security in the Seveso Emergency Plans?	Differential	Yes: 71.4% No: 28.6%
6	Security testing can be performed live.	Differential	Yes: 28.6% No: 28.6% Partially: 42.9%
7	Security testing interferes with accident prevention policies.	Likert	Strongly agree: 40.2% Mostly agree: 31.9% Neither agree nor disagree: 0% Mostly disagree: 20.5% Completely disagree: 7.4%
8	The misuse of the system can entail unexpected chemical reactions.	Likert	Strongly agree: 36.1% Mostly agree: 24.9% Neither agree nor disagree: 12% Mostly disagree: 17.5% Completely disagree: 9.5%
9	Results of security testing can be shared with other Seveso operators.	Likert	Strongly agree: 28.6% Mostly agree: 20.2% Neither agree nor disagree: 18.9% Mostly disagree: 27.7% Completely disagree: 4.6%
10	The infrastructure can go under security testing without the knowledge of employees.	Differential	Yes: 14.3% No: 42.9% Partially: 42.9%
11	The organization shares sensitive information for threat intelligence.	Likert	Strongly agree: 0% Mostly agree: 9.7% Neither agree nor disagree: 20.4% Mostly disagree: 32.6% Completely disagree: 37.3%
12	Does your infrastructure have simulators/emulators software?	Differential	Yes: 42.9% No: 57.1%

Table 1: Questionnaire responses

and has gradually become a producer of special acrylic fibres, namely pre-dyed fibres, functional fibres and fibres for technical application, being, more recently, also a carbon fiber precursor producer. Fisipe has been classified as a Seveso industry, since dangerous substances are used as raw materials that are stored in a tank farm inside the facility. A firefighting brigade (with a total of 36 members) is continuously present in the facility. The plant is equipped with a fire fighting system such as foam spreaders, water curtains, fire detectors and other prevention and fire extinguishing equipment. Fisipe has 320 employees, with some undertaking normal working hours and others on shift rosters, as the plant works 24-7.

PETROL Luka Koper (Slovenia) — Coastal petrol storage. PETROL represents an important critical infrastructure (CI) in the energy supply sector and shares the same location with the Port of Koper (also known as Luka Koper, the Slovenian translation of Port of Koper), which is also another important transport CI. Both companies are also categorized as ”upper-tier” sites according to the provisions of the national legislation implementing Seveso III (EU directive 2012/18/EC). The PETROL site comprises storage facilities for consumer oil products (fuels) and a distribution tank farm situated at the Sermin industrial zone, close to the city of Koper, where it neighbors the Luka Koper site. PETROL shares pipelines, piers and other logistical, communication and control infrastructure with Luka Koper. The Terminal Instalacija Sermin (TIS) is the largest and most modern equipped petroleum storage facility in the northern part of Adriatic Sea. It is located between the river Rižana, Adriatic Sea and Škocjanski zatok (Natura 2000 site – Special Protected Area). With its 23 aboveground tanks (reservoirs), TIS has a total capacity of 480.000 m³. In 2017, TIS surpassed 3 million tons’ throughput of petroleum products for the first time.

In our requirement elicitation, we submitted a questionnaire to 12 participants consisting of the five previously mentioned Seveso operators and their supporting providers. The questionnaire was defined in accordance with all the project consortium partners, and submitted in January 2021. It is composed by a total of 12 questions, whose responses can be of *differential* or *likert* semantic. Besides the questionnaire, we also conducted bilateral meetings with the operators to better discuss and identify their requirements.

A summary of questions, responses, and the related semantic is reported in Table 1. It can be observed from *resp. 1* and *resp. 2* that both cyber and physical security are extremely important for all the participants. However, only a small fraction of operators included cybersecurity in the Seveso Safety Report and Seveso Emergency Plans (i.e., 14.3% and 28.6%, respectively). The majority of respondents accepted live security testing only on a specific part of the production system (*resp. 6*). Hence, it is important that our framework enables representative testing and, at the same time, meets the requirement of Seveso operators. Usually, testing methodologies such as the TIBER-EU only take into account testing on the sole production environment. The Seveso context is particularly critical as a misuse of the monitoring infrastructure could interfere with policies of accident prevention (*resp. 7*). Thanks to the questionnaire, we also know that the majority of respondents (*resp. 10*) accept that a subset of employees is not aware of an ongoing security testing campaign. This is important as it allows us to obtain testing results with a higher degree of accuracy. On the other hand, operators seem skeptical in sharing the outcomes of the testing (*resp. 9*). Another piece of useful additional information relates to the availability of simulation software. The 57% of respondents do not own any tool that could simulate specific parts of the physical industrial process (*resp. 11*). All of them think it is acceptable to use third-party simulation platforms and also share sensitive information with the external teams under a Non-Disclosure Agreement.

5. Problem and Requirements Elicitation

The outcome of the consultation phase led us to the conclusion that the adoption of the TIBER-EU framework as-is, is not feasible. In fact, all the involved Seveso operators raised their concerns about doing live testing on their infrastructures, especially when employees were not aware of it. Live testing under these circumstances introduces the possibility of causing a denial of service incident, systems crash, release of hazardous substances into the environment, and modification or disclosure of data. Security, safety and availability could all potentially suffer from systems' misuse, which could ultimately result in a violation of the Seveso Directives. More precisely, the directive asks the operator to communicate the dangerous substances present in the plant, a forecast of the substances that can be generated following an accident, and a description of the possible accident scenarios. Given the complexity of the chemical reactions involved, it is not always easy to carry out forecasting operations. [31]. Carrying out a test on a live production system could destabilise the plant, and place it in unstable and difficult to predict state. In the event of an accident, this could trigger irreversible chain reactions with the consequent release of unexpected dangerous substances, without the presence of adequate mitigation actions as required by the Seveso directive. A different testing framework that includes a robust risk management and a reliable testing procedure is needed. The requirements we set for the framework are the following:

- *REQ-1:* activities and processes of the plant must be evaluated by identifying which critical elements cannot go under live testing.
- *REQ-2:* the infrastructure must be adequately prepared in order to support a hybrid testing environment that accurately reproduces the real activities of the plant, and guarantees a high level of safety for people and the environment.
- *REQ-3:* third-party solutions that allow simulations or emulations of processes and sub-processes must be integrated with technologies in use at the plant.
- *REQ-4:* operations of Threat Intelligence and the development of attack scenarios must take into account the accident prevention policies provided for by the Seveso directive.
- *REQ-5:* roles and responsibilities of all interested parties must be clearly defined, the operator must implement all the procedures provided for in the accident prevention policies and accurately define the scope of the test and related flag.
- *REQ-6:* third party suppliers must also possess specific requirements in terms of skills, experience in industrial security and must be approved by the competent authority.
- *REQ-7:* teams must agree on the management and destruction of sensitive plant data, on prohibited activities and on any insurance and liability.

