Alma Mater Studiorum - Università di Bologna

DOTTORATO DI RICERCA IN

INGEGNERIA CIVILE, CHIMICA, AMBIENTALE E DEI MATERIALI

Ciclo 35

Settore Concorsuale: 09/D3 - IMPIANTI E PROCESSI INDUSTRIALI CHIMICI

Settore Scientifico Disciplinare: ING-IND/25 - IMPIANTI CHIMICI

SYNERGIES AMONG SAFETY AND SECURITY IN THE PREVENTION OF MAJOR ACCIDENTS RELATED TO DANGEROUS SUBSTANCES

Presentata da: Matteo Iaiani

Coordinatore Dottorato

Alessandro Tugnoli

Supervisore

Alessandro Tugnoli

Co-supervisore

Valerio Cozzani

Esame finale anno 2023

Abstract

Historical evidence shows that industrial infrastructures where hazardous materials are stored or handled (e.g., chemical industry, process industry, Oil&Gas critical infrastructures) are target of deliberate malicious attacks (security attacks) aiming at interfering with normal operations. In the last decades, the trend of security incidents affecting these facilities has increased and it is expected to increase further in the next years (e.g., cybersecurity processes more stressed due to higher remote workforce after Covid pandemic, ongoing conflicts, etc.), making security of critical infrastructures something that can no longer be disregarded. In fact, physical attacks (i.e., malicious interferences aimed at causing damage bypassing PPS (Physical Protection System) elements) and cyber-attacks (i.e., malicious interferences aimed at causing damage through the IT (Information Technology) and OT (Operational Technology) system) may generate events with consequences on people, property, and the surrounding environment that are comparable to those of major accidents caused by safety-related causes (e.g., random failure of equipment, human error, natural hazards).

The security aspects of chemical, process, and Oil&Gas facilities is commonly addressed using Security Vulnerability Assessment (SVA) or Security Risk Assessment (SRA) methodologies to evaluate the actual level of security risk and to determine if existing security measures and process safeguards are effective or need improvement. With this aim, these methodologies require the identification of potential threats, the selection of reliable security scenarios (cause-consequence chain from attacks to impacts), the evaluation of consequences of attacks, and the identification of effective safety/security countermeasures. However, most of available SVA/SRA methodologies are semi-quantitative and non-systematic approaches that strongly rely on expert judgment, leading to security assessments that are typically not reproducible. Some are also specific to a single industrial sector and therefore do not allow generalization to any critical industrial infrastructure. Moreover, only a few methods take into account the synergies among safety and security aspects, leading to potential conflicts or inconsistencies between requirements defined by the safety assessment and the security assessment taken separately, and to overlooked risks.

The present 3-year research is aimed at filling the gap outlined by providing knowledge on deliberate malicious attacks, as well as rigorous and systematic methods supporting existing SVA/SRA studies suitable for the chemical, process, and Oil&Gas industry. The different nature of cyber-attacks compared to that of physical attacks in terms of systems affected and attack paths carried out by the attackers, resulted in the development of hazard identification and quantitative methods suitable for the cybersecurity domain and the physical security domain characterized by differences in the core-mechanism. The first part of the research was devoted to the development and consequent statistical analysis using synergic approaches of two structured databases (one with the scope on the chemical and process industry and the other on the offshore Oil&Gas industry) allowing to develop new knowledge and lessons learnt on security threats affecting industrial critical infrastructures. The acquired background supported the development of hazard identification methods. In particular, a Bow-Tie based approach was developed for the identification of reference scenarios caused by physical attacks, while two reverse-HazOp based methodologies were developed for the systematic case-specific identification of the sets of manipulations of the BPCS (Basic Process Control System) and the SIS (Safety Instrumented System) which lead to major event scenarios (PHAROS methodology) and production outage scenarios (POROS methodology). To support the quantitative estimation of the security risk of a facility, a quantitative procedure based on the Bayesian Network modelling was developed allowing to calculate the probability of success of physical attacks, which is intended to be adapted to cyber threats in future work. All the developed methods have been applied to case studies addressing chemical, process and Oil&Gas facilities proving the quality of the results that can be achieved in

improving cyber and physical site security. Furthermore, the outcomes achieved allow to step forward in developing synergies and promoting integration among safety and security management.

Table of Contents

1. State of the Art of security management in the Chemical, Process and Oil&Gas industry

This Chapter outlines the state of the art of the security management in the chemical, process, and offshore Oil&Gas industry, pointing out the attractiveness of such facilities to be target of deliberate malicious attacks, the current legislation and requirements, the existing methodologies addressing security issues, and the security risk formulation framework.

1.1. Attractiveness of chemical, process, and O&G facilities

Industrial infrastructures, in particular those where hazardous materials (e.g., flammable, toxic, explosive materials) are stored or handled (e.g., chemical, process, and Oil&Gas facilities), may be the target of deliberate malicious attacks (security attacks) aiming at interfering with normal operations [1,2]. Attackers with different motivations (e.g., terrorists motivated by political gain or destruction; insiders motivated by ego, revenge or curiosity; saboteurs motivated by status or rebellion; etc.) may be attracted by industrial installations due to several aspects:

1. the socio-political location of the target facility, especially for the Oil&Gas industry [3];
2. the potential of triggering impacts with similar consequences to those originated by unintentional causes (i.e., safety-related causes such as random failure of components, human errors, natural disasters (NaTech)) for people, the surrounding environment, and the company itself (e.g., reputation damages, especially for multinational companies) [4];
3. the presence of materials that can be used as precursors for the production of weapons such as explosives [5];
4. the potential of obtaining proprietary information important for the business (e.g., through a cyber intrusion to the network system) [6].

Attackers such as terrorist groups or hackers, may exploit the vulnerabilities of the Physical Protection System (PPS, i.e., the totality of people, procedures, and physical elements for the protection of assets against deliberate malicious attacks [7]) of the target facility or of its OT system (Operational Technology, i.e., the BPCS, Basic Process Control System, plus the SIS, Safety Instrumented System) and start events such as the releases of hazardous substances, fires, explosions, and loss of process control [2].

For example, on February 2nd, 1993, in the United Kingdom, attackers crossed the site fences overnight and placed an explosive device on a side of the middle lift of a gasholder containing natural gas at low pressure. After its detonation, the tank collapsed, and 33 tons of natural gas were released and immediately ignited resulting in an airborne fireball. The detonation also originated a breach on the shell of a nearby gasholder and the resulting gas jet became ignited (cascading event with escalated consequences) [8]. Another example is that occurred on August 6th, 2008, where cyber criminals over-pressurized remotely a section of the BTC (Baku-Tbilisi-Ceyan) pipeline causing an explosion, the release of more than 30,000 barrels of oil in an area above a water aquifer, a fire lasting more than two days, and economic losses due to the production outage of about $5 million a day [9,10]. A more recent example is the well-known ransomware attack to Colonial Pipeline that occurred on May 7th, 2021 in USA [11]. In that case, attackers were able to access the CP billing system and stealing 100 GB of sensitive data [12]: the operators, in order to contrast the spreading of the intrusion and avoid the attacker to access the OT system, forced the pipeline to shutdown causing huge economic losses due to 6-days production outage, together with fuel shortages to refineries, airports, filling stations, etc.

The latter examples are two of the many incidents triggered by the malicious manipulation of the OT system of chemical, process, and Oil&Gas facilities that occurred in the last decades [13]. This is due to the digital transition towards higher levels of automation that the chemical, process, and Oil&Gas industry is undergoing (e.g., digital sensors, improved network protocols, increased interconnection with external networks such as the Internet of Things, IoT). While ensuring advantages such as efficient process control, quick and safe response to abnormal conditions, improved product quality, and continuous process optimization, this exposes the chemical, process, and Oil&Gas sites to cyber threats [14].

Overall, recent studies on the topic [2,15–17] evidence that the number of incidents (both physical-related and cyber-related) in the chemical and process industry, as well as in the Oil&Gas industry (onshore and offshore) has significantly increased after the year 2000, making the security of chemical, process, and Oil&Gas facilities an issue that can no longer be disregarded in the management of all the risks that can arise both from the inside and the outside of the site boundaries.

1.2. Legislation and requirements

The American and European scenarios are quite different with respect to security issues in the chemical and process industry, as well as in the offshore Oil&Gas industry. In the following two sections, this aspect is better clarified with current legislation and security requirements.

1.2.1. The chemical and process industry

So far and even before the terrorist attacks of "9/11", the US played a leading role in the development of policies and legislation to enhance the preparedness against such attacks (i.e., security attacks). In fact, according to a study published by the US Department of Justice [5], a chemical plant storing and processing hazardous materials (e.g., flammable, toxic, explosive materials) can be converted into a Weapon of Mass Destruction.

In 2002, the American Chemistry Council published the Security Code (within the existing Responsible Care initiative [18]) which is designed to help companies in achieving continuous improvement in security performance using a risk-based approach to identify, assess, and address vulnerabilities, prevent or mitigate incidents, enhance training and response capabilities [19]. However, no US law at the time required chemical and process facilities to implement security measures: in fact, only few chemical and process facilities implemented the non-regulatory programs to enhance security [20].

Later, in 2007 (and re-codified in 2014 through the "Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014") the US Department of Homeland Security, issued the CFATS (Chemical Facility Anti-Terrorism Standards) [21] which require a Security Vulnerability Assessment (SVA) or Security Risk Assessment (SRA) for those process facilities in possession of specific quantities of Chemicals of Interest (COI) in order to protect their assets and employees, maintain the integrity of the operations and preserve the value of investments [19]. In order to be compliant with the CFATS, chemical and process facilities needed to pass an inspection: this gave an important impulse to the developments of SVA/SRA methodologies (see Section 1.3).

Differently, in Europe, the Seveso Directives [22–24] focus on safety-related issues and on accidents triggered by natural events (NaTech), without addressing security issues, even if a mention to unauthorized accesses may be part of some country-specific transpositions of the Directives. For instance, the Italian transposition of the 2012/18/EU Directive [24] suggests to consider malicious acts and unauthorized accesses in the definition of the internal emergency plan. The prevention, preparedness, and response to terrorist attacks involving installations of the energy sectors (electricity and Oil&Gas) is promoted by the EPCIP (European Programme for Critical Infrastructure Protection) [25], but no extension is made to the chemical and process

industry. Furthermore, the EU Member States presently consider security a matter of national interest, which falls inside the sovereignty boundary and shall not be shared, except transnational security matters, for instance concerning near-border nuclear power plants.

1.2.2. The offshore Oil&Gas industry

In the United States the security of offshore Oil&Gas assets is led by the US Department of Homeland Security (US-DHS) along with the US Coast Guard (USCG) and the Department of Energy (DOE). In 2002, the US-DHS promulgated the Maritime Transportation and Security Act of 2002 [26], which required vessels and port facilities to conduct SVA/SRA studies and develop security plans such as passenger, vehicle and baggage screening procedures, security patrols, personnel identification procedures, access control measures, etc. The USCG enforced legislation requirements for security of Offshore Oil&Gas assets through the Navigation and Vessel Inspection Circular n. 03 03 (2009) and n. 05 03 (2003). They cover the required submittal of security related documentation to ensure compliance to the Maritime Transportation and Security Act of 2002. Within the US-DHS, the Transportation Security Administration (TSA) is among other tasks charged with the security of transportation of hazardous materials by any mode, including water (e.g., vessels) and pipelines.

As anticipated in the previous section (see Section 1.2.1), the European Union (EU) covers the subject of security of Oil&Gas assets through the concept of Critical Infrastructure Protection (CIP). The EU Directive 2008/114/EC [27], which provides the criteria for assessing the criticality of an infrastructure in terms of the severity of the impacts that its disruption or destruction would cause in an EU member state, classifies Oil&Gas production facilities as European Critical Infrastructure (ECI); nevertheless, it does not cover Oil&Gas exploration facilities. In addition to the aforementioned directive, the European Union published the EU Directive 2013/30/EU [28] which focuses on the safety of offshore Oil&Gas operations: it does not examine the security aspects, but it covers the safety and environmental implications of the aftermath of an accident that may have resulted due to a security breach.

1.3. Security Vulnerability/Risk Assessment

In the framework outlined in Section 1.2, several different Security Vulnerability/Risk Assessment (SVA/SRA) methodologies were developed by professional organizations, governmental authorities, and academic institutions to evaluate and manage security risks. The quite rapid development of such methodologies, in a time span of about ten years, often caused the use of different terminologies to identify the same key concepts, and the application of apparently different approaches to qualitative and quantitative assessment [29].

In the following sub-sections, the security risk is formulated and then, the key elements of the classical SVA/SRA methodologies, of the cybersecurity risk assessment proposed by the ISA/IEC 62443 series of standards, and of some academic proposals, are briefly described, pointing out scope and limitations.

1.3.1. Security risk formulation

In the process safety domain, risk is usually defined as a scenario combination of consequences and associated probabilities or associated uncertainties (probability is typically interpreted as a “frequentist probability”, thus as the fraction of time in which the event occurs and continuously repeats over time) [19]. In the security domain, risk is commonly defined without any explicit reference to a probabilistic component by the triplet asset/value, threat, and vulnerability [30]:

$$R = asset \times threat \times vulnerability \tag{1}$$

However, in spite of its widespread use, Cox has asserted that the formula expressed in eq. (1) for quantifying security risk is insufficient as a foundation for allocating resources and establishing priorities to contrast deliberate malicious attacks (security attacks) [31]. In particular, the main issues concern the inability to account for correlations between its components, the non-additivity of risks estimated using the formula, the inability of risk-scoring results to best allocate resources, and the inherent subjectivity and ambiguity of the score associated to each component (asset, threat, vulnerability).

Recently, Amundrud et al. [32] studied the compatibility between safety and security risk frameworks and traced a blue line in which also security risk may be defined by events-consequences and uncertainties, and according to Kriaa et al. [33], an approach to express the uncertainties is to refer to probability.

Based on the aforementioned considerations, the security risk can be defined as follows [34,35]:

$$R^i = f(P_1^i, P_2^i, C^i) \tag{2}$$

where, R^i: security risk of a certain scenario i; P_1^i: the probability of an attempted attack against an asset according to scenario i; P_2^i: conditional probability of successful execution of attack given the attempt according to scenario i; C^i: expected consequences of the attack according to scenario i.

Quantification of P_1^i requires data, knowledge, or modeling of the motivations, intents, characteristics, capabilities, and tactics of attackers, as well as of the socio/political context of the target facility [36]. Clearly, this poses a considerable challenge and falls largely into the domain of intelligence analysts, sociologists, and political analysts, rather than risk analysts. Therefore, as these analyses go beyond the specificity of the industrial sector to which the analyzed facility belongs, the approaches for the evaluation of P_1^i are largely inter-disciplinary, applicable to any critical infrastructure.

Quantification of P_2^i requires the understanding of how attackers can reach the assets they are targeting through vulnerabilities in the system being attacked [36,37] (the PPS in case of physical attacks, and the IT-OT network in case of cyber-attacks). In other words, it requires identifying the potential physical attack paths and cyber-attack paths that the attackers have to carry out to generate damage to the target. This generally requires knowledge of multiple disciplines, including process engineering, control systems engineering, physical and cybersecurity, and process safety. Therefore, unlike evaluation of P_1^i, the assessment of P_2^i strictly depends on the design of the Physical Protection System and/or of that of the IT-OT network, which may vary considerably (especially the PPS) for facilities belonging to different industrial sectors (e.g., offshore Oil&Gas platforms are surrounded by water, making the attack paths inherently different from the ones targeting onshore process facilities): hence, the need for industrial sector-specific approaches for the evaluation of P_2^i.

Finally, quantification of C^i requires capabilities in modelling scenarios such as releases of hazardous materials, fires, explosions, and toxic dispersions, which are typical of process safety and risk analysts.

In the following, available SVA/SRA methodologies are briefly described, pointing out scope and limitations.

1.3.2. Classical SVA/SRA methodologies

In 2003, the cross-sectorial initiative “Sources Sought for Vulnerability Assessments of Physical Assets” promoted by the US Department of Homeland Security (US-DHS) [38], gathered 44 private sector contributions and 24 public (federal, state and local government) methodologies aimed at the SVA/SRA in order to catalogue risk assessment methodologies, automated tools, and available software. Few responders provided specific methodologies or tools, while others indicated that they were making use of quite general well-known, existing methodologies [29]. On the basis of these results, the report evidenced that the application of methodologies developed for commercial sectors other than that for which they were

specifically designed, was cumbersome and, in most cases, required extensive modification to be fully effective. Therefore, in the following, reference to existing SVA/SRA methodologies is restricted to public, non-proprietary methodologies reported in the US-DHS document, which have been developed, tested, and validated for the Chemical and Petrochemical sector (chemical and process industry and Oil&Gas industry), within the cooperation of the government and industry.

Examples of SVA/SRA methodologies suitable for the chemical, process, and Oil&Gas (onshore and offshore) industry are reported in **Table 1**, each of which employs traditional risk assessment techniques and provides a well-defined, systematic framework to identify threats, vulnerabilities, and security risks. The reader is referred to [29,38] where an extended review and comparison of such methodologies is carried out.

Table 1 SVA methodologies for the chemical, process, and Oil&Gas (fixed and offshore) industry. Adapted from [29,38].

SVA/SRA methodology	Developer	Sector	Reference
Guidelines for Analyzing/Managing Security Vulnerabilities of Fixed Chemical Sites (CCPS - Center for Chemical Process Safety - methodology)	American Institute of Chemical Engineers – Center for Chemical Process Safety	Chemical and process industry (onshore facilities)	[39]
Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF)	Sandia National Laboratories	Chemical and process industry (onshore facilities and transport activities)	[40]
Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries (API RP 780)	American Petroleum Institute & National Petrochemical and Refiners Association	Petroleum and Petrochemical Industry (onshore facilities)	[35]
Security for Offshore Oil and Natural Gas Operations (API RP 70)	American Petroleum Institute	Offshore Oil&Gas facilities	[41]
Security for Worldwide Offshore Oil and Natural Gas Operations	American Petroleum Institute	Offshore Oil&Gas facilities	[42]
Risk Analysis and Management for Critical Asset Protection (RAMCAP) Security Vulnerability Assessment	American Society of Mechanical Engineers Innovative Technologies Institute, LLC (ASME ITI, LLC)	Chemical Manufacturing, Petroleum Refining, LNG	[43]
Guideline Combating Interfetence by Unauthorised Persons	German Hazardous Incidents Commission (Störfall-Kommission – SFK)	Chemical and process industry (onshore facilities)	[44]

The cited methodologies (**Table 1**) shared the basic backbone structure prescribed by CCPS criteria [39]:

1. **Project planning.** This step involves the selection of a multidisciplinary team skilled in security and process safety to conduct the analysis, the definition of objectives and scope, and the development of a plan to address the individual sites.

2. **Facility characterization.** This step includes identifying the potential target assets, locating information that describes the technical details of the selected assets to support the analysis, identifying the hazards and consequences of concern for the site and its surroundings, identifying existing layers of protection, and determining factors of the likelihood (target attractiveness).

3. **Threat assessment.** This step provides the characterization of the credible threatening agents based on several factors, either pertaining to the facility (e.g., type of industrial sector or reputation of the company), or external (e.g., socio-political situation of the region or war conflicts).

4. **Vulnerability analysis & Risk assessment.** This step includes the relative pairing of each asset and threat to identify potential vulnerabilities related to process security scenarios. This involves the identification of existing countermeasures and their level of effectiveness in reducing those vulnerabilities. The degree of vulnerability of each valued asset and threat pairing is evaluated by the formulation of security-related scenarios or by an asset protection basis.

5. **Identify countermeasures.** Based on the consequences and likelihood that the layers of protection are breached, appropriate enhancements to the security countermeasures may be recommended. These include improved countermeasures that follow the process security doctrines of deter, detect, delay, diminish, mitigate, and possibly prevent. This step should also include the development of an appropriate SVA/SRA report or documentation that can be used to communicate the results of the SVA/SRA to management for appropriate action.

Each of the 5 points is generally developed as sub-steps in the different SVA/SRA methodologies: the reader is referred to the reference sources provided in **Table 1** for the details of each methodology. As an example, **Figure 1** reports the flowchart of the CCPS methodology [39].

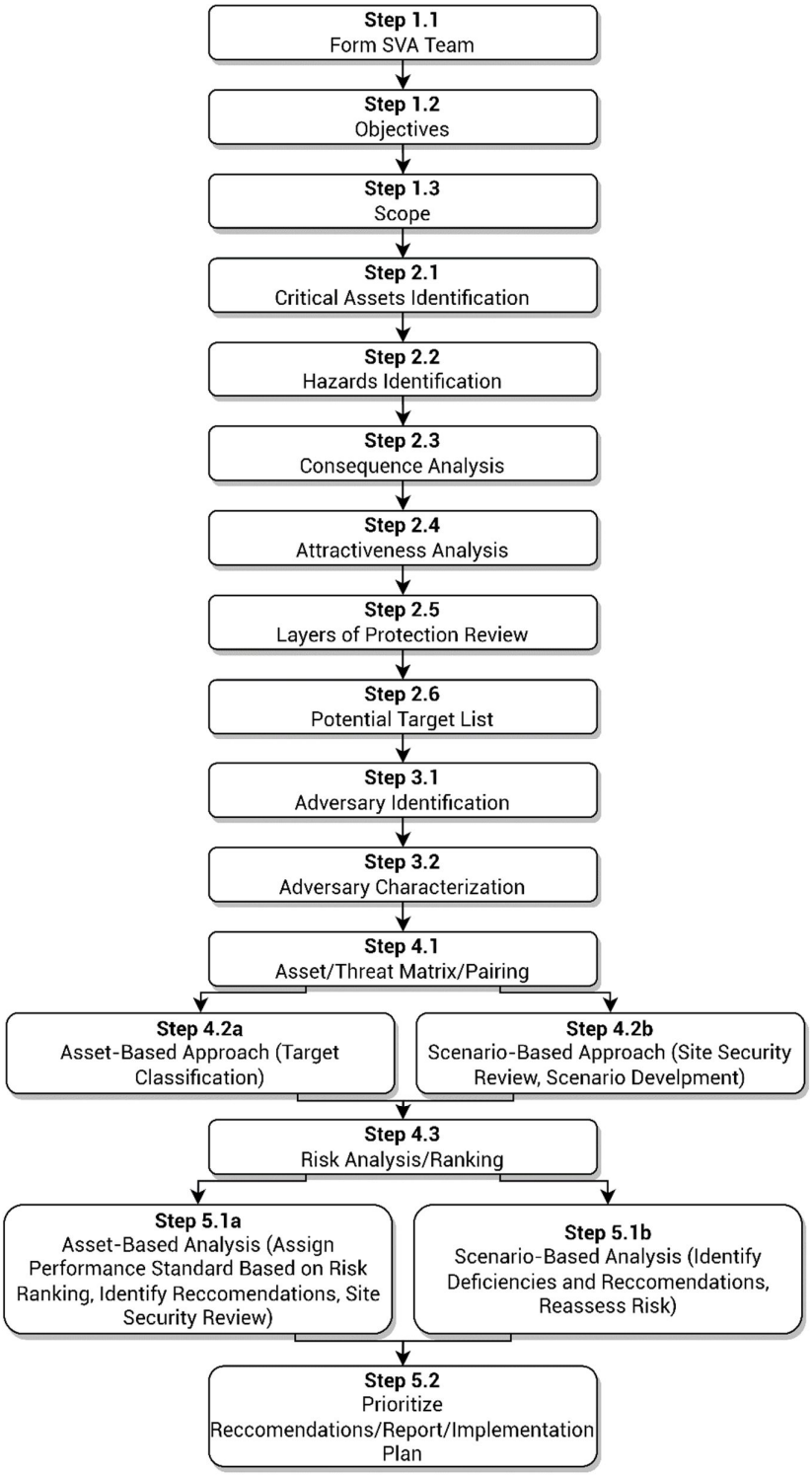

Figure 1 Flowchart of the CCPS methodology [39].

1.3.3. Cybersecurity risk assessment proposed by standard ISA/IEC 62443-3-2

The typical structure of the IT (Information Technology) system, OT (Operational Technology), and physical process system in the chemical, process, and offshore Oil&Gas industry, is shown in **Figure 2**. The IT system includes all the hardware and software dedicated to storing, retrieving, transmitting, and manipulating data or information: the corporate network and a local network are typically within the IT system. The latter is

connected to the OT system which includes all the hardware and software dedicated to detecting or causing changes in the physical process through direct monitoring and/or control of physical devices such as valves, pumps, compressors, etc. For example, the control and supervision network, which includes the IACS (Industrial Automation and Control Systems) such as the BPCS (Basic Process Control System), the SIS (Safety Instrumented System), and the SCADA (Supervisory Control And Data Acquisition) system, is part of the OT system. The physical process system is, instead, composed of the process equipment units and pipework, whose functioning is governed by the OT system.

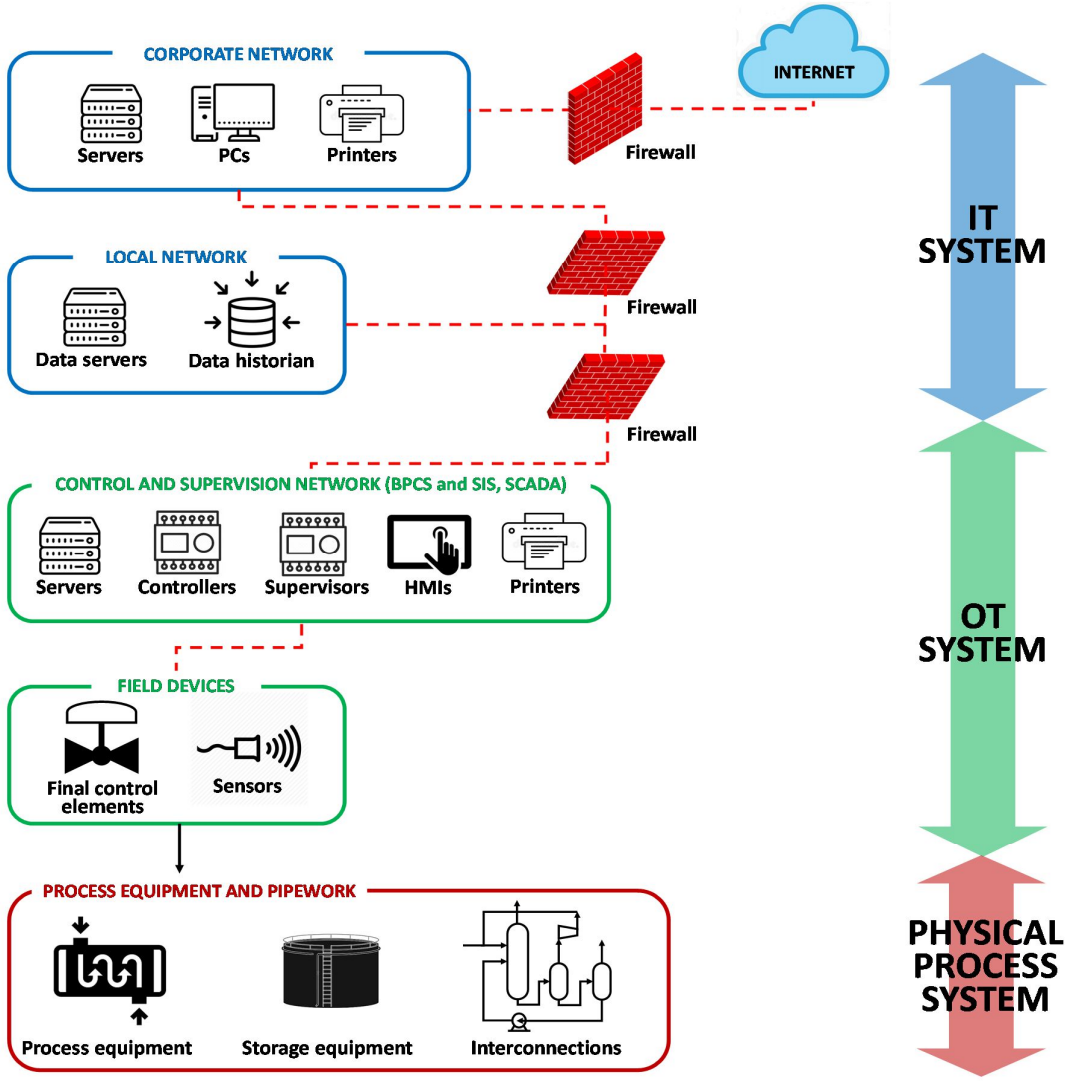

Figure 2 Typical structure of the IT-OT network system and the physical process system in the chemical, process, and Oil&Gas industry. Adapted from [13].

In this context, part 3-2 of the ISA/IEC 62443 series of standards [45], published by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), provides a semi-quantitative cybersecurity risk assessment procedure which takes into account the IT-OT part of the architecture shown in **Figure 2**. In fact, it can be applied to the IACS adopted by the chemical, process, and Oil&Gas industry. The work process can be integrated with an existing risk assessment program and represents a recognized and generally accepted good engineering practice. The benefits of using this standard include reducing the

likelihood of a successful cyber-attack, the use of a common set of requirements among stakeholders, the improvement of security throughout the lifecycle, and a reduction in overall lifecycle cost.

The flowchart of the detailed cybersecurity risk assessment procedure proposed by ISA/IEC 62443-3-2 is shown in **Figure 3**. It requires the identification of the possible threats targeting the IACS under assessment (e.g., authorized support personnel logically accessing the OT system using an infected laptop), of the vulnerabilities of the IT-OT network that can be exploited by the attackers to perform the attack (e.g., 0-day vulnerability), of the consequences of attacks in terms of worst-case impact (e.g., release of hazardous material or process shutdown), of the existing cybersecurity countermeasures (e.g., firewall between IT and OT system), and of the likelihood of having the considered threat. Overall, all this information is used to evaluate the cyber-risk associated to the cyber threat under assessment through the use of risk matrices provided by the standard itself, and, based on this, it is discussed whether additional cybersecurity countermeasures are needed or not.

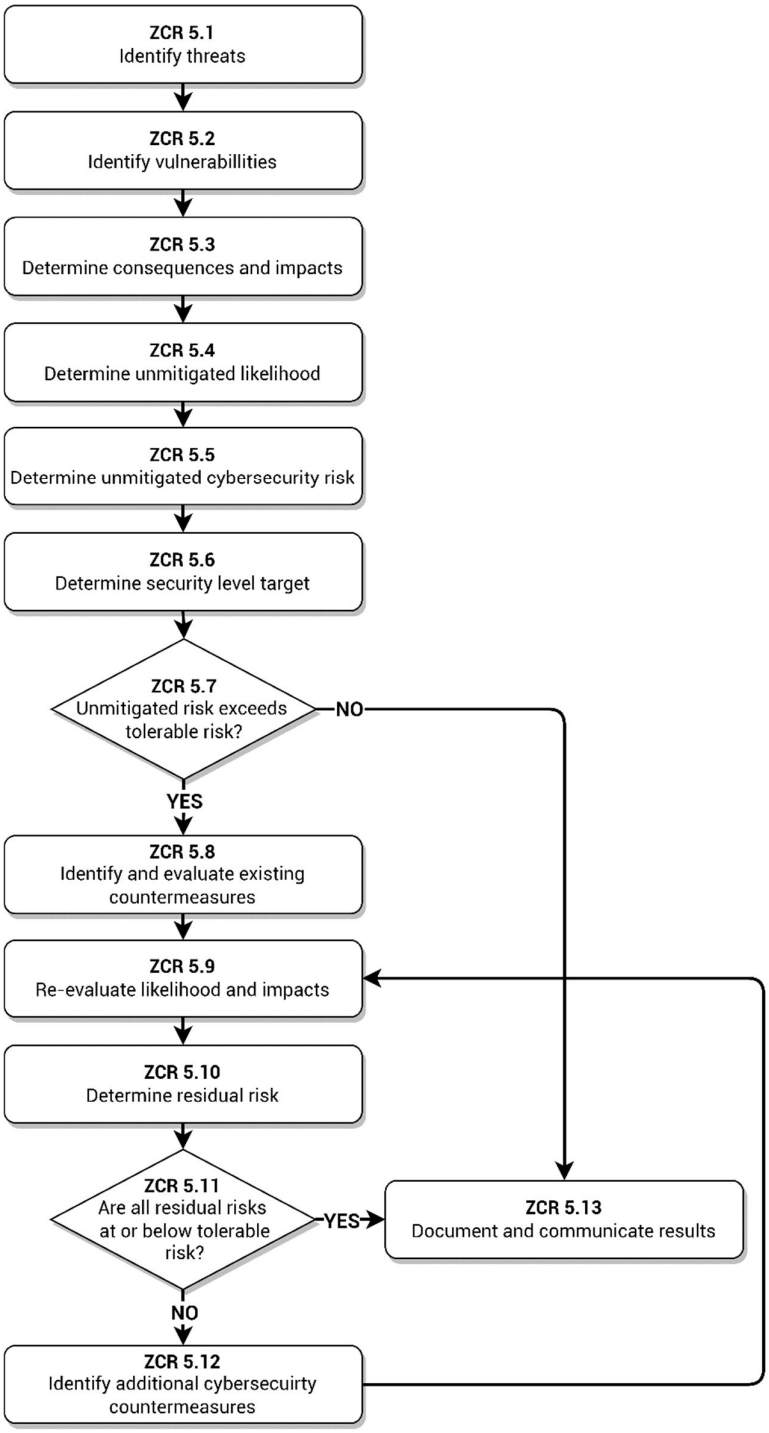

Figure 3 Detailed cybersecurity risk assessment proposed by standard ISA/IEC 62443-3-2 [45].

1.3.4. Academic proposals

Some of the available semi-quantitative and quantitative approaches aimed at supporting SVA/SRA studies that have been developed in the context of academic institutions are summarized in **Table 2**. The Bow-Tie (BT) modelling, the static and dynamic Bayesian Network (BN) modelling, the game theory, and the dynamic graph theory, are the core-models adopted by these approaches. For more detailed information on each approach, the reader is referred to the sources provided in the table for the sake of brevity.

Table 2 List of approaches from academic institutions that contribute to SVA/SRA studies.

Source	Description	Sector	Reference
Bajpai and Gupta (2005, 2007)	Semi-quantitative SRA methodology aimed at determining whether the security measures employed within a chemical facility are adequate or need enhancement.	Chemical and process industry (onshore facilities)	[46,47]
Staalduinen at al. (2017)	Quantitative SRA methodology aimed at assisting the management in the decision-making process where and when to protect critical assets of a chemical facility. It is based on the mapping of a Bow-Tie (BT) risk model into a Bayesian Network (BN).	Chemical and process industry (onshore facilities)	[48]
Talarico et al. (2015)	Quantitative multi-modal security-transportation model aimed at allocating security resources within a chemical supply chain featuring different transport modes. It is based on game theory.	Chemical supply chain (including transportation)	[49]
Argenti (2015)	Semi-quantitative procedure aimed at evaluating the attractiveness of chemical and petro-chemical facilities to deliberate malicious attacks. It includes the political and social context in the assessment, as well as public aversion issues.	Chemical and process industry (onshore facilities)	[50]
Landucci (2017)	Quantitative approach aimed at evaluating the attack likelihood and incorporating the functional analysis of the Physical Protection System (PPS). It is based on the application of a dedicated Bayesian Network (BN).	Chemical and process industry (onshore facilities)	[34]
Argenti (2018)	Quantitative approach aimed at the probabilistic assessment of the vulnerability of chemical and process facilities against deliberate physical malicious attacks. It is based on the application of a dedicated Bayesian Network (BN).	Chemical and process industry (onshore facilities)	[51]
Rezazadeh (2019)	Quantitative SRA methodology aimed at analyzing and predicting possible terrorist threats to Oil&Gas pipelines and allocating limited security resources to predict critical route segments. It is based on game theory.	Oil&Gas pipelines	[52]
Feng (2019)	Quantitative method aimed at optimizing the allocation of resources for chemical plant defense, considering the presence of multiple facilities and different types of attackers. It is based on game theory and Bayesian Network (BN).	Chemical and process industry (onshore facilities)	[53]
Misuri et al. (2018)	Quantitative approach aimed at protecting critical infrastructures via cost-effective allocation of security measures, including attack characterization through the analysis of the socio-economic and socio-political. It is based on Limited Memory Influence Diagram (LIMID).	Industrial critical infrastructures	[54]
Chen et al. (2019)	Quantitative approach aimed at integrating safety and security resources for the reduction of the risk of cascading events triggered by deliberate malicious attacks. It is based on dynamic graph modelling.	Chemical industrial parks	[55]

Khakzad (2018)	Quantitative approach aimed at the identification of the critical units which may lead to worst-case escalation scenarios (cascading effect) in case of a deliberate malicious attack. It is based on graph theory and dynamic Bayesian Network (BN).	Chemical and process industry (onshore facilities)	[56]
Zhang et al. (2019)	Quantitative SRA methodology aimed at analyzing and predicting possible terrorist threats to chemical and process facilities and allocating limited security resources to predict critical route segments. It is based on game theory.	Chemical and process industry (onshore facilities)	[57]
Abdo et al. (2017)	Semi-quantitative approach aimed at the evaluation of the cyber-risk of a chemical and process facility caused by safety-related causes and by security-related causes (cyber-attacks). It is based on the Bow-Tie modelling.	Chemical and process industry (onshore facilities) and batch processes	[58]
Hashimoto et al. (2013)	Semi-quantitative approach aimed at the evaluation of the detectability and reachability of process plant manipulations leading to a security event of concern. It supports "zone and conduit" division and allocation as required by ISA/IEC 62443 series of standards.	Industrial Automation and Control Systems (IACSs).	[59]
Cusimano and Rostick (2018)	Semi-quantitative methodology (CyberPHA) aimed at conducting a cybersecurity risk assessment of Industrial Automation and Control Systems (IACSs).	Chemical and process industry (onshore facilities)	[60]

1.3.5. Limitations of existing SVA/SRA approaches

All SVA/SRA approaches (classical, ISA/IEC 62443-3-2, academic proposals) require the identification of the chain of events from the attack scenarios to the physical damage scenarios (e.g., pool fire, fireball, etc.) that can be triggered, or in other words, the identification of reliable security scenarios that can occur in the facility under assessment [61]. This basic information is used in SVA/SRA to define the scope of the work and to support decision making aimed at improving the security with respect to attacks involving the hazardous material present on site. For example, information on physical damage scenarios is required in step 2.3 of the CCPS methodology ("Consequence analysis"), step 3.1 and 3.2 of the one proposed by API RP 780 ("Evaluate scenarios" and "Evaluate Consequences"), step 1.1 of the VAM-CF methodology ("Specify undesired events"), step 3 of the RAMCAP methodology ("Consequence analysis"), and ZCR 5.3 of the cybersecurity risk assessment proposed by ISA/IEC 62443-3-2 ("Determine consequences and impacts"). Despite the request for scenario identification, both the classical SVA/SRA methodologies, the SRA proposed by ISA/IEC 62443-3-2, and the novel academic proposals, do not provide any detailed practical procedure (e.g., with a clear methodological framework, tools, and/or mathematical formulations) to this purpose, and only occasionally checklists on sample security scenarios are included in the reference sources.