6. The InfraStress-EU Framework

In this section, we present our security testing framework designed for sensitive industrial plants, which ensures controlled and safe testing strategies in compliance with constraints and requirements that emerged during the consultation with industrial Seveso operators. The framework (Figure 1) was defined starting from the fundamental principles of the TIBER-EU methodology and is composed of three main phases:

1. *Preparation.* In this phase, internal and external teams participating in the testing activity are identified. A crucial aspect of this phase is the plant analysis; the operator defines the test objectives, carries out risk management and evaluates the best approach to preparing the environment by identifying critical infrastructures activities. After recovering tools and technologies, the preparation phase ends with the testing scenario setup.
2. *Testing.* External teams perform threat intelligence operations by retrieving information on the plant technologies used, staff organization, infrastructure activities, and also evaluate the general national context on the main threats relating to the sector of interest. Based on the

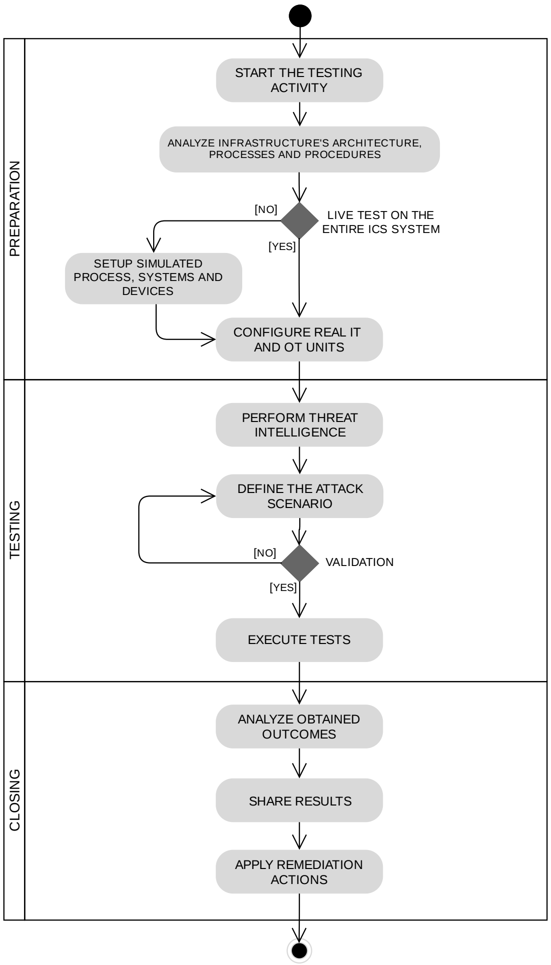

PREPARATION
START THE TESTING ACTIVITY
ANALYZE INFRASTRUCTURE'S ARCHITECTURE, PROCESSES AND PROCEDURES
[NO]
LIVE TEST ON THE ENTIRE ICS SYSTEM
[YES]
SETUP SIMULATED PROCESS, SYSTEMS AND DEVICES
CONFIGURE REAL IT AND OT UNITS
TESTING
PERFORM THREAT INTELLIGENCE
DEFINE THE ATTACK SCENARIO
[NO]
VALIDATION
[YES]
EXECUTE TESTS
CLOSING
ANALYZE OBTAINED OUTCOMES
SHARE RESULTS
APPLY REMEDIATION ACTIONS

Figure 1: High-level view of the InfraStress-EU Framework

intelligence report, possible attack scenarios are developed. The team inside the plant validates the proposed scenario and the testing operations begin.

3. *Closing.* The teams involved during the test phase draw up reports with strategies used and objectives achieved. In the final meeting the whole process is reviewed and discussed. Based on the results obtained, the operator implements a remediation plan, updates internal Seveso incident prevention policies by including scenarios triggered by cyberattacks and shares the testing experience with other Seveso operators.

The framework is adopted by the competent authorities who decide which operator should participate in the test. In the following sections, we will describe in detail the foreseen operations of each phase.

6.1. Preparation phase

Launch activities. The launch phase begins with the creation of the teams that will participate in the various activities, the authority creates a coordination team that supervises and provides support for all phases of the test, the Seveso operator establishes the White Team, i.e., the staff plant aware of the test. The White Team collaborates with third-party providers, sets the scope of the test and carries out the risk analysis, managing any escalation during the attack phases. The parties have a kick-off meeting to discuss the overall project activities and objectives, roles and responsibilities and expected results, establish a timeline for each phase and to formally start the test.

Overall Infrastructure analysis. The competent authority and the operator, through the members of the white team, define the scope of the test and set the objectives (flags) to be achieved by the attack team. Based on the scope of the test and the accident prevention policies set out in the Seveso directive, the white team carries out risk management, identifying and mitigating possible risks and implementing the necessary procedures to perform the test safely. In order to meet *REQ-1* and *REQ-2*, the operator assesses whether the test can take place entirely on live production systems or a hybrid environment, identifying critical components and processes, which could trigger unpredictable chain reactions in the event of an accident. The preparation of the hybrid testing environment can follow different approaches:

- Use external third party solutions for the IT/OT (Information Technology and Operational Technology) scenario virtualization and for the development-simulation of critical components and processes.
- Adapt internal simulation tools on virtualization platforms; consider, for example, the development of business process simulation tools necessary for any certifications.
- Equip and prepare a “digital twin”, i.e., a digital replica of a physical entity in a virtual space, in order to observe its functioning, simulate behaviors and solve problems.

Third party procurement. This activity concerns the involvement of external teams for the activities envisaged within the framework. The participating external teams are the following:

- *Threat Intelligence Team:* identifies threats and proposes intelligence-based attack scenarios.
- *Red Test Team:* prepare and performs the attack.
- *Technology provider:* provides tools and platforms to prepare the Seveso plant for testing operations.

As previously mentioned, to guarantee the validity and effectiveness of the test, attack and threat intelligence operations are committed to external third party providers rather than an internal team inside the plant for the purposes of producing a fresh and independent perspective. To meet *REQ-4*, thus ensuring a controlled and safe test, external teams must have proven experience in the areas of threat intelligence, cybersecurity and knowledge of industrial control systems, in particular regarding activities and processes involving dangerous substances.

The technology provider supports the Seveso operator in the hybrid environment setup. The technologies supplied must meet technical requirements (*REQ-3*), in detail:

- Virtualization of IT-OT scenarios.

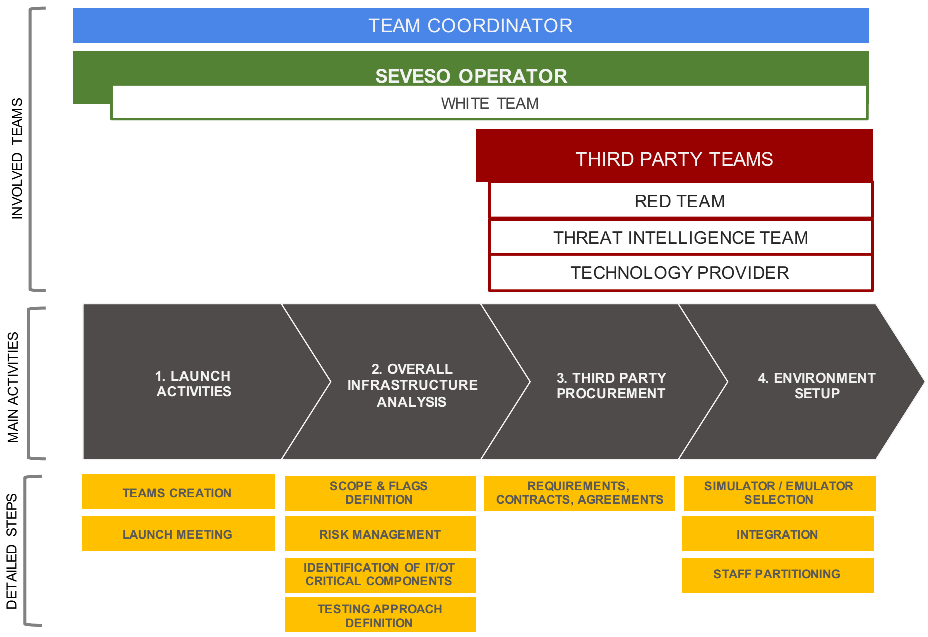


Figure 2: Preparation Phase

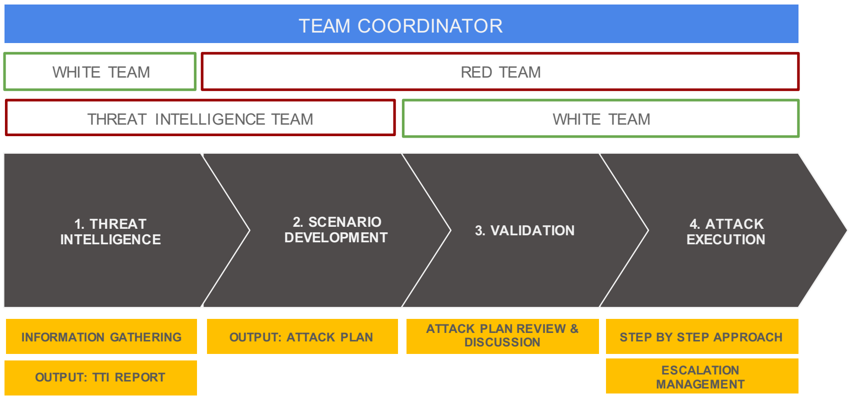


Figure 3: Testing Phase

- Support for standard communication protocols used in industry.
- Ability to perform simulations of physical processe.
- Interaction between simulated data and software already in use in the plant, e.g. simulation data output to SIEM or IDS.

The Seveso operator and the external teams must agree on prohibited actions and operations during the attack phases, the protection of people, the management of sensitive data, and non-disclosure agreements regarding the critical assets of the plant.

Environment Setup. The operator, after choosing the best approach for the hybrid environment setup, collaborates with the technology providers for the use of virtualization and simulation tools. In this phase, simulation models of physical processes are developed and all technologies integrated into the business workflow. Test secrecy is a crucial aspect of the framework, in addition to the white team, the plant personnel are not aware of the ongoing operations. The operator must, therefore, divide the staff in a manner consistent with the hybrid environment, with a number of the employees working on the simulated systems.

6.2. *Testing phase*

Threat Intelligence. The first activity of the testing phase is the threat intelligence operation. Based on the scope of the test and the objectives set in the preparation phase, the external Threat Intelligence Team (TI) identifies possible threat scenarios for the establishment under test and provides a realistic description of the threat landscape. During the information gathering step, the TI team collects information on the technologies, activities, staff organization and physical infrastructure of the plant. Due to time constraints and, or, ethical limitations that separate the TI team's approach from real attackers, the white team can share information with this team. For the elaboration of the threat scenarios, the team can use the GTL report in the first analysis, multiple input sources such as Open Source Intelligence (OSINT), Human Intelligence (HUMINT), and consult the information

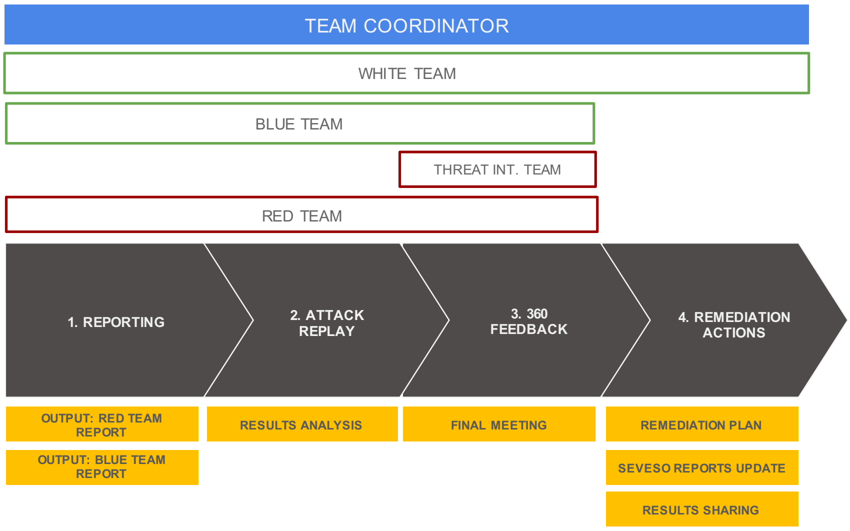


Figure 4: Closing Phase

contained in the MINERVA platform of the European Commission to gain an overview of major accidents. The result of this activity is a targeted threat intelligence-led report.

Scenario Development. The external red team uses the target threat intelligence-led report provided by the TI team to develop attack plans, detailing all the steps necessary to reach the flags. The entire attack plan is written from the attackers' point of view, trying to mimic the techniques and methodologies used by cyberterrorist in the real world, but also experimenting with innovative and never used approaches. The red team must consider the hybrid nature of the scenario in drafting the plan; in this case, the white team can again share information of a technical nature, e.g, the internal network organization. The result of this activity is the Red Team Test Plan.

Validation. The attack plan is discussed and reviewed together with the Seveso operator, the approach used is analyzed and the risk management procedures are validated. The attack plan must be compatible with the accident prevention policies adopted by the operator in the plant.

Attack execution. The red team executes the attack plan defined and validated in the previous activities. The entire execution of the attack is carried out in a controlled manner following a step-by-step approach in order to limit and reduce the risks for the plant and its critical functions. The red team informs the white team about the status of operations, the flags captured and the next moves, while the white team manages any escalations resulting from the execution of the attack based on the risk management carried out in the preparation phase and on Seveso emergency plans. Please note that the blue team represents the plant personnel who are not aware of the test, therefore, in this phase, it is possible to evaluate their real ability to detect, respond and mitigate cyber attacks.