Moreover, most of these methods (especially the classical SVA/SRA methodologies, see Section 1.3.1) are semi-quantitative and non-systematic approaches that strongly rely on expert judgment, leading to security assessments that are typically not reproducible. Some are also specific to a single industrial sector and therefore do not allow generalization to any critical industrial infrastructure.

Another issue to underline is the fact that only a few methods proposed take into account the synergies among safety and security aspects (e.g., the ones developed by Abdo et al. [58] and Chen et al. [55], see **Table 2**). This is of particular relevance, since it may lead to potential conflicts or inconsistencies between the requirements defined by the safety assessment and the security assessment taken separately, and to

overlooked risks (e.g., because deemed unlikely in the safety assessment or out of the scope in the security assessment). Moreover, the absence of a "common language" between the two disciplines establishes an ineffective interdisciplinary communication and understanding which leads to a non-integrated management of safety and security risks. On the contrary, shared understandings and effective communication provide necessary common ground for jointly asking and answering questions across disciplinary boundaries.

2. Research questions, existing gap, and carried studies

This Chapter outlines the Research Questions of the present 3-year research and provides a brief description of the studies carried out, pointing out their contribution in filling the existing gaps in the current literature (see the overall framework in **Figure 4**).

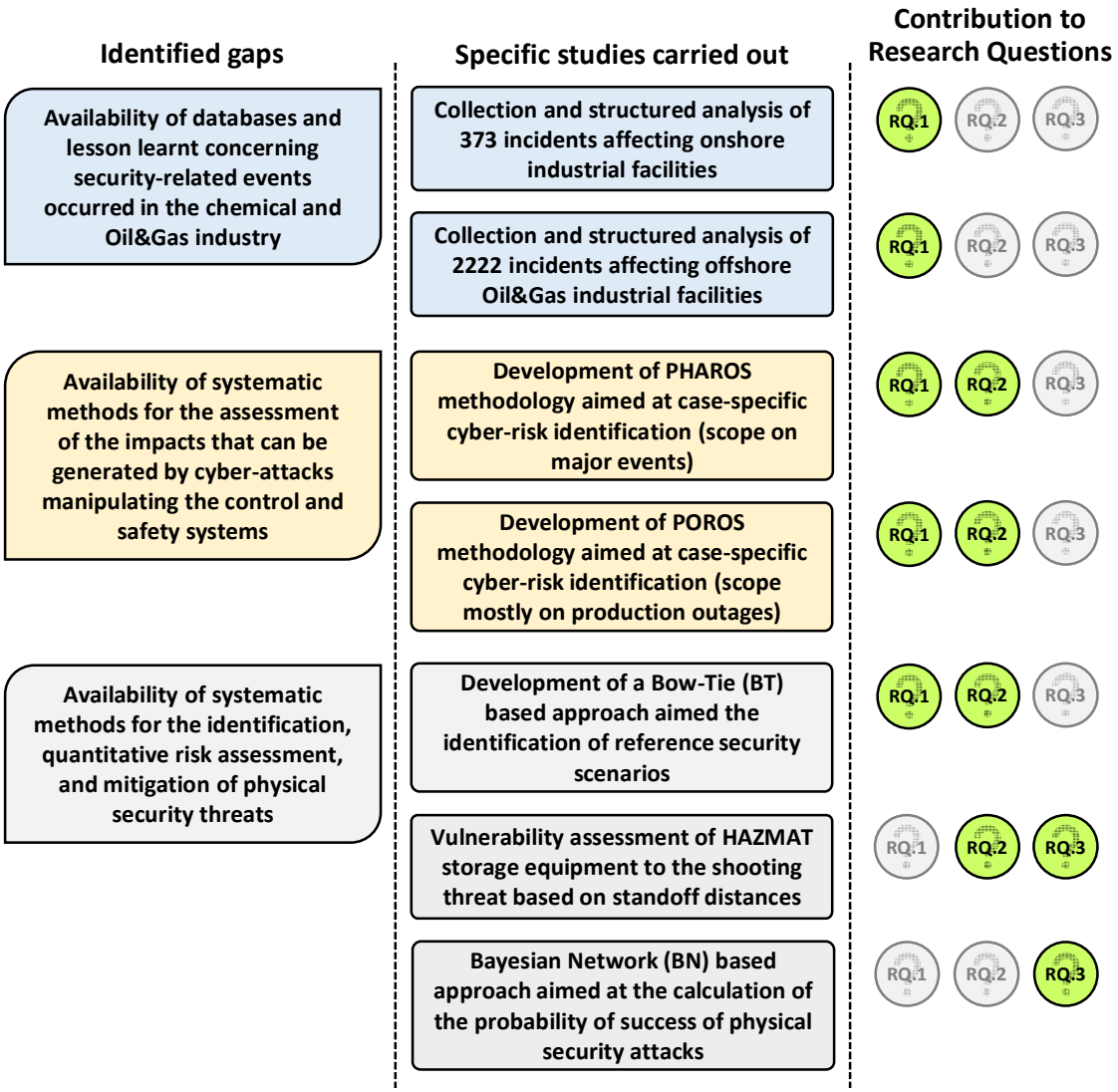

Figure 4 Schematization of the interactions between identified gaps in the literature, specific activities carried out, and research questions (RQ). RQ.1, RQ.2, RQ.3 are defined in Section 2.1

2.1. Research Questions

Given the limitations identified in the classical SVA/SRA methodologies, the cybersecurity risk assessment proposed by the standard ISA/IEC 62443-3-2, and the novel academic proposals (see Section 1.3), the present 3-year research activities are aimed at answering the following Research Questions:

1. Are there identifiable patterns in the cause-consequence relationship between the deliberate malicious attacks to process plants (chemical industry, process industry, Oil&Gas critical infrastructures, etc.), the impacts of such attacks, and the preventive or mitigative safety/security barriers in place?
2. How hazard identification methods consolidated in the safety domain can be integrated in the development of methods for security scenario identification? How can the inherent differences between cyber and physical threats can be taken into account consistently? Which role do safety-related barriers in the plant play in security attacks?
3. How quantitative risk approaches applicable to major accident hazards in the safety domain can be integrated in the development of quantitative methods for the evaluation of the security risk?

2.2. Studies carried out

Based on the Research Questions outlined above, the studies carried out during the 3-year research period addressed 3 main areas, each briefly described in the following sub-sections:

- Gathering of knowledge and lessons learnt from past security events, intended as the physical and/or remote access to the assets of a facility with the aim of giving rise to adverse consequences such as loss of life, loss of production capability, loss of equipment and property, including sensitive data [39].
- Development of methods for the identification and mitigation of cyber threats (focus on the chemical and process industry and offshore Oil&Gas industry).
- Development of methods for the identification, quantitative risk assessment, and mitigation of physical security threats (focus on the chemical and process industry and offshore Oil&Gas industry).

The domains of cybersecurity and physical security required separate research activities because of the different nature of cyber-attacks (malicious interferences aimed at causing damage through the IT-OT network system) compared to that of physical attacks (malicious interferences aimed at causing damage bypassing elements of the Physical Protection System) in terms of systems affected and attack paths carried out by the attackers. This resulted in the development of hazard identification and quantitative methods suitable for the cybersecurity domain and for the physical security domain.

2.2.1. Gathering of knowledge and lessons learnt from past security events

The studies grouped into this macro area are aimed at an in-depth characterization of the deliberate malicious attacks (both cyber and physical interferences) that affects chemical and process facilities, as well as offshore Oil&Gas installations. These activities are briefly described below, after the existing gap in the current literature is outlined.

2.2.1.1. Review of the existing gap in the current literature and practice

The current availability of databases and studies reporting security-related incidents populated with data of specific interest for the chemical and process industry, as well as for the offshore Oil&Gas industry, is still limited.

In particular, as regards the chemical and process industry and the offshore Oil&Gas operations sectors, very few studies are available. For example, Casson Moreno et al. [15] analyzed more than 300 security-related incidents that occurred in facilities belonging to the process industry and similar sectors, providing knowledge and lessons learnt on deliberate malicious attacks to these facilities.

Kashubsky [62] published a dataset containing 60 past attacks (between 1975 and 2010) against maritime and petroleum infrastructures. However, no statistical analysis of the database was performed, and the

incident records show limited information such as date, place and a brief description of the event. Similarly, Karmon [63] published a study concerning an ad-hoc analysis of the trends of terrorist attacks (88 events) against Oil&Gas resources, but also in this case a structured analysis is lacking and thus no support to SVA/SRA is provided.

Differently, a greater number of studies are present in the available literature reporting cybersecurity-related incidents due to the increasing concern worldwide towards this type of threat [14,64]. In particular, the following studies report the analysis of security events triggered by interferences to the IT-OT network system, but either lack extensive statistical analysis, or consider a limited number of events, or consider incidents beyond the scope of the present analysis.

For example, Vaidya [65] performed a survey of major cyber-attacks from 2001 to 2013 with the aim of understanding the motivations, targets, and techniques employed by the attackers. However, the analysis is not specific to industrial facilities and OT systems, and hence the specific applicability of the resulting lessons learnt warrant verification for this sector.

Ogie [66] provides a classification scheme for categorizing cybersecurity-related incidents in critical infrastructures and industrial control systems. A single data source was investigated, and events that occurred in sectors out of the scope of current analysis were included (e.g., pulp, paper and metal industries). Moreover, some incidents recorded were the result of safety-related causes (e.g., random system failures) and not really triggered by cyber-attacks.

Miller and Rowe [67] explored the issue of cyber-attacks in industrial automation control systems (IACS), but the small number of incidents considered (15) limited the ability to gain a deep insight into the trends and patterns related to the events.

Lezzi et al. [68] performed a literature review on cybersecurity in industry 4.0, proposing guidelines and solutions to manage cybersecurity issues. No statistical analysis of data is provided, and just a brief mention of the hacking techniques used by the attackers is present, without any link to the typical phases of a cyber-attack.

Nicholson et al. [69] published a study which provides an overview of threats, risks and mitigation strategies in the area of SCADA (Supervisory Control And Data Acquisition) security. The analysis covers events outside of the current scope (random malfunctions, human errors) and presents only a short statistical data analysis. The report “Cybersecurity in Industry” [70], available in the ARIA database [9], provides categories of threat and lessons learnt for IT systems and SCADA systems, but it is focused on information security rather than on operational security, and only four noteworthy cyber-attacks to process plants are described.

A brief overview of cyber-terrorism in the process industry was also performed by Willems [71], but only two cases were considered.

In the panorama outlined, while some notable data and event description can be found in several sources addressing the issue of physical and cyber-attacks to chemical and process facilities, or offshore Oil&Gas facilities, often the information provided is not categorized to support SVA/SRA studies and/or specific sectorial data can not be extracted. Moreover, since information is fragmented, no complete sectorial statistical analysis is available for the incidents occurred in the sectors of interest.

2.2.1.2. Analysis of past security events occurred in onshore and offshore industrial facilities

Given the gap outlined in Section 2.2.1.1, in the context of this study, a past incident analysis aimed at gathering knowledge and lessons learnt from past security events occurred in the chemical and process industry and in the offshore Oli&Gas industry, was carried out. Therefore, the results obtained from the analysis of past security events help answer Research Question 1 (see Section 2.1).

The past incident analysis was selected as several authors (e.g., Kjaerland [72], Churchwell et al. [73], Konstandinidou et al. [74], Lam and Tai [75], Milch and Laumann [76], Tauseef et al. [77], Jung et al. [78], Gunasekera and Alwis [79], Sales et al. [80], Fu et al. [81], Zhang et al. [82]), who made use of this tool in different industrial fields (e.g., IT networks, construction industry, chemical industry, offshore Oil&Gas industry, etc.), point out the simplicity and potentiality of this technique in providing invaluable insight, e.g., on causes and consequences of events, as well as on preventive and mitigating barriers.

In particular, the analysis started with the development of two databases:

- A structured database collecting 373 security-related events (SREs) affecting onshore industrial process facilities, including transportation via pipelines (data was gathered from scientific literature, web archives, and specific open-source databases). A specific subset of 82 SREs triggered by cyber-attacks and another subset of 104 SREs occurred in the chemical and petrochemical industry were extrapolated and more in-depth detailed and analyzed.
- A structured database collecting 2222 security-related events (SREs) affecting offshore Oil&Gas industrial facilities, including transportation at sea (data was gathered from scientific literature, web archives, and specific open-source databases). A specific subset of 99 SREs affecting the offshore fluid production sector was extrapolated and more in-depth detailed and analyzed.

The two developed databases (both the overall datasets and the specific subsets of incidents) were then analyzed using a set of complementary synergic tools in order to frame a clear picture of the security threats affecting onshore and offshore industrial facilities. In particular, the following tools were used: Exploratory Data Analysis (EDA), Correspondence Analysis (CA), Root Cause Analysis (RCA), Attacker Sequence Diagrams (ASD), and Cause-Consequence Chains (CCC).

The aspects that have been investigated (individually or in pairs to identify any correlations) are: time trend, geographical distribution, distribution among the industrial sectors considered, types of security threats, attack modes perpetrated by the attackers, motivations of the attackers, consequences/impacts of the attacks, final outcomes suffered by the affected facilities, and the role of the safety/security barriers in preventing or mitigating the attacks.

Section 3.1 reports the detailed method used for the development of the database collecting the 373 SREs occurred in onshore industrial process facilities and the results obtained from its structural analysis, while Section 3.2 reports the same framework for the database collecting the 2222 SREs occurred in offshore Oil&Gas industrial facilities.

2.2.2. Development of methods for identification and mitigation of cyber threats to process plants

The studies grouped into this macro area are aimed at supporting hazard identification in SVA/SRA studies with regards cyber threats (interferences through the IT-OT network system), and in particular the SRA approach proposed by ISA/IEC 62443 series of standards. These activities are briefly described below, after the existing gap in the current literature is outlined.

2.2.2.1. Review of the existing gap in the current literature and practice

The cybersecurity risk assessment proposed by ISA/IEC 62443-3-2 (see Section 1.3.3) supports the issues related to the OT system, but lacks in providing guidelines for the identification of the impacts resulting from its malicious manipulation (e.g., business interruption, damage of machinery, loss of containment of hazardous material, etc.). Since such information is required in the security risk assessment, simplified assumptions are frequently adopted (e.g., considering the worst-case consequences, as expected from the safety assessment). However, the impacts and consequences that can be originated by an attack to the OT

system are potentially different from those considered in the safety study: e.g., some abnormal states of the plant can not be induced through the BPCS and the SIS, and some combinations of induced deviations may have been dismissed as unlikely in the safety study. Therefore, a dedicated analysis addressing the identification of potential impacts and the role that physical and instrumented safety barriers may play during the malicious attack, is required.

A review of the scientific literature identified only few contributions devoted to security of the OT system in facilities processing and/or storing hazardous materials, as well as to the assessment of the major accidents that can be triggered by malicious manipulations of the BPCS and the SIS.

For example, Byres et al. [83] make use of Attack Trees (ATs) to assess vulnerabilities of SCADA systems. The specific ATs adopted provide a structured view of events leading to an attack (the node of the tree is the attacker goal in this case) and, ultimately, help with the identification of appropriate security countermeasures. Nevertheless, the specific scenarios resulting from the malicious manipulation of the SCADA system are not assessed in the proposed approach.

A scenario-based approach allowing decision makers to place financial and personnel resources in-place to protect nuclear power plants is described in Gertman et al. [84]. It consists of a step-by-step approach (very similar to the framework of SVA/SRA methodologies) that can be easily adapted to the chemical and process industry, but again, the specific manipulations required by the attacker are not taken into account.

Beggs and Warren [85] developed a risk framework to measure and protect SCADA systems from the threat of cyber terrorism within Australia. However, it is not tailored to the specific issue of the link between remote manipulations of the BPCS and the SIS and the scenarios affecting the operability and system integrity of a process plant.

A cybersecurity risk assessment methodology that may be exploited in the process of the design of instrumentation and control systems in nuclear power plants is suggested by Song et al. [86]. Possible attack scenarios are listed to be used in threat analysis, but no systematic tools for identification are provided.

Guan et al. [87] developed a digraph model of a SCADA system for a chemical distillation column. The model provides a formal representation of the structure and behavior of a SCADA system and may be exploited for risk impact assessment and fault diagnosis, but is limited in applicability to the specific case.

Hashimoto et al. [59] developed a systematic, qualitative and quantitative approach to evaluate the detectability and reachability of process plant manipulations, but the identification of the specific set of manipulations required to trigger specific events as outages and/or asset damages are out of the scope of the methodology.

Abdo et al. [58] proposed an approach that allows to assess the vulnerabilities and hacking techniques that can be exploited by the attackers to infect the IT-OT network system of a facility and initiating critical events, but no support is provided to the identification of the manipulations of the physical devices of the process system that can lead to such events.

Cusimano and Rostick [60] developed the CyberPHA methodology as a safety-oriented methodology to conduct a cybersecurity risk assessment for industrial control and safety systems. The proposed methodology is a consequence-driven approach based upon industry standards such as ISA/IEC 62443-3-2. However, the absence of guidelines in systematic identification of adverse scenarios and manipulations required may undermine reproducibility in application.

2.2.2.2. Development of a method for cyber-risk identification focused on major events

Given the gap outlined in Section 2.2.2.1, in the context of this study, the PHAROS (Process Hazard Analysis of Remote manipulation through the cOntrol System) methodology was developed. It is aimed at the

systematic identification of the major accidents caused by malicious manipulation of the control and safety systems (e.g., BPCS and SIS). Therefore, the results that can be obtained from the application of PHAROS help answer Research Question 1 and Research Question 2 (see Section 2.1).

In particular, PHAROS is based on a reverse-HazOp concept and its outputs include the specific set of manipulations of the BPCS and SIS through which a major event (intended as a loss of containment of hazardous material and/or a release of energy) can be initiated and the effective safety barriers (active/procedural and inherent/passive safeguards) that can prevent it. This information can be used to define the security level and protection requirements for such barriers. The application of PHAROS methodology and the potential use of the results in supporting cyber-risk identification (e.g., SVA/SRA methodologies, ISA/IEC 62443) is demonstrated on case studies.

The detailed description of PHAROS methodology and an example of its application are reported in Section 4.2.

2.2.2.3. Development of a method for cyber-risk identification focused on operability issues

Given the gap outlined in Section 2.2.2.1, in the context of this study, the POROS (Process Operability analysis of Remote manipulations through the cOntrol System) methodology was developed. It is aimed at the systematic identification of the security events that may lead to the plant arrest and consequent interruption of productivity for a certain period of time caused by a malicious manipulation of the control and safety systems (e.g., BPCS and SIS). Therefore, the results that can be obtained from the application of POROS help answer Research Question 1 and Research Question 2 (see Section 2.1).

In particular, POROS is based on a reverse-HazOp concept and its outputs include the specific set of manipulations of the BPCS and SIS through which a security event affecting the operability and/or system integrity of a facility can be initiated and the effective safety barriers (active/procedural and inherent/passive safeguards) that can prevent it. This information can be used to define the security level and protection requirements for such barriers. The application of POROS methodology and the potential use of the results in supporting cyber-risk identification (e.g., SVA/SRA methodologies, ISA/IEC 62443) is demonstrated on case studies.

The detailed description of POROS methodology and an example of its application are reported in Section 4.3.

2.2.3. Development of methods for identification, quantitative risk assessment, and mitigation of physical security threats to process plants

The studies grouped into this macro area are aimed at supporting hazard identification and quantitative assessment in SVA/SRA studies with regards physical security threats (malicious interferences aimed at causing damage bypassing Physical Protection System – PPS – elements). These activities are briefly described below, after the existing gap in the current literature is outlined.

2.2.3.1. Review of the existing gap in the current literature and practice

All SVA/SRA studies require the identification of the physical damage scenarios that can be originated through deliberate malicious attacks (see Section 1.3) [61]. This basic information is used in SVA/SRA to define the scope of the work, to evaluate the security risk of a facility, and to support decision making aimed at improving the security with respect to attacks involving the hazardous material present on site (processed or stored). However, Landucci and Reniers [1] identify an evident lack of specific procedures and guidelines for the identification of the security scenarios for process plants in the current practice. In fact, despite the request for scenario identification, these methods do not provide any detailed practical procedure, and only occasionally checklists on sample security scenarios (cause-consequence chain from attack scenarios to

physical damage scenarios) are included in the reference sources. Moreover, most of these methods are semi-quantitative and non-systematic approaches that strongly rely on expert judgment, leading to security assessments that are typically not reproducible. Some are also specific to a single industrial sector and therefore do not allow generalization to any critical industrial infrastructure.

Scenario identification, sometimes exploiting the Bow-Tie concept, is a step required also by the novel and more complex approaches that were recently proposed by academic institutions to address security issues. While these methods differ in both core-mechanism and objective, they all need the identification of the chain of events from causes (attacks) to final outcomes (damage to people, reputation, environment, and property), or at least of one element of that chain (e.g., the physical damage scenarios) as starting point of the analysis.

Several new methods are based on both static and dynamic Bayesian Networks (BN), which in recent years have been widely adopted in engineering applications due to their ability to predict the probability of unknown variables or to update the probability of known variables [88]. For example, Landucci et al. [34] developed a probabilistic risk analysis approach supported by a BN-based model in order to assess the attack likelihood and to incorporate the functional analysis of the Physical Protection System. This requires the definition of the set of attack modes as starting point for the design of the BN. However, the method is intended for application in the chemical and process industry only, and it is path-independent, i.e., it is based on the simplifying assumption that the same set of elements of the PPS is present along each potential attack path. Similarly, attack characterization is an input information for the application of the BN-based model proposed by Argenti at al. [51] aimed at the assessment of the external threats targeting chemical facilities. The method takes into account only one preventive security intervention strategy (i.e., the intervention of the security personnel), and it is specifically dedicated to chemical and process facilities; moreover, the method does not provide guidelines for the construction of the case-specific BN. Analogously to what was done by Khakzad et al. [89] in the safety framework, a Bow-Tie model of the security chains of events mapped in a Bayesian Network is utilized by van Staalduinen et al. [48] allowing dynamic updating of security risk in changing plant conditions: therefore, information on both attack modes and physical damage scenarios that can be generated are required in the early steps of the analysis. Furthermore, the likelihood of having an attempt is calculated with a non-probabilistic approach and eventually combined with the other required probabilities into an overall security risk value. The scope of application is still the chemical and process industry, and the method does not include a specific approach for BN construction.

As events of concern in the security framework frequently have the property of a Markov chain (i.e., stochastic processes occurring at any time and place due to different causes [90]), the Markov modelling is typically used for solving BNs (Markov Chain Monte Carlo framework) [91–94], or it is coupled to them (e.g., the coupled Continuous-Time Markov Chain – Bayesian Network Model developed by Badr et al. [95]). Again, the proper definition of BN and related Markov Chains requires the knowledge of the cause-consequence chain from the specific attack mode to the physical damage scenarios which can potentially be triggered.

Approaches based on game theory are also available in the open literature to address security issues. For example, Feng et al. [53] presented a game-theoretic method for optimizing the allocation of defensive resources to protect chemical and process facilities against multiple types of attackers. Similarly, Zhang et al. [57] and Rezazadeh et al. [52] developed respectively the CPP (Chemical Plant Protection) game and the PSG (Pipeline Security Game) with the intent of modelling the interactions between defenders and adaptive attackers and improving the protection of chemical plants and pipelines respectively. Game theory was also adopted in the field of cybersecurity of chemical and process facilities by Hausken [96], addressing the effects of information sharing between firms and between attackers in order to identify the best defense strategies. Identification of the attack patterns and a proper characterization of the potential outcomes are needed also in these cases.

The identification of primary security scenarios is also required by the consequence-based method including a Dynamic Vulnerability Assessment Graph (DVAG) model proposed by Chen et al. [55] to integrate safety and security resources for security risk reduction of chemical industrial parks.

Finally, it is worth mentioning the alternative semi-quantitative SRA approach developed by Bajpai and Gupta [46,47] which, following the typical steps of a standard SVA/SRA study, requires inputs like knowledge of credible threats, plant vulnerabilities, and expected consequences.

In this panorama, the techniques commonly used in process hazard analysis/identification in the field of process safety, such as HazOp analysis [97], What if Analysis [19], Failure Modes and Effects Analysis (FMEA) [98], the Methodology for the Identification of Major Accident Hazard (MIMAH) [99], are not suitable to take into account security aspects. In fact, given the different theoretical foundation of security issues with respect to safety issues [36], these techniques developed for safety aspects do not provide for systematic approaches and tools aimed at accounting for the mechanisms of deliberate malicious attacks.

Specific hazard identification techniques were recently proposed for the specific field of cybersecurity for plants handling hazardous materials. These include the cyber Bow-Tie approach proposed by Abdo et al. [58], the CyberPHA method developed by Cusimano and Rostick [60], the two reverse-HazOp methods for attacks to BPCS and SIS described in Chapter 4 and developed by Iaiani et al. [100,101], and the toolkit for risk identification suggested by Carreras and Guzman [102]. However, the different nature of cyber-attacks (malicious interferences through the network system) compared to that of physical attacks (malicious interferences though the physical protection system) in terms of systems affected and mechanism of action does not allow the straightforward extension of these methods from the cybersecurity to the physical security domain.

In addition to the gap highlighted above regarding hazard identification, another important issue to underline is the fact that, while the vulnerability of industrial process and storage installations to attacks with homemade explosives and with incendiary means has been assessed in the available literature by Landucci et al. [103] and by Dusso et al. [104] respectively, who provided standoff distances (minimum distance between the asset of interest and the location where an attack takes place without causing any damage) for such types of attacks, no works aimed at providing standoff distances for shooting attacks to critical assets of the chemical and process industry and similar sectors were found in the literature [51]. In fact, the available studies dedicated to equipment damage from fragments originated by the rupture of industrial installations in domino events consider projectiles with shape, mass and velocity very different from the ones used in shooting attacks and thus can not be extended to the case [105–108]. Actually, most of available perforation models focus on targets with design features and materials quite different from the atmospheric and pressurized storage tanks used in the chemical and process industry (e.g., armors, bulletproof glasses, bulletproof vests, buildings). Thus, only few studies provide a suitable assessment and a critical comparison of the available models for the vulnerability assessment of atmospheric and pressurized tanks to perforation.

For example, Anderson et al. [109] provides a review of nine analytical penetration models; however, they were validated for armour steels or aluminium targets and no focus on the steels typically used for industrial storage tanks is present. Two perforation models addressing the impact of rigid sharp-nosed projectiles on ductile metallic targets (aluminium alloy) were compared by Chen et al. [110]. Similarly, a small set of perforation models (three) was considered by Kohout et al. [111] to determine the local impact of projectiles (both flying fragments generated from the catastrophic failure of plant equipment and bullets shot by firearms) on LNG storage tanks. Stewart and Netherton [112] carried out a perforation fragility analysis of mild steels and High Hardness Armour (HHA) plates using five models only and a single projectile, the 7.62mm M61 AP (armour piercing) ammunition. A more comprehensive survey of perforation models that can be used in case of “ideal impact” (i.e., normal impact of a purely translating projectile against a stationary object [113]) is proposed in Backman and Goldsmith [114]. However, no cross-validation with experimental data

and no comparison of the model performances were carried out. An extensive summary of analytical, numerical, and experimental investigations of targets subjected to non-standard collisions (non-ideal projectile impact such as oblique impact, yaw impact, rotating penetrators, etc.) was published by Goldsmith [113]: also in this case, the extension of the study and the application of the models to the case of the atmospheric and pressurized equipment used in the chemical and process industry is not straightforward. Generic values for the thickness of steel plates able to resist to projectile impacts, is reported by the US Department of Defense [115], but limited information is disclosed on the models and experimental data used for the analysis. Schonberg and Ryan [116] tested the ability of nine existing empirical and semi-analytical penetration models with experimental data of ballistic tests to predict the plugging-mode ballistic limit velocity of monolithic plates of metallic armor. These models were then improved by the authors in a later study [117], introducing empirical adjustments and reformulations of the target strength dependency. However, even if both the analyses are based on an extended dataset of experimental data (650), they are limited only to blunt nose (or flat nose) fragments simulating projectiles, and to materials not used in the construction of industrial storage tanks such as titanium alloy, aluminum alloy, and steel alloy.

The few available studies specifically dedicated to the perforation of process and storage equipment from shooting attacks focus on projectiles with high initial velocities (≥ 960 m/s) [118,119], but do not address perforation of projectiles suitable for small/light weapons such as handguns and rifles, which are characterized by lower values of initial velocities.

2.2.3.2. Development of a method for the identification of reference security scenarios

Given the gap outlined in Section 2.2.3.1, in the context of this study, a novel set of reference security scenarios (cause-consequence chain from attack scenarios to physical damage scenarios) and of a step-by-step procedure based on Bow-Tie formalism for the identification of reference security scenarios for an installation or substance other than those for which reference scenarios are provided, were defined. Therefore, the results obtained from this study help answer Research Question 1 and Research Question 2 (see Section 2.1).

Generally speaking, the definition of sets of reference scenarios for the chemical and process industry is deemed to be a suitable approach to bridge the existing gap in hazard identification phase in the context of SVA/SRA when physical threats are assessed. Reference scenarios are generic sets of cause-consequence chains that link the initiating causes (attack scenarios) of a security event (intended as a production shutdown or a loss of containment of hazardous material) to its potential consequences (physical damage scenarios such as pool fire, fireball, etc.) that can be used by practitioners as a reference starting point to undertake a case-specific hazard identification.

The use of reference scenarios to support hazard identification is well consolidated in the safety management practice, where it provides the baseline for the authorities and practitioners to analyze more consistently the specific cases. Examples include reference major accident scenarios that can be obtained by the application of MIMAH (Methodology for the Identification of Major Accident Hazards) and MIRAS (Methodology for the Identification of Reference Accident Scenarios) methodologies developed in the framework of the EU FP6 ARAMIS project [99], those reported in the "Handbook of Scenarios for Assessing Major Chemical Accident Risks" [120] aimed to assist the EU Member States in land-use planning (LUP), and those proposed for LUP decision making purposes [121].

The extension of the approach based on reference scenarios to the domain of physical security of chemical and process plants is considered to be possible, given the existence of similarities among plant layout elements (fences, access control points, building accesses, internal road network [7]) and model equipment types across the chemical and process sector that allows generalization. Moreover, the use of a similar approach in the field of physical security and safety of chemical and process plants may lead to several

benefits. It promotes diffusion of a "common language" between the two disciplines which allows to establish an effective interdisciplinary communication and understanding, yielding a more integrated management of safety and security risks [122]: shared understandings and effective communication provide necessary common ground for jointly asking and answering questions across disciplinary boundaries [123]. Moreover, an integrated management of safety and security clearly leads to the definition of a single set of safety/security requirements, and therefore it may also contribute to the increase of the operational resilience of both cyber and physical systems [124–128]. This is of particular relevance since potential conflicts or inconsistencies between requirements defined in isolation by the safety assessment and the security assessment are avoided, and since it may allow the recognition of risks which could otherwise be overlooked (e.g., because deemed unlikely in the safety assessment or out of the scope in the security assessment) [129–132].

Overall, the reference security scenarios have been identified for the more widely used storage units in chemical and process plants and with reference to a general classification of possible attack modes. The results are reported using the Bow-Tie (BT) diagrams, which links the attack modes (Attack Tree, AT) with the release scenarios that can be triggered (Security Event, SE), and the physical damage scenarios that can occur (Event Tree, ET). The concept of standoff distance, intended as "the minimum distance between the asset of interest and the location where an attack takes place without causing any damage", is adopted in the AT part of the BT to deny the success of a particular attack mode and prevent/mitigate the resulting SE. Standoff distances were calculated for each defined reference attack mode using existing models for consequence assessment (e.g., models for pool fires, explosions, projectile impacts). Validation of the Bow-Tie diagrams obtained was provided by the information available in the records of the incidents collected in the context of the past incident analysis discussed above. The potential use of the developed reference Bow-Tie diagrams within the proposed step-by-step procedure for reference scenario identification has been demonstrated on case studies.

The detailed description of this study is reported in Section 5.1.

2.2.3.3. Assessment and mitigation of the shooting threat against plant equipment units

Given the gap outlined in Section 2.2.3.1, in the context of this study, an extended review and validation of projectile perforation models using experimental data from perforation tests, was carried out, and the most reliable ones (selected according to appropriate statistical performance indicators) were used to evaluate generic standoff distances for atmospheric and pressurized storage equipment considering a set of standardized handgun and rifle projectiles (according to EN 1522 and EN 1063). Such standoff distances can be adopted to investigate the conditions for a successful shooting attack and to support the design of passive protection barriers within the Physical Protection System of a facility, and thus were used within the reference Bow-Tie diagrams developed in the context of study briefly described in the previous section and detailed in Section 5.1. Overall, the results obtained from this study help answer Research Question 1 and Research Question 2 (see Section 2.1).

The detailed description of this study is reported in Section 5.2.

2.2.3.4. Development of a method for the calculation of the probability of success of physical attacks

Given the gap outlined in Section 2.2.3.1, in the context of this study, a systematic quantitative procedure based on the Bayesian Network (BN) modelling for the calculation of the probability of success of physical deliberate malicious attacks, able to take into account both preventive and mitigative security intervention strategies, was developed. Therefore, the results obtained from this study help answer Research Question 3 (see Section 2.1), supporting the quantitative evaluation of the security risk of an industrial facility.

The Bayesian Network modelling was chosen as many authors agree that it is a flexible tool for knowledge elicitation and reasoning under uncertainty [54,133], allowing a convenient procedure for a multitude of problems in which one wants to come to conclusions that are not warranted logically but, rather, probabilistically [88,134]. In fact, the capability for bidirectional interferences, combined with a rigorous probabilistic foundation, makes the BN modeling a suitable technique for accident analysis and more importantly, for the design and evaluation of protective measures (i.e., the security barriers in the security domain), replacing earlier ad hoc rule-based schemes [135]. As a matter of fact, BNs are increasingly used nowadays to construct system reliability models, risk management, and safety/security analysis based on probabilistic and uncertain knowledge [88].

The proposed procedure is applied in the context of the offshore Oil&Gas industry; however, given its generic nature, the approach can be customized and applied to a wider range of critical infrastructures such as the security of airports, or that of chemical and process plants. The application of the proposed procedure and the potential use of the results in supporting quantitative SVA/SRA is demonstrated on case studies.

The detailed description of this study is reported in Section 5.3.

3. Gathering of knowledge and lessons learnt from past security events

The studies described in this Chapter are aimed at the in-depth characterization of the deliberate malicious attacks (both cyber and physical interferences) that affects chemical and process facilities, as well as offshore Oil&Gas installations.

3.1. Analysis of security events occurred in the process industry and similar sectors

This Section presents a study aimed at gathering knowledge and lessons learnt on security threats affecting the chemical and process industry and similar sectors. Therefore, the results obtained from this study help answer Research Question 1 (see Section 2.1 and **Figure 4**). In particular, the study consists in the development and the related structured analysis of a database collecting 373 security-related events (SREs) affecting onshore industrial process facilities, including transportation via pipelines. A specific subset of 82 SREs triggered by cyber-attacks and another subset of 104 SREs occurred in the chemical and petrochemical industry were extrapolated and more in-depth detailed and analyzed.

3.1.1. Method

The method applied for the analysis of past security-related events (SREs) consisted of three main steps (see **Figure 5**):

1. retrieval of past SREs from available data sources according to specific inclusion criteria which define the scope of the analysis;
2. population of a structured database (with free fields and itemized fields) with all the SREs retrieved;
3. analysis of the total number of SREs and of specific subsets of SREs using dataset analysis tools in order to frame a clear picture of the security threats affecting the process industry and similar sectors and to provide information supporting SVA/SRA studies.

Each step is detailed in the following sub-paragraphs.

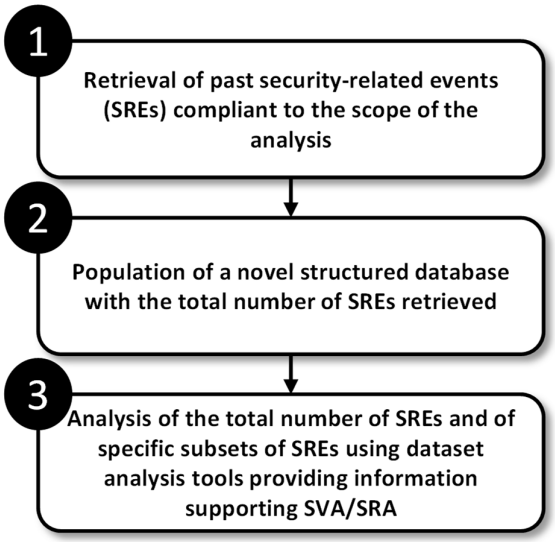

Figure 5 Flowchart of the method applied for the analysis of past security-related events (SREs).

3.1.1.1. Retrieval of past security-related events

In order to give a more complete vision of the issue, the scope of the data collection from available sources was expanded beyond the limit of Seveso plants in Europe (chemical and petrochemical facilities), including the broader sectors of energy production, hazardous material transportation (via rail, road, pipeline), and water/wastewater treatment. These sectors were selected as they present at least some features in common with HAZMAT sites (e.g., similarity in process equipment and facility structures, similarities in materials handled).

The database was obtained revising and extending the database developed in a previous study by Casson Moreno et al. [15]. Particular attention in the extension of the existing database was paid in collecting security-related events that occurred between 2017 and 2019, since the previous version of the database was last updated in 2017. Specific attention was also devoted to collect security events that occurred in nuclear power plants since they were not previously included in the database, as well as cybersecurity-related events. The database in intended to be updated every 5 years.

Data for the update were gathered from different sources: scientific literature, web archives, and specific open-source databases reporting data on industrial accidents/incidents and near misses (as defined by Rathnayaka and coworkers [136]) such as the ARIA database [9], Dechema ProcessNet [137], E.U. Concawe [138], E.U. EGIG [139], eMARS [8], Global Terrorism Database (GTD) [140], Infosis ZEMA [141], Repository of Industrial Security Incidents (RISI) [142], U.S. DoT PHMSA [143], CSIS (Center for Strategic and International Studies) proprietary database [144].

Two criteria were used to include security-related events in the database:

i. the event should originate as a result of a malicious act aimed at interfering with normal operations (not necessarily with the intentionality of triggering a major accident such as a fire or explosion);
ii. the event involves an industrial facility belonging to one of the following sectors: Chemical&Petroleum, energy production, pipelines, transportation, bioprocesses and water/wastewater treatment.

The sets of keywords used for querying the data sources were different for the investigation of the open-source databases (and differentiated by groups of databases) with respect to the investigation of the open literature. In addition, the mining for physical security- versus cybersecurity-related events required different

sets of keywords. **Figure 6-a** shows the complete list of keywords that were used for querying the data sources, divided into 7 groups.

Each group contains synonyms or equivalent terms:

- group A: type of physical-attacker;
- group B: type cyber-attacker;
- group C: generic terms referring to security-related events;
- group D: generic terms referring to cybersecurity-related events;
- group E: generic terms referring to physical industrial infrastructures;
- group F: generic terms referring to hardware and software;
- group G: generic terms referring to industrial sectors.

Starting from these groups of keywords, the total sets of keywords for querying the open-literature to search both for cybersecurity-related events and for physical security-related events, as well as for querying all the databases forehead mentioned (with the exception of GTD and RISI), can be generated by taking one keyword per group and solving the trees reported in **Figure 6-b** by using the rules of Boolean algebra. Since GTD, RISI, and the CSIS proprietary database collect security-related events only, records in these two databases were simply found by selecting the industrial sectors of interest.

When looking for security-related events in the open literature, the keywords were translated into several European languages (i.e., English, Italian, French, German, and Spanish), while each database was investigated also in its native language. Only English terms are reported in **Figure 6-a**. Due to the high number of open-sources exploited, particular attention was posed in avoiding double counting of events. Specific checks were carried out considering the date, country, and type of facility involved in the event.

Some modifications concerning the categories of classification of the incidents in the database were applied to the current version with respect to the database developed by Casson Moreno et al. [15]. In particular:

- Events that occurred in “Manufacturing” sector were removed from the database because of the different features of this sector with respect to those characterizing the process industry;
- Nuclear power plants were added to the “Energy Production” sector because of the presence of similar process equipment to those typically present in process plants;
- “Other” was added among the scenarios, referring to a scenario that does not involve process equipment, but that still leads to impacts in the affected facility;
- “Insider Threat” replaced “Disgruntled Employee” in order to generalize the category of insiders;
- “Cyber-attack” was added among the attack modes;
- “Property damage / economic loss” and “Environmental damage” were added among the final outcomes.

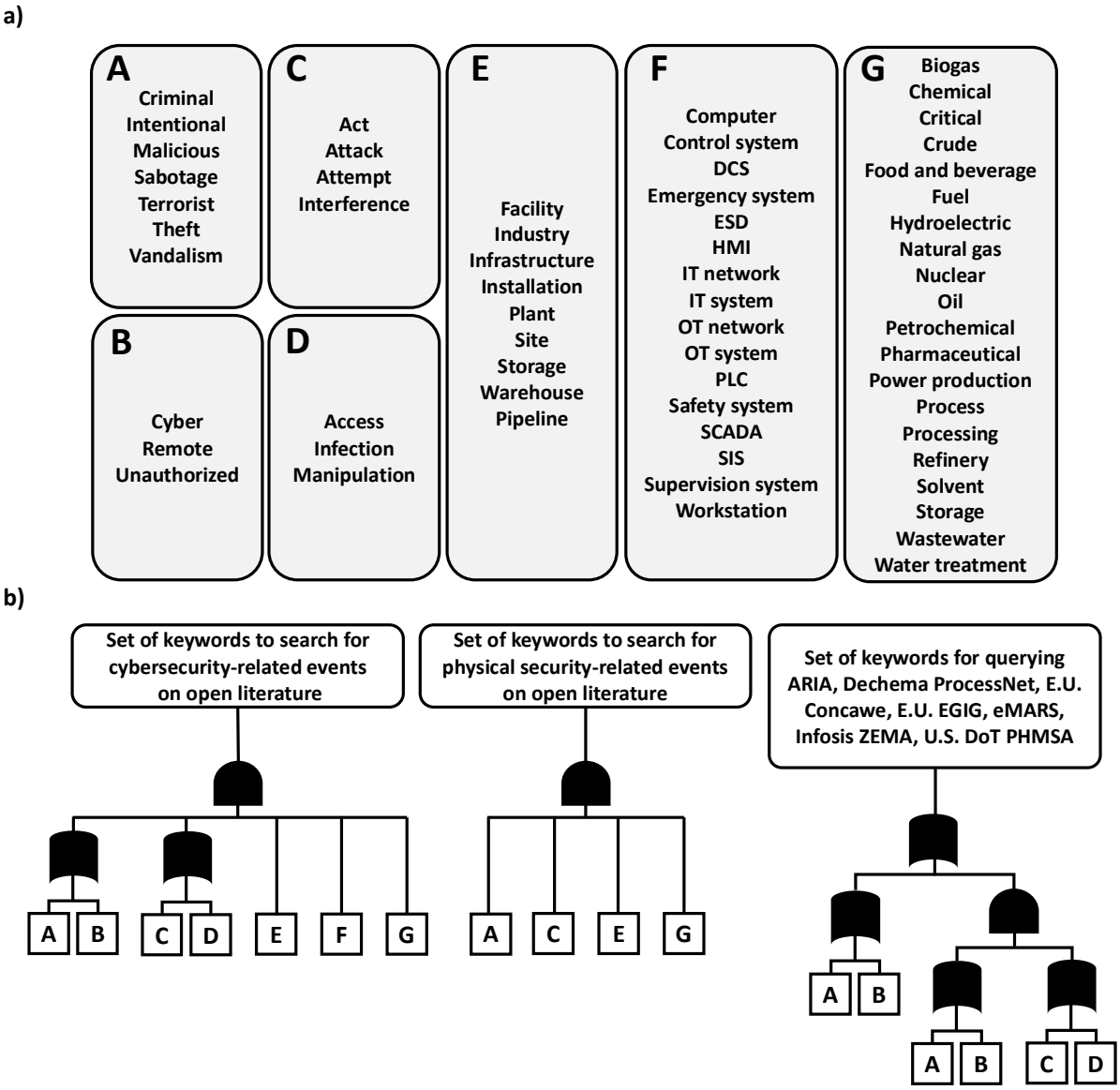

Figure 6 a) Complete list of keywords (in English) used for querying the data sources, divided into 7 groups labelled from A to G; b) Method based on Boolean algebra used to define the sets of keywords employed to query each different category of data source. Adapted from [2].

3.1.1.2. Structured database of past security-related events

A dataset of 373 security-related events (SREs) was populated (see the structure in **Figure 7**): the total entries with related relevant information can be found in the Supplementary Material of Iaiani et al. [2].

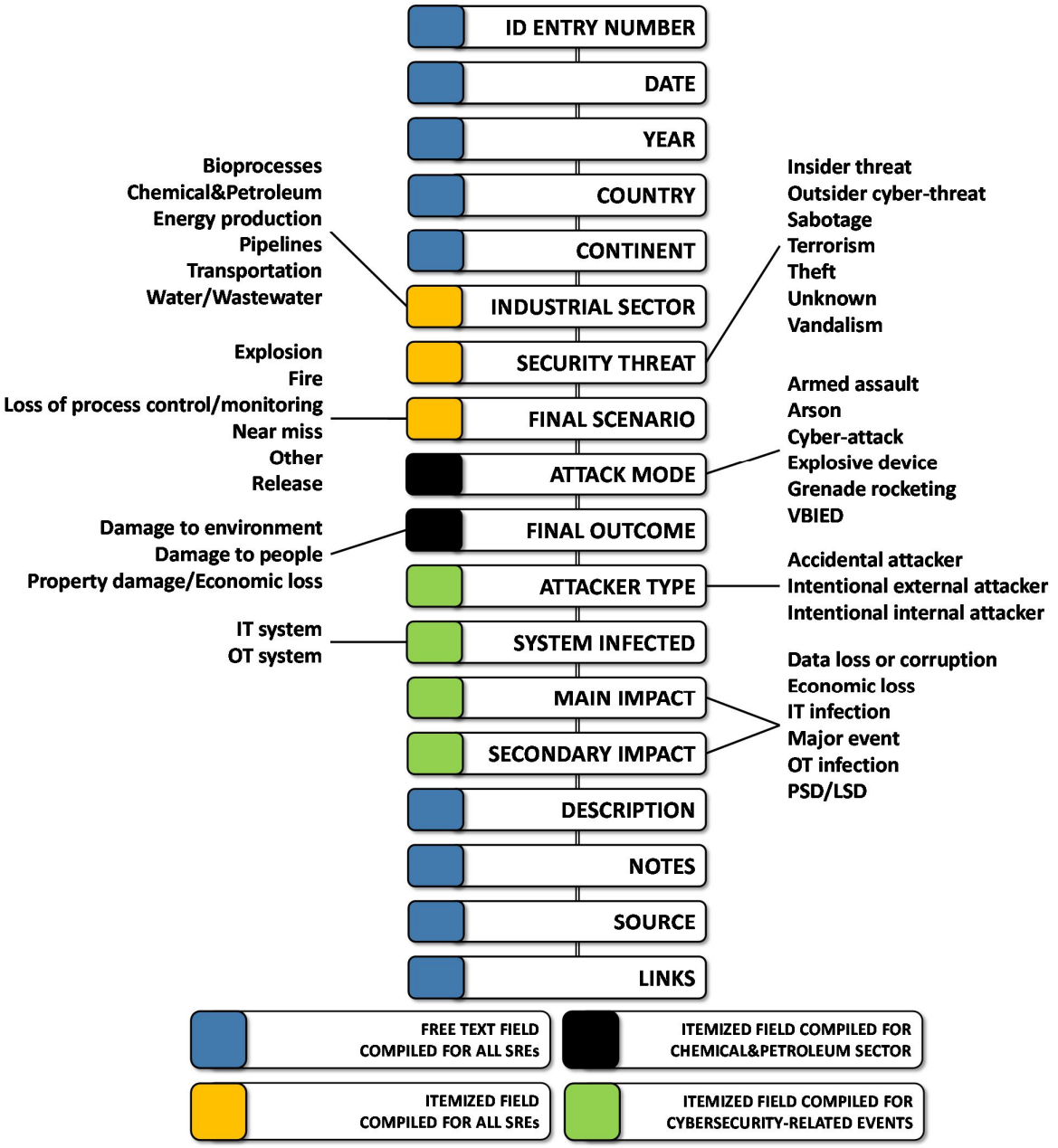

Figure 7 Structure of the database collecting the retrieved SREs occurred in the process industry and similar sectors.

Each entry in the database consists in the compilation of free text fields and itemized fields. Free text fields allow retaining general details concerning the record (ID entry number, date, year, country, continent, description, notes, source, links), while itemized fields help describe unambiguously a certain characteristic of the event. **Table 3** reports the definitions of the itemized fields considered for the total number of the SREs, i.e., "Industrial Sector", "Security Threat" and "Final Scenario". The availability of more detailed information on the events that occurred in the Chemical&Petroleum sector allowed to consider two additional itemized fields for these events, i.e., "Attack Mode" and "Final Outcome", both described in **Table 4**. Moreover, given the different nature of the cyber-attacks with respect to the physical attack modes, four further itemized fields were considered for the cybersecurity-related events (all defined in **Table 5**): "Attacker Type", "System Infected", "Main Impact", and "Secondary Impact".

Table 3 Definitions of the itemized fields "Industrial Sector", "Security Threat", and "Final Scenario" used in the collection of all the SREs. Adapted from [2].

Class	Definition
	Industrial Sector
Bioprocesses	Treatment of organic waste and waste fermentation juices. Food industry.
Chemical&Petroleum	Chemical production and storage installations, including pesticides production, pharmaceutical industry, production of basic chemicals. Petrochemical production and storage installations, including refineries.
Energy production	Electric power production plants using hydrocarbons (petroleum and natural gas-based fuels), hydroelectric and nuclear plants.
Pipelines	Oil and Gas transportation via pipelines.
Transportation	Transportation of hazardous materials via road, rail, water.
Water / Wastewater treatment	Water and wastewater treatment for industrial and domestic purposes, including water supply systems (excluding bioprocesses-related waters and slurries).
	Security Threat
Insider threat (physical security and cybersecurity)	The attacker is an insider, i.e., an individual who normally has authorized access to the assets of the company (e.g., employee, contractor, business partner, vendor, etc.). The motivation is related to working dissatisfaction or possibility of gaining personal advantage (e.g., stealing items or materials). Insider threat refers both to physical security and cybersecurity.
Outsider cyber-threat (cybersecurity)	Events collected in this category are characterized by an attack, via cyberspace, targeting the IT-OT system of the target facility with the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. Usually, the malwares used by the attackers were not tailored for industrial control systems, but they breached the company network protection compromising operations.
Sabotage (physical security)	Events collected in this category are characterized by an attack mode aimed to disrupt normal operations, but not defined in their threatening agent, as well as in their driving motivations.
Terrorism (physical security)	Terrorist organizations/groups, highly capable, well organized and equipped. Events included in this category have a terrorist matrix, often focused on targeting a facility with the aim of causing a high-impact event, not only in terms of casualties, but also on media.
Theft (physical security)	Criminal groups or individuals attacking facilities with the intent of stealing material. It includes both events of attempted theft that caused an accident and cases of intrusion without reaching the target.
Unknown (physical security and cybersecurity)	An interference in normal production activities has been achieved via certainly intentional acts, but no more details were given concerning attackers or motivations of the act. This category refers both to physical security and cybersecurity.
Vandalism (physical security)	Poorly equipped groups or individuals with low level of preparedness and usually no tactic in attack execution.
	Final Scenario
Explosion	Event consisting in a physical and/or chemical explosion.
Fire	Event consisting in a pool fire, jet fire, fireball, flash fire, or flame.
Loss of process control/monitoring	Event consisting in the physical or cyber interference with the OT system (software and hardware), without the occurrence of a release of hazardous substances, a fire, or an explosion.
Near miss	An event that does not result in an actual final scenario such those described above, but the attack perpetrated by the attackers has the potential to do so. This can be due to the intervention of the security forces to stop the attack and/or the effectiveness of the physical protection system in place.

Other	Event that does not result in a release of substances, a fire, an explosion, or a loss of process control/monitoring (e.g., infection of the IT system of a process facility, use of explosives without involving chemical equipment).
Release	Event consisting in the discharge of a chemical from its containment, i.e., the process and storage equipment in which it is kept, without any further consequence such as an explosion or a fire.

Table 4 Definitions of the itemized fields "Attack Mode" and "Final Outcome" used in the collection of the SREs occurred in the Chemical&Petroleum sector. Adapted from [2].

Class	Definition
	Attack Mode
Armed assault	An armed attack that involves people with guns or other carrying weapons.
Arson	An attack that deliberately consists in setting a fire (e.g., using incendiary weapons or improvised sources of ignition).
Cyber-attack	An attack via the cyberspace to the IT-OT network system of a facility that can be accidental (i.e., it is not directed towards a specific target, but that infects any vulnerable host) or intentional (i.e., it is carried out against a specific target and designed to exploit specific weaknesses of the target system).
Explosive device	An attack that involves explosives, i.e., devices that relies on the exothermic reaction of an explosive material to provide a violent release of energy (e.g., dynamite). The explosive device can be placed directly on the target asset or launched from a point far from it.
Grenade rocketing	An attack that consists in the shooting of missiles launched at distance by a rocket launcher or by remotely controlled drones.
VBIED	Vehicle Borne Improvised Explosive Device. An attack that consists in an improvised explosive device placed and detonated inside a car or other vehicle.
	Final Outcome
Damage to environment	Damages to the ecosystems due to air and/or water pollution, or land contamination.
Damage to people	Injury or fatality.
Property damage / economic loss	Physical and economic damages due to loss of an asset for the affected facility, whether it is a loss of production capability, loss of equipment and property, including loss of sensitive data. Loss of life is not included.

Table 5 Definitions of the itemized fields "Attacker Type", "System Infected", "Main Impact", and "Secondary Impact" used in the collection of the cybersecurity-related events (CSREs). Adapted from [13].

	Attacker Type
Accidental attacker	A cyber-attack that is not directed towards a specific target, but that infects any vulnerable host. The attacker is generally unknown.
Intentional external attacker	A cyber-attack that is carried out against a specific target and designed to exploit specific weaknesses of the target system. The attacker is not an insider, i.e. he has not authorized access to the assets of the company. The attacker generally claims the attack.
Intentional internal attacker	A cyber-attack that is carried out against a specific target and designed to exploit specific weaknesses of the target system. The attacker is an insider, i.e. an individual who normally has authorized access to the assets of the company (e.g. employee, contractor, business partner, vendor, etc.). The attacker is generally identified by an investigation.
	System Infected
IT system	The hardware and software dedicated to store, retrieve, transmit, and manipulate data, or information.
OT system	The hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, compressors, etc.
	Main/Secondary Impact
Data loss or corruption	Theft and/or corruption of sensitive information regarding the company knowhow, employee data, process data (e.g., equipment data sheets, PFDs, P&IDs, historical data, etc.), economic data, etc.
Economic loss	The attacked company suffers serious economic losses due to e.g., the loss of productivity (downtime), the collapse of the company shares on the stock exchange.
IT infection	Infection of the IT system (e.g., infection of IT server, PCs, etc.)
Major event	Loss of containment of hazardous material, explosion, fire, toxic dispersion, soil contamination, etc.
OT infection	Infection of the OT system (e.g., infection of HIM workstations, OT servers, etc.)
PSD/LSD	PSD (Process Shut Down) or LSD (Local Shut Down) originated either directly or by inducing an anomalous condition or abnormal mode of operation.

3.1.1.3. Structured toolbox applied for the analysis of the database

A set of complementary synergic tools was used to carry out a structured analysis of the populated database, with the aim of characterizing the attacks, the threats, the attackers, the scenarios generated by the attacks, and the outcomes of the attacks, thus providing data and results useful to support SVA/SRA studies and for the definition of reference security-related scenarios to be considered in the security assessment of facilities under the 2012/18/EU ("Seveso-III") Directive.

In addition to the commonly adopted Exploratory Data analysis (EDA) for retrieving simple statistical results, specific tools were adopted to analyse the total number of SREs and the specific sub-sets of interest considered in the analysis. In particular, **Figure 8** shows the framework built for data analysis and the features and aim of each of the specific tools applied: Exploratory Data Analysis (EDA), Correspondence Analysis (CA), Cause-Consequence Chains (CCCs), Root Cause Analysis (RCA), and Attacker Sequence Diagrams (ASDs). Each tool, providing a specific piece of information, contributes to build an unprecedented, detailed

representation of the threats, the scenarios, and the attackers involved in security-related events affecting chemical and process facilities.

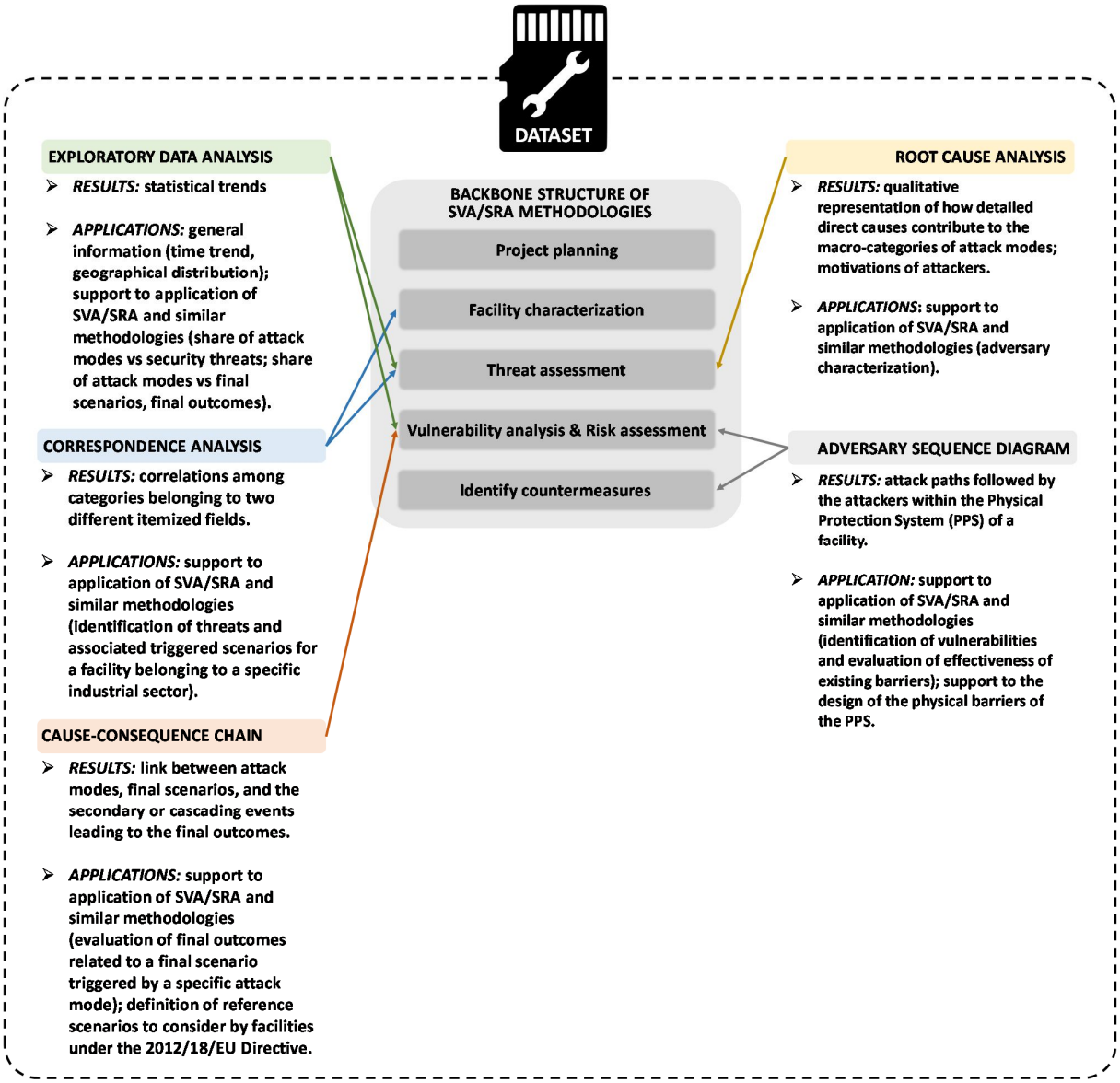

Figure 8 Framework and scope of dataset analysis and link with backbone structure of SVA/SRA methodologies.

Exploratory Data Analysis (EDA) is an approach of analysis of datasets that is used to summarize their main characteristics, often using statistical graphics and other data visualization methods [145]. In the present study, EDA was used to gather general information from the total number of SREs collected and from specific subsets of them (i.e., SREs collected for the Chemical&Petroleum sector and the cyber-related SREs).

Correspondence Analysis (CA) is a statistical technique which is helpful in analysing cross-tabular data in a graphical form that reveals the relative relationships between and within two groups of variables (i.e., the itemized fields of the database) [146]. The input data are given in the form of a contingency table, i.e., a table with row and column labels filled with the combined frequencies of the variables (i.e., the number of security-related events in this case). In order to compute the CA, the Matlab script developed by Seva et al. [147] was adopted. The reader is referred to [146] for the theoretical framework of CA, while the key elements are reported in **Table 6**.

In the present study, Correspondence Analysis (CA) [146] was carried out on the total number of SREs in order to investigate correlations between couples of itemized fields, and more specifically, to identify the specific correlations between the industrial sectors, the security threats, and the final scenarios, allowing to better understand the actual security-related scenarios affecting industrial installations.

Table 6 Description of the key elements of Correspondence Analysis (CA) [146]

Concept	Description
Correspondence Analysis	A method of displaying the rows and columns of a table as points in a spatial map, with a specific geometric interpretation of the positions of the points as a means of interpreting the similarities and differences between rows, the similarities and differences between columns and the association between rows and columns.
Contingency table	A table with row and column labels filled with the combined frequencies of two variables; hence the grand total of the table is the number of individuals/events.
Profile	A row or a column of the contingency table divided by its total (i.e., a set of relative frequencies); the profiles are the points visualized in CA, elements of a multidimensional space. Such sets, or vectors, of relative frequencies have special geometric features because the elements of each set add up to 1. In particular, if the profiles are points in a m-dimensional space, they actually occupy a limited region of that space, i.e., a (m-1)-dimensional subspace.
Mass	The marginal total of a row or a column of a table, divided by the grand total of the table; used as weights in CA.
Centroid	The average profile of a row or a column: its elements are respectively the column or row masses.
Vertex	A unit profile, i.e., a profile with all elements zero except one with value 1.
Principal coordinates	Coordinates of a set of points projected onto a principal axis, such that their weighted sum of squares along an axis equals the principal inertia on that axis.
Standard coordinates	Coordinates of a set of points such that their weighted sum of squares along an axis equals 1.
Chi-square distance	Weighted Euclidean distance measure between profiles, where each squared difference between profile elements is divided by the corresponding element of the average profile.
Inertia	Weighted sum of squared distances of a set of points to their centroid; in CA the points are profiles, weights are the masses of the profiles and the distances are chi-square distances. The inertia can assume zero as minimum value (i.e., all the row or column profiles coincide with the centroid), to a maximum value coinciding with the size of the (m-1)-dimensional subspace (i.e., all the row or column profiles lie exactly on the vertices).
Reduction of dimensionality	Profiles consisting of m elements are situated exactly in spaces of dimensionality m-1. Hence, profiles with more than four elements are situated in spaces of dimensionality greater than three that cannot be observed directly. The reduction of dimensionality is the process consisting in the identification of a subspace of lower dimensionality (2D or 3D) which lies close to all the profile points so that it is possible to project the profiles onto such a subspace and look at their projected positions in this subspace as an approximation to their true higher-dimensional positions. What is lost in this process of dimensionality reduction is the knowledge of how far and in what direction the profiles lie "off" this subspace. What is gained is a view of the profiles that would not be possible otherwise.
Percentage of inertia	It is the measure of the accuracy of the reduction of dimensionality (e.g., 85% of the inertia of the profiles is represented in the subspace, then the residual inertia, or error, which lies external to the subspace, is 15%).

Cause-Consequence Chains (CCCs) are the sequences of events from the attack scenarios to the physical damage scenarios and related final outcomes [148]. In the present study, they were built thanks to the information present in the recorded SREs for the Chemical&Petroleum sector for which more details were

available, in order to further investigate the link between attacks, consequences and final outcomes (e.g., potential of secondary of cascading effects) identified through CA and EDA.

Root Cause Analysis (RCA) is a systematic process used for identifying the root causes of a focus event, widely used in different fields of engineering, including accident/incident analysis [149]. According to the RCA-specific standard IEC 62740 [150], which lists all the possible tools and techniques for RCA application and data visualization, the Ishikawa diagram (more commonly known as fishbone diagram for its shape) was adopted to show the results. It graphically illustrates the relationship between an event and all the factors that influence it. In the present study, RCA was carried out to the subset of SREs collected for the Chemical&Petroleum sector for which more information was available in order to identify the specific features of each attack mode identified by CA, as well as the motivations and the level of competence of the attackers.

The Attacker Sequence Diagram (ASD) is a tool developed in the context of the nuclear power industry which consists of a graphical representation of the Physical Protection System of the facility analyzed, divided into physical areas and layers of protection between areas, that allows for an easy identification of the possible paths an attacker might follow to attack a specific target [7]. The reader is referred to [7] and to Section 5.3.2 for more details on ASDs. In the present study, the ASD was applied to the subset of SREs collected for the Chemical&Petroleum sector for which more information was available, to allow the understanding of the level of penetration of the attackers required to perpetrate the successful attack scenarios identified in CA and further analysed by RCA.

Summarizing, the following sets of SREs have been investigated:

- total number of SREs (see Section 3.1.2);
- SREs collected in the Chemical&Petroleum sector (see Section 3.1.3);
- SREs caused by cyber-attacks (see Section 3.1.4).

3.1.2. Results from the analysis of the total number of SREs

3.1.2.1. Time trend and geographical distribution (results from EDA)

To investigate the trend over time and the geographical location of the SREs recorded, Exploratory Data Analysis was applied. **Figure 9-a** shows the quinquennial time trend of the total number of SREs included in the database. After year 2000, there was a significant increase (almost quadruple) in the number of the incidents recorded. In particular, only 5 cybersecurity-related events (CSREs) occurred before 1999, which started to be significant in the last 20 years. This can be justified by the fact that cybersecurity was not a significant threat for process facilities at the time (lower attractiveness, lower level of digitalization and network interconnection). The time trend of the collected SREs shows two peaks: one during the five-year period 2000-2004 (75 SREs), due to a high number of cyber-attacks all over the world, and one during the five-year period 2010-2014 (79 SREs), due to a high number of physical attacks. The latter peak might be due to the greater attention paid to the topic in the last decades, promoting incident reporting. For instance, for what concerns cybersecurity, in the last years, companies have increasingly implemented cyber-risk analysis in the management of their IT-OT systems: this was supported by the definition of international standards, such as the ISO/IEC 27000 series for IT systems and the ISA/IEC 62443 for the industrial automation and control systems (IACSs, see Section 1.3.3). Moreover in Europe, in 2016, the NIS Directive was issued by the European Parliament and Council, setting several goals in the direction of security of IT-OT systems that all EU countries must achieve with specific national regulations.

The geographical distribution of the entries recorded in the database is shown in **Figure 9-b**. Most of the events took place in Europe (128 SREs, 34% of the total), followed by America (116 SREs, 31%, 90 of which in North America and 26 in South America), Asia (77 SREs, 21%), Africa (42 SREs, 11%), and Oceania (3 SRE, 1%).

For 7 SREs (2% of the total) the location is unknown. This result could be in part ascribed to the different reporting practices of each geographic area. For instance, in Australia, accidental events have to be reported when entailing a "serious risk", defined as “the death of a person, a serious incident or illness, or an incident that exposes any person to a serious risk (even if no one is injured)” [151]. A similar legislation is present in U.K. [152]. Differently in U.S., reporting is included in the National Incident Management System, which requires reporting “for all the departments and agencies as well as for the private sector, regardless of cause, size or complexity of the incident”. A probable under-reporting concerns Asia, as the continent has the greatest number of industrial establishments (UNIDO Statistic Data Portal [153]), but only the 20% of the incidents recorded took place in this continent.

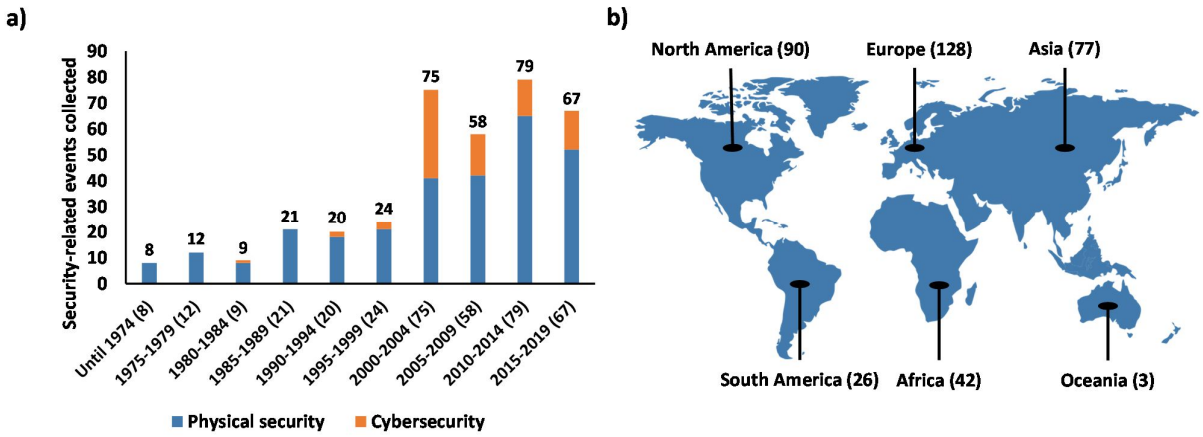

Figure 9 a) Time trend of the SREs collected; b) Geographical distribution of the SREs collected (7 SREs are of unknown location). Adapted from [2].

3.1.2.2. Security threats, industrial sectors and final scenarios (results from CA)

Correspondence Analysis (CA) was used to investigate correlations among the different itemized fields considered in the database. In particular, CA was used to test the presence of correlations among the type of security threat, the geographical area, the industrial sector, and the final scenario triggered by the attacker. More specifically, four couples of itemized fields were investigated:

- "Location" – "Security Threat";
- "Industrial Sector" – "Security Threat";
- "Industrial Sector" – "Final Scenario";
- "Security Threat" – "Final Scenario".

“Location” categorizes the events based on the continent where the affected facility is located: Africa, Asia, Europe, North America, Oceania, or South America. “Security Threat” addresses the threat agent (i.e., outsider cyber-threat, insider threat, sabotage, terrorism, theft, vandalism). “Industrial Sector” indicates the specific sector to which the affected facility belongs (i.e., bioprocesses, chemical&petroleum, energy production, pipelines, transportation, water/wastewater). “Final Scenario” reports the adverse event triggered by the deliberate malicious attacks (i.e., release of hazardous material, explosion, fire, loss of process control/monitoring, near miss or other minor scenarios). A detailed definition of each class used in each itemized field is provided in **Table 3**.

Due to both a low inertia (i.e., the behaviour of the profiles is similar to that of the average profile) and a low quality of the 2D-map of the profiles (i.e., percentage of inertia less than 80%, see definition in **Table 6**), the outputs of the CA for the couples "Location" vs. "Security Threat" and "Industrial Sector" vs. "Final Scenario" resulted of scarce interest and therefore they are not reported below. On the contrary, some strong

correlations were found for the other two couples of itemized fields (i.e., “Industrial Sector” vs. “Security Threat” and “Security Threat” vs. “Final Scenario”).

Figure 10-a shows the contingency table of the couple "Industrial Sector" vs. "Security Threat". The numbers correspond to the combined numbers of security-related events that were collected for couples of labels "sector - scenario". It may be remarked that the grand total of events in the table (337) does not coincide with the total number of the events recorded in the database (373), as the events with unknown security threat or unknown industrial sector were not considered in the CA.

Figure 10-b shows the 2D-map of the CA based on the contingency table discussed above. The graph displays the security threats in principal coordinates (i.e., those deriving from the row profiles) and the industrial sectors in standard coordinates (i.e., as unit vectors). It is important to remark that the map contains the projections of the real points in the best-fitting 2D-plane (see reduction of dimensionality in **Table 6**): this means that some information is missing. The information lost is represented by the “inertia” (or “total inertia”, in percentage) that measures how “far” the row profiles are from their average profile: the higher the inertia, the less information is lost. In this case, the percentage of inertia shown in the map is 95.1% and, consequently, the information lost is 4.9%, meaning that the correlations that can be obtained from the analysis are reliable.

a)

	Bioprocesses	Chemical&Petroleum	Energy Production	Pipelines	Transportation	Water/Wastewater	TOT
Insider threat	0	8	2	2	2	2	16
Outsider cyber threat	3	33	24	6	0	9	75
Sabotage	0	5	5	28	0	2	40
Terrorism	0	31	35	34	1	3	104
Theft	0	2	1	46	1	0	50
Vandalism	2	5	0	8	35	2	52
TOT	5	84	67	124	39	18	337

b)

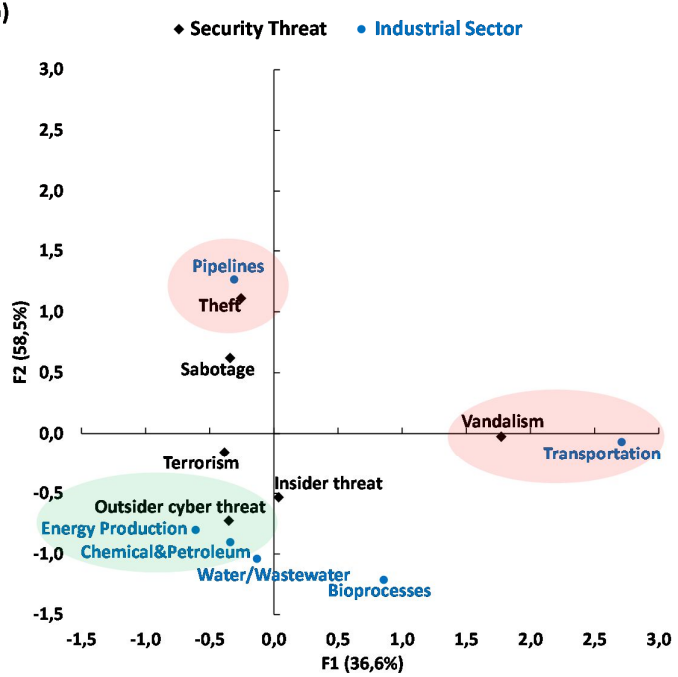

Figure 10 a) Contingency table reporting the combined number of security-related events for the couple of itemized fields “Security Threat” and “Industrial Sector”; b) 2D-map reporting the results of Correspondence Analysis for the couple of itemized fields “Security Threat” and “Industrial Sector” (total inertia of the map is 95.1%). Adapted from [2].