6.3. Closing phase

Reporting. The red team draws up a summary report which describes the approach used in the test phase, the objectives and flags achieved and suggestions for improvement in terms of technical controls, policies and procedures, useful for the Seveso operator in the subsequent drafting of the remediation plan. The red team also indicates any help received by the white team to overcome obstacles during the test. Only during this phase is the blue team informed of the test. The red team draws up a report describing the actions, measures and responses taken in case of detection of the attacks.

Attack Replay. After the drafting of the respective reports, the red and blue teams organize a debrief workshop whereby both teams re-analyze the steps of the attack and evaluate what further measures could have been implemented, both regarding the attack and defensive measures.

360 Feedback. All teams participate in the final meeting by providing feedback on the overall process, with the aim of improving the activities and critical points of the framework. Evaluations are also made on the performance achieved by external third-party providers.

Remediation actions. The Seveso operator, based on the results observed during the test, draws up a remedy plan with the aim of correcting all vulnerabilities and improving security policies. Regarding the Seveso directive, the operator updates the accident prevention reports—such as MAPP and the Safety Report—including scenarios triggered by cyber attacks. The third-party tools used to create the hybrid scenario could become part of the industrial workflow in order to continue to carry out internal penetration testing exercises and cyber security assessments. Finally, the test results are shared with other Seveso establishments in order to draw useful lessons for improving the level of cyber resilience within the European Union.

7. A Reference Implementation of the ICS simulator

The availability of technologies and tools that enable the proposed hybrid security testing is fundamental. According to the

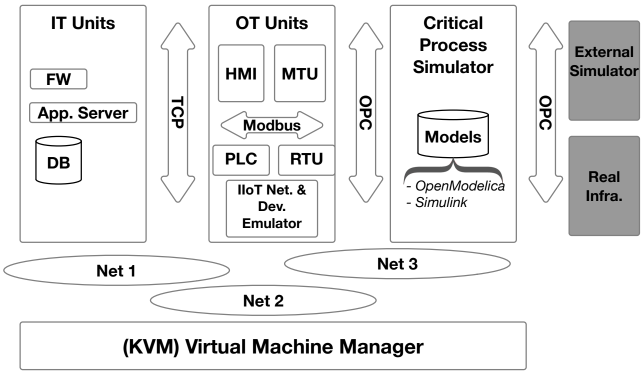
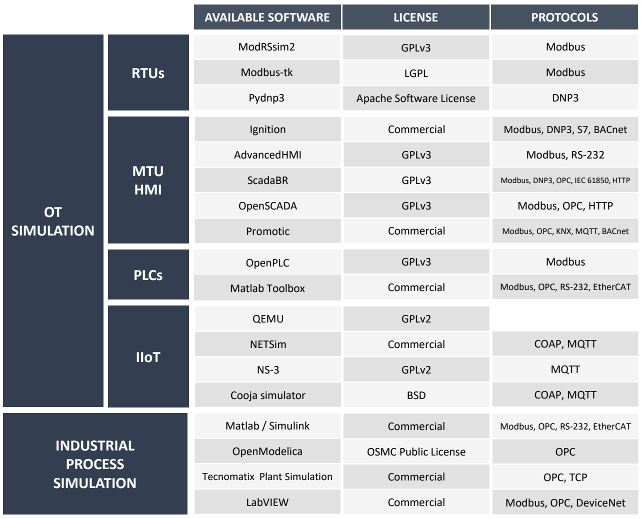


Figure 5: Simulator Architecture

outcomes of the consultation activity, some operators already have their own simulators that can be used for this purpose. Conversely, others need a dedicated solution to be defined as the framework cannot be applied without it. For this reason, in this section, we report a reference implementation of a simulation platform that would ease the InfraStress-EU usage. We propose an approach which takes advantage of *cyber-range* platforms to ensure flexibility, configurability, and ease of deployment. These provide virtual, legal, economic and controlled environments to perform security operations, organize attack and defense challenges and develop cybersecurity skills. Typically, these platforms provide simulations of IT systems reproducing the full range of information processing technologies such as software, hardware, network communications and related services. However, the cyber range *as-is* is not enough for an ICS. In fact, in this context, support for the virtualization of OT solutions and the simulation of industrial processes is required. The literature in this field establishes ICS-oriented cyber range solutions [32] [33], which are built on a specific physically simulated process with limited tuning possibilities in terms of scenarios and ICS components customization.

Figure 5 shows the architecture of our implemented solution. At the core of the industrial simulator there is a KVM-based Virtual Machine Manager (VMM), which is responsible for spawning three categories of VMs and the related inter-connected networks. The first category of VMs comprises IT-related units (i.e., application server, database, firewall), which are virtualized in the same way as cyber-range tools. The other two categories of units needed for the simulation are specific of the industrial domain, i.e., OT units and the critical process simulator. OT units communicate with IT machines and devices via TCP, while the OPC protocol is used to exchange data between the critical process simulator and the OT units. OPC is also leveraged by the simulator to consume data produced in the real infrastructure. The reason in the adoption of OPC is in its widespread use in the industrial automation field, which enables an easier interoperability with existing systems and devices. In our solution, any critical process simulator can be easily plugged in thanks to OPC, which ensures a loosely coupled integration with the surrounding units. It can either use a set of models defined offline, or interact with an external simulator that may be provided by the infrastructure administrator.

In the following, we give an insight on the solutions we adopted for the simulation of industrial-related units. At the same time, we report other tools available in the market (see Table 2), which can be a useful reference for to a security engineer willing to set up a simulator.



		AVAILABLE SOFTWARE	LICENSE	PROTOCOLS
OT SIMULATION	RTUs	ModRSsim2	GPLv3	Modbus
		Modbus-tk	LGPL	Modbus
		Pydnp3	Apache Software License	DNP3
	MTU HMI	Ignition	Commercial	Modbus, DNP3, S7, BACnet
		AdvancedHMI	GPLv3	Modbus, RS-232
		ScadaBR	GPLv3	Modbus, DNP3, OPC, IEC 61850, HTTP
		OpenSCADA	GPLv3	Modbus, OPC, HTTP
		Promotic	Commercial	Modbus, OPC, KNX, MQTT, BACnet
	PLCs	OpenPLC	GPLv3	Modbus
		Matlab Toolbox	Commercial	Modbus, OPC, RS-232, EtherCAT
	IIoT	QEMU	GPLv2	
		NETSim	Commercial	COAP, MQTT
		NS-3	GPLv2	MQTT
		Cooja simulator	BSD	COAP, MQTT
INDUSTRIAL PROCESS SIMULATION		Matlab / Simulink	Commercial	Modbus, OPC, RS-232, EtherCAT
		OpenModelica	OSMC Public License	OPC
		Tecnomatix Plant Simulation	Commercial	OPC, TCP
		LabVIEW	Commercial	Modbus, OPC, DeviceNet

Table 2: Tools supporting ICS simulation

OT Units. The way of simulating OT units varies depending on their typology, i.e., weather it is a machine or a device. HMI and MTU can be simulated via VMs equipped with a general-purpose OS and with a dedicated simulation software. RTUs and PLCs, instead, need to be deployed using VMs equipped with hardware emulators and with an embedded OS. Regarding the simulation of the bus for OT-related communications, it is clearly dependent on what is actually used in the real infrastructure.

- *PLC:* these microprocessor-based industrial controllers were simulated using the OpenPLC tool [34], which offers the possibility of writing PLC code using the IEC 61131-3 standard language. OpenPLC is also composed by a multi-platform runtime module that executes the PLC code easily on any platform. It provides support for open communication buses (e.g., *Modbus*), while it lacks support for other commercial industrial protocols.
  As an alternative PLCs can be reproduced with non-free platforms such as LabView [35] or Simulink [36], which allow to write PLC driver code and interface using commercial PLC devices available in the market. The advantage of this software is in the availability of a large set of supporting code and comprehensive documentation, at the cost of expensive license fees. In terms of free solutions, we suggest the

- *RTUs:* the simulation of *remote terminal units* that acquires in real-time inputs from the physical world and transmits to one or more master SCADA server is highly influenced by the adopted ICS communication protocol. In fact, the available simulators always provide the pair RTU-Bus. We used *ModRSsim2* [37], which is for RTUs sending data over the Modbus protocol.
  An alternative is *Modbus-tk* [38], and other tools for

proprietary communication protocols such as DNP3, namely Pydnp3 [39].

- *MTU-HMI:* the *master terminal unit* communicates with low-level devices, such as RTUs and PLCs, to monitor/control the infrastructure, while the *human-machine interface* allows human operators to interface with the monitoring system. In simulation contexts, it is common to find solutions where the HMI and MTU are put together offering a *all-in-one* product that ease the users' experience. Different software solutions exist in the market, mainly with commercial license. The *AdvancedHMI* project [40]—based on Microsoft .NET—allows the user to build a dedicated customized HMI and develop additional modules, relying on the support of a large community. In terms of open source solution, we highlight *ScadaBR* [41], which allows users to view, record, graph, create alarms on sensors data, RTUs and PLCs. This solution is supported by major industry standard protocols. However, there are limitations in the scripts handling and in triggered actions when a certain event occurs.

- *IIoT Network & Device Emulator:* Generic IIoT devices needs to run on top of emulated hardware. In our solution we leveraged the open-source QEMU [42] emulator, which offers emulation support for the majority of ARM-based embedded architectures. Our approach was to spawn a VM containing Qemu and the related device software on top of it. In terms of network, instead, we used the open source NS-3 [43] network simulator, which supports most accepted IIoT networks such as *LoRa, SigFox, ZigBee*.
  A valid commercial alternative is *NetSim* [44], which supports all layers of typical IoT stacks and provides an environment to run simulated experiments via a user-friendly interface. Otherwise, another open-source solution is the Cooja [45] simulator.

Critical Process Simulator. The critical process simulation is crucial for accurate testing. Our approach was to reproduce the dynamic of the industrial process via a model-based representation of real physical components working together. Based on the physical properties of components, as well as mathematical models, the software can reproduce the dynamic of the particular process. Among simulation and modeling tools available in the market, in our solution we used the following simulators, which are better documented and accompanied by different sample codes:

- *Simulink:* it is the widely-known commercial software of the Matlab ecosystem for modeling, simulating and analyzing stationary and dynamic systems using a graphical interface that allows users to build models using block diagrams. The wide availability of toolboxes for specific technical domains (e.g. Simscape, Robot Control, Signal Analysis) provide good versatility in model development and make it one of the best choices for systems control. On the other hand, some specific areas (e.g., load and power flow) can be difficult to simulate and it may be preferable to use third party software dedicated to these purposes. Simulink comes with a commercial license that can be expensive.

- *OpenModelica:* [46] it is an open source environment based on the Modelica language for modeling, simulating, optimizing and analyzing complex dynamic systems. Modelica is an object-oriented language designed to model the dynamic behavior of engineering systems. The strengths of the software are the causal modeling and the concept of connectors, which allows easier interconnection of various physical domains (e.g., mechanical, electrical, hydraulic), and makes OpenModelica the best choice for multi-domain physical modeling. Compared to Simulink, the documentation of OpenModelica and its external libraries is often less comprehensive, and moreover, it is less intuitive and easy to use.

It is important to highlight that the interoperability of the simulator is crucial. It is the enabler for the co-existence of the real and simulated worlds. There is a large and diverse set of communication protocols usable at different levels of the ICS such as Profinet, Modbus, EtherNet/IP, MQTT, LoRa, AMQP. The simulator has to be equipped with a standardized communication protocol that allows the different tools to communicate with each other within the virtual network, and—most importantly—interface and transmit information with the real systems installed in the plants. As already mentioned, we used OPC. Both Simulink and OpenModelica support the protocol and allow simulation data to be exposed through OPC nodes, thus facilitating interconnection with real devices and tools. Most of the suggested tools support, for example, communication via Modbus; therefore, it might be a good choice to interface virtual components of a SCADA system such as PLC, RTU, HMI through this protocol.

8. The Chemical Storage Case Study

In this section we demonstrate the use of the InfraStress-EU framework in a chemical storage infrastructure. Specifically, we refer to the terminal managed by the *Attilio Carmagnani "AC" S.p.A.* company (presented in Section 4), which covers an area of about $30,000m^2$ and includes a set of 31 semi-buried or underground tanks with a total capacity of $26,840m^3$. *Attilio Carmagnani "AC" S.p.A.* is connected to Porto Petroli (Genoa - Italy) via three stainless-steel pipelines and is equipped with trucks and rail loading platforms connected to the main highways and railways, allowing for an easy transportation of goods towards national and international main commercial hubs.

8.1. Preparation phase

Launch activities. The preliminary and organizational aspects of the testing campaign were discussed with the *Attilio Carmagnani "AC" S.p.A.* staff. Before starting the actual test it was necessary to set-up teams. For this case study, our university team played the role of the red team, whereas *Attilio Carmagnani "AC" S.p.A.* identified the personnel to be included in the white team, which, according to the framework specification, was in charge of setting test objectives and defining risk management activity.