The origin of the graph represents the centroid, i.e., the average row profile of the entire dataset, considering all the security threats. The points representing the security threats that are close to the centroid are those that differ the least from the average profile, while the points that are more distant from the origin are those for which it is possible to find correlations with a specific industrial sector, as they have a different behaviour with respect to the average profile.

The correlation between security threats and industrial sectors is shown in the 2D-map by the distance between the two respective points: a smaller distance indicates a higher correlation. In particular, two strong correlations were found (red shaded in the 2D-map): one between "Vandalism" and "Transportation", and

the other between "Theft" and "Pipelines". This means that the infrastructures for transport via road, rail, or water such as trucks, trains and ships, are those which are mainly affected by acts of vandalism, and that the trend of vandalism strongly differs from the average behaviour of all the threats with respect to the industrial sectors. In other words, there is a correlation. Unlike fixed installations (which may have a sophisticated safety/security system, e.g., perimeter barriers, structural barriers, intrusion detection, etc.), infrastructures for transportation require less complex attack patterns, and therefore are targeted by poorly equipped attackers, having a low level of preparedness and not applying any specific tactic in attack execution. Similarly, thefts are closely correlated with pipelines: this is due to the high market value of oil fractions as gasoline, diesel, and kerosene, together with an inherent difficulty in protecting such installations given their extension, although they are in general buried. Moreover, a weak correlation between "Outsider cyber threat" with both “Chemical&Petroleum” and “Energy Production” sectors, was found (green shaded in the 2D-map). Hackers and cyber-criminals are attracted by these installations not only for the high media visibility achievable due to the potential severity of the consequences, but also for the possibility to access proprietary information important for the business together with the high socio-political impact of the events (especially for plants and lifeline facilities owned by multinational companies). This correlation is weak because the point corresponding to "Outsider cyber threat", despite being at a very small distance from the points representing “Chemical&Petroleum” and “Energy Production”, is not so far from the centroid. Finally, it was not possible to find correlations between "Insider threat", "Terrorism", "Sabotage", and the industrial sectors: from the contingency table (**Figure 10-a**) it is possible to notice that these security threats mainly affect the Chemical&Petroleum sector, the energy production sector and the pipelines, but this trend is similar to that of the average profile of all the security threats (i.e., the corresponding points are close to the centroid).

The outlined distribution of the security threats with respect to the industrial sectors (**Figure 10**) supports the identification of the more likely threats that can affect an industrial installation belonging to a specific industrial sector. It provides information about the threat history to be investigated in order to evaluate the attractiveness to deliberate attacks. This applies to specific steps of many common SVA/SRA methodologies, as steps 2.4 and 3.1 of CCPS methodology (“Attractiveness analysis” and “Attacker identification”), steps 2.1 and 2.2 of the methodology proposed by API RP 780 (“Evaluate potential threats” and “Assign threat ranking”), steps 3 and 5 of VAM-CF methodology (“Characterizing the facility” and “Assessing threats”), as well as steps 2 and 5 of RAMCAP methodology (“Threat characterization” and “Threat assessment”). For example, terrorism and outsider cyber threat are the more likely threats that affect chemical and petrochemical facilities and, therefore, shall be considered when a security assessment is performed for such type of installations. In other words, attractiveness of chemical, petrochemical and energy production plants to terrorist attacks is high (i.e., a terrorist attack is likely), while, on the other hand, the attractiveness is lower in case of installations belonging to bioprocesses, transportation, and water/wastewater sectors.

Figure 11-a shows the contingency table for the couple of itemized fields “Security Threat” and "Final Scenario". The grand total of the contingency table is equal to 313 since, for 60 out of 373 security-related events collected, the threat and/or the final scenario triggered by the attackers was unknown. The 2D-map of CA resulting from this table is shown in **Figure 11-b**. The graph represents the row analysis and displays the security threats in principal coordinates and the final scenarios in standard coordinates. The percentage of inertia shown by the map is 97.7% and, consequently, the information lost is 2.3%. Thus, the correlations obtained from the analysis are an extremely good representation of reality.

a)

	Explosion	Fire	Loss of process C/M	Near miss	Other	Release	TOT
Insider threat	4	1	7	0	3	1	16
Outsider cyber threat	2	0	36	0	37	0	75
Sabotage	21	5	1	0	1	6	34
Terrorism	73	6	1	2	3	1	86
Theft	7	0	0	0	0	42	49
Vandalism	1	3	0	0	0	49	53
TOT	108	15	45	2	44	99	313

b)

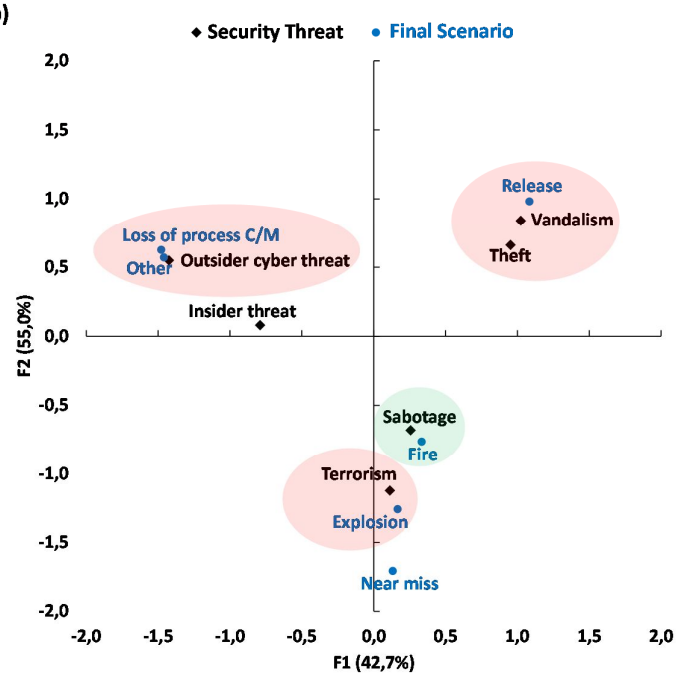

Figure 11 a) Contingency table reporting the combined number of security-related events for the couple of itemized fields "Security Threat" and "Final Scenario"; b) 2D-map reporting the results of Correspondence Analysis for the couple of itemized fields "Security Threat" and "Final Scenario" (total inertia of the map is 97.7%). Adapted from [2].

Five strong correlations (red shaded in the 2D-map) and a weak correlation (green shaded) were identified. "Vandalism" and "Theft" resulted to be strongly correlated with "Release". This means that a loss of containment of a hazardous substance can be considered as a reference scenario triggered by deliberate attacks performed by vandals and thieves. This can be explained by the fact that vandals and thieves use different tools/equipment (e.g., hand tools such as sledgehammers, or power tools such as drill roto hammers) than other types of attackers such as terrorists (which mainly use explosive devices or grenades that may trigger explosions and fires), and that they have different goals (i.e., stealing materials for thieves, and causing any type of damage even if it does not result in a major event for vandals) with respect to terrorists aimed at generating impacts with the most severe consequences on humans and the assets of the target facility. Since from the analysis of the correlation among "Security Threat" and "Industrial Sector" reported in **Figure 10**, "Theft" resulted correlated with "Pipelines", and "Vandalism" with "Transportation", a release turns out to be a scenario that shall be considered in a security risk assessment of such industrial infrastructures. For this reason, **Figure 11** may support step 2.3 of CCPS methodology ("Consequence analysis"), step 3.1 and 3.2 of API-RP 780 ("Evaluate scenarios" and "Evaluate Consequences"), step 1.1 of VAM-CF ("Specify undesired events"), and step 3 of RAMCAP ("Consequence analysis") in the identification of potential scenarios triggered by the deliberate attacks.

Similarly, "Outsider cyber threat" resulted strongly correlated with both the final scenarios "Other" (the two points are almost coincident) and "Loss of process control/monitoring". This means that these two scenarios shall be considered when cyber threats are assessed in the framework of SVA/SRA methodologies and similar procedures. Furthermore, since from **Figure 10-b** resulted that outsider cyber threat is correlated (even if weakly) to chemical, petrochemical and energy production facilities, a malicious interference with the Basic Process Control System (BPCS) and/or the Safety Instrumented System (SIS) shall be taken into account in the security analysis of such facilities.

Moreover, "Terrorism" turned out to be closely correlated with the final scenario "Explosion", which therefore can be considered as a reference scenario when terrorism is assessed in a SVA/SRA methodology. This can be explained by the fact that terrorists use weapons such as explosives devices and grenades with the potential of causing explosions of process equipment due to the blast wave originating from the detonation. Finally, “Sabotage” resulted being weakly correlated with "Fire": the correlation is weak because of both the small distance from the centroid of the point corresponding to "Sabotage" and the small number of events labelled as "Fire" (14).

No correlation with final scenarios was identified for the “Insider threat” security threat.

3.1.3. In-depth analysis of the SREs collected for the Chemical&Petroleum sector

An in-depth analysis concerning the attack modes performed by the attackers and the chain events that lead to the recorded final outcomes suffered by the attacked facilities was carried out for the SREs occurred in the Chemical&Petroleum sector since more detailed information was available in the incident records. EDA, RCA, CCCs, and ASDs were applied to gain different information to support SVA/SRA studies. Definitions of the classes of attack modes and of final outcomes used in this Section are reported in **Table 4** in Section 3.1.1.2.

3.1.3.1. Attack modes triggering final scenarios (results from EDA, RCA, and CCCs)

For 91 security-related events out of 104 recorded for the Chemical&Petroleum sector, it was possible to identify the attack mode through which the attackers attempted to penetrate the security barriers in place and to give rise to impacts in the target facilities. **Figure 12** shows the 3D-plot reporting the share of the attack modes with respect to the security threats. Moreover, the information available in 34 records also allowed retrieving details on the type of attacker and its motivations, which were used for a root cause analysis of the security attacks.

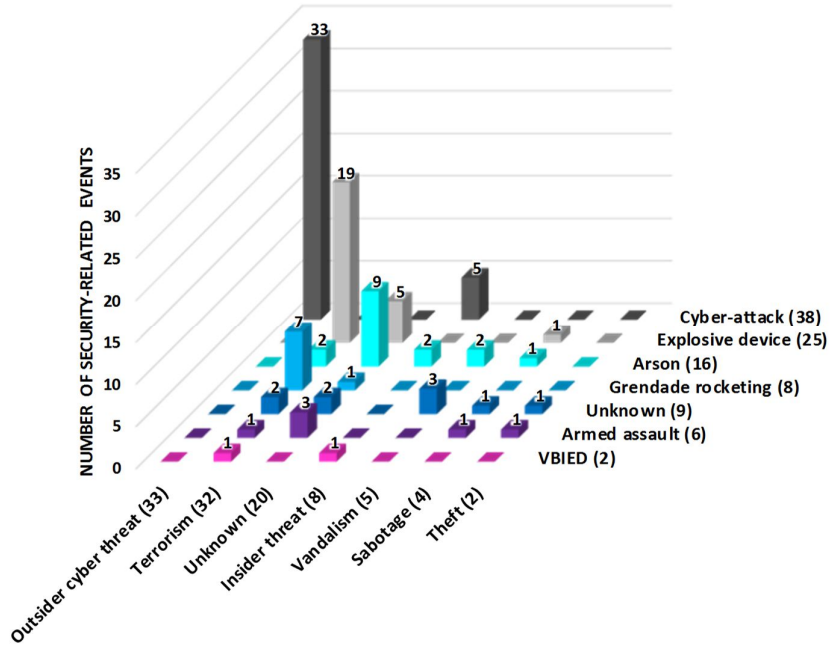

Figure 12 3D-plot reporting the share of the attack modes with respect to the security-threats (VBIED: Vehicle-Born Improvised Explosive Device). Adapted from [2].

Cyber-attacks (i.e., attacks via the cyberspace to the IT-OT network system of a facility) resulted the attack mode with the highest number of events recorded (38). Almost all of these events are related to outsider

cyber threats: in 2 SREs a nation-state or state-sponsored group/organization was identified as the attacker. Motivations included compromising, stealing, changing, or destroying information, as well as damaging the assets of the target facilities in the context of geopolitical threats (e.g., the hacking of the German chemical giant Bayer by the "Winnti Group" that caused the theft and deletion of proprietary secret information). With respect to cyber-attacks performed by insiders (5 SREs recorded), in 3 incidents a single-man attacker was identified, but the motivations underlying the attacks are unknown, even if revenge is suspected: actually both the infection of the control system and of other sub-systems of a EU chemical plant in 2001, and the hacking of a US pharmaceutical facility in 2011 causing the deletion of data and the sabotage of almost 90 servers in 2011, were performed by former employees. More information on this type of events is reported in Section 3.1.4, where the results of the in-depth analysis of the cybersecurity-related events are shown and discussed.

In case of insiders performing physical actions, in 2 SREs a single-man attacker was reported: in one incident the attacker was a disgruntled employee motivated by revenge, while in the other a supplier was responsible of the detonation of explosives contained in a truck. Strikers motivated by the claim of rights were the responsible of the attack to the US Potash plant in Trona in 1970 that was the scene of a major worker strike.

Among the physical attack modes performed by external attackers, the use of explosive devices (i.e., devices that provide a violent release of energy when detonated) resulted the most common (25 SREs). This type of attack is usually carried out by highly capable and well-motivated attackers such as terrorist organizations (19 of 32 SREs related to terrorism were caused by the detonation of explosive devices). The same resulted for grenade rocketing (i.e., shooting of missiles through a rocket launcher or remotely controlled drones): 7 out of 8 SREs originated from a terrorist matrix. A left-wing guerrilla military group was found to be the most frequent type of attacker (13 SREs), the majority of which designated as a terrorist organization in at least one country around the world. Among these, attacks performed by "Omega-7" in Cuba, "Revolutionary People's Liberation Party" in Turkey, "Movement for the Emancipation of the Niger Delta" in Nigeria, "Shining Path", "Movement of the Revolutionary Left" and "Túpac Amaru Revolutionary Movement" in Perù, "Revolutionary Cells" and "Rote Armee Fraktion" in Germany, the "National Liberation Army" and "Colombian Patriotic Resistance" in Colombia, "Euskadi Ta Askatasuna" in Spain, were recorded. Motivations included the demonstration of anti-government and anti-US sentiment, as well as obtaining political independence for specific regions. For example, the political emancipation of the Basque region was the reason under two terrorist attacks in Spain, one against a petrochemical plant located in Tarragona in 1990 and one against a chemical plant located in Bergara in 2005.

A terrorist organization of Islamic matrix was found in 6 SREs: three related to the "Houti movement Ansar Allah" that claimed responsibility for multiple attacks with ballistic missiles (grenade rocketing) against the Saudi Arabian Oil Company Aramco (the last in Sempteber 2019), two related to the "Shia Islamist" political party and militant group based in Lebanon, and one related to "Ansar al-Sharia" operating in Libya.

A total of 16 cases of arson were recorded, revealing that this is a common attack mode as it does not require the attackers to be highly equipped, nor well-motivated: actually, in most of the cases (9 out of 16) the security threat leading to arson is unknown. Furthermore, six (6) cases of armed assault with firearms (one performed by five men that stolen aluminium dust in order to manufacture explosives) and 2 cases of vehicle borne improvised explosive device (VBIED) were also recorded for chemical and petrochemical facilities.

Figure 13 shows the 3D-plot reporting the share of the attack modes with respect to the final scenarios triggered by such attacks. A physical explosion of a chemical equipment is by far the most common event that occurred as a direct consequence of the detonation of an explosive device (20 cases out of 25). Industrial fires involving process equipment is definitely the most frequent final scenario triggered by arsons (11 cases out of 16). It is interesting to remark that in two cases of grenade rocketing a near miss occurred: actually,

the attacks did not have success since the missiles were intercepted by the air-defence forces [43]. The same happened for one case of armed assault in which the security guards succeeded in interrupting the assailants.

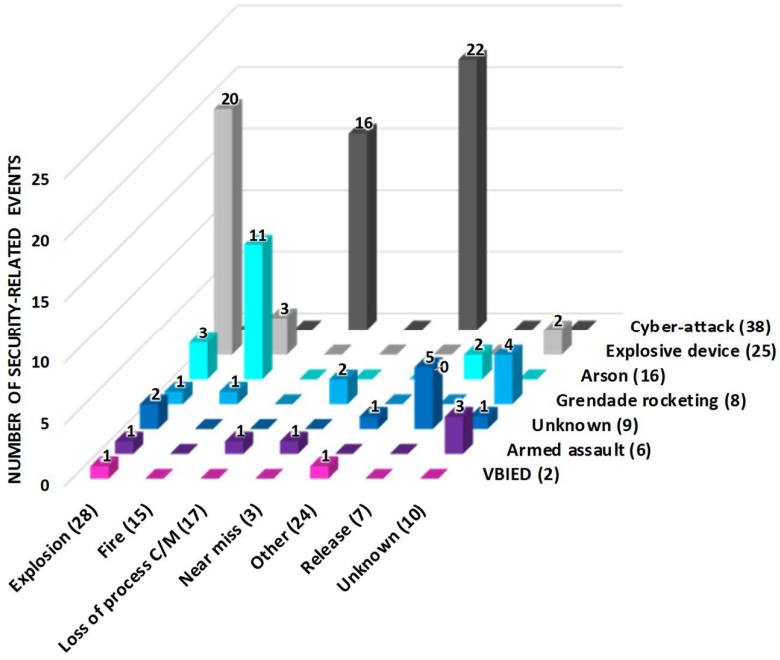

Figure 13 3D-plot reporting the share of the attack modes with respect to the final scenarios triggered by the attackers (VBIED: Vehicle-Born Improvised Explosive Device). Adapted from [2].

When cyber-attacks are considered, in case of infection of the OT system, the impacts experienced by the affected facilities spanned from an infection of the HMI workstations (14 events) to a Local or Process Shutdown (LSD/PSD, 4 SREs). On the other hand, when only the IT system became infected, a data theft or corruption (10 SREs) and technical inconveniences at IT level (10 events) were registered. No major events occurred in chemical and petrochemical facilities as a consequence of cyber-attacks. Thus, as shown in **Figure 13**, a loss of process control/monitoring and an "other" scenario resulted as the two only final scenarios that followed cyber-attacks, respectively 16 and 22 SREs recorded.

Only a single event recorded a loss of process control/monitoring as a consequence of a physical attack mode, more specifically an armed assault. In the event, which took place in Libya in 2018, the assailants entered El Sharara Oilfield and physically threatened employees to shut down the oil pumps [140].

An explosion and an “other” scenario were registered in the two events recorded related to VBIED.

It is also interesting to notice that the attack mode is unknown for 5 out of 7 SREs leading to releases of chemicals: since these events often result from intentional acts realized by the use of simple hand tools or even by opening valves manually, the events are characterized by low media interest when compared to the other attack modes, and therefore such information might often not be reported.

The Ishikawa diagram [149] (also called fishbone diagram) of a generic final scenario was obtained from the analysis of thirty-five (35) security-related events that occurred in the Chemical&Petroleum sector and that included sufficient details about the attack modes. The diagram, shown in **Figure 14**, reports the direct causes of a final scenario in terms of deliberate attacks performed by the attackers.

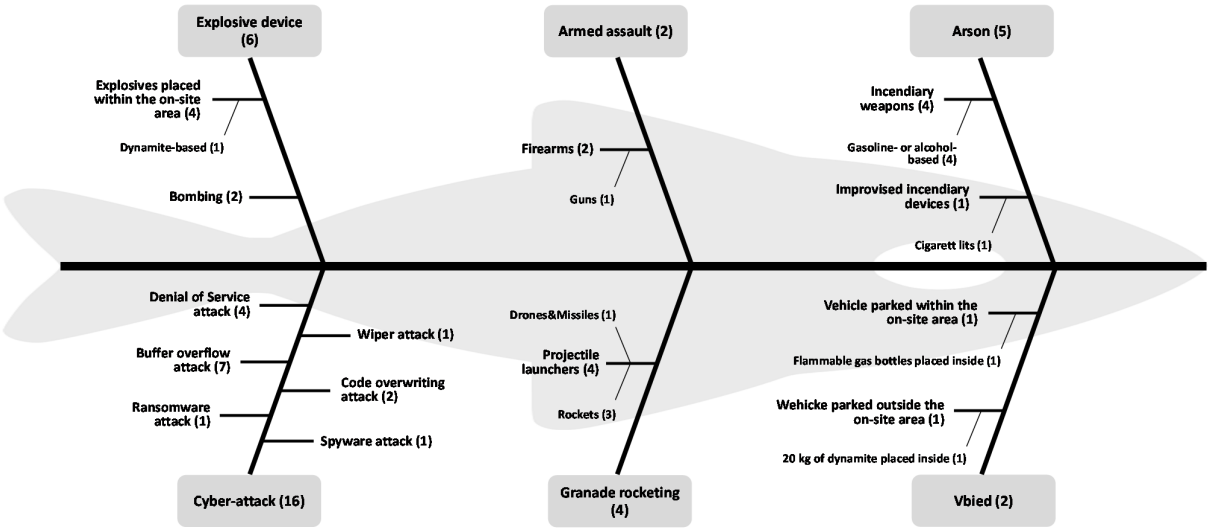

Figure 14 Ishikawa diagram (fishbone diagram) reporting the specific features of the attack modes that resulted in a successful final scenario (i.e., explosion, fire, release, loss of process control/monitoring, other, near miss). Adapted from [2].

In four cases where "Explosive device" was the attack mode, the explosives were placed within the on-site area of the target chemical or petrochemical facility: i.e., the attackers managed to enter inside the perimeter of the facility bypassing the barriers in place without being interrupted. In two other cases the specific attack consisted of an external bombing. In two cases where "Armed assault" was the attack mode, the attackers made use of firearms. Incendiary weapons (gasoline- or alcohol-based) where used in four cases by the attackers for triggering an arson, while in one case arson was originated through an improvised source of ignition (i.e., a cigarette lit) that was able to ignite a flammable gas mixture. With respect to the category "VBIED" (2 events recorded), in one case a vehicle with flammable gas cylinders entered the plant and exploded near to the facilities, while in the other case a car bomb with 20 kg of dynamite inside was detonated close to the facility fences, in the off-site area. Missiles launched by drones (one case) and rockets launched by rocket launchers (3 cases) were used in the case of "Grenade rocketing".

With respect to cyber-attacks, the following specific attack modes were detected:

- 7 cases of buffer overflow attacks (i.e., an attack aimed at overwriting parts of memory data);
- 4 cases of Denial of Service attacks (i.e., an attack aimed at making a machine or a network resource unavailable);
- 2 cases of software reprogramming attacks (i.e., an attack aimed at reprogramming parts of the software code);
- 1 case of ransomware attack (i.e., an attack aimed at publishing the data contained in the target machine or perpetually block access to it unless a ransom is paid);
- 1 case of wiper attack (i.e., an attack aimed at permanently erase the hard drive of the target machine);
- 1 case of spyware attack (i.e., an attack aimed at gathering information about a person or organization).

Overall, the results shown in **Figure 12**, **Figure 13**, and **Figure 14** support SVA/SRA methodologies in the steps addressing attacker characterization (step 3.2 of CCPS methodology, step 2.2 of the methodology proposed by API RP 780, step 5 VAM-CF methodology, step 2 of RAMCAP methodology) and of security scenarios identification (step 4.2 of CCPS methodology, step 3.1 the methodology proposed by API RP 780, step 6 of VAM-CF, step 3 of RAMCAP methodology). **Figure 12** and **Figure 13** provide useful information on the attack

modes used by the categories of security threats considered in the analysis, and identify reference scenarios that can be triggered by each attack. Moreover, **Figure 14** provides an insight into the specific tools and/or substances used by the attackers in order to carry out the attacks. For example, an attack scenario where explosive devices are placed next to equipment in the plant area should be considered when the terrorist threat is assessed for a petrochemical facility. This information was used to validate the branches of the developed reference security-related Bow-Tie diagrams in the context of the study described in Section 5.1.

Figure 15 reports the event-specific Cause-Consequence Chains [148] obtained from 7 records having sufficiently detailed information available. Despite being a limited set of data, the events selected for this analysis still represent different significant combinations of attack modes and threats. The Cause-Consequence Chains link the attack modes perpetrated by the attackers, the final scenarios triggered, and the secondary or cascading events which lead to the final outcomes suffered by the target facility. Cause-Consequence Chains were obtained applying the "Why Tree" technique [154], considering two levels of "attack event" connecting the attack mode to the final scenario and three levels of “cascading events” from the scenario to the final outcome.

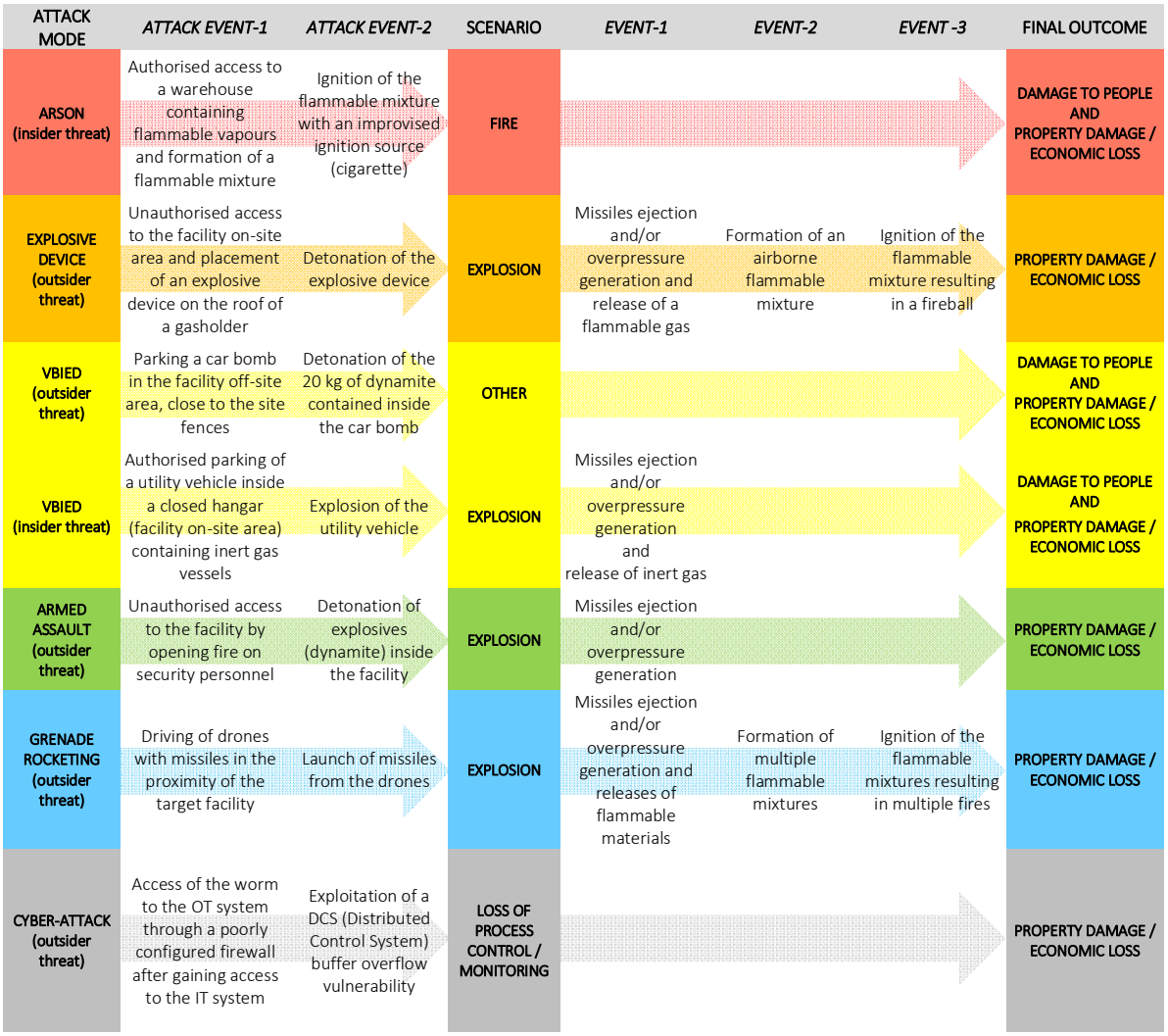

Figure 15 Cause-consequence chains (from the attack modes to the final outcomes on the process facility under attack), based on seven records which reported detailed information on the event. Adapted from [2].

The case of “Explosive device” is of particular interest, since the details available for the incident were sufficient to fill all the boxes in the chain. The attackers entered the facility bypassing the physical barriers in place (e.g., the site fence), and positioned an explosive device on the roof of a gasholder. The detonation of the explosive caused the physical explosion of the gasholder with the consequent release of the flammable gas contained inside, as well as the ejection of missiles and the generation of overpressure. The direct event that occurred was the formation of an airborne flammable mixture that, once ignited, resulted in a fireball, causing property damages and huge economic losses to the facility affected [8]. Information on the qualification and expertise of the attackers, as well as on their motivations, is not provided in the incident report, and therefore it is not known if they aimed to trigger cascading events such those described above. Actually, omitting such information is common in incident reporting, as reports are mainly focused on scenarios and outcomes, rather than on the characterization of the attackers. However, attackers that are conscious of the inherent hazard of the target installations and of how to exploit it, such as insiders with a chemical engineering background and sufficient knowledge about the process, may aim at generating cascading events resulting in the escalation of consequences with respect to those caused by the primary event (i.e., the final scenario triggered by the attack).

The two cases of “VBIED” confirmed that impacts on the target facility can also be generated by physical attacks that do not involve the intrusion of the attackers within the restricted areas of the site. In fact, in one case the attacker parked a car bomb with 20 kg of dynamite outside the site, near the fence, and detonated it causing damages to the facility buildings and injuring two operators [140] (“Other” final scenario as defined in **Table 3**). In the other case, the explosion of a vehicle with cylinders containing a flammable gas parked in a closed hangar within the facility caused the physical explosion of the inert gas vessels contained in the hangar, leading to one fatality, two injuries and property damages, because of the missiles ejection and overpressure generation that followed the explosion.

The case of “Armed assault” confirmed that the attackers executing the attack were highly trained, well-motivated and highly equipped: they entered the facility by opening fire on security personnel with guns and then detonated dynamite-based explosives on buildings and on the plant, giving rise to physical explosions that caused property damages and related economic losses to the facility affected [140].

The case of “Grenade rocketing” is also particularly significant, since the attackers air-bombed the plant with missiles launched by several drones, possibly controlled from a remote site far away from the attacked facility, causing several explosions leading to the release of flammable substances which resulted in multiple fires [155]. Also in this case, it is not clear if the attackers were specifically aimed at triggering cascading events such those described, but given the multiple number of missiles launched with drones, the attackers seemed more oriented to cause as much damage as possible through the primary scenarios triggered by the attack, rather than by the secondary events triggered by the bombing. The prevention from this type of attack is very challenging, since drones, missiles or rockets have to be destroyed or diverted before they physically impact the facility. Nevertheless, there have been recorded cases of successful defense from such type of attacks: e.g., as occurred in two different air-attacks in Saudi Arabia in 2018 where the air-defense forces succeeded in destroying the missiles [140].

The case of "Cyber-attack" shows a typical attack pattern through the network architecture of a process facility. According to Iaiani et al. [13], a worm managed to access the OT system of a chemical facility through a poorly configured firewall after accessing its IT system. Then, by exploiting a DCS (Distributed Control System) buffer overflow vulnerability (see the buffer overflow attack discussed above), it disabled two HMI workstations located in the control room. No production was lost thanks to the AV (antivirus) software that revealed and stopped the worm infection [142].

The Cause-Consequence chains obtained can be used as a starting point for security scenarios identification when applying SVA/SRA methodologies (step 4.2 of CCPS methodology, step 3.1 of the methodology

proposed by API-RP 780 methodology, step 6 of VAM-CF, step 3 of RAMCAP methodology), providing a useful visualization of the sequence of events interconnecting the attack modes with the final scenarios and related outcomes.

3.1.3.2. Attack paths related to physical security threats (results using ASD)

Physical attack paths are inherently different from those performed via the cyberspace (i.e., the cyber-attacks). In the latter case, the attacks need to overpass the barriers of the IT-OT network system, e.g., authentication systems, firewalls, AV software, etc. In a physical attack the threat actors have to bypass the barriers of the Physical Protection System (PPS), e.g., fences, gates, locked doors, etc. Therefore, attack modes such as "Armed assault", "Arson", "Explosive device", "Grenade rocketing" and "VBIED" have similar attack patterns, since they are aimed at causing damage bypassing PPS elements of the target facility, while the "Cyber-attack" has its specific features. An analysis of the steps of a cyber-attack within an IT-OT system of a process facility and a list of the most common cybersecurity countermeasures based on the historical analysis of cybersecurity-related incidents are presented in Section 3.1.4 where the results of the in-depth analysis of the cybersecurity-related events are shown and discussed. Thus, in the following, only the SREs occurred in the Chemical&Petroleum sector and caused by physical attacks, are taken into account. In particular, 7 records reporting sufficiently detailed information allowed the identification of the specific paths through the PPS of the affected facilities that were followed by the attackers.

The Attacker Sequence Diagram (ASD) [7] was found to be a useful tool to represent physical attack patterns and to show the level of penetration reached by the attackers within the facility, as well as the most vulnerable access points exploited, revealing vulnerabilities of the PPS that need to be considered in the framework of SVA/SRA and similar techniques. The VAM-CF methodology makes use of the ASD tool in order to identify all the paths that attackers can follow to accomplish the attack, and all the barriers in place (i.e., those assembling the PPS). For a specific PPS and a specific threat, the methodology provides the identification of the most vulnerable path (this path establishes the effectiveness of the total PPS) and of the protection system upgrades [40]. In the current analysis, in order to represent more effectively the paths in a general framework, they were adapted to a reference chemical and petrochemical site and are reported in a single ASD.

The layout of the sample chemical and petrochemical facility is shown in **Figure 16-a**. An off-site area, an on-site area, buildings, a warehouse, a control room, a tank farm and a process plant are the physical areas considered in the reference layout adopted. Site fences and the manned reception with personnel and vehicle gateways are considered to separate the off-site area of the facility from the on-site area. Walls and roofs are considered to protect the buildings (including the control room), which are accessible through doors and vehicle doorways. A dike is present around the plant, that is interrupted in correspondence of a portion that is used for the entrance of personnel and vehicles. The Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) remotely connect the control room and the process plant.