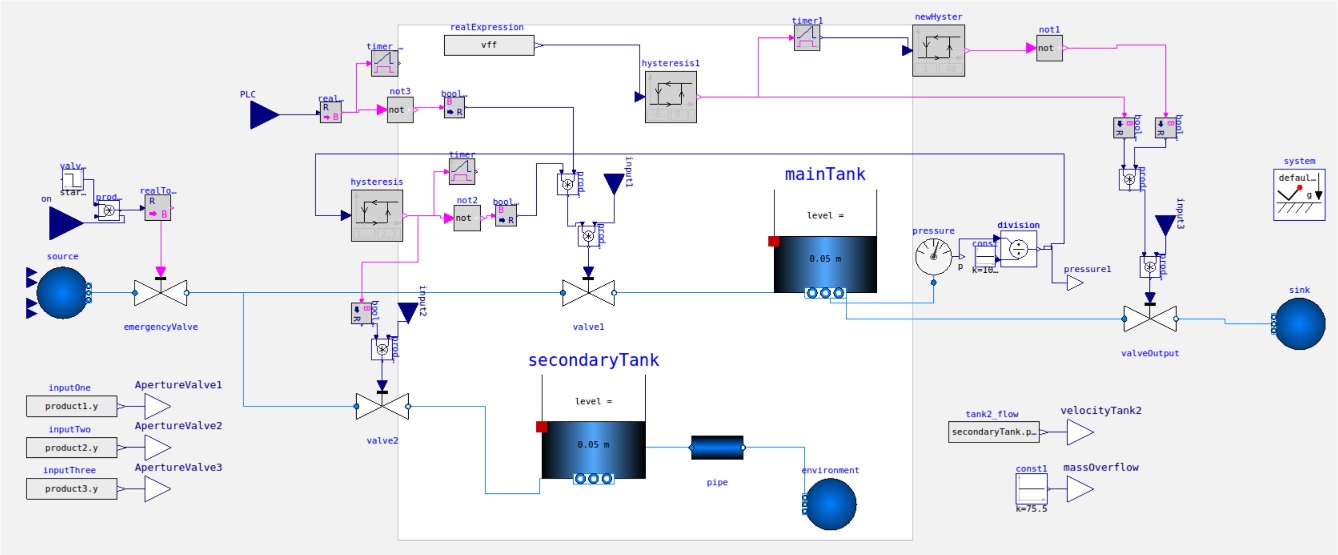


Figure 6: The Simulated Chemical Storage Critical Process

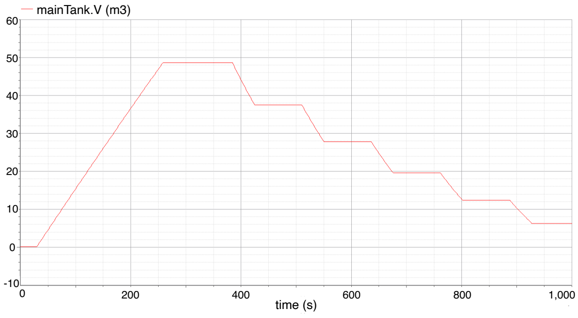


Figure 7: Simulation of the tank filling / emptying cycle

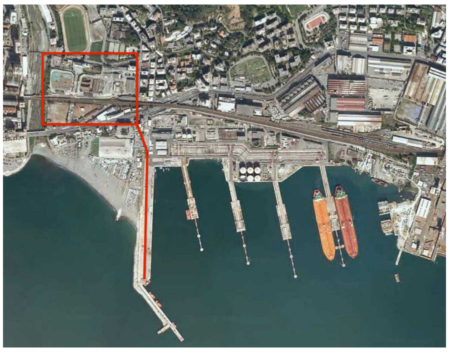


Figure 8: Map of the Critical *Attilio Carmagnani “AC” S.p.A.* Process

Overall Infrastructure Analysis. At this stage, preliminary meetings with *Attilio Carmagnani “AC” S.p.A.* took place to detail the organization of the overall IT-OT infrastructure, identify critical processes of the industrial plant, and analyze the Seveso plans currently adopted by the company. The ICS of *Attilio Carmagnani “AC” S.p.A.* is composed of: 14 RTUs and 9 PLCs spread throughout the infrastructure, 1 MTU, a control room equipped with one Siemens SCADA system including an HMI, 2 database servers configured in High-Availability mode for the storage of historical sensor measurements, and 2 replicated application servers. It is important to notice that we provide no details of devices, systems, OS versions for confidentiality reasons.

Among different industrial processes, one was considered as extremely critical for the overall infrastructure safety. It refers to the loading/unloading procedure of dangerous chemicals (highly flammable and hazardous to the aquatic environment) whose alteration could indeed result in catastrophic consequences. The critical process involves stainless-steel pipelines connected to the facility of Genoa Oil Terminal, which are used to transfer the chemicals from vessels to above-ground tanks (Figure 8). One specific flow is dedicated to highly flammable products and it involves a special tank equipped with sensors and radars to control the level of stored chemicals. If thresholds are reached, a three-way valve is activated by the ICS and the chemicals flow is switched to a secondary reservoir. Based on *Attilio Carmagnani “AC” S.p.A.* requirements, it was agreed that this process would have been simulated and integrated with the real infrastructure to guarantee a safe security testing.

Environment Setup. Setting up of the hybrid environment required interactions between the white team and the red team (i.e., our team). Since *Attilio Carmagnani “AC” S.p.A.* does not have a simulator of the identified critical process, we used — and properly configured — our solution described in Section 7. We modeled in *OpenModelica* the critical process, including the vessel, pipes, valves, and the primary-secondary tanks belonging to the identified process. The final structure is shown in Figure 6. The white team provided information regarding the dynamic behaviour of process components, e.g., tanks capacities, opening/pressure values of valves, thresholds. This allowed to define and tune the dynamic model into *OpenModelica*. As an example, Figure 7 shows the behavior of the primary tank during loading and unloading stages. Based on the provided technical documents, we selected a subset of OT units of *Attilio Carmagnani “AC” S.p.A.* to be recreated through the simulator. In particular, we integrated: 5 PLCs for controlling automatic valves and pumps, emulated through *OpenPLC* running a custom PLC program using IEC 61131-3; 6 RTUs for monitoring the status of valves, vessel's pumps, and tanks, which were emulated via *ModRSsim2*; 2 buses for supporting communications among OT units, i.e., *Modbus* and *OPC*.

The emulated process was thus configured to exchange I/O data with the real system. In particular, it was connected to the corporate Siemens SCADA server in order to provide it with the simulated field sensors' data, and to the IT machines installed in the *Attilio Carmagnani "AC" S.p.A.* control room. In this way, the critical process has been integrated with real systems and devices. The setup phase was then completed by partitioning the *Attilio Carmagnani "AC" S.p.A.* staff in two dedicated teams of operators — one aware and one unaware of the on-going testing activity — responsible for monitoring the infrastructure status. This was possible by interfacing the Siemens HMI with two different versions of the back-end: one providing only real data (used by the test-aware subgroup), and another one providing real-simulated data (used by the test-unaware subgroup).

8.2. Testing Phase

Threat Intelligence and Scenario Development. Threat Intelligence and Scenario Development activities were carried out by the red team in parallel. The threat intelligence activity was driven by the current cyber-physical security procedures as shared by the Seveso operator with the red team.