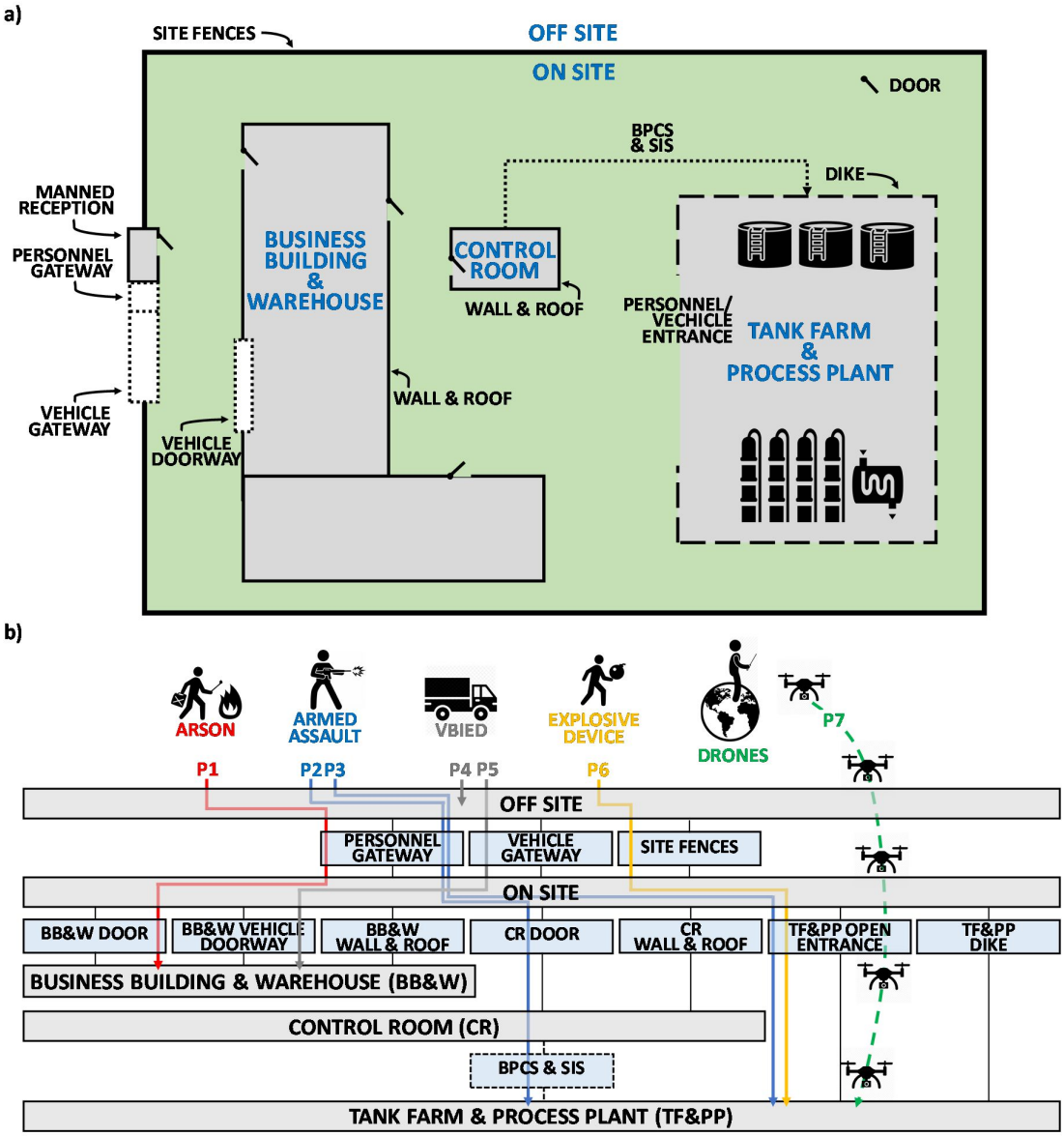

Figure 16 a) Reference layout representing the position of the different targets considered in the simplified Attacker Sequence Diagram (ASD); b) Attack patterns derived from events for which sufficient details were available, represented through a simplified ASD. Adapted from [2].

Figure 16-b shows the simplified ASD corresponding to the sample chemical and petrochemical site described above and shown in **Figure 16-a**. The main simplification introduced in the ASD shown in **Figure 16-b** consists in reporting the physical areas and the elements of the PPS without considering the respective probabilities of detection and delay times as in the complete ASDs [7], since these parameters are out of the scope of the present analysis.

As shown in the simplified ASD, the tank farm and process plant area (TF&PP) can be accessed by the attackers both directly and indirectly. Actually, in 2 cases the assailants managed to physically enter the TF&PP area through the dedicated personnel and vehicle entrance after accessing the on-site area: in one case the on-site area was accessed through the personnel gateway by opening fire on the security personnel (P3 in the ASD), while in the other case the attackers entered in the facility crossing the site fences, bypassing the manned reception (P6 in the ASD). In a further attack path, the TF&PP area was accessed indirectly

through the manipulation of the control and supervision system (BPCS and SIS) once the assailants had physically accessed the control room: in particular, the assailants entered the facility through the personnel gateway and, by threatening the employees with firearms, they gained access to the control room and forced the operators to shutdown oil pumps (P2 in the ASD). Moreover, path number 7 in the ASD (P7) shows that the process or storage equipment can also be accessed by air, and more specifically by remotely controlled drones: unlike all the other cases reported in **Figure 16-b**, in this specific attack mode the attackers may carry out the attack from a remote site, also far away from the target facility.

In two cases (P1 and P5 in the ASD), the target of the attackers was the warehouse area of the facility. In both cases the threat actors were insiders: in path P1, a former employee managed to enter with his old credentials and to access the warehouse where he triggered a fire with an improvised source of ignition (a cigarette lit). In path P5, a certified delivery driver entered the facility through the dedicated gateway and drove his light-duty vehicle (containing flammable substances) inside a closed hangar where he caused the physical explosion of the inert gas vessels contained in the hangar. Moreover, path P4 in the ASD highlights that the threat may arise from the off-site area immediately close to the facility fences: in this case the attacker did not enter the industrial site, but rather parked a vehicle containing explosives close to the external side of the fences and detonated it.

Overall, **Figure 16** may support the evaluation of the effectiveness of existing security barriers in the framework of SVA/SRA methodologies (steps 4 and 5 of CCPS methodology, step 3 of the methodology proposed by API RP 780 methodology, step 9 of VAM-CF methodology, step 4 of RAMCAP methodology) highlighting possible paths of attackers within the PPS of a facility and possible vulnerabilities. For example, in 4 out of the 7 events with more detailed information that allowed to build the simplified ASD shown in **Figure 16-b**, the attackers entered the on-site area of the target facilities through the personnel and vehicle gateways (i.e., through the site entrance). The site entrance can be crossed by insiders without any detection, as they have authorized access to the facility, while, when considering the outsiders, the main entrance can be crossed by counterfeit authorization (e.g., counterfeit badge) or by force (e.g., armed assault). Overall, the analysis of the available data indicates that the site entrance is a key element when designing the PPS of a process facility.

3.1.3.3. Final outcomes of the attacks (results from EDA)

EDA was also applied to investigate the severity of the SREs collected for the Chemical&Petroleum sector. In particular, **Figure 17-a** shows the distribution of the final outcomes that were experienced by the chemical and petrochemical facilities. Property damages and economic losses turned out to be the most frequent outcomes experienced by the affected facilities (81 incidents, 78% of the total). At least an injury or a fatality occurred in 15 SREs (14%), while a damage to environment was registered for 3 SREs (3%). Moreover, no final outcome was recorded for 3 SREs (3%), i.e., those where a near miss took place, and in 2 SREs (2%) no information was available concerning the outcomes.

Figure 17-b reports the number of injuries and fatalities associated to the SREs. In particular, 114 injuries and 41 fatalities were recorded. When compared to the data reported by Casson Moreno et al. [15], these values result smaller than those obtained in the case of pipelines for oil and gas transportation and are similar to those of energy production sector: this is due to the fact that fixed installations have a more limited extension than pipelines, together to the fact that they are generally better protected from outsider physical threats by security barriers [15]. Moreover, in facilities where hazardous substances are stored or handled, a more intense surveillance is usually in place, thus a timely activation of safety systems that may contribute to the mitigation of the consequences of the deliberate attacks can be achieved.

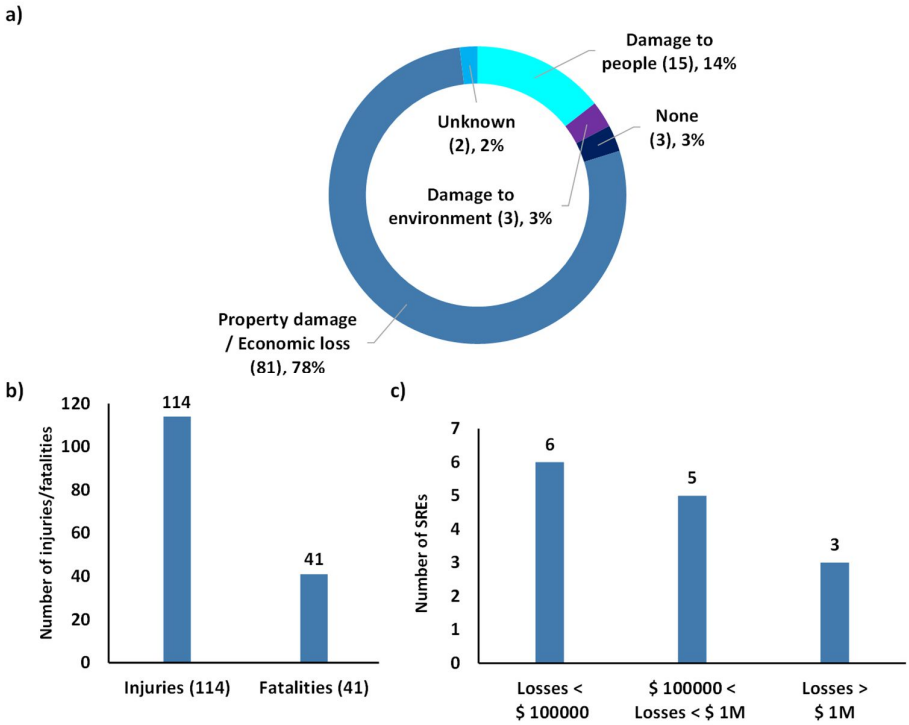

Figure 17 a) Distribution of the final outcomes experienced by chemical and petrochemical facilities (based on 104 records); b) Number of injuries and fatalities (based on 15 records); c) Number of physical security-related incidents which sufficient details to estimate the economic losses suffered by the affected facilities (based on 14 records). Adapted from [2].

More in detail, 23 fatalities and 15 injuries were directly caused by the attack modes perpetrated by the attackers, while 8 fatalities and 61 injuries were caused by the scenarios triggered by the attacks. No data were available for the remaining 10 fatalities and 38 injuries. The event with the largest number of fatalities and injuries (respectively 8 and 27) occurred in 2014 in Pakistan where attackers bombed a chemical plant, whereas the event with the highest number of fatalities (19) was recorded in 2014 in Libya, where assailants with firearms and missiles attacked the military personnel protecting a petrochemical plant [140].

Figure 17-c reports additional information about the economic losses that were suffered by chemical and petrochemical facilities associated to 14 SREs for which these data are available. In particular, 6 SREs led to losses of less than 100 k$, 5 SREs to losses between $ 100 k$ and 1 million$, and 3 SREs to losses higher than 1 million$. For example, in 1997, a warehouse of 30'000 m^2, including a refrigeration plant using ammonia and a battery charging plant, was intentionally burnt down in an act of sabotage, resulting in economic losses of over 2 million$ for the affected company [8]. Another relevant case occurred in 2015 in France, where two tanks (one containing gasoline, and the other containing naphtha) were set on fire because of a malicious act, causing damages for over 2 million $ [8].

Since only 3 cases of environmental damage were registered for the Chemical&Petroleum sector, it was not possible to obtain relevant results, as for the other final outcomes. However, a relevant incident occurred in Italy in 2016, where, as a consequence of a malicious act, 2600 tons of hydrocarbons (diesel fuel and heavy fuel oil) spilled from the pipes of a plant loading docks and poured through the sewer into the river Lambro and the river Po, causing huge environmental damages [8], confirming the possibility and potential severity of this type of consequences.

Overall, the results discussed above in terms of final outcomes, proved that impacts with severe consequences on humans (fatalities and injuries), facilities (asset damages and economic losses) and environment, can be originated by deliberate malicious attacks.

3.1.4. In-depth analysis of the cybersecurity-related events (CSREs)

An in-depth analysis of the security-related events caused by cyber-attacks (CSREs in the following) was carried out since more detailed information was available in the incident records. EDA and RCA were applied to gain different information to support SVA/SRA studies, including the cybersecurity risk assessment proposed by ISA/IEC 62443-3-2 (see Section 1.3.3). Definitions of the types of attacker, types of system infected, and of the classes of impacts used in this Section, are reported in **Table 5** in Section 3.1.1.2.

The codes of the cybersecurity-related events (CSRE#-codes) reported in the following sections refer to events reported in **Table 7**, i.e., the ones with more available details.

Table 7 Cybersecurity-related events (CSREs) with some information available on attack path, type of attacker, impacts, and implemented countermeasures. Adapted from [13].

CSRE	Attack description	Description of attacker	Impact description	Implemented countermeasures
#01	A trojan horse was introduced into the control system of the Trans-Siberian gas pipeline. The trojan ran during a pressure test, doubling the usual operating pressure by resetting the pump speeds and valve settings.	Intentional external attacker: state-sponsored group (United States). Attacker reason: political motivations.	The pressure inside the pipeline increased far beyond that acceptable to pipeline joints and welds, giving rise to an explosion (major event) that caused huge economic losses. There were no fatalities.	Not reported
#02	An unspecified type of worm was introduced by a computer programmer into one of the computer stations in an attempt to sabotage a nuclear reactor.	Intentional internal attacker: single-man disgruntled employee. Attacker reason: personal advantage.	The cooling system in one reactor broke down resulting in the reactor LSD.	Not reported
#04	A trojan horse was introduced into the control system of a Russian pipeline.	Intentional external attacker	The central switchboard of gas flows was under the control of external users for a period of time.	Not reported
#07	A rootkit was installed into the servers that were part of the Cal-ISO network system in order to take administrator-level access, and therefore total control of it.	Intentional external attacker	Two servers became infected.	A firewall separating internet and the two servers was installed.
#15	An unidentified individual (likely an insider) restarted the control room operator's LAN computer with a changed IP address, the same of an analyser computer used for continuous emissions monitoring.	Intentional internal attacker	The analyser computer locked-up as a result of the network error message due to duplicate IP addresses. The loss of signal from the analyser computer forced a plant shutdown until the network communication problem was resolved 2 hours later.	A firewall separating the analyser computer from the plant network was installed.
#16	Blaster worm entered the OT system of a chemical plant through a poorly configured firewall, and it spread by exploiting a buffer overflow vulnerability. Blaster worm was later discovered by the AV software.	Accidental attacker	Two HMI workstations became infected by the Blaster worm.	The firewall rules were tightened.
#19	A corporate user installed a software unaware that it included an unpatched version of msSQL. The PC was then connected to the Internet to access email (violation of company policy) contracting Slammer worm. The latter spread within the corporate network.	Accidental attacker	A data acquisition server became infected by Slammer worm causing the loss of some history data during server downtime.	Raised awareness of digital security issues; data acquisition servers were patched; a firewall separating the data acquisition servers from

				the corporate network was installed.
#21	MUMU worm entered the OT system of a petrochemical plant owing to a weak admin password in a HMI workstation.	Accidental attacker	A fiscal metering leak system became infected by MUMU worm and remained out of order for an unspecified number of days.	Admin passwords were tightened.
#23	Slammer worm entered the OT system of a petrochemical facility owing the fact that the corporate network and the control & supervision network shared common devices such as routers and switches and no firewall was present. Slammer was able to perform a Denial of Service (DoS) attack that produced large enough quantities of traffic to use up resources on such devices.	Accidental attacker	Traffic was intermittent between HMI workstations and DCS servers. Several PCs connected to the corporate network were also infected by Slammer worm. It took several days to track down and patch all the affected machines.	The affected servers / machines were patched; a firewall, routers and switches separating the OT system and the corporate network were installed.
#28	Slammer worm entered the OT system of the Ohio's Davis-Besse nuclear power plant. The worm began by penetrating the unsecured network of an unnamed Davis-Besse contractor, then squirmed through a T1 line bridging that network and Davis-Besse's corporate network, bypassing the firewall in place. From the corporate network, the worm spread to the control & supervision network, where it found purchase in several unpatched Windows servers.	Accidental attacker	The monitoring system became unavailable for nearly 5 hours and the process control system for 7 hours. No production was lost since both systems had redundant analogic backups that were unaffected by the worm.	Network services to document all external connections to internal network were required; the affected servers were patched; a firewall separating the OT system and the corporate network was installed; a cybersecurity management system was implemented.
#34	Sasser worm entered the OT system of a petrochemical plant owing a poorly configured firewall. The spread of the worm was favoured both by the absence of AV software in the HMI workstations and the fact that they were not patched.	Accidental attacker	Un unspecified number of HMI workstations became infected by the Sasser worm.	AV software was installed in all HMI workstations and these were all patched.
#37	During a security audit a trojan backdoor containing a keylogger and reverse tunnel to an outside website was found to be located in an HMI workstation. It is believed that the HMI was infected	Accidental attacker	One HMI workstation became infected.	Firewalls were modified in order to prevent HTTP tunneling; AV software were installed in all

	by an operator browsing external hot-mail websites (phishing attack).			devices connected to the OT system.
#38	The computer of an operator, loaded with file-swapping software, was attacked by an unspecified worm.	Intentional external attacker	Confidential data for several Japanese nuclear plants was leaked to the internet. The files contained inspection forms, reports and manuals used from 2003 to 2005.	Corporate security policies were tightened.
#44	An employee was victim of a phishing attack. The malicious email contained information claiming to be about employee benefits: it contained an attachment that released a malicious executable that gave the attackers access to the employee computer. The latter resided on the same segment as the plant controllers were located, favoring the attackers to access the OT system. The attackers gained a level of access that allowed them to control, view and modify everything related to the business.	Intentional external attacker	The corporate network was compromised after the phishing attack.	Not reported
#46	A disgruntled employee accessed and disabled the leak detection system for three oil derricks.	Intentional internal attacker: single-man disgruntled employee	The leak detection system was shutdown for a period of time.	Note reported
#50	Attackers were able to exploit vulnerabilities of the camera communication software in order to access the OT system and compromising the leak detection system, the automated pressure reliefs, the alarm servers, the input traffic from field devices and the PLCs operating on the pipeline valves. Attackers were able to pressurize the pipeline and misreport pressure values back to the control room (man-in-the-middle attack).	Intentional external attacker: state-sponsored group (Russia). Attacker reason: political motivations.	The attack resulted in an explosion, in the release of more than 30,000 barrels of oil in an area above a water aquifer, in a fire lasting more than two days, and in losses for BP and its partners of $5 million a day.	Note reported
#54	Attackers infected the network system of the Natanz nuclear power plant with Stuxnet worm. The worm consists of a layered attack against three different systems: the Windows operating system, industrial software applications that run on Windows and the software operating on the PLCs. Stuxnet was also able to misreport process variable values back to the	Intentional external attacker: state-sponsored group (United States) called “Equation Group”. Attacker reason: political motivations.	The spinning speed of thousands of centrifuges was fluctuating without the monitors detected any malfunctions, causing their damage. The uranium enrichment was stopped for about one week, causing huge economic losses.	The use of USBs was minimized; systems for Stuxnet detection and removal were installed.

	control room (man-in-the-middle attack). The infection started with an infected USB.			
#60	An unspecified type of worm was introduced into the corporate network of a petrochemical facility via an infected USB stick.	Accidental attacker	Infection of an operator panel.	Not reported
#61	Attackers infected the network system of a Saudi Aramco oil plant with Shamoon worm, aiming at stopping oil and gas production in Saudi Arabia.	Intentional external attacker: anonymous hacking group called “Cutting Sword of Justice”.	Approximately, 30,000 computers were affected by the Shamoon, which spread through the corporate network and wiped computer hard drives clean.	Not reported
#66	Attackers entered the IT system of an energy production facility by exploiting a weak password by means of a brute force attack.	Intentional external attacker	The corporate network was compromised after the brute force attacks.	Not reported
#67	The industrial espionage group Dragonfly entered the IT systems of many energy production facilities by means of infected emails (phishing attack), compromised websites and malware inserted in third-party software packages.	Intentional external attacker: state-sponsored group (Russia) called “Dragonfly”. Reason: industrial espionage.	Loss of confidential data.	Not reported
#70	Attackers entered the IT system of a water facility by means of infected emails (phishing attack). Then, once gained access to the OT system, the attackers were able to reprogram the PLCs that act on the plant devices such as valves and pumps.	Intentional external attacker: hacktivist hacking group. Reason: political, social, ideological motivations.	The levels of chemicals used to treat tap water were changed. Confidential data concerning the costumers were stolen.	Not reported
#76	The chemical company Momentive was victim of a ransomware attack.	Intentional external attacker	Files were encrypted and the corporate system was shutdown.	Not reported

3.1.4.1. Characterization and steps of a cyber-attack (results from EDA)

Foot-printing, scanning, gaining access, escalating privileges and final hacking are the well-known steps for cyber-attacks to IT systems [76].

Foot-printing and scanning allow an intentional attacker to collect as much information as possible about the target system (e.g., reachable IP addresses, authentication mechanisms, network topology, etc.), and to identify the vulnerabilities that can be exploited in order to gain the access [156,157]. The description of the recorded CSREs generally lacks information on these steps, as the details are usually unknown and/or undisclosed in public reports. Even in the well-known case of Stuxnet (CSRE#54 in **Table 7**[1]) only hypotheses are available regarding how the network system of the Natanz nuclear power plant was spied on [158,159].

Gaining access to the IT-OT network system consists of penetrating the network of the target system through its vulnerable access points. Different type of attackers (see definitions of the classes associated to "Attacker Type" reported in **Table 5**) can access the network by different techniques. Intentional external attackers obtain the necessary access information by foot-printing and scanning steps. The analysis of 8 CSREs with sufficient level of details from the database evidenced that different hacking techniques were applied in external attacks: brute force password-cracking (CSRE#66), phishing (CSRE#67) and trojan horse (CSRE#01). Four entries in the database showed that gaining remote access can also involve physical actions on the IT-OT network system, most commonly by use of infected USB (Universal Serial Bus) sticks (e.g., in CSRE#60 a USB stick connected to a computer started the spread of the malware into the network). No recorded CSRE features an unauthorized attacker physically accessing the hardware to infect the system or launch the attack (i.e., cyber-attack following a physical security breach).

Accidental attacks penetrate the IT system when they are able to exploit its vulnerabilities. For example, in CSRE#37 an operator browsing external mail websites accidentally installed a mail-based trojan backdoor on an HMI workstation.

As regards intentional internal attackers, 8 CSREs were documented in the database as caused by individuals related to the target organization (e.g., employees, contractors, etc.). These attackers took advantage of their own credentials and knowledge of the system and were able to access at least some levels of the network architecture shown in **Figure 2** in Section 1.3.3, without the need of footprinting and scanning phases. For example, in CSRE#46, a disgruntled employee accessed and disabled on purpose the leak detection system of three oil derricks by his own authentication credentials. As insiders usually have extensive knowledge of both the process and the plant, they are potentially a very critical category of attackers.

Figure 18-a shows the overall results of the analysis of the recorded CSREs with concern to the type of attacker. Intentional and accidental CSREs are found to be equally credible patterns (respectively 47 and 35 CSREs), although a slightly greater number of intentional attacks was recorded. The figure confirms that the external cyber-threat against process facilities is the most frequently reported. Nevertheless, the role of insiders is also evidenced as a possible threat (about 13% of the total CSREs recorded).

The motivation of the attacker was further investigated, collecting the available information in the event files retrieved. Only for 23 records specific information was available and reported in the specific field of the compiled database ("Description of the attacker"). As regards to the intentional external attackers, in 8 CSREs, a nation-state or state-sponsored group/organization was identified as the threat actor. Motivations included compromising, stealing, changing, or destroying information, as well as damaging the assets of the target facilities in the context of geopolitical threats. Examples of such groups/organizations include: Equation Group [160] (CSRE#54), Dragonfly [161] (CSRE#67), Winnti Group [162] (CSRE#80), Lazarus Group

[1] In the following of this paragraph, "in **Table 7**" will be omitted when reporting a CSRE#-code for the sake of repetitiveness.

[163] (CSRE#81), Cutting Sword of Justice (CSRE#61). In one incident (CSRE#70), the attackers were non-governmental activists with political, social, and ideological motivations.

A single-man intentional external attacker was instead identified as the threat actor in 5 recorded CSREs. For example, the hacker called “Dr. Chaos” is considered the actor of a power outage and service interruption of an energy production facility (CSRE#05). Similarly, the hacker called “pr0f” was able to infect the OT system of two US water treatment plants (CSRE#56 and CSRE#58) with the intent to expose vulnerabilities in critical industrial automation and control systems and show how easily they can be compromised.

In case of intentional internal attackers (i.e., insiders), only single-man attackers were recorded (8 CSREs). In the majority of cases, the attacker was a disgruntled employee (CSRE#06, CS#45, CSRE#46, CSRE#55). In a few cases, more details on the motivation of the attack are known: revenge (CSRE#53, CSRE#64) or gaining personal advantage (CSRE#02) are the two motivations that emerged as root causes of the attack. In a single case, the attacker was a supplier (CSRE#11).

Figure 18-b shows the geographical distribution of the events collected with respect to the classification on the accidentality or intentionality of the attack. The figure seems to suggest that the distributions of accidental and intentional attack patterns are not strongly influenced by geographical location, though for Asia a slightly higher percentage of intentional cyber-attacks was reported (i.e., 86%). In the case of Africa and Oceania, the percentages are not relevant, given the small number of CSREs recorded (respectively 2 and 3 CSREs).

Escalation of the privileges consists in obtaining elevated access to resources that are normally protected from an application or user (e.g., admin, root, kernel resources), in order to more deeply manipulate the system [164,165]. In the case of an attack to a system with a structure like that reported in **Figure 2** in Section 1.3.3, escalating of privileges also includes gaining access to sections of the network with major restrictions (e.g., from IT to OT system). In particular, this step is necessary to infect the OT system after access is granted to the IT system. The network of the OT system is generally a trusted network, separated from the IT system by means of network security systems (e.g., firewalls, see **Figure 2**) [166]. However, 6 recorded CSREs confirm that a network design lacking in firewalls (e.g., CSRE#28) or with a wrong firewall configuration (e.g., CSRE#16 and CSRE#34) can result in escalation of the infection spreading from IT to OT systems. In CSRE#54 (Stuxnet worm) the escalation of the privileges used 0-day vulnerabilities (i.e., unknown computer-software vulnerabilities), allowing the bypass of network security systems [167]. Attackers commonly make use of rootkits in order to take administrator-level access, increasing their privileges within the target network system (CSRE#07).

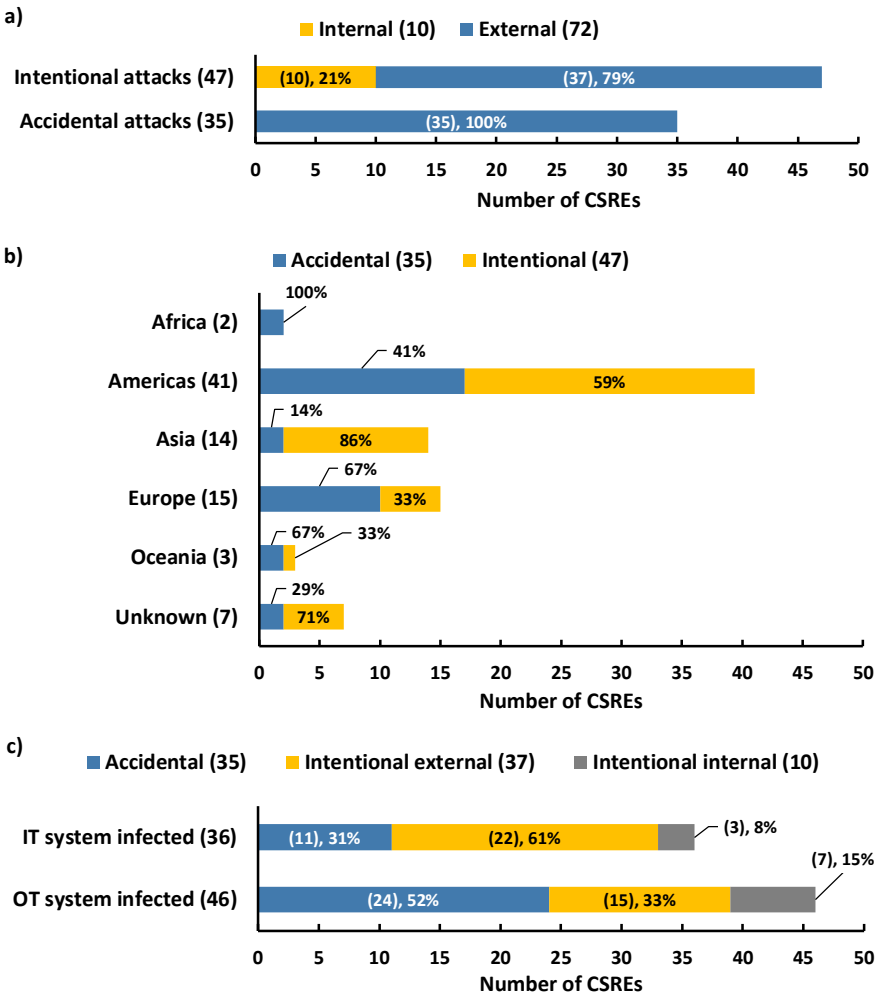

Figure 18 Distribution of the recorded CSREs: a) based on the type of attacker; b) with respect to the geographical areas; c) affected system. Adapted from [13].

The classification of the collected CSREs with respect to the type of system infected is reported in **Figure 18-c**. As shown in the figure, CSREs that affected the OT system resulted to be more than those affecting the IT system only. As an attack to the OT generally implies a former intrusion in the IT system, this result can be a consequence of a higher attention worldwide towards reporting attacks that resulted/may have resulted in physical effects in a facility. The CSREs featuring detail on the specific sub-system of the OT network affected by the attackers allowed to identify as ultimate target of the attack the control system (8 cases, CSRE#01, CSRE#02, CSRE#04, CSRE#23, CSRE#28, CSRE#44, CSRE#50, CSRE#54), the monitoring system (12 cases, CSRE#15, CSRE#16, CSRE#19, CSRE#23, CSRE#28, CSRE#34, CSRE#37, CSRE#44, CSRE#50, CSRE#54, CSRE#60, CSRE#70), and the automated safety and alarm system (3 cases, CSRE#21, CSRE#50, CSRE#46). The targeted systems suggest the possibility for the attacker not only to tamper with the physical remote-controlled devices of the plant (e.g., valves, pumps, compressors, etc.) by hacking the control system, but also to manipulate the information directed from the plant sensors to the HMI workstations located in the control room (e.g., values of process variables). In particular, the recorded CSREs evidenced cases of information made unavailable (CSRE#15, CSRE#19, CSRE#28) or, even, misreported (CSRE#54), potentially paving the way to trigger inappropriate or ineffective human control and corrective actions. As regards to the possibility of making automated safety devices ineffective, the recorded CSREs reported the deactivation of the leak

detection system (CSRE#21, CSRE#50, CSRE#46), the automated pressure relief valves (CSRE#50), and the alarm system (CSRE#50).

Figure 18-c also shows that an appreciable number of events classified as "accidental attacks" (i.e., 24 CSREs, 30% of the total), were able to affect the OT system: therefore, the infection of the control and supervision network (see **Figure 2** in Section 1.3.3) is proved to be possible also in this type of attack. A wrong configuration of the IT-OT network architecture (network topology), especially due to a low attention to security/cybersecurity issues, was tracked as a cause of these events.

The final hacking is the last part of the cyber-attack, through which impacts on the assets of the affected facility are originated. **Figure 19** shows the connection between the system infected and the impacts in selected entries of the database for which a detailed description was available. No recorded CSREs with the infection of the IT system alone resulted in impacts on the process system, confirming that in the process industry, gaining access to the Operational Technology (OT) is a distinctive feature required to achieve impacts on the physical process system (i.e., the plant). The analysis of the 5 CSREs for which more detailed information about the final hacking was available revealed some attack techniques used by the attackers in order to originate impacts on the assets of the target company: Denial of Service (e.g. CSRE#23, where attacker made the traffic intermittent between HMIs, PLCs, and SCADA systems of a petrochemical facility), Man in the Middle (CSRE#54, where signals between field sensors and control rooms were intercepted and modified in order to manipulate process parameters), and data encryption (e.g., CSRE#76, where attackers encrypted data of a chemical company and demanded payment for the release of the decryption key - ransomware attack).

Overall, the results discussed in this Section support the implementation of SVA/SRA studies in the steps addressing the characterization of the attackers (e.g., ZCR 5.1 of the detailed cybersecurity risk assessment of ISA/IEC 62443-3-2, see **Figure 3** in Section 1.3.3), providing types of attackers and possible cyber-attack paths that can be performed.

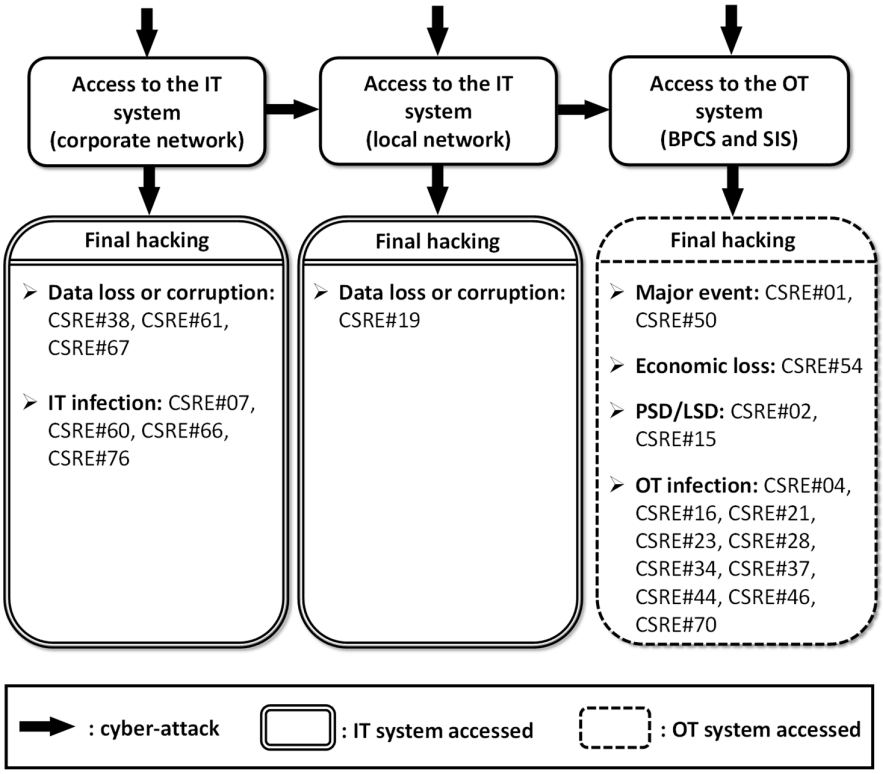

Figure 19 General steps of a cyber-attack to the IT-OT system of a process facility. The potential impacts that can be originated by a cyber-attack based on the level of access obtained by the attackers in the IT-OT network architecture is also provided (refer to **Table 7** for CSRE#-codes). Adapted from [13].

3.1.4.2. Impacts of the cyber-attacks (results from EDA)

EDA was also used to further investigate the impacts of the cyber-attacks affecting the industrial sectors of concern. **Figure 20-a** reports the distribution of the collected incidents with respect to the classes defined in **Table 5** for the itemized field "Main Impact". **Figure 20-b** reports the count of the secondary impacts recorded for CSREs belonging to the same "Main Impact" class.

The potentially most severe main impact (i.e., occurrence of a major event) is also the least frequent (only 2 CSREs recorded in the transportation of hydrocarbons by pipeline, see CSRE#01 and CSRE#50 in **Table 7**[2]). The number of recorded CSREs generally increases progressing through the defined "Main Impact" classes towards those having a lower severity. In fact, the highest number of occurrences is reported for impacts that require only access to the IT system. This can be explained by the presence of a higher number of safety and security barriers (e.g., safety instrumented functions, cybersecurity countermeasures, passive safety devices, etc.) between the attacker and the target system when access to OT system is required. Furthermore, while the IT system of process facilities is generally similar to the one of other business sectors, the OT system resorts to proprietary and therefore specific design solutions. In other words, deeper and more difficult scanning and escalating phases are required to an attacker that aims to infect the OT system, rather than the IT system only. **Figure 19** also reports the potential impacts that can be originated by a cyber-attack based on the level of access obtained by the attackers in the IT-OT network architecture of the target process facility. In the figure, reference to the CSREs reported in **Table 7** is provided for each impact class so that the reader can find more information on the incidents reporting such impacts.

[2] In the following of this paragraph, "in **Table 7**" will be omitted when reporting a CSRE#-code for the sake of repetitiveness.

No fatalities followed the two major events collected in the database that were triggered by the malicious manipulation of the BPCS and SIS. However, huge economic losses (e.g., due to business interruption and repair costs, see CSRE#01) and environmental damages (e.g., release of more than 30.000 barrels of oil in an area above an aquifer, see CSRE#50) were reported in these incidents. **Figure 20-b** demonstrates that the classes "Economic loss" and "OT infection" were associated with both major events.

Large economic losses were reported as the main impact in a significant number of cases. It should be noted that most of the incident reports provided only a verbal description of the economic losses: for example, expressions as "huge economic loss", "significant financial impact", "loss of production", "loss of revenue" were frequent.

From **Figure 20-b** it can be observed that "Economic loss" is frequently associated with a local shutdown or a process shutdown (class "PSD/LSD") causing operations outage ("PSD/LSD" was reported in 6 out of 7 cases of "Economic loss"), while in one case significant financial impacts were due to the effort (cost of 4 person-months) of repairing the SCADA system that remained infected for two weeks.

In 7 recorded CSREs the attackers induced a local or process shutdown via remote manipulation. For example, in CSRE#02 the attack resulted in the failure of the cooling system of a nuclear reactor, which triggered a shutdown. Recorded downtimes span from 30 minutes up to 1 week. **Figure 20-b** shows that the totality of these events is associated with the infection of some devices connected to the OT system (class "OT infection").

Several cases of infection of the OT (30 CSREs) did not result in major events, economic losses or LSDs/PSDs (class "OT infection"). The analysis of the descriptions of such incidents evidenced the following types of events as belonging to this class: infection of the SCADA system (23 CSREs), short term loss of plant control (3 CSREs), malfunction of the detection system of dangerous substances (3 CSREs), remote manipulation of plant devices (1 CSE, see CSRE#70 where automated control valves were manipulated). **Figure 20-b** shows that for 3 CSREs a theft or corruption of data (class "Data loss or corruption") was also reported, while for the majority of these incidents (25 CSREs) the secondary impact "IT infection" was also associated. For 5 CSREs the secondary impacts were not reported.

Most of the CSREs, however, only affected the IT system. "Data loss or corruption" was recorded in 14 CSREs. These incidents featured sensitive data theft (e.g., plant historian data) and data loss (e.g., CSRE#61). The majority of such attacks resulted also in technical inconveniences at IT level (class "IT infection", such as server crashes, PC locks, file encryption, etc.): for example, CSRE#61 reports the infection with the Shamoon worm of approximately 30,000 computers of the Saudi Aramco oil plant and the removal of data in several servers.

In case of infection of the IT system, occurrence of technical inconveniences only at IT level (class "IT infection") resulted to be the most frequent impact. Since this is the least severe impact class considered, no secondary impacts were associated the CSREs reporting this class (thus "IT infection" is not reported as "Main impact" class in **Figure 20-b**).

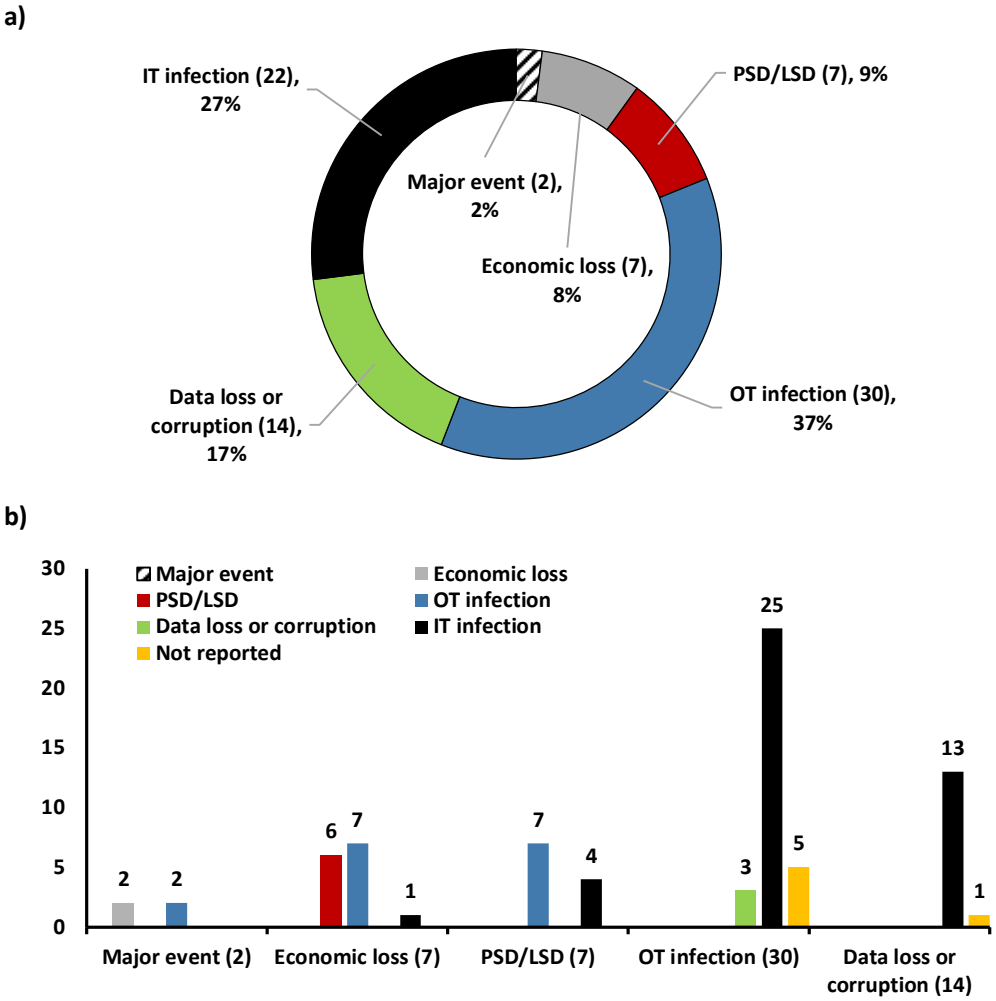

Figure 20 a) Main impacts recorded for the reported CSREs; b) Secondary impacts recorded for CSREs belonging to the same "Main Impact" class. Adapted from [13].

Figure 21 shows the distribution of the "Main Impact" classes with respect to the industrial sectors. It can be observed that the distribution is roughly similar to the distribution of the total number of CSREs recorded for the considered sectors. A few exceptions can be easily explained considering the peculiarities of the sector: e.g., water/wastewater treatment is expected to have fewer major events and economic losses than other sectors, due to the lower quantities of hazardous materials handled and to the lower revenues.

The similarity in the profile of impacts confirms the initial choice of the present study to include sectors similar to the process industry in the analysis of the database, providing a broader basis for the analysis.

Overall, the results discussed in this Section support the implementation of SVA/SRA studies in the steps addressing the identification of the scenarios that can be triggered by cyber-attacks to the IT-OT network system (e.g., ZCR 5.3 of the detailed cybersecurity risk assessment of ISA/IEC 62443-3-2, see **Figure 3** in Section 1.3.3).

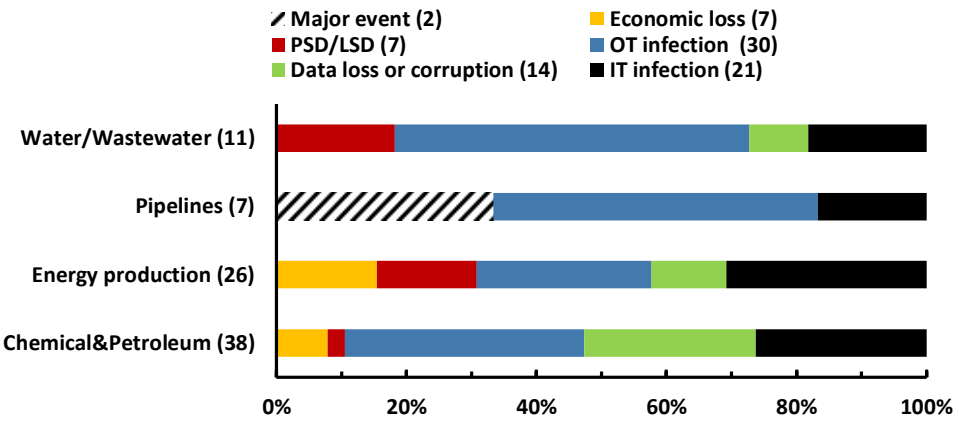

Figure 21 Distribution of the "Main Impact" classes with respect to the industrial sectors considered in the present analysis. c

3.1.4.3. Countermeasures and lessons learnt

The CSREs for which a more detailed description was available allowed some insights on the key role that security countermeasures may have in preventing such events. Countermeasures are implemented for reducing the cyber-risk. The definition of countermeasures and their requirements is necessarily system-specific and requires a detailed analysis of threat sources (motivation and capabilities), vulnerabilities and potential impacts (see e.g., ISO/IEC 27005). Part 3-3 and part 4-2 of ISA/IEC 62443 series of standards provide guidance on types of countermeasures applicable to industrial automation and control systems (IACSs).

The list of countermeasures reported in the above standards was systematically cross-checked with the information present in the "Description" field of the developed database for each CSRE recorded. If the countermeasure was present in the attacked system, its failure or success in contrasting the attack was noted. Given the limited detail on description of the systems infected, no discussion of the security level provided by the countermeasure and its role in risk reduction with reference to specific types of attackers is possible. In the following, the countermeasures that resulted playing a key role in contrasting recorded cyber-attacks to the IT-OT system of a process facility (see **Figure 22**) are listed and described. Reference is made to the relevant CSREs as described in **Table 7**.

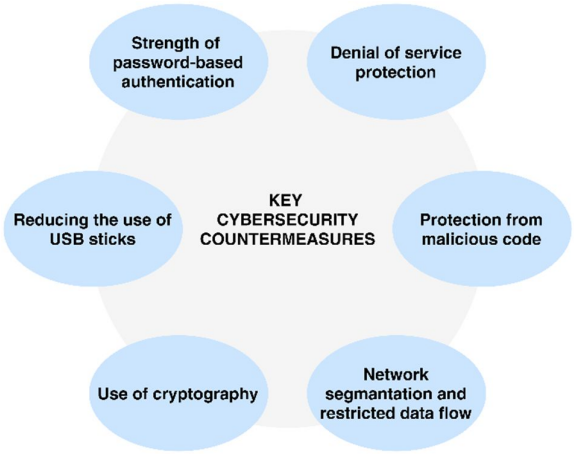

Figure 22 Cybersecurity countermeasures that resulted to have a key role in contrasting recorded cyber-attacks. Adapted from [168].

Network segmentation and restricted data flow

Network segmentation and restricted data flow are part of the more general defense-in-depth strategy and provide for the separation between non-control system networks and control system networks (e.g., the corporate network and the control and supervision network), allowing communication only through properly controlled and configured devices (e.g., firewalls, switches and routers). Moreover, the addition of a DMZ (demilitarized zone, i.e., an isolated network which contains services accessible both from external unprotected networks, and from internal terminals of the company) provides a segmentation of the internal network with improved restricted data flow. CSRE#28 in **Table 7**[3] was caused by a worm that started from penetrating the unsecured network of an unnamed contractor, then squirmed to the company corporate network. The firewall in place was ineffective, as it was bypassed by an unprotected T1 line bridging the two networks. From the corporate network, the worm further spread to the control and supervision network where it infected several machines. This narrative shows the importance of network segmentation and restricted data flow countermeasure: a properly installed firewall between the IT and the OT networks would have prevented the infection and/or reduced the severity of the impacts (infection confined to the original network). Such a measure was part of the corrective actions implemented after the incident.

The Slammer infection described in CSRE#23 was similarly due to a poor network architecture (network topology). Also in this case, firewalls, routers and switches were installed as corrective actions after the incident, reducing the risk of future OT infections. Other CSREs supporting this conclusion are CSRE#15 and CSRE#07. CSRE#44 reports a case of phishing attack: a malicious email contained an attachment that allowed the attackers to gain access to the company network and then to infect the OT system. The incident would not have occurred if a DMZ containing email servers had been in place.

Protection from malicious code

Verification of the intended operation of security functions shall be provided for the components of the network. For example, the security rules of firewalls should be periodically verified by appropriate audits. The Blaster infection of the OT system reported in CSRE#16 was due to a poor firewall configuration. In CSRE#37 the firewall filtering from IT network to OT network was bypassed by the attackers with HTTP tunneling hacking technique through port 80. In both cases the implemented corrective action reported in the records of the database concerned the verification and strengthening of the security rules.

This category of countermeasure also provides for the installation and proper testing of antivirus (AV) software suitable for the prevention, detection and removal of malwares. The Sasser infection of HMI workstations reported in CSRE#34 would have been avoided or, at least, detected by AV software installed on such devices. Similarly, in CSRE#37 a security audit evidenced several components connected to the OT system without AV software, as well as an infection in an HMI workstation located in the control room.

Strength of password-based authentication

Password-based authentication is typically utilized by many components connected to the computer network (both IT and OT). The password strength shall be enforced according to internationally recognized and proven password guidelines (e.g., long alphanumeric passwords with special characters). In CSRE#21 the MUMU worm entered the OT system of a petrochemical plant and infected the fiscal metering system thanks to a weak administrator password in an HMI workstation. A weak password was also evidenced in CSRE#66, allowing for a successful brute force password-cracking attack of the system.

[3] In the following of this paragraph, "in **Table 7**" will be omitted when reporting a CSRE#-code for the sake of repetitiveness.

Denial of service protection

Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a Denial of Service (DoS) event. For example, this can be obtained by patching and updating software without impacting the essential functions of high availability systems. Slammer infection of the data acquisition server reported in CSRE#19 was initiated by a corporate user installing an unpatched software in a PC and violating company policy by connecting the machine to the Internet. The infection could had been prevented if the corporate laptop had a version of SQL software with a patch fixing the buffer overflow vulnerability exploited by the Slammer worm. Lack of patching was also found in several servers of the Ohio's Davis-Besse nuclear power plant (CSRE#28), causing the spread of Slammer in its OT system.

Use of cryptography

Components shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations. CSRE#38 describes a theft of confidential information (inspection forms, reports and manuals for several Japanese nuclear plants) due to an unspecified worm attacking the computer of an operator. Encryption of such data on the attacked computer would have significantly reduced the severity of the impact from the theft.

Other

The use of USB sticks was found to pay a role in the spreading of malware in two recorded CSREs. The first is the well-known case of Stuxnet (CSRE#54): in that case the network system of the Natanz nuclear power plant started from an infected USB stick of an unaware employee that was plugged into his/her PC located in the office. The second is the incident CSRE#60: also in that case, the infection of the IT system of a petrochemical facility started from an infected USB stick.

Use of USB devices in the network system (both IT and OT) shall be restricted by appropriated policies. Part 4-2 of ISA/IEC 62443 also suggests implementing protection from malicious code in USB host accesses.

The analysis of the CSREs confirms that the success of cyber-attacks to the computer network system of process facilities can be prevented or mitigated by general and not sophisticated countermeasures as those suggested by standards on security of OT systems. The analyzed CSREs evidence the key role of these measures for the accidental attacks, where footprinting and scanning phases specifically aimed at bypassing the implemented countermeasures are not performed. For intentional cyber-attacks, the presence of multiple countermeasures (e.g., defense-in-depth) is as well an important defense strategy, as the attackers must perform complex attack patterns to generate impacts on the target systems. Finally, it should be remarked that an integrated design of hardware and software countermeasures may allow for a more robust protection of the system.

Overall, the results discussed in this Section support the implementation of SVA/SRA studies in the steps addressing the identification of the vulnerabilities present in the IT-OT network system and of possible countermeasures (e.g., ZCR 5.2 and ZCR 5.8 of the detailed cybersecurity risk assessment of ISA/IEC 62443-3-2, see **Figure 3** in Section 1.3.3).

3.2. Analysis of the security events occurred in the offshore Oil&Gas industry and similar sectors

This Section presents a study aimed at gathering knowledge and lessons learnt on security threats affecting the offshore Oil&Gas industry and similar sectors. Therefore, the results obtained from this study help answer Research Question 1 (see Section 2.1 and **Figure 4**). In particular, the study consists in the development and the related structured analysis of a database collecting 2222 security-related events (SREs) affecting offshore Oil&Gas industrial facilities, including transportation at sea. A specific subset of 99 SREs occurred in the offshore fluid production sector was extrapolated and more in-depth detailed and analyzed.

3.2.1. Method

The method applied for the analysis of past security-related events (SREs) occurred in offshore Oil&Gas industrial facilities is the same described in Section 3.1.1 to which the reader is referred. In the following, the details on the specific data sources investigated, the inclusion criteria adopted, and the description of each class of itemized fields, are reported.

3.2.1.1. Retrieval of past security-related events

Data were gathered from different sources: scientific literature (Kashubsky [62]), web archives, and specific open-source databases reporting data on industrial accidents/incidents and near misses (as defined by Rathnayaka and co-workers [136]) such as the Maritime Safety Information [169], Global Terrorism Database (GTD) [140], and the Repository of Industrial Security Incidents (RISI) [142].

Other databanks reporting accidents/incidents were investigated as well, but no SREs matching the two inclusion criteria were identified. These sources include: Dechema ProcessNet [137], E.U. Concawe [138], E.U. EGIG [139], eMARS [8], Infosis ZEMA [141], U.S. DoT PHMSA [143].

Two criteria were used to include security-related events in the database:

i. the event should originate as a result of a malicious act aimed at interfering with normal operations (not necessarily with the intentionality of triggering a major accident such as a fire or explosion);
ii. the event involves an industrial facility belonging to one of the following sectors: offshore drilling and exploration, offshore fluid production, offshore logistics, transportation.

The sets of keywords used for querying the data sources were different for the investigation of the open-source databases (and differentiated by groups of databases) with respect to the investigation of the open literature. In addition, the mining for physical security- versus cybersecurity-related events required different sets of keywords. **Figure 23-a** shows the complete list of keywords that were used for querying the data sources, divided into 7 groups (the reader is referred to Section 3.1.1.1 where they are described).

Starting from these groups of keywords, the total sets of keywords for querying the open-literature to search both for cybersecurity-related events and for physical security-related events, as well as for querying all the databases forehead mentioned (with the exception of GTD, RISI, and the dataset reported by Kashubsky), can be generated by taking one keyword per group and solving the trees reported in **Figure 23-b** by using the rules of Boolean algebra. Since GTD, RISI, and the dataset reported by Kashubsky (2011) collect security-related events only, records in these two databases were simply found by selecting the industrial sectors of interest.

When looking for security-related events in the open literature, the keywords were translated into several European languages (i.e., English, Italian, French, German, and Spanish), while each database was investigated also in its native language. Only English terms are reported in **Figure 23-a**. Due to the high

number of open-sources exploited, particular attention was posed in avoiding double counting of events. Specific checks were carried out considering the date, country and type of facility involved in the event.

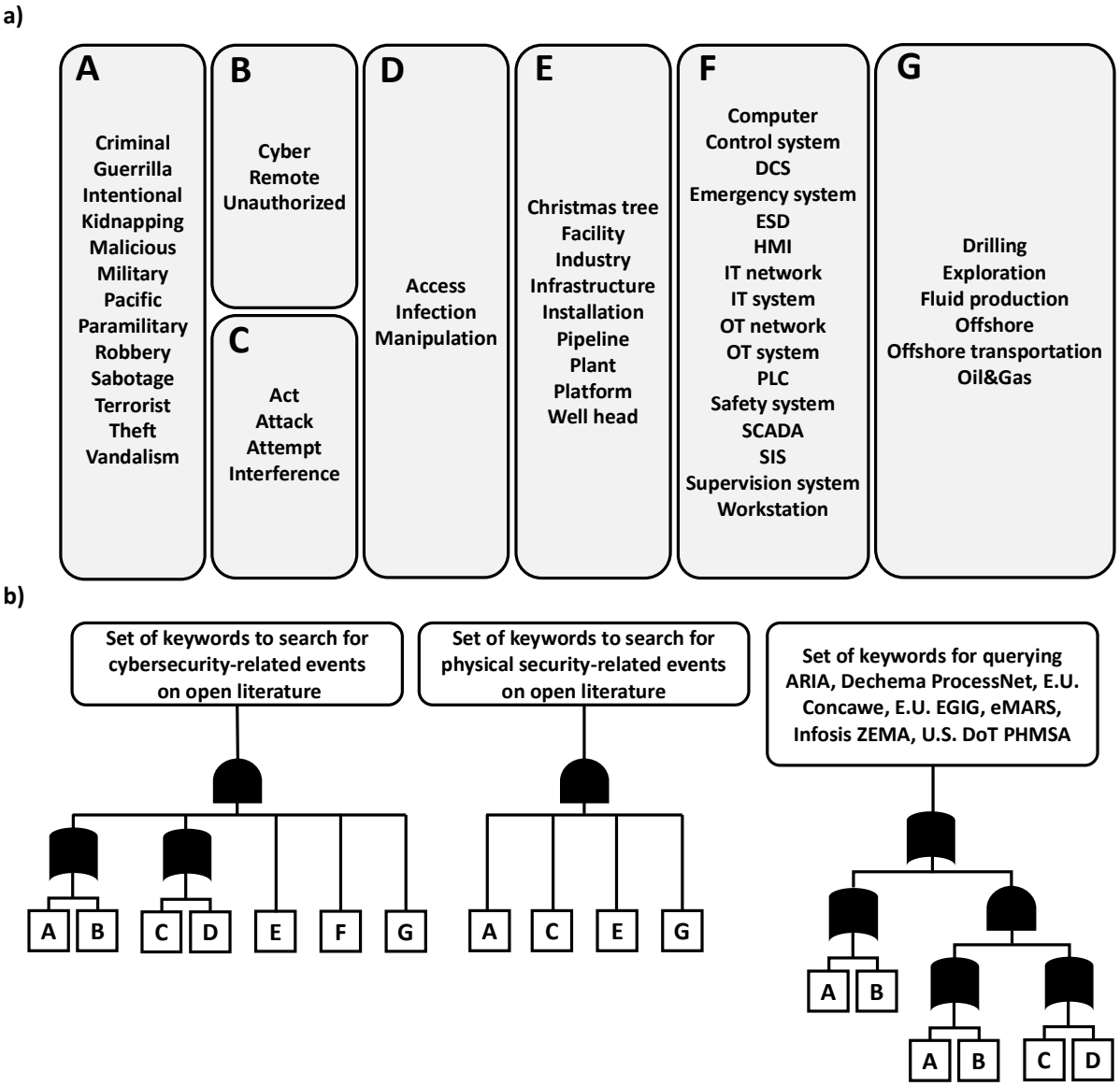

Figure 23 a) Complete list of keywords (in English) used for querying the data sources, divided into 7 groups labelled from A to G; b) Method based on Boolean algebra used to define the sets of keywords employed to query each different category of data source.

3.2.1.2. Structured database of past security-related events

A dataset of 2222 security-related events (SREs) was populated (see the structure in **Figure 24**).

Each entry in the database consists in the compilation of free text fields and itemized fields. Free text fields allow retaining general details concerning the record (ID entry number, date, year, country, continent, description, notes, source, links), while itemized fields help describe unambiguously a certain characteristic of the event. **Table 8** reports the definitions of the itemized fields considered for the total number of the SREs, i.e., "Industrial Sector" and "Security Threat". The availability of more detailed information on the events that occurred in the offshore fluid production sector allowed to consider three additional itemized fields for these events, i.e., "Attack Mode", "Final Scenario", and "Final Outcome", all described in **Table 9**.

Figure 24 Structure of the database collecting the retrieved SREs occurred in the offshore Oil&Gas industry and similar sectors.

Table 8 Definitions of the itemized fields "Industrial Sector" and "Security Threat" used in the collection of all the SREs. Codes are used in the Venn diagrams for the sake of brevity.

Code	Class	Definition
		Industrial Sector
IS1	**Offshore drilling and exploration**	Exploration of sites suitable for future offshore production purposes.
IS2	**Offshore fluid production**	Production of oil and/or gas from offshore wells.
IS3	**Offshore logistics**	Transportation of personnel or equipment via water. It includes offshore platforms transported by tugs or other means.
IS4	**Transportation**	Transportation of hazardous materials via road, rail, water.
IS5	**Other**	Industrial sector not described by the previous definitions.
		Security Threat
ST1	**Insider threat**	The attacker is an insider, i.e., an individual who normally has authorized access to the assets of the company (e.g., employee, contractor, business partner, vendor, etc.). The motivation is related to working dissatisfaction or possibility of gaining personal advantage (e.g., stealing items or materials). Insider threat refers both to physical security and cybersecurity.
ST2	**Military / Paramilitary organization**	An interference in normal operations or damage to people, equipment or installations perpetrated by a regular or irregular army. In the latter case, however, the organizational structure, tactics, training, subculture, and often function are similar to those of a professional military organization.
ST3	**Outsider cyber threat**	Events collected in this category are characterized by an attack, via cyberspace, targeting the IT-OT system of the target facility with the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. Usually, the malwares used by the attackers were not tailored for industrial control systems, but they breached the company network protection compromising operations.
ST4	**Pacific interference**	Events collected in this category are characterized by an attack mode aimed to disrupt normal operations defined by nonviolent means of protesting.
ST5	**Robbery/Kidnapping**	Criminal groups or individuals attacking facilities with the intent of stealing cash or valuable items or extorting money by kidnapping or hostage taking. It includes both events of attempted attacks that caused an accident and cases of intrusion without reaching the target.
ST6	**Sabotage**	Events collected in this category are characterized by an attack mode aimed to disrupt normal operations, but not defined in their threatening agent, as well as in their driving motivations.
ST7	**Theft of hazardous material**	Criminal groups or individuals attacking facilities with the intent of stealing hazardous material. It includes both events of attempted theft that caused an accident and cases of intrusion without reaching the target. Theft of goods (not hazardous materials) are not included.
ST8	**Terrorism / Guerrilla operation**	Terrorist organizations or criminal groups, highly capable, well organized and equipped, focused on targeting a facility with the aim of causing a high-impact event, not only in terms of casualties, but also on media. Operations performed by guerrillas are included.

ST9	**Unknown**	An interference in normal production activities has been achieved via certainly intentional acts, but no more details were given concerning attackers or motivations of the act. This category refers both to physical security and cybersecurity.

Table 9 Definitions of the itemized fields "Attack Mode", "Final Scenario", and "Final Outcome" used in the collection of the SREs occurred in the offshore fluid production sector. Codes are used in the Venn diagrams for the sake of brevity.

Code	Class	Definition
		Attack Mode
AM1	**Aircraft impact**	Aircraft impact aimed to release hazardous substances or damage/destroy important parts of the installation.
AM2	**Arson**	Incendiary attacks.
AM3	**Deliberate interference with or w/o aids**	Deliberate acts involving simple operations without the use of instruments, or deliberate interference using tools and aids that are present on site, or prepared destruction of installation parts by force using heavy tools.
AM4	**Armed assault**	An armed attack that involves people with guns or other carrying weapons.
AM5	**Grenade rocketing**	An attack that consists in the shooting of missiles launched at distance by a rocket launcher or by remotely controlled drones.
AM6	**Explosive device**	Use explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks
AM7	**WBIED**	Water Borne Improvised Explosive Device. An attack that consists in an improvised explosive device placed and detonated inside a boat or vessel.
AM8	**Vessel impact**	Vessel impact aimed to release hazardous substances or damage/destroy important parts of the installation.
AM9	**Unknown**	The information available do not provide details on the attack mode.
		Final Scenario
FS1	**Release**	Scenario consisting in the discharge of a chemical from its containment, i.e., the process and storage equipment in which it is kept, without any further consequence such as an explosion or a fire.
FS2	**Explosion**	Scenario consisting in a physical and/or chemical explosion.
FS3	**Fire**	Scenario consisting in a pool fire, jet fire, fireball, flash fire, or flame.
FS4	**Shootout**	Scenario consisting in a gun battle between armed groups, or between one armed and one unarmed group.
FS5	**Seizing of workers**	Scenario during which hostages are taken among the workers in the facility, or during which workers are kidnapped.
FS6	**Stolen goods**	Goods of workers, cash or equipment belonging to the facility, including hijacked vessels, helicopters or other transportation means are stolen by the attackers.
FS7	**Operation shutdown**	Production and/or operation interruption.
FS8	**Pacific occupation**	Presence of unauthorized people without major interaction with process/assets.

FS9	**Loss of process control/monitoring**	Scenario consisting in the physical or cyber interference with the OT system (software and hardware), without the occurrence of a release of hazardous substances, a fire, or an explosion.
FS10	**Near miss**	Scenario not resulting in an actual one such those reported in this Table, but the attack perpetrated by the attackers has the potential to do so.
FS11	**Other**	Scenario not described by the other definitions.
	Final Outcome	
FO1	**Asset damage / Economic loss**	Physical and economic damages due to loss of an asset for the affected facility, whether it is a loss of production capability, loss of equipment and property, including loss of sensitive data. Loss of life is not included.
FO2	**Damage to environment**	Damages to the ecosystems due to air and/or water pollution, or land contamination.
FO3	**Damage to people**	Injury or fatality.
FO4	**Damage to reputation**	Damage to the reputation of the Company affected with potential impacts to the ability of the Company to sustain business position.

3.2.1.3. Structured toolbox applied for the analysis of the database

A set of complementary synergic tools was used to carry out a structured analysis of the populated database, with the aim of characterizing the attacks, the threats, the attackers, the scenarios generated by the attacks, and the outcomes of the attacks, thus providing data and results useful to support SVA/SRA studies, and in particular the one proposed by API RP 70 and API RP 70I which are specific for the offshore Oil&Gas operations.

In particular, **Figure 25** shows the framework built for data analysis and the features and aim of each of the specific tools applied: Exploratory Data Analysis (EDA) [145], Correspondence Analysis (CA) [146], and Root Cause Analysis (RCA) [149], all described in Section 3.1.1.3 to which the reader is referred. Each tool, providing a specific piece of information, contributes to build an unprecedented, detailed representation of the threats, the scenarios, and the attackers involved in security-related events affecting offshore Oil&Gas installations.

The following set of events have been investigated:

- total number of SREs (see Section 3.2.2);
- SREs collected in the offshore fluid production sector (see Section 3.2.3).

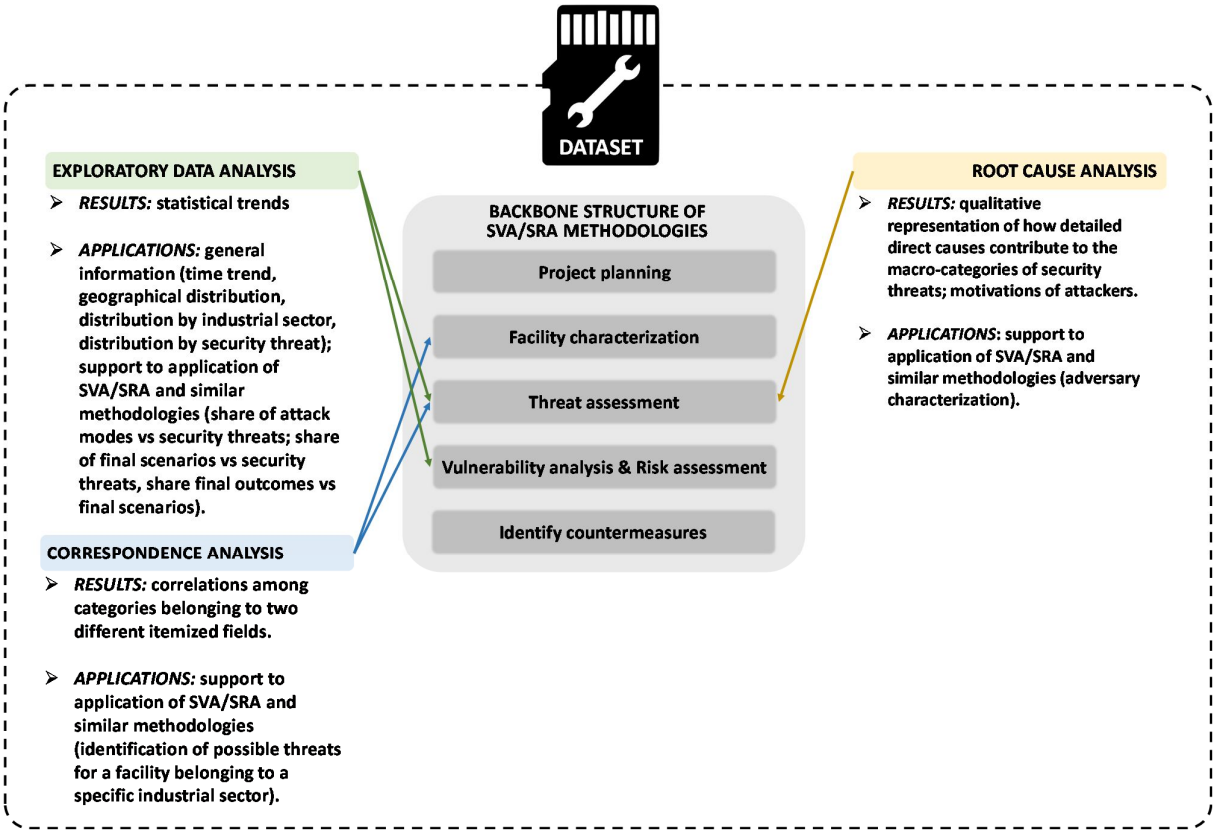

Figure 25 Framework and scope of dataset analysis and link with backbone structure of SVA/SRA methods.

3.2.2. Results from the analysis of the total number of SREs

3.2.2.1. Time trend and geographical distribution (results from EDA)

To investigate the trend over time and the geographical location of the SREs recorded, Exploratory Data Analysis was applied. **Figure 26-a** shows the quinquennial time trend of the SREs collected in the database. Prior to the year 2000 only 36 SREs were recorded, justifiable by an increased attention to the practice of reporting security-related incidents after the "9/11" terrorist attacks in New York. For the following years, the time trend shows an average of 530 SREs per 5-year period, with a peak of 680 SREs recorded in the 2010-2014 period, confirming that security of offshore Oil&Gas operations is a real issue to be taken into account in the management of all the risks.

The geographical distribution of the incidents recorded is showed in **Figure 26-b**. Most of the incidents took place in Asia (1292 SREs, 60%) followed by Africa (722 SREs, 32%), South America (112 SREs, 5%), North America (47 SREs, 2%), Europe (25 SREs, 1%), and Oceania (4 SREs, < 1%). Eighteen (18) of the SREs recorded could not be classified by continent as they occurred on a body of water between two continents, such as the Bab el-Mandeb strait between Africa and Asia, or in open ocean. The geographical regions most affected resulted to be the Strait of Malacca (between Indonesia and Malaysia) and the Gulf of Guinea (mainly Nigeria), due to strategic location for international maritime shipping routes, in conjunction with a complex piracy issue, compounded in opportunistic attackers, organized criminal syndicates, and terrorist groups [170]. Nigeria, and in general the Gulf of Guinea, is characterized by violent and frequent piracy and guerrilla attacks [171] affecting both the high number of offshore installations present in the region and ships used for transportation of hazardous materials or to support offshore operations.

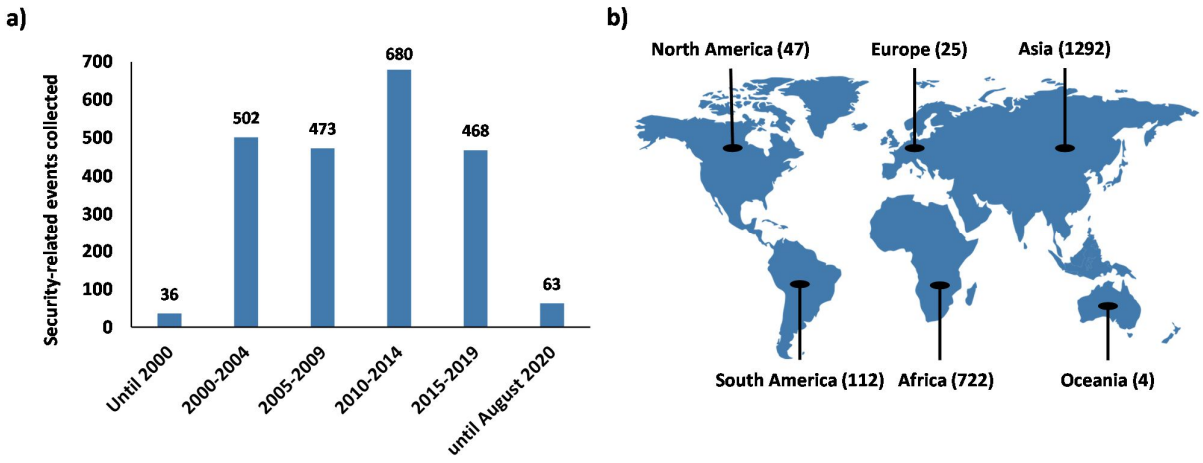

Figure 26 a) Time trend of the SREs collected; b) Geographical distribution of the SREs collected (18 SREs are of unclassifiable location). Adapted from [16].

3.2.2.2. Security threats and industrial sectors (results from EDA and CA)

In order to investigate how the collected SREs are distributed with respect to both the industrial sectors and the security threats, Exploratory Data Analysis and Correspondence Analysis were applied.

In particular, **Figure 27-a** shows the distribution of the collected SREs by the industrial sectors considered in the analysis (see definitions in **Table 8**). The transportation of hazardous materials (via road, rail, water) resulted the most affected by deliberate malicious attacks (1979 out of 2222 SREs, 89%), followed by the offshore fluid production sector (100 SREs, 5%), the offshore logistics sector (87 SREs, 4%), and the offshore drilling and exploration sector (28 SREs, 1%).

Similarly, **Figure 27-b** shows the distribution of the collected SREs with respect to the security threats considered in the analysis (see definitions in **Table 8**). Robbers and kidnappers with the intent of stealing cash or valuable items or extorting money by kidnapping or hostage taking, resulted the most recorded type of attackers with 1472 out of 2222 SREs recorded (89%) reporting this threat. High-capable and well-organized terrorist organizations and criminal groups aimed at causing high-impact events are the second most recorded security threat (86 SREs, 4%). The latter is followed by the theft of hazardous material (e.g., the crude oil) with 38 SREs collected (2%), and by pacific interferences (33, 1%). The categories “Sabotage”, “Insider threat”, and “Outsider cyber threat” collect less than 10 SREs each. However, almost a quarter of the incidents could not be categorized by security threat, and thus were labeled as “unknown”. These situations are commonly encountered in failed assaults to ships, such as the attempted boarding of the Liberian-flag tanker Louise on December 6th, 1999, where unidentified persons opened fire on the tanker after failing to board it [169], or in unclaimed attacks perpetrated by unknown assailants, such as the one occurred in Nigeria on June 10th, 2008, when fire was opened by unknown perpetrators upon an oil facility [62].

The preponderance of SREs occurred in the transportation sector can be explained by the fact that ships are vulnerable to opportunistic attacks perpetrated by disorganized criminals, which are more common than organized, large-scale attackers. This also justify why theft of personal belongings or equipment (i.e., “Robbery/Kidnapping” security threat) is more often encountered than theft of hazardous substances (i.e., “Theft of hazardous material” security threat) such as in the case of syphoning of oil from tankers or well-heads, which requires a high level of knowledge and skill.