The most representative attacks on ICS - e.g CrashOverride, a framework designed to attack power grids, Triton/Trisis, a rootkit designed to target a specific model of Schneider Electric's Triconex and used in a Saudi Arabian oil and gas facility, BlackEnergy, a trojan used to attack power utility companies in Ukraine - were revised to exploit sector-relevant vulnerabilities. The implementation of the attack scenario required an in-depth study of the targeted physical process and some preliminary tests were performed to gather additional information, e.g. the interaction between PLCs and valves was reproduced and tested at the red-team premises.

Validation and Attack Execution. The attack scenario has been defined in collaboration with the Seveso operator and focused on a multistage attack whose ultimate goal is to alterate sensitive process data. The attack mimics the lateral movements typically observed in Advanced Persistent Threat (APT) and was performed as follows:

1. *IT Discovery:* we executed a TCP/UDP scan and an OS fingerprinting to collect information about machines, devices, and services communicating over the network.
2. *DMZ intrusion:* we exploited a remote software vulnerability and got access to the application server
3. *Privilege Escalation:* we performed a privilege escalation on the application server machine by leveraging CVE-2017-16995 vulnerability.
4. *Information gathering:* we gathered credentials from within the compromised machine using a dictionary attack.
5. *ICS discovery:* once entered the internal network, we performed a network scan searching for ports typically used in an OT environment, thus identifying available devices and related communication protocols such as Modbus.
6. *ICS intrusion:* we created an SSH tunnel towards the PLC device using the Metasploit tool and the stolen credentials.
7. *Evasion:* we installed a rootkit on the compromised ICS machine to remove system indicators (i.e., network connections and services) and make the attacker undetectable.
8. *ICS Sniffing and Data exfiltration:* we captured and analyzed the ICS network traffic using network probes.
9. *Attack execution:* we attempted two types of attacks, i.e., injecting a number of malicious Modbus packets in the communication flow, and injecting a malicious firmware in the PLC device. The first attempt failed, while the second one was successful.
10. *Response Inhibition:* finally, we disabled the alarm notification to prevent the intervention of the plant operators.

8.3. Closing phase

Reporting and Attack replay. The execution of the attack, although performed on the simulated physical process, occurred during a real chemical transport operation inside the plant. The attack actions performed in stage 9 involved generating malicious Modbus TCP packets to change the open state of the valves. However, the authentication mechanism implemented for data exchange prevented the attack. The second attempt targeted the PLC. The red team was able to reprogram the PLC and execute a custom code thanks to the possibility of uploading a new firmware. The PLC was successfully tampered with, thus causing a malfunctioning of the three-stage valve, and inhibiting the chemicals flow to the reservoir tank. This has led — in the simulated environment — to the main tank overflow, with a consequent leakage into the surrounding environment. Although the overflow was not occurring in the real world, the *Attilio Carmagnani "AC" S.p.A.* internal team — unaware of the testing activity (i.e. the blue team) — implemented the procedures foreseen in the emergency plans to avoid explosions and chain reactions. Once the attack finished, the blue team was informed of the test and both the teams involved drew up the reports as required by the framework.

360 feedback and Remediation actions. We had a final meeting with *Attilio Carmagnani "AC" S.p.A.* to discuss the achieved results. The blue team managed to correctly apply mitigation measures to avoid a serious emergency, but failed to prevent the tank overflow and chemical leakage. If the attack had occurred on the real physical system, it would have disastrous effects. The Seveso operator leveraged the testing experience to remove the vulnerabilities, which were exploited to perform the successful attack. Then, we jointly established a work plan in order to further improve the infrastructure's cyber-physical security.

9. Summary and Conclusions

This paper presented a framework, called InfraStress-EU, which provides operators of sensitive industrial plants (SIPs) – i.e., industrial plants where dangerous substances are handled and are thus subject to the Seveso III Directive – with a technically sound approach for cybersecurity testing. The approach driving the testing activity was inspired by a project with similar goals – but in a completely different context, namely: TIBER-EU – and developed based on the requirements contributed by five operators managing sensitive industrial plants in Europe. In addition to this important methodological contribution, the paper also makes a major contribution in the technological plane. The framework comes with an accompanying tool, enabling penetration testing on "hybrid"—meaning consisting of a mix of real and simulated components—setups, with the ultimate goal of improving the resilience of critical processes to cyber-physical attacks. By relieving operators from their main concern, i.e., the risk of compromising the normal functioning of control systems when performing key security testing activities, the tool enables a leap forward in security testing practice. The InfraStress-EU framework and accompanying tool was then validated in the context of a real case study, specifically the chemical storage infrastructure managed by the *Attilio Carmagnani "AC" S.p.A.* company. Experiments demonstrated that the proposed solution has the advantage of allowing accurate and non-intrusive evaluation, and was thus very well received by the operators who participated in the campaigns. We focused on the most critical processes, which were analyzed using the hybrid simulator. Further validation experiments will be done with respect to the other four Seveso plants, which took part to the requirements elicitation phase. It is worth emphasizing that our work was very well received by the standardization community, too. In fact, it is now part of the *DIN SPEC* 91461 standard proposal [47], namely: "*Framework for stress-testing resilience of industrial plants and sites (critical entities) exposed to cyber-physical attacks*".

Acknowledgements

We are grateful to the *Attilio Carmagnani "AC" S.p.A.* company for the availability and the support provided during the framework validation activity.

This project has received funding from: the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 833088 (InfraStress), the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883284 (7Shield), the Italian Ministry of Economic Development CUP B66G20000630005 (ICShield).

References

[1] D. E. of the European Parliament, of the Council. [link].
URL `https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012L0018&from=EN`

[2] F. Argenti, G. Landucci, G. Spadoni, V. Cozzani, The assessment of the attractiveness of process facilities to terrorist attacks, Safety Science 77 (2015) 169–181.

[3] V. C. Moreno, G. Reniers, E. Salzano, V. Cozzani, Analysis of physical and cyber security-related events in the chemical and process industry, Process Safety and Environmental Protection 116 (2018) 621–631.

[4] M. Lezzi, M. Lazoi, A. Corallo, Cybersecurity for industry 4.0 in the current literature: A reference framework, Computers in Industry 103 (2018) 97–110.

[5] S. Peisert, J. Margulies, D. M. Nicol, H. Khurana, C. Sawall, Designed-in security for cyber-physical systems, IEEE Security & Privacy 12 (5) (2014) 9–12.

[6] Y. Ashibani, Q. H. Mahmoud, Cyber physical systems security: Analysis, challenges and solutions, Computers & Security 68 (2017) 81–97.

[7] S. Amin, G. A. Schwartz, A. Hussain, In quest of benchmarking security risks to cyber-physical systems, IEEE Network 27 (1) (2013) 19–24. `doi:10.1109/MNET.2013.6423187`.

[8] I. dos Anjos, A. Brito, P. Motta Pires, A model for security management of scada systems. `doi:10.1109/ETFA.2008.4638433`.

[9] J. Hieb, J. Graham, J. Guan, An ontology for identifying cyber intrusion induced faults in process control systems, in: C. Palmer, S. Shenoi (Eds.), Critical Infrastructure Protection III, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, pp. 125–138.

[10] R. Langer, Robust Control System Networks: How to Achieve Reliable Control after Stuxnet, Momentum Press, 2012.

[11] J. H. Castellanos, M. Ochoa, J. Zhou, Finding dependencies between cyber-physical domains for security testing of industrial control systems, in: Proceedings of the 34th Annual Computer Security Applications Conference, ACM, 2018. `doi:10.1145/3274694.3274745`.
URL `https://doi.org/10.1145%2F3274694.3274745`

[12] C. Wang, L. Fang, Y. Dai, A simulation environment for scada security analysis and assessment, in: 2010 International Conference on Measuring Technology and Mechatronics Automation, Vol. 1, 2010, pp. 342–347. `doi:10.1109/ICMTMA.2010.603`.

[13] B. Genge, C. Siaterlis, I. Nai Fovino, M. Masera, A cyber-physical experimentation environment for the security analysis of networked industrial control systems, Computers & Electrical Engineering 38 (5) (2012) 1146–1161, special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing. `doi:https://doi.org/10.1016/j.compeleceng.2012.06.015`.
URL `https://www.sciencedirect.com/science/article/pii/S0045790612001243`

[14] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, D. Nicol, Scada cyber security testbed development, in: 2006 38th North American Power Symposium, 2006, pp. 483–488. `doi:10.1109/NAPS.2006.359615`.

[15] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, S. Hariri, A testbed for analyzing security of scada control systems (tasscs), in: ISGT 2011, 2011, pp. 1–7. `doi:10.1109/ISGT.2011.5759169`.

[16] C. Queiroz, A. Mahmood, Z. Tari, Scadasim—a framework for building scada simulations, IEEE Transactions on Smart Grid 2 (4) (2011) 589–597. `doi:10.1109/TSG.2011.2162432`.

[17] S. E. M. Agency, Guide to Increased Security in Process Control Systems for Critical Societal Functions, 2008.

[18] M. Caselli, F. Kargl, A security assessment methodology for critical infrastructures, in: C. G. Panayiotou, G. Ellinas, E. Kyriakides, M. M. Polycarpou (Eds.), Critical Information Infrastructures Security, Springer International Publishing, Cham, 2016, pp. 332–343.

[19] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, Guide to industrial control systems (ics) security (2015-06-03 2015). `doi:https://doi.org/10.6028/NIST.SP.800-82r2`.

[20] C. Eagle, Computer security competitions: Expanding educational outcomes, IEEE Security & Privacy 11 (4) (2013) 69–71.

[21] European Central Bank, Tiber-eu framework.
URL `https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf`

[22] InfraStress. [link].
URL `https://www.infrastress.eu/`

[23] MotorOil. [link].
URL `https://www.moh.gr/en/`

[24] DePuy Synthes. [link].
URL `https://www.jnjmedicaldevices.com/global`

[25] Attilio Carmagnani AC SpA. [link].
URL `http://www.carmagnani.com/`

[26] Fisipe Synthetic Fiber. [link].
URL `https://www.sglcarbon.com/en/`

[27] Petrol Group. [link].
URL `https://www.petrol.eu/`

[28] B. Reaves, T. Morris, An open virtual testbed for industrial control system security research, International Journal of Information Security 11 (08 2012). `doi:10.1007/s10207-012-0164-7`.

[29] A. C. K. Scarfone, M. Souppaya, A. Orebaugh, Nist special publication 800-115: Technical guide to information security testing and assessment (2008).

[30] Rathore, Brunner, Dilaj, Herrera, Brunat, Subramaniam, Raman, , Chavan, Issaf 0.2.1 - information systems security assessment framework (2006).

[31] A. Pey, P. Lerena, Implementing the seveso directive requirement on the anticipated presence of dangerous substances, Chemical Engineering Transactions 31 (2013) 1–6.

[32] D. Formby, M. Rad, R. Beyah, Lowering the barriers to industrial control system security with GRFICS, in: 2018 USENIX Workshop on Advances in Security Education (ASE 18), USENIX Association, Baltimore, MD, 2018. URL `https://www.usenix.org/conference/ase18/presentation/formby`

[33] A. P. Mathur, N. O. Tippenhauer, Swat: a water treatment testbed for research and training on ics security, in: 2016 international workshop on cyber-physical systems for smart water networks (CySWater), IEEE, 2016, pp. 31–36.

[34] T. R. Alves, M. Buratto, F. M. de Souza, T. V. Rodrigues, Openplc: An open source alternative to automation, in: IEEE Global Humanitarian Technology Conference (GHTC 2014), 2014, pp. 585–589. `doi:10.1109/GHTC.2014.6970342`.

[35] P. A. Blume, The LabVIEW style book, Prentice-Hall, 2007.

[36] H. Klee, Simulation of dynamic systems with MATLAB and Simulink, Crc Press, 2018.

[37] ModRSsim2. [link].
URL `https://sourceforge.net/projects/modrssim2/`

[38] modbus tk. [link].
URL `https://github.com/ljean/modbus-tk`

[39] P. DNP3. [link].
URL `https://pypi.org/project/pydnp3/`

[40] AdvancedHMI. [link].
URL `https://www.advancedhmi.com/`

[41] M. S. Almas, L. Vanfretti, S. Løvlund, J. O. Gjerde, Open source scada implementation and pmu integration for power system monitoring and control applications, in: 2014 IEEE PES General Meeting — Conference Exposition, 2014, pp. 1–5. `doi:10.1109/PESGM.2014.6938840`.

[42] F. Bellard, Qemu, a fast and portable dynamic translator., in: USENIX annual technical conference, FREENIX Track, Vol. 41, Califor-nia, USA, 2005, p. 46.

[43] G. F. Riley, T. R. Henderson, The ns-3 network simulator, in: Modeling and tools for network simulation, Springer, 2010, pp. 15–34.

[44] P. Nayak, Comparison of routing protocols in wsn using netsim simulator: Leach vs leach-c, International Journal of Computer Applications 106 (11) (2014).

[45] C. Simulator. [link].
URL `https://github.com/contiki-os/contiki`

[46] P. Fritzson, P. Aronsson, H. Lundvall, K. Nyström, A. Pop, L. Saldamli, D. Broman, The openmodelica modeling, simulation, and development environment, in: 46th Conference on Simulation and Modelling of the Scandinavian Simulation Society (SIMS2005), Trondheim, Norway, October 13-14, 2005, 2005.

[47] DIN, Spec 91461 framework for stress-testing resilience of industrial plants and sites (critical entities) exposed to cyber-physical attacks.
URL `https://www.din.de/en/wdc-beuth:din21:337874172`