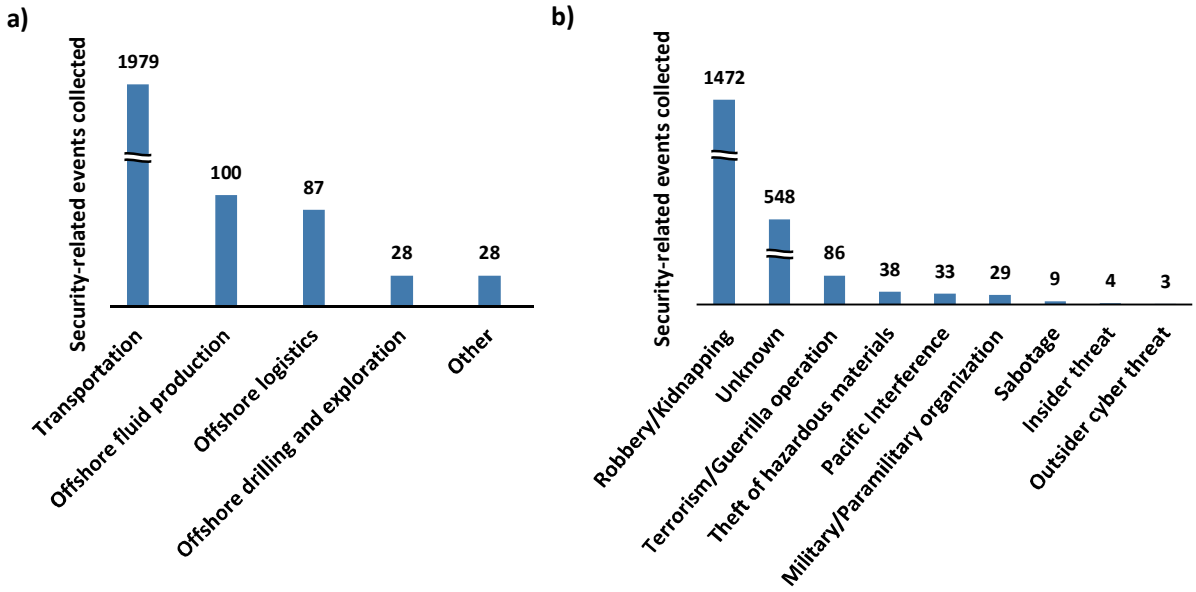

Figure 27 a) Distribution of the collected SREs with respect to the industrial sector; b) Distribution of the collected SREs with respect to the security threat. Adapted from [16].

In order to identify any possible correlations among security threats and indus trial sectors, Correspondence Analysis (CA) was carried out. Refer to **Table 6** in Section 3.1.1.3 where the key elements of CA are reported.

Figure 28 shows the 2D-map of the (CA) displaying the security threats in principal coordinates (i.e., those deriving from the row profiles, see **Table 6**) and the industrial sectors in standard coordinates (i.e., as unit vectors). It is important to remark that the map contains the projections of the real points in the best-fitting 2D-plane (see reduction of dimensionality in **Table 6**): this means that some information is missing. The information lost is represented by the "inertia" (or "total inertia", in percentage) that measures how "far" the row profiles are from their average profile: the higher the inertia, the less information is lost. In this case, the percentage of inertia shown in the map is 97% and, consequently, the information lost is 3%, meaning that the correlations that can be obtained from the analysis are reliable.

A high degree of correlation is displayed by couples of points that are distant from the origin of the graph (which represents the average behavior of the dataset), and that form acute angles with it, together with a high cross-count of events belonging to the points considered [146]. In particular, from **Figure 28**, the transportation sector results strongly correlated with the "Robbery/Kidnapping" security threat (red shaded in the 2D-map), and weakly correlated with the theft of hazardous materials (yellow shaded in the 2D-map). This means, for instance, that ships transporting hazardous material are those which are mainly affected by acts of robbery and kidnapping, and that the trend of robbery and kidnapping strongly differs from the average behaviour of all the threats with respect to the industrial sectors. In other words, there is a correlation.

In the same way (see **Figure 28**), the offshore fluid production sector resulted to be weekly correlated (yellow shaded in the 2D-map) with acts of terrorism and guerrilla. This can be justified by the fact that terrorist organizations are more attracted by fixed installations rather than by ships due to their strategic value and inherent hazard that can be exploited to trigger incidents with severe consequences on people, property, and surrounding environment (i.e., major events).

The outlined distribution of the security threats with respect to the industrial sectors (**Figure 28**) supports the identification of the more likely threats that can affect an industrial installation belonging to a specific industrial sector. It provides information about the threat history to be investigated in order to evaluate the

attractiveness to deliberate attacks. This applies to specific steps of many common SVA/SRA methodologies, as step 1 ("Potential Threat") of the SRA proposed by standards API RP 70 and API RP 70I which are specific for the offshore Oil&Gas operations. For example, opportunistic attacks (robbery/kidnapping acts) to ships transporting hazardous material shall be considered when a SVA/SRA is performed for such type of transportation infrastructures.

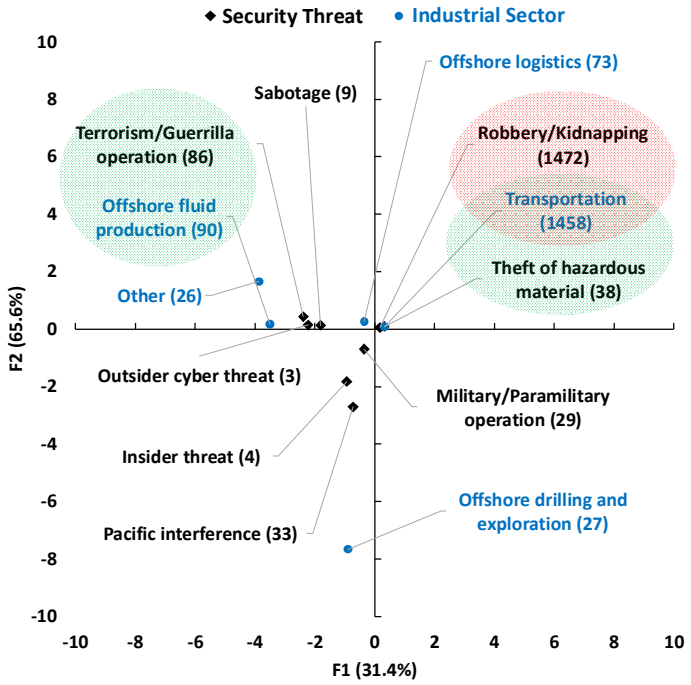

Figure 28 2D-map reporting the results of Correspondence Analysis for the couple of itemized fields "Security Threat" and "Industrial Sector" (total inertia of the map is 97%). Adapted from [16].

3.2.3. In-depth analysis of the SREs collected for the offshore fluid production sector

An in-depth analysis concerning the attack modes, the reasons/motivations behind the attacks, the final scenarios triggered by such attacks, and the final outcomes suffered by the attacked offshore infrastructures was carried out for the offshore Oil&Gas fluid production sector as it is within the scope of the present research (focus on offshore and onshore plants handling and/or storing hazardous materials) and the fact that more detailed information was available in the incident records. EDA and RCA were applied to gain different information in support of SVA/SRA studies. Definitions of the classes of attack modes, the final scenarios, the final outcomes used in this Section are reported in **Table 9** in Section 3.2.1.2.

3.2.3.1. Attack modes triggering final scenarios (results from RCA and EDA)

Figure 29 shows the Ishikawa diagram (or fishbone diagram for its shape) obtained from the application of RCA. It displays the security threats as main rib branches, types of attackers as secondary rib branches, and reasons/motivations behind the attacks as tertiary rib branches. Numbers in brackets refer to the number of SREs in the dataset reporting the information of interest.

As regards "Terrorism/Guerrilla operation" security threat, acts performed by criminals (attackers belonging to syndicates or similar illegal organizations), guerrillas (attackers belonging to small independent group taking part in irregular fighting), terrorists (attackers belonging to an organization designated of terrorist matrix in at least one country all around the world), and regionalists/nationalists (attackers belonging promoting ideals of regionalism/nationalism), were reported. Financial discontent and gaining political

power and influence were found the reasons driving the attacks performed by guerrillas, together with an act of strength in the context of an ongoing conflict. The latter characterizes also acts performed by terrorist organizations, along with motivations related to religious extremism, territorial autonomy, and obtaining political power and influence. Regionalists or nationalists, instead, were found driven by monetary gain, environmental awareness, political decentralization and territorial autonomy.

Regionalists and nationalists turned out to be attackers performing also acts of robbery and kidnapping. These acts were also carried by criminals, popular protesters, activists, and armed militants, mainly driven by financial discontent and monetary gain.

Acts of pacific interference were found to be performed by popular protesters and people belonging to non-profit organizations, especially motivated by the promotion of environmental awareness. Similarly, a hostile nation army in an act of show of strength turned out to be a potential attacker type in case of "Military/Paramilitary organization" security threat.

When "Insider threat" is assessed, instead, disgruntled employees (i.e., employees dissatisfied with their job) moved by financial discontent, were reported. Given the fact that insiders generally have knowledge of both the process and the platform equipment, they turn out to be a very critical threat, able to cause severe damages.

Finally, cyber-criminals targeting the IT-OT network system through cyber-attacks aimed at corrupting and/or destroying information were found to be a possible attacker type belonging to "Outsider cyber threat" security threat.

Overall, the results shown in **Figure 29** support the implementation of SVA/SRA studies in the steps addressing the characterization of the attackers (e.g., step 1 of the SRA proposed by API RP 70 and API RP 70I), providing types of attackers for each security threat, together with possible reasons/motivations behind the attacks.

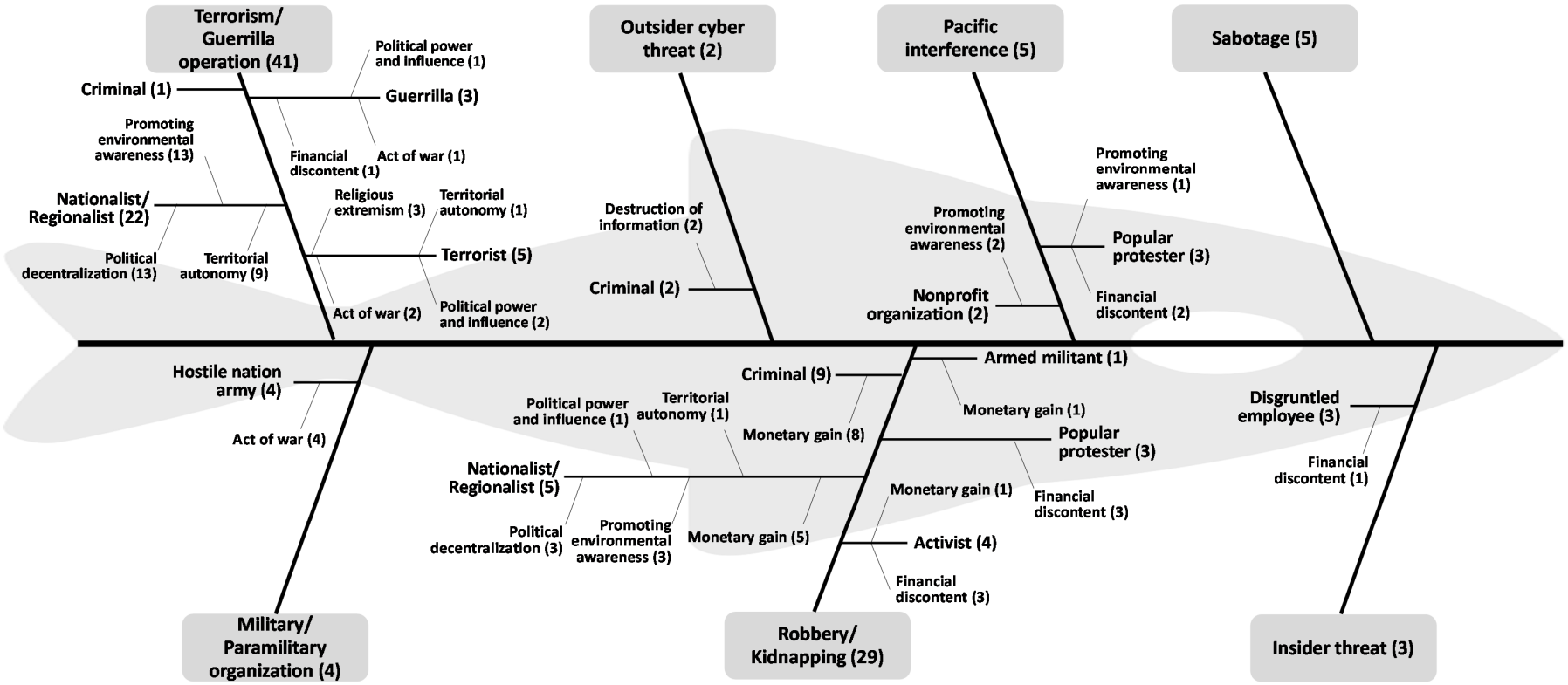

Figure 29 Ishikawa diagram (fishbone diagram) reporting security threats, type of attackers, and the reasons/motivations behind the attacks in main, secondary, and tertiary rib branches respectively.

Figure 30 shows the Venn diagram obtained from the application of EDA. It displays the share of the attack modes (AMs) with respect to the security threats considered in the present study. Venn diagrams were chosen as they allow to display the overlap between the categories investigated, which is typically present when the attack modes are assessed due to the fact that attackers may perform more than one AM in a single attack.

In particular, with reference to **Figure 30**, most of the attackers belonging to "Terrorism/Guerrilla operation" security threat performed attacks consisting in armed assaults (AM4, 18 SREs) and in the detonation of explosive devices (AM6, 16 SREs): 4 SREs among them reported the adoption by the attackers of both the AMs (overlap). Therefore, AM4 and AM6 are deemed very likely attack modes that shall be considered in the context of SVA/SRA of an offshore Oil&Gas fluid production facility. However, there is historical evidence of other types of attacks performed by terrorists and/or guerrillas such as the detonation of large amounts of explosives contained inside vessels (AM7, 3 SREs), grenade rocketing (AM5, 2 SREs), and deliberate interferences with or without the use of aids (AM3, 2 SREs).

Almost all the SREs recorded for the "Robbery/Kidnapping" security threat consisted in armed assaults (AM4, 25 SREs), one of which also reporting an incendiary attack (AM2, 1 SRE). For this reason, AM4 shall be considered as a likely attack mode when this security threat is assessed in the context of SVA/SRA.

Only grenade rocketing (AM5, 3 SREs) and the use of explosive devices (AM6, 3 SREs), even simultaneously (overlap of 2 SREs), were recorded in the case of "Military/Paramilitary organization" security threat, confirming that attackers belonging to this threat are well-equipped and potentially able to cause damages with severe consequences (e.g., major events).

In the case of "Outsider cyber threat" and "Pacific interference" security threats, given their inherent nature, only deliberate interferences (AM3) were recorded (respectively 2 and 5 SREs); while both deliberate interferences (AM3) and armed assaults (AM4) were recorded for "Insider threat" and "Sabotage".

Overall, the results shown in **Figure 30** support the implementation of SVA/SRA studies in the steps addressing the characterization of the attackers (e.g., step 1 of the SRA proposed by API RP 70 and API RP 70I), providing possible attack modes for attackers belonging to a specific security threat.

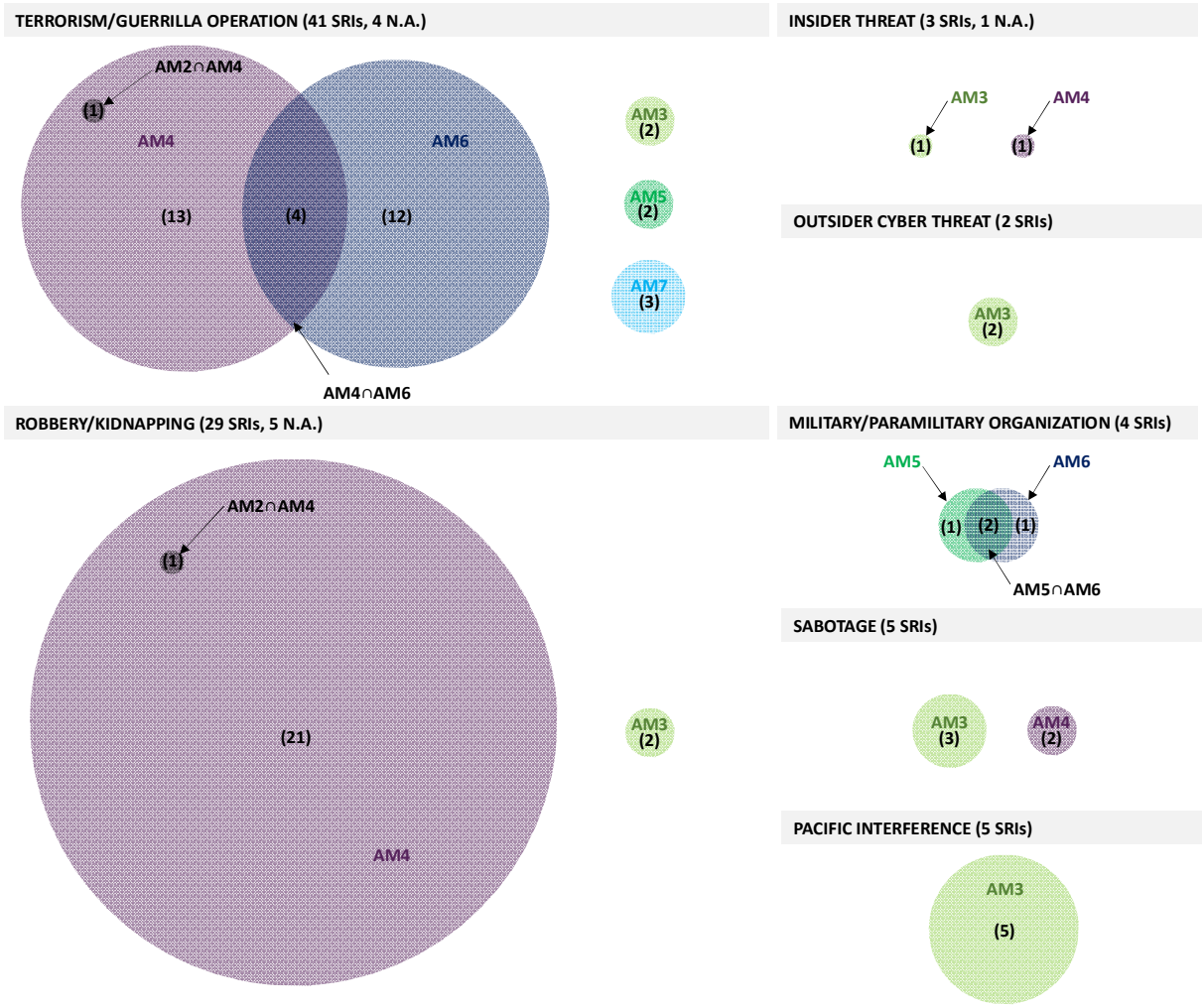

Figure 30 Venn diagrams displaying the share of the attack modes (AMs) with respect to the security threats. AM-codes are reported in **Table 9**.

Figure 31 shows the Venn diagram obtained from the application of EDA. It displays the share of the final scenarios (SCs) with respect to the security threats considered in the present study. Analogously to the analysis of the attack modes, Venn diagrams were chosen in order to show the overlap between the categories of final scenarios as more than a SC may be triggered by a single attack.

In particular, **Figure 31** shows that the most common observed scenarios that followed attacks performed by terrorist organizations or guerrilla operations are the physical explosion (FS2, 7 SREs), the shootout (FS4, 13 SREs) and the operation shutdown (FS7, 10 SREs), with a little overlap between them (see **Figure 31**). Nevertheless, cases of releases of hazardous substances (FS1, 1 SRE), of seizing of workers (FS5, 4 SREs), of stolen goods (FS6, 4 SREs), and of near misses (FS10, 3 SREs) were also recorded, together with a scenario labelled as "other" (FS11, 1 SRE).

In the case of "Robbery/Kidnapping" security threat, almost the totality of the records reported scenarios of shootouts (FS4, 6 SREs) and seizing of workers (FS5, 22 SREs), with overlap with stolen goods (FS6, 4 SREs) and operation shutdowns (FS7, 7 SREs). As expected, due to both the reasons/motivations and the attack modes performed by this type of attackers (see discussion above and **Figure 29**), no major events (from FS1 to FS3 as defined in **Table 9**) were recorded.

When the category of insiders is assessed, it is worth considering separately the cyber-insiders from the ones who do not interfere with the IT-OT network system of the target facility. In the latter case, seizing of workers (FS5, 2 SREs) was recorded, while in case of cyber-attack, a loss of process control and monitoring (FS9, 1 SRE) was suffered by the affected offshore Oil&Gas fluid production facility.

Only loss of operations control and supervision (FS9, 2 SREs) followed the cyber-attacks performed by outsider cyber attackers. Nevertheless, as shown and discussed in Section 3.1.4 (see also Iaiani et al. [100]), also major scenarios are possible when the OT system is remotely or physically malicious manipulated (e.g., induced over-pressurization of equipment leading to a breach and consequent release of the hazardous substance contained inside).

On the contrary, both releases (FS1, 1 SRE), physical explosions (FS2, 2 SREs) and fires (FS3, 1 SRE) (i.e., the major event scenarios) were recorded as a direct consequence of attacks performed by attackers belonging to “Military/Paramilitary organization” security threat, along with shootouts (FS4, 2 SREs) and operation shutdowns (FS7, 1 SRE). Generally speaking, given the similarity in the attack modes, it is not surprising that these scenarios turn out to closely match the ones registered for “Terrorism/Guerrilla operation” security threat.

As expected in case of attackers performing pacific interferences, operation shutdowns (FS7, 2 SREs) and physical occupations of the platform (FS8, 3 SREs) were reported in the records of the incidents, while in case of sabotage, scenarios labelled as “other” (FS11, 1 SRE) and production shutdowns (FS7, 3 SREs) followed the attacks. A near miss (FS10, 1 SRE) was also recorded.

Overall, the results shown in **Figure 31** support the implementation of SVA/SRA studies in the steps addressing the identification of the scenarios triggered by the attackers, as well as those addressing the evaluation of the consequences (to people, property, reputation, and surrounding environment) for each scenario considered (e.g., step 1 and step 2 of the SRA proposed by API RP 70 and API RP 70I), providing possible final scenarios for each security threat considered in the analysis.

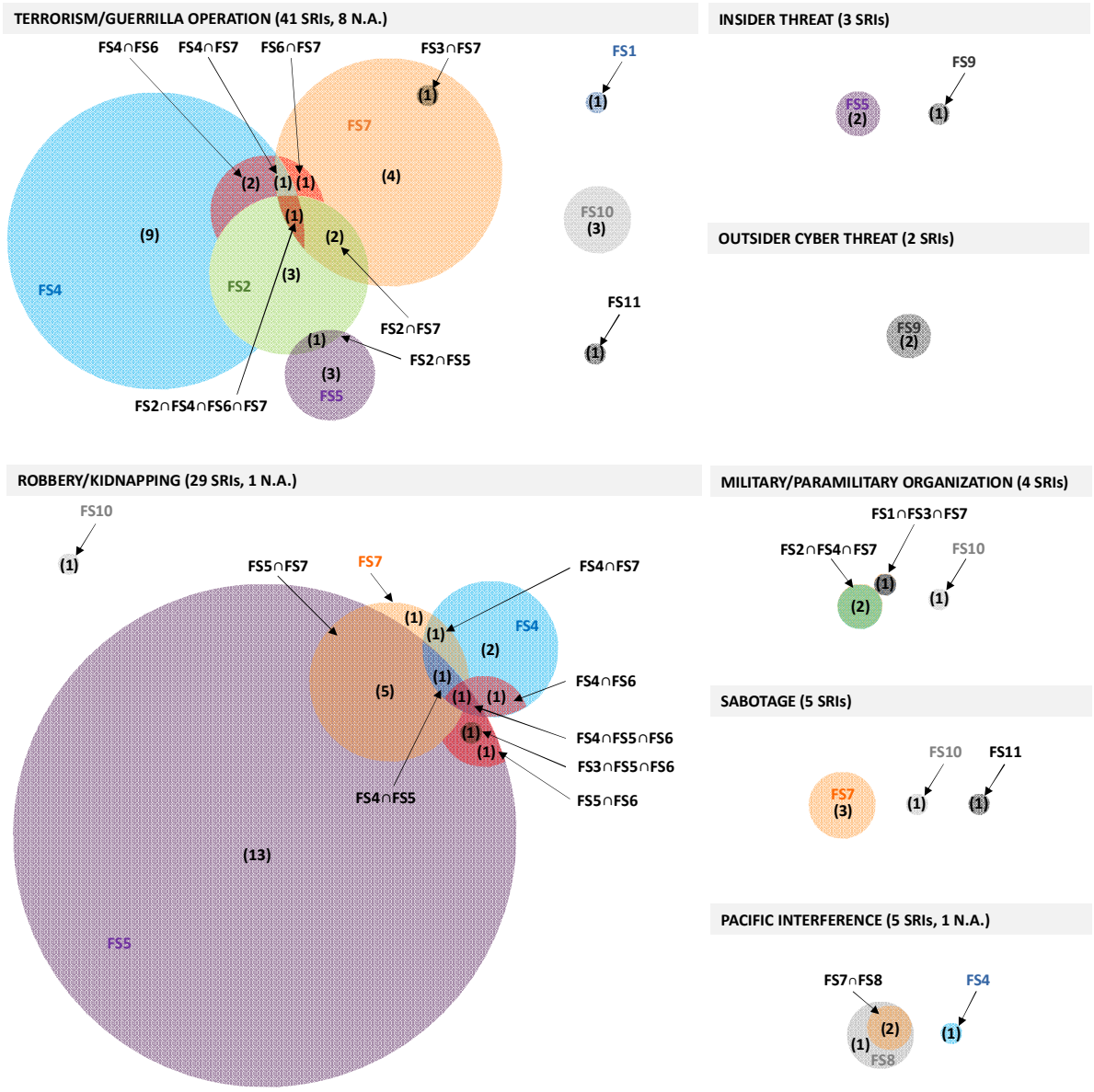

Figure 31 Venn diagrams displaying the share of the final scenarios (FSs) with respect to the security threats. FS-codes are reported in **Table 9**.

3.2.3.2. Attack paths related to physical security threats (results from EDA)

The information provided in this Section was obtained by analysing the incident descriptions reported in the respective database records. The AM-codes reported in the following description are described in **Table 9** in Section 3.2.1.2.

Overall, with the exception of aircraft impacts (AM1) and vessel impacts (AM8) which were not recorded in any of the collected SREs, and the cases of incendiary attacks (AM2) for which no information was available to better detail the attack (e.g., information on the specific means used by the attackers), all the other AMs were in-depth characterized.

In case of deliberate interferences with or without the use of aids (AM3), four different paths were found: the first consisted in the threatening of people who were manning the platform so that they initiated emergency procedures interfering with normal operations (e.g., process shutdown leading to production

outage); the second consisted in a false attack notification (also in this case emergency responses were started); the third consisted in a cyber-attack targeting the IT-OT network system of the offshore Oil&Gas fluid production facility; and the fourth in the physical occupation of the platform (occupation time ranged from couples of hours to couples of days).

The use of hand-held firearms (both handguns and rifles) covers almost the totality of the cases of armed assaults (AM4) that were recorded. In a single case attackers made use of a grenade launcher, which is a weapon that fires specially-designed large-calibre projectiles, often with explosive, smoke or gas warhead. The latter case, along with the shooting of equipment using automatic or semi-automatic rifles, is particularly critical due the higher weights and velocities of bullets with respect to those commonly suitable for handguns [172,173], which make them able to penetrate equipment deeper.

On the other hand, when the shooting occurred at long distance (i.e., attackers did not access the platform, AM5 – grenade rocketing), gunshots coming from both air (military aircraft) and water (warship) environments were recorded, resulting thus potential attack patterns, especially in hostile areas (e.g., warzones). No information on the specific weapon used was available in the reports of the incidents.

When attacks involving explosives (AM6) are considered, the use of military dynamite was reported. These dynamite-based explosives are safe to handle with high energy density and a long shelf life, generally adopted by well-equipped attackers such as militia, armies and terrorist organizations. No homemade explosives (less efficient, but more easily achievable) such as ANFO (Ammonium Nitrate – Fuel Oil) or TATP (Triacetone Triperoxide Peroxyacetone) were found in the records. In a single incident, a system for remote activation of the bomb (unknown explosive material) was reported, and due to its complexity, also this case is expected to be adopted by well-equipped attackers.

Particularly interesting is the case of Water Borne Improvised Explosive Device (AM7). In fact, two patterns were found: the first consisted in a suicide attack as attackers directly triggered the explosive and died because of the induced explosion, and the second consisted in a boat controlled and detonated remotely. The latter attack pattern is particularly critical due to the absence of personnel on board to interact with in order to interrupt the advance (e.g., warning from Coast Guard or Navy).

Overall, the information provided above supports the implementation of SVA/SRA studies in the steps addressing the characterization of the attackers (e.g., step 1 of the SRA proposed by API RP 70 and API RP 70I), providing possible attack paths for each attack mode considered in the present analysis.

3.2.3.3. Final outcomes of the attacks (results from EDA)

It is important to underline that, most of the incident records did not report detailed information on the final outcomes suffered by the attacked offshore Oil&Gas fluid production facilities, and in case of economic losses, no quantitative data was available. However, some statistical information was provided by EDA application, and shown herein.

In particular, **Figure 32** reports the distribution of the final outcomes with respect to the final scenarios considered in the present analysis. All the major event scenarios (i.e., release, explosion, fire) caused asset damages and economic losses to the company owning the damaged installation. Moreover, in the specific case of fires and explosions, also damages to people (both injuries and fatalities) were recorded. Environmental damages were also reported in case of releases of hazardous substances.

Asset damages and economic losses were found to be common final outcomes also in case of attacks causing non-major event scenarios such as seizing of workers, stolen goods, and operation shutdown. Clearly, given the absence of a loss of containment of hazardous material, no environmental damages followed these scenarios. As regards damages to people, instead, they were recorded for shootouts and seizing of workers. However, unlike scenarios such as fires and explosions which are potentially able to damage people by

themselves, these are not capable to do so, but the attacks causing these scenarios involve the use of firearms and/or physical actions on people with the potential of hurting them. Only reputation damages were registered in case of pacific physical occupations.

Overall, the results shown in **Figure 32** support the implementation of SVA/SRA studies in the steps addressing the evaluation of the consequences (to people, property, reputation, and surrounding environment) for each scenario considered (e.g., step 2 of the SRA proposed by API RP 70 and API RP 70I), providing possible final outcomes for major and non-major scenarios triggered by deliberate malicious attacks.

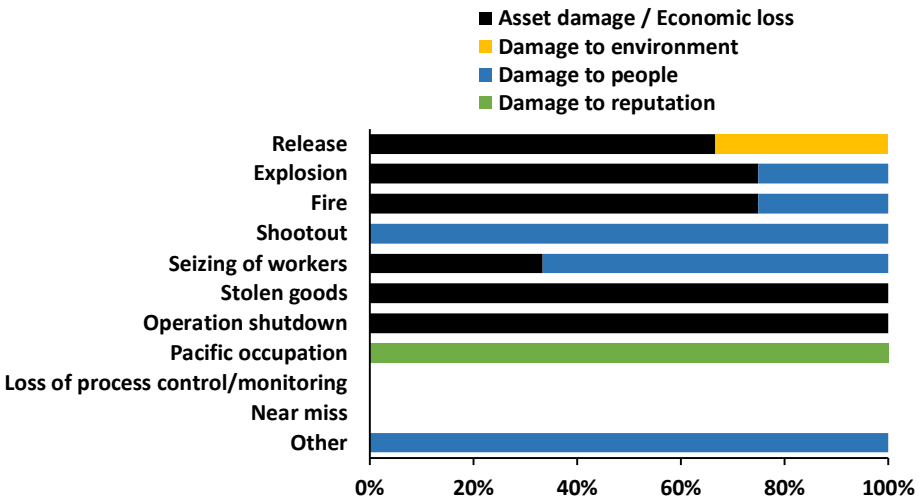

Figure 32 Distribution of the final outcomes with respect to the final scenarios considered in the present analysis.

4. Development of methods for the identification and mitigation of cyber threats to process plants

The studies described in this Chapter are aimed at supporting hazard identification in SVA/SRA studies (in particular the SRA approach provided by standard ISA/IEC 62443-3-2) with respect to cyber threats (interferences through the IT-OT network system).

4.1. Overview of PHAROS and POROS methodologies

This Section provides an overview of the two methodologies developed in order to support cyber-risk identification (e.g., ISA/IEC 62443-3-2) in chemical and process facilities, as well as in the offshore Oil&Gas industry. Therefore, these methodologies contribute to answering Research Question 1 and Research Question 2 (see Section 2.1 and **Figure 4**).

In particular, PHAROS (Process Hazard Analysis of Remote manipulations through the cOntrol System) is a methodology aimed at the identification of the critical events originated from process equipment (major accidents such as material and/or energy releases, eventually resulting in fires, explosions and toxic cloud dispersions) that can be triggered through a malicious manipulation of the BPCS and the SIS. Similarly, POROS (Process Operability analysis of Remote manipulations through the cOntrol System) is aimed at the identification of the security events that may lead to the plant arrest (outage) and consequent interruption of productivity for a certain period of time (downtime) caused by a malicious manipulation of the OT system, and therefore it addresses also operability issues.

The output of the PHAROS and POROS methodologies includes the identification of the set of manipulations of the BPCS and SIS through which a security-related event can be initiated and the effective safety barriers (procedural, active, inherent and passive barriers) that can prevent it. The two methodologies aim to address part of the risk identification step foreseen by the risk assessment framework introduced by standards ISO/IEC 27005 and ISA/IEC 62443-3-2. Actually, even if the methodologies are qualitative, the output information is suitable to support the quantitative or semi-quantitative methods used in the steps of assessment of consequences and of assessment of likelihood. Examples of methods that can use input information from POROS include the approach for likelihood estimation proposed by the German DIN VDE V 0831-104 [174], the CyberPHA developed by Cusimano et al. [60], the scenario-based approach developed by Gertman et al. [84], and the safety/security risk analysis approach using cyber bow-ties developed by Hashimoto et al. [59].

Application of PHAROS and/or POROS methodologies may be based on preliminary cyber-risk identification carried out with information provided by the analysis of past cybersecurity-related events (see Section Section 3.1.4). This information includes the characterization of potential attackers, the definition of the class of impact that can be generated, and the possible extent of consequences. However, systematic assessments of the link between malicious manipulations of the BPCS and SIS are required as cyber-attacks to the OT system of process facilities and offshore Oil&Gas facilities are rare events, and thus it is possible that some specific features of the BPCS and SIS of the facility analysed may lead to unprecedented events when they are manipulated.

Figure 33 shows the integration of PHAROS and POROS with the “detailed cybersecurity risk assessment workflow” of ISA/IEC 62443-3-2 (see also Section 1.3.3). With particular focus on the analysis of the process system part of the plant (see **Figure 2** in Section 1.3.3), PHAROS and POROS provide the information needed for the characterization of the impacts potentially originated from the malicious manipulation of the BPCS

and the SIS (ZCR 5.3), for the evaluation of the unmitigated and mitigated likelihood (ZCR 5.4 and ZCR 5.8) and for the assessment of additional countermeasures or design modifications (ZCR 5.12).

The two methodologies focus on the response of the physical process system to malicious manipulation of the BPCS and SIS. Hence, they are based on the assumption that the attacker successfully managed to infect the IT-OT network system of the target system by overcoming any IT-OT defence barrier and, therefore, is able to impart any instruction. This assumption clearly portraits a worst-case scenario, as effective access of the attacker to all the devices of the target system may be limited by IT countermeasures (e.g., presence of suitably configured firewall between IT and OT systems) as analysed by the standard ISA/IEC 62443.

PHAROS and POROS are systematic, qualitative and formally rigorous methodology of process schemes and should be performed by a team with knowledge of the process plant system, the control system and the loss prevention system. As for HazOp and HazId analyses [19,97], a typical team includes a team leader, a secretary, a project engineer, a process design engineer, an instrumentation and control engineer, and a safety engineer. Given the initial assumption on full access of the attacker to the IT-OT system, only generic IT skills are required in the team. The application of the methodologies is possible since the front-end design phase.

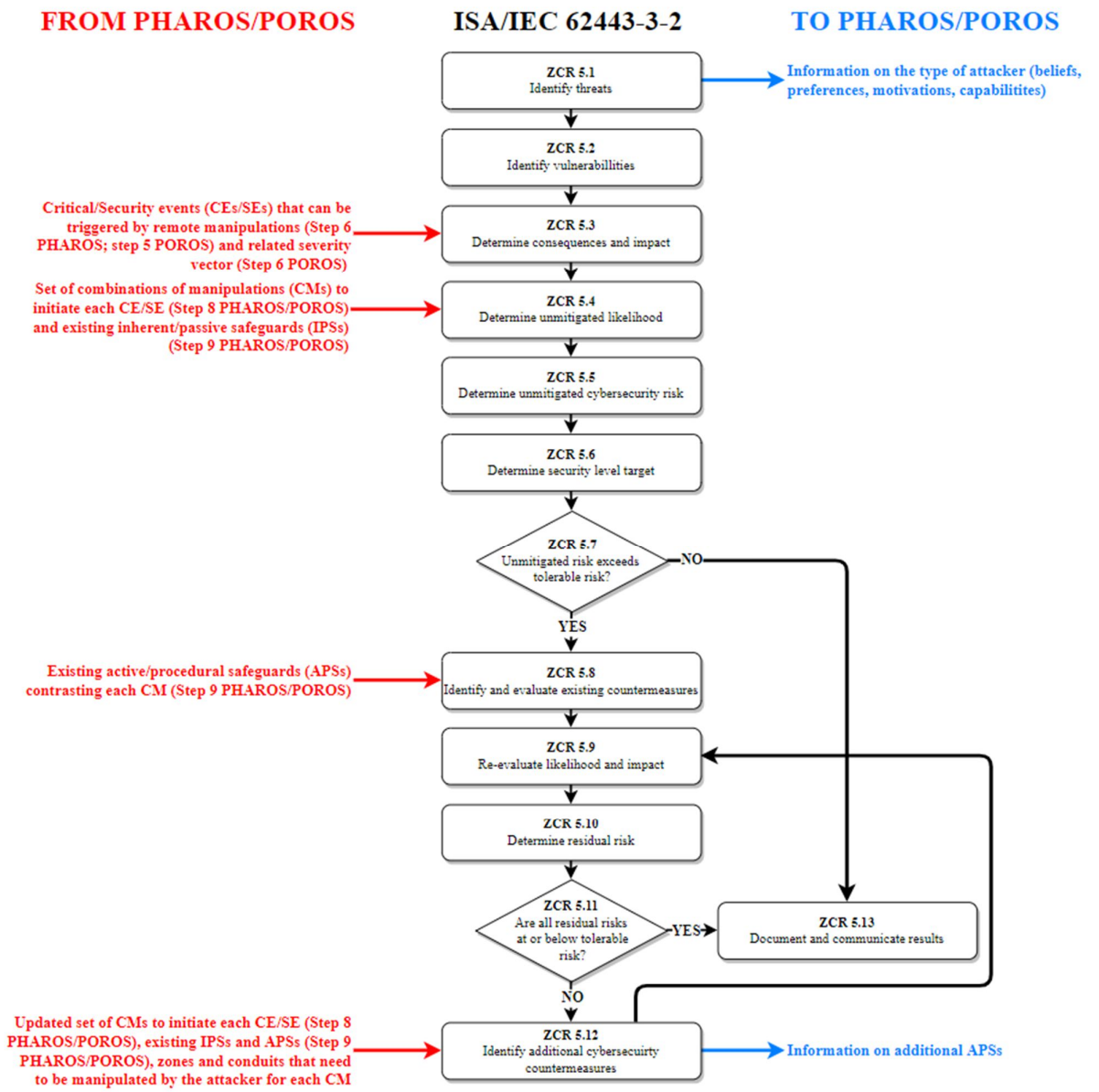

Figure 33 Integration of PHAROS/POROS with the "detailed cybersecurity risk assessment workflow" of ISA/IEC 62443-3-2. Adapted from [100].

Figure 34 shows the conceptual model of the attack as considered by the methodologies. An attacker pursuing a goal based on his/her beliefs, preferences and motivations, aims at causing an undesired event in a plant (i.e., a critical event (CE) for PHAROS such as a major event; a security event (SE) for POROS such as a production shutdown). He/she exploits his/her capabilities of control over the BPCS and SIS systems and his/her knowledge of the system to remotely initiate a physical mechanism (mechanism of action, MA) leading to such CE/SE. An example is inducing a LSD (local shutdown) by rising the liquid level in a process separator. The MA is achieved by manipulating the remote manipulable components (RMCs) in the plant (e.g., valves, motors, etc.) according to a certain pattern. The remote manipulation (RMs, e.g., set point change) of a RMC occurs through a manipulative element (ME) (e.g., the PID controller of the BPCS) and results in a local consequence (LC) on the physical plant (e.g., valve closed). Typically, a MA requires to successfully implement a combination of more than one LC (combination of local consequences, CM).

The success of a MA in causing a CE/SE can be limited by the presence of effective safeguards (e.g., safety instrumented functions and physical safety devices).

In order to reduce the subjectivity in the application of the method and promote repeatability of results, the PHAROS and POROS were developed as structured step-by-step procedures, similar to well-known procedures of HazOp, Hazid and FMEA [19]. In addition, guideline tables provide reference checklists of the most common classes of CEs, SEs, RMCs, MEs, RMs, LCs and MAs for chemical and process plants.

The proposed framework of methodologies is currently limited to the scope of identification of malicious manipulations of the BPCS and the SIS in the physical process system. As such, it does not provide quantitative evaluation of the risk associated to cyber-attacks. However, the clear identification of the CMs, APSs, and IPSs provided by the two methodologies, paves the way for future developments aimed at the quantification of the probability of success of a cyber-attack, which is a key part of the quantitative evaluation of the cyber-risk. Moreover, the practical application of PHAROS and POROS methodologies may require considering large numbers of combinations of manipulations when applied to complex plants with many nodes. This limitation may, in the future, be overcome by the development of software tools allowing easy management of relevant data and automation of some steps of the procedures (e.g., identification of RMCs).

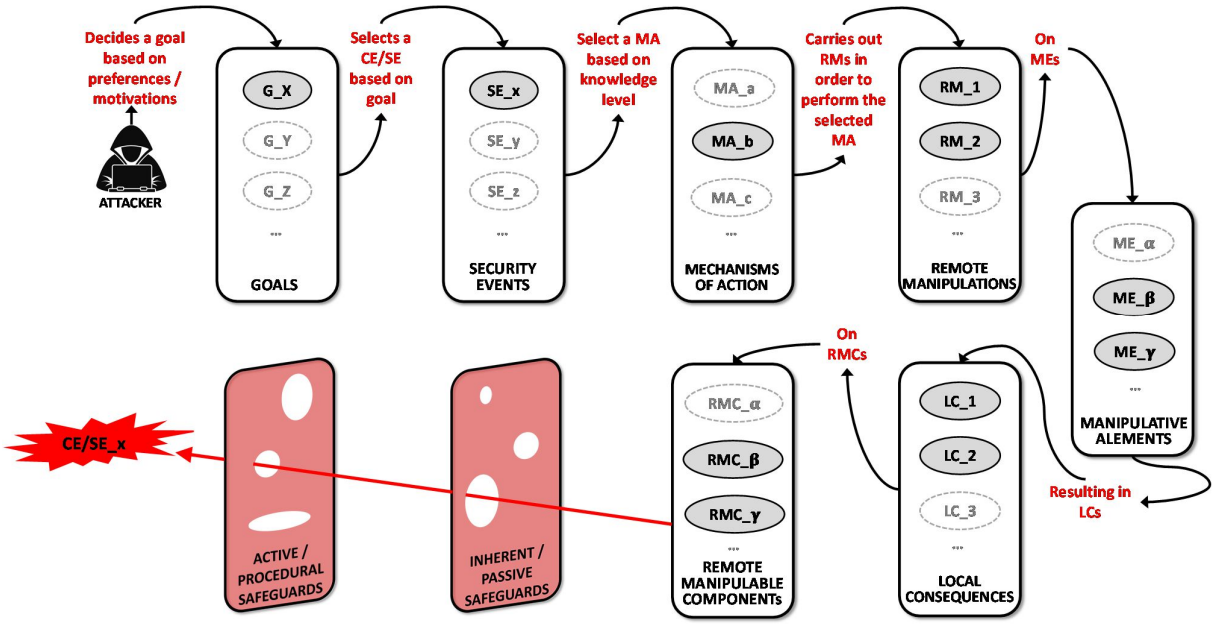

Figure 34 Relationship between, RMs, MEs, LCs, RMCs, CMs, MAs and CEs/SEs (RM: Remote Manipulation; ME: Manipulative Element, LC: Local Consequence; RMC: Remote Manipulable Component; CM: CoMbination of local consequences; MA: Mechanism of Action; CE: Critical Event; SE: Security Event). Adapted from [100].

In the next paragraphs, PHAROS and POROS are described in detail and are applied to case studies to demonstrate the quality of the results that can be achieved in the context of cyber-risk identification (e.g., support to ISA/IEC 62443-3-2). For the sake of brevity, each methodology will be applied to a single case study: PHAROS to an onshore Oil&Gas plant for the preliminary treatment of the crude oil, while POROS to an offshore Oil&Gas platform for the pressurization of the natural gas. However, case studies of the application of PHAROS and POROS, including the ones here presented, can be found in [100,101,175–177].

4.2. PHAROS methodology

4.2.1. Detailed description of the methodology

The PHAROS methodology consists in nine steps, as shown in **Figure 35**.

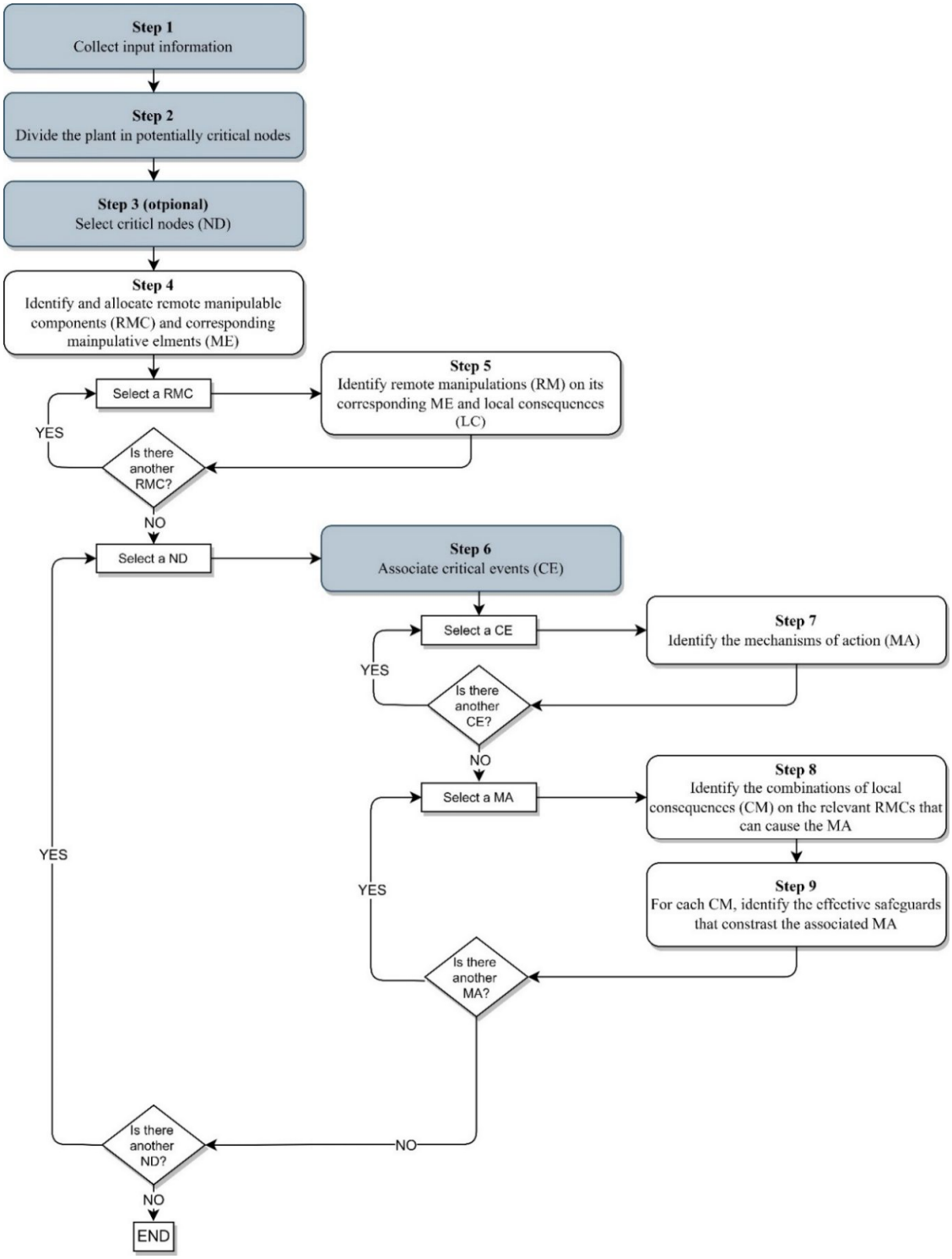

Figure 35 Flowchart of the PHAROS methodology. Shaded steps can be integrated with conventional safety studies. Adapted from [101].

In Step 1, the input data for the application of the procedure are collected: the PFD (Process Flow Diagram), the material balances, the P&ID (Piping and Instrumentation Diagram), the list of substances stored or handled and their hazardous properties, the operating conditions of each process unit, the logics of the BPCS and the SIS (e.g., the functional block diagrams, the control diagrams, etc.), and the data sheets of each process unit.

In Step 2, the plant is divided into process nodes. Only the nodes in which hazardous substances are processed or stored (i.e., potentially critical nodes) are of concern in the assessment. Each node is typically composed of a main process unit (e.g., storage tanks, columns, reactors, heat exchangers, etc.), some auxiliary units (e.g., pumps, drums, etc.), and the pipework. **Table 10** reports the main general categories of process equipment units based on the classification provided by [99,178]. The division in process nodes may be carried out by a procedure similar to that applied in the HazOp study, as described by the standard IEC 61882 [97]: if such a study is already available for the same plant, the HazOp nodes can be adopted.

Table 10 Main general categories proposed for the classification of plant items [99,178].

General categories	Sub-categories	Code
Vessel-like equipment	Atmospheric vessel (storage, process, etc.)	EQ1.1
	Pressurized vessel (storage, column, reactor, etc.)	EQ1.2
	Mobile vessel (tank wagon, road tanker)	EQ1.3
Tube bundle equipment	S&T heat exchanger, reactor, etc.	EQ2.1
Plate and frame equipment	Filter, plate heat exchanger, etc.	EQ3.1
Pipe	Pipeline, manifold, loading arm, etc.	EQ4.1
Pumping equipment	Pump (centrifuge, alternative, etc.)	EQ5.1
	Compressor (centrifuge, alternative, etc.)	EQ5.2
Warehouse	Packed materials (bags, barrels, etc.)	EQ6.1
	Spare materials (piles, etc.)	EQ6.2
Special equipment	Solid handling (conveyors crushers, etc).	EQ7.1
	Other	EQ7.2

Step 3 consists in identifying the critical nodes (ND). This step is aimed at reducing the number of nodes to be analysed, focusing on those from which the more severe consequences can originate. Hence, the critical nodes shall be selected on the basis of the inherent hazard (potential to originate accident scenarios due to inherent characteristics of the process, such as high inventory of hazardous materials or severe operating conditions). Inherent safety indicators such as UPI by Tugnoli et al. [178,179], I2SI by Khan et al. [180], and PSI by Shariff et al. [181], can be used for this purpose. Conventional methodologies for the hazard ranking of process units can be used as well (e.g., Dow F&EI [182], Mond Index [183,184]), provided that only the hazard factors scoring consequence severity are considered (e.g., penalties for high frequencies of equipment failure are neglected since they are not relevant to security threats). Reviews of such procedures and of their application to inherent safety scoring are provided by Mannan [19] and Tugnoli et al. [179].

The selection of the most critical nodes may be based either on absolute terms (for example the nodes whose criticality indexes exceed a given threshold) or on relative terms (for example the nodes whose criticality indexes exceed the first quartile in the ranking). Clearly enough, all the nodes can be selected as critical nodes if deemed necessary, making step 3 an optional step.

Step 4 consists in the identification of the remote manipulable components (RMCs), of their manipulative elements (MEs), and in the allocation of RMCs to the critical nodes. RMCs are the physical objects in the plant whose operation is regulated by the BPCS and the SIS (e.g., automatic valves, pumps, compressors, etc.). The MEs are the elements of the BPCS and the SIS by which the manipulation action is carried out (e.g., controllers and their logics). **Table 11** provides a classification of the most common RMCs and corresponding MEs in process plants. The identification of RMCs and MEs is based on a review of process documentation (P&IDs, valve and motor datasheets, etc.).

Each RMC is then allocated to one or more critical nodes, on the basis of the influence it can have on that node (ND). The following guidelines can support the allocation of RMCs:

- if a RMC is located on a stream that directly connects process units belonging to two different NDs, it is allocated to both nodes;
- if a RMC is located on a stream connecting a unit belonging to a critical node with a non-critical node, it is allocated to the critical node;
- if a RMC is located on a stream internal to a critical node, it is allocated only to that node.

If relevant consequences on the node of concern are identified during the next steps of the procedure, the list of allocated RMCs developed in this stage can be integrated (that is, additional RMCs are included, even if initially allocated only to other NDs).

Table 11 Proposed categories of remote manipulable components (RMCs), manipulative elements (MEs) and remote manipulations (RMs). Adapted from [101].

Remotely manipulable components	Code	Manipulative elements for all RMCs	Code	Remote manipulations for each ME	Code
Shut-off valve	RMC1	BPCS device (e.g., PID controller)	ME1	Signal shutdown	RM1
Control valve	RMC2			Setpoint change	RM2
Mechanical pump and its driver	RMC3	SIS device (e.g., PLC controller)	ME2	Function reprogramming	RM3
Compressor/fan and its driver	RMC4			Signal shutdown	RM1
Other (e.g., conveyor belts, rotary filters, mills, extruders, rotary furnaces, etc.)	…			Function reprogramming	RM3

Step 5 consists in identifying, for each ME, all the possible remote manipulations (RMs) that can be carried out through an attack (e.g., the setpoint change or the signal shutdown for a BPCS controller). **Table 11** provides guidelines of the typical RMs possible for each ME. Next, for each ME, the local consequences (LCs) on the corresponding RMC are identified (e.g., the increase in the opening degree of the controlled valve). **Table 12** shows typical associations of RMs and LCs. This step requires due care, as specific features of the RMC may lead to different LCs even for very similar items (e.g., a fail closed valve behaves differently than a fail open valve in case of signal shutdown).

Table 12 Proposed categories for local consequences (LCs) and their association with RMs. Adapted from [101].

Remote manipulations	Local consequences on RMCs	Code
RM1 to ME1 and ME2	Valve opening (F.O., fail open)	LC1
	Valve closing (F.C., fail close)	LC2
	Valve actuator lock (F.L., fail locked)	LC3
	Indeterminate position of the valve actuator (F.I., fail indeterminate)	LC4
	Stop of the operating machine	LC5
	The operating machine continues to run (as for fail safe specification)	LC6
RM2 to ME1	Increase in valve opening degree, also up to 100%	LC7
	Decrease in valve opening degree, also up to 0%	LC8
	Opening-closing cycles of the valve	LC9
	Increase of the rotational speed of the operating machine	LC10
	Decrease of the rotational speed of the operating machine	LC11
	Cycles of increase-decrease of the rotational speed of the operating machine	LC12
RM3 to ME1 and ME2	Valve opening	LC1
	Valve closing	LC2
	Stop of the operating machine	LC5
	The operating machine continues to run	LC6
	Increase in valve opening degree, also up to 100%	LC7
	Decrease in valve opening degree, also up to 0%	LC8
	Opening-closing cycles of the valve	LC9
	Increase of the rotational speed of the operating machine	LC10
	Decrease of the rotational speed of the operating machine	LC11
	Cycles of increase-decrease of the rotational speed of the operating machine	LC12
	Start of the operating machine	LC13
	Start and stop cycles of the operating machine	LC14

Step 6 consists in associating to each critical node the compatible critical events (CEs). A CE is a loss of containment (LOC) or a loss of physical integrity (LPI) which "unleashes" the material or physical hazards normally present in the system [99]. The categories of LOCs and LPIs proposed e.g., by the standard API 581 [185], the MIMAH methodology [99] and the "Purple Book" [186] can be used as reference. Case specific LOC or LPI emerging from available safety and operability studies (e.g., HazOp [97], failure modes and effect analysis (FMEA) [98], DyPASI [187]), shall be included in the list of CEs for the node. This step is based on the review of the P&IDs, of the list of substances stored or handled and their hazardous properties, of the control philosophies, and of the safety instrumented functions. As an example, **Table 13** shows the CEs suggested by the MIMAH procedure [99].

Table 13 Proposed critical events (CEs) and related categories of mechanisms of action (MAs). Adapted from [101].

Critical events	MA category	Code
CE1: thermal or chemical decomposition	Temperature increase	MA1
	Give rise to a punctual or permanent energy source	MA2
	Addition of an incompatible reagent to the system	MA3
	Addition of an appropriate catalyst to the system	MA4
CE2: explosion	Addition of explosive material to the system	MA5
	Give rise to a type of ignition	MA6
	Addition of a highly reactive substance to the system	MA7
	Give rise to a punctual or permanent energy source	MA2
	Addition of an incompatible reagent to the system	MA3
	Addition of an appropriate catalyst to the system	MA4
CE3: materials set in motions (entrainment by air)	Addition of potentially mobile material to the system	MA8
	Addition of an air vector to the system	MA9
CE4: materials set in motions (entrainment by a liquid)	Addition of potentially mobile material to the system	MA8
	Addition of a liquid vector to the system	MA10
CE5: start of fire (LPI)	Addition of an oxidising substance to the system	MA11
	Addition of a combustible (reducing) substance to the system	MA12
	Temperature increase	MA1
	Give rise to a type of ignition	MA6
CE6: breach on the shell in vapour phase	Give rise to internal overpressure	MA13
	Give rise to mechanical stress of the structure	MA14
	Embrittlement of the structure	MA15
CE7: breach on the shell in liquid phase	Give rise to internal overpressure	MA13
	Give rise to mechanical stress of the structure	MA14
	Embrittlement of the structure	MA15
	Increase in the liquid level (hold up)	MA16
CE8: leak from liquid pipe	Give rise to internal overpressure	MA13
	Give rise to mechanical stress of the structure	MA14
	Embrittlement of the structure	MA15
CE9: leak from gas pipe	Give rise to internal overpressure	MA13
	Give rise to mechanical stress of the structure	MA14
	Embrittlement of the structure	MA15

CE10: catastrophic rupture	Give rise to internal overpressure	MA13
	Give rise to mechanical stress of the structure	MA14
	Embrittlement of the structure	MA15
CE11: vessel collapse	Give rise to internal depressurization	MA17
CE12: collapse of the roof	Give rise to internal depressurization	MA17

Step 7 consists in identifying all the mechanisms of action (MAs) by means of which each CE can be initiated through an attack to the control system. The MAs are the physical mechanisms that the attackers may use to initiate the CE (e.g., increase the internal pressure of a vessel by closing the gas outlets). **Table 13** shows reference MA categories for each CE. These provide a guideline in the identification of MAs tailored to the node under assessment. Tailoring of the MA is required as inherent design features of the process may negate some mechanisms. If a HazOp study or a fault tree analysis [99,188] has been performed for the node, it can complement the identification of the MAs.

If there are no possible MAs for a CE, the CE is removed from those previously associated for the ND. Some MAs may require actions from a nearby node to occur (i.e., manipulation of RMCs belonging to a nearby node is required). In these cases, the information is propagated from a node to another similarly to deviations propagating among different nodes in a traditional HazOp study. Cross checking with an HazOp study for the same nodes (if available) is expected to be very useful since many of the applicable mechanisms of deviation propagation among nodes were already identified by such a study.

Step 8 consists in identifying the combinations (CMs) of LCs from the allocated RMCs by means of which each MA in a node can be carried out. In general, not all the RMCs present in a node need to be manipulated in order to carry out a given MA: those that are manipulated constitute the set of relevant RMCs for a CM of that MA.

Step 9 consists in identifying, for each CM, the effective safeguards (i.e., safety devices) which are present in the node being analysed. “Effective” means that the safeguard is able to contrast, directly or indirectly, the MA associated to a particular CM, avoiding the occurrence of the corresponding CEs. Therefore, a safeguard can be effective for one CM and not for another. Effectiveness shall be checked case by case, as it also depends on design specifications of the barrier (e.g., matching or not the requirements from physical scenarios deriving from the attack).

Safeguards can be classified in active/procedural safeguards (APSs) and inherent/passive safeguards (IPSs) [189]. The first ones are automated or human-mediated actions, which involve a response by the same IT-OT system under attack. Procedural safeguards include monitoring systems informing the operators of malfunctions or anomalies in process equipment (e.g., alarms and warning lights), remote controls that allow carrying out corrective actions on the process equipment from the control room or local panels (e.g., hand switches) and any other human-mediated action. As such their success is influenced by both the correct operation of the IT-OT system and by the response of the control room operators (i.e., behavioural factors affecting human errors). Active safeguards, instead, include the logics which carry out automatic response actions on the process equipment (safety instrumented functions as, e.g., shutdown and blowdown logics). The IPSs are devices that provide their safety action independently of the IT-OT system (e.g., PSVs, rupture disks, vent systems, emergency hatches, etc.).

It is important to emphasize that the active/procedural safeguards, unlike the inherent/passive safeguards, can be manipulated by the attackers. Nevertheless, the identification of the active/procedural safeguards is included in the method for two main reasons. First, it may be argued that the attackers, despite being able

to tamper with the BPCS and the SIS, may not have full knowledge or ability to deactivate all the APSs that may contrast the MAs. Second, the identification of the relevant APSs allow taking specific IT-OT countermeasures and human error reduction measures to protect the APSs more relevant in preventing a successful cyber-attack. This is a very useful information for the design of the IT-OT network system and human barriers, which is required for security management (ISA/IEC 62443, 2018; ISO/IEC 27000s, 2018; IEC 61511, 2017).

Step 8 and Step 9 of the procedure can be supported for each ND by the worksheet shown in **Figure 36**. The first four rows of the worksheet report the identification of the node, the CEs associated to the ND, and the MAs by means of which each CE can be originated. The first column lists the RMCs allocated in the node plus any relevant virtual RMC. The columns in the body of the worksheet report the LCs for each relevant RMC by which the considered MA can be carried out; each of these columns constitutes a combination of local consequences (CM). The code names for CMs are reported in a dedicated row. The two bottom rows of the worksheet identify the active/procedural safeguards (APS) and the inherent/passive safeguards (IPS) effective for each CM.

Similarly to an HazOp study, once all the steps have been performed, a completeness check is required. It consists in verifying that all the critical nodes have been analysed, and that all the MAs, by which the associated CE can be originated were developed as combinations of LCs on the relevant RMCs. Moreover, for the CEs (and corresponding MAs) that require actions from a nearby ND to occur, it must be verified that the additional CEs have been fully developed in the relevant nodes.

The worksheet contains and tracks all the findings obtained by the application of the method to each ND. The results can be also summarized and presented through a number of conventional approaches that evidence specific findings of interest (e.g., attack trees [58], cause-consequence chain diagrams [187]).

ND name													
Critical events (CEs)		CEx, CEy				CEz				Additional CEs			
Categories of mechanisms of action		MAα				MAα+MAπ				Additional category of MAs			
Mechanisms of action (MAs)		MAα.1		MAα.2		MAα+π.1		MAα+π.2		Additional MAs			
Combinations (CMs)		CM1	CM2	…	…	…	…	…	…	…	…	…	CMm
Remote manipulable components (RMCs)	RCM1	Local Consequences (LCs)											
	…												
	RCMn												
	Virtual RCMs												
Active/Procedural safeguards (APSs)		Names of APSs and IPSs for each CM											
Inherent/Passive safeguards (IPSs)													

Figure 36. Worksheet proposed for PHAROS analysis of each critical node (ND). Adapted from [101].

4.2.2. Illustrative case study

4.2.2.1. Set-up of the case study

An onshore upstream Oil&Gas plant for the preliminary treatment of crude oil is considered in the case study. The main goals of the plant are the separation of the production water and the oil and gas processing up to specification for transport via pipeline.

Figure 37 shows the simplified block diagram of the plant. The inlet stream from wells is crudely separated by the Slug Catcher VQ001. The two liquid phases are further separated in the Three Phase Separator VS003; the salts are removed in the First/Second Stage Desalting Drum VU001A/B and vapour pressure is adjusted

in the Stabilizer Column VE001, making the crude suitable for storage in Tank TA001 and for pipeline delivery. The associated gas stream is sent to a low temperature separation system (Low Temperature Separator VS001, Glycol/Condensate Separator VS002) and joined with the compressed gas from the Three Phase Separator VS003 and the Stabilizer Column VE001.

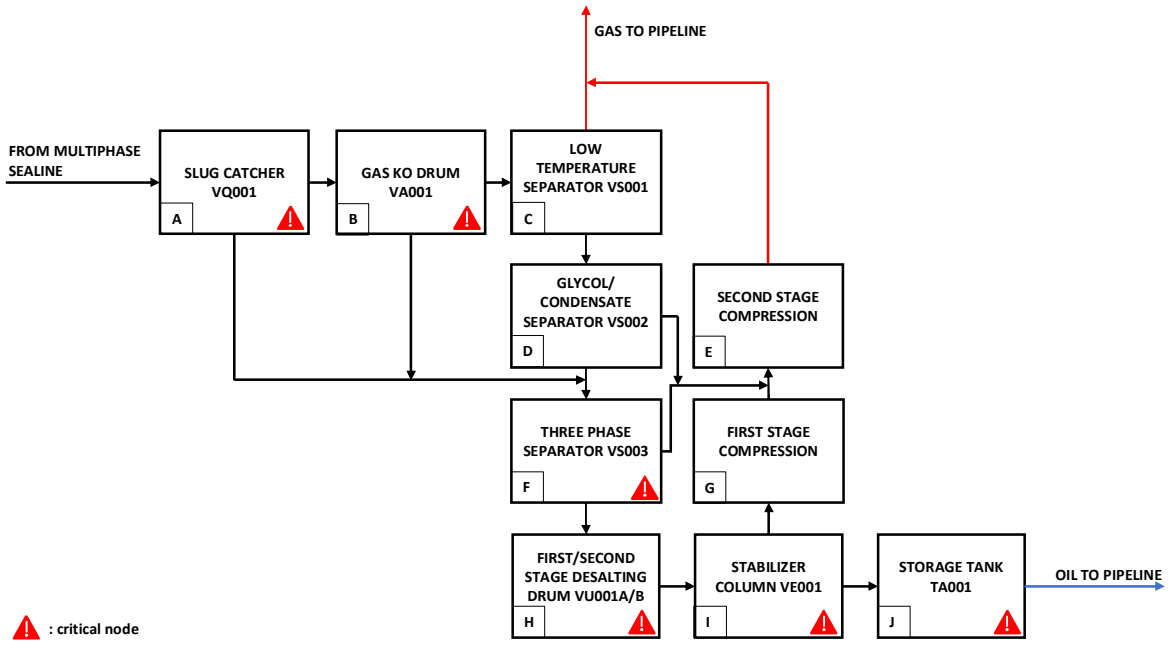

Figure 37 Simplified block diagram of the Oil&Gas Plant considered in the case study. Critical nodes (from Step 3) are also evidenced. Adapted from [101].

Following the collection of the necessary documentation (see Step 1 in Section 4.2.1), the Oil&Gas plant was divided into process nodes according to the typical rules of the HazOp study [97] (Step 2), which coincide in this case with the blocks shown in **Figure 37**. **Figure 38** shows an example of the node definition. Subsequently, the nodes where hazardous substances are processed or stored (i.e., potentially critical nodes), and in particular the ones with greater inventory/holdup and/or more critical operating conditions, were considered for further assessment. These steps are common to many safety management procedures (e.g., for QRA – Quantitative Risk Analysis[19]) and, for sake of brevity, are not detailed in the current example. The critical nodes identified are evidenced in **Figure 37**: more details can be found in the Supplementary Material of Iaiani et al. [101].

In the following, the application of the PHAROS methodology is demonstrated on the critical process node featuring the Three Phase Separator VS003 (operating pressure = 19 barg; operating temperature = 16 °C; internal diameter = 2150 mm; length = 6500 mm), named ND_F as it coincides with block F in the block diagram shown in **Figure 37**. **Figure 38** reports a simplified P&ID of the node. This node was chosen as a reference case study both because it is a very common equipment in the Oil&Gas industry and for its high inherent hazard due to the large inventory of hazardous material processed (about 12 m^3 of flammable liquid and gas) and the moderately high pressure (19 barg). **Table 14** shows the description of the items which are present in ND_F.

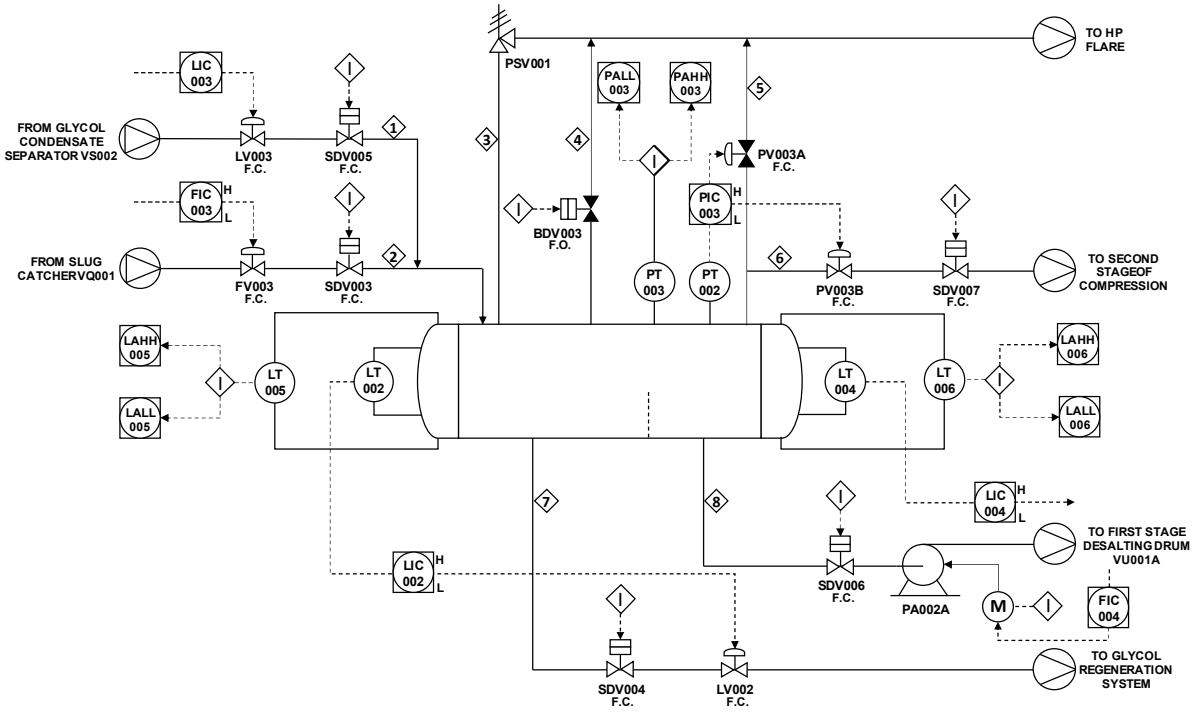

Figure 38 Simplified P&ID of the node ND_F ("Three phase separator"). Adapted from [101].

Table 14 Items present in node ND_F (see also **Figure 38**) and selected critical events (CEs). Adapted from [101].

EQ codes (Step 2)	Items (Step 2)	Description	Selected CEs (Step 6)
EQ1.2	Three Phase Separator VS003	Pressurized vessel for the separation of oil, water, and hydrocarbon gases (main process unit)	CE5, CE6, CE7, CE10
EQ5.1	Desalter Feed Pump PA002A	Centrifugal pump in Stream 8	CE7, CE8
EQ4.1	Stream 1	Process inlet stream from Glycol/Condensate Separator VS002	CE5, CE8, CE9, CE10
	Stream 2	Process inlet stream from Slug Catcher VQ001	
	Stream 3	Emergency stream (PSV) to HP Flare	
	Stream 4	Emergency stream (blowdown) to HP Flare	
	Stream 5	Emergency PV outlet stream (gas phase) to HP Flare	
	Stream 6	Process outlet stream (gas phase) to second stage of compression	
	Stream 7	Process outlet stream (hydrocarbon liquid phase) to First Stage Desalting Drum VU001A	
	Stream 8	Process outlet stream (aqueous liquid phase) to glycol regeneration system	

4.2.2.2. Results of the case study

Following the division in nodes, the remote manipulable components (RMCs) which are present in the Oil&Gas plant and their corresponding manipulative elements (MEs) were identified following the guidelines provided in **Table 11** (Step 4 of the methodology). The identified RMCs were allocated to the critical process nodes in accordance with the guidelines described in Step 4 (Section 4.2.1). The allocated RMCs and the respective MEs for ND_F are listed in **Table 15**. The RMCs include emergency valves (blowdown and

shutdown valves), control valves and a motor-driven pump. The shutdown valves and the blowdown valve of the node are shut-off valves controlled by the SIS by means of PLCs (Programmable Logic Controllers), which constitute the MEs on which an attacker can intervene in this case. The control valves are manipulated by the PID controllers of the BPCS, while the centrifugal pump is driven by an electric motor controlled by both the BPCS and SIS.

The remote manipulations (RMs) for the MEs were identified in accordance with the guidelines provided in **Table 11** (Step 5 of the methodology). As regards the PLCs of the SIS which control the automated shut-off valves, the RMs considered are the signal shutdown (code RM1) and the function reprogramming (code RM3). For the PID controllers of the BPCS, which manage the automated control valves, two manipulations were considered: the signal shutdown (code RM1) and the setpoint change (code RM2).

The local consequences (LCs) on the RMCs corresponding to each RM on the related MEs were identified, following the typical associations of RMs and LCs shown in **Table 12**. This requires to consider the fail-safe type of all the automated valves [190], the type of action of the PID controllers (direct or reverse) and the logics of the SIS.

Table 15 summarizes the remote manipulations (RMs) and the local consequences (LCs) on the RMCs allocated to the node ND_F. For example, as regards the control valve PV003B (see **Table 15** and **Figure 38**), a possible remote manipulation to the PID controller PIC003 (i.e., the ME by which the valve is controlled) is the signal shutdown (RM1): as a result of this RM, the valve closes (LC2) as it fails in the closed position.

Table 15 Remote manipulations (RMs) and local consequences (LCs) for each RMC allocated to the node ND_F. Adapted from [101].

RMCs (Step 4)	RMC codes (Step 4)	ME codes (Step 4)	RM codes (Step 5)	LC codes (Step 5)
SDV003 SDV004 SDV005 SDV006 SDV007	RMC1: shut-off valves (F.C.)	ME2: SIS device	RM1: signal shutdown	LC2: valve closing
			RM3: function reprogramming	LC2: valve closing
BDV003	RMC1: shut-off valve (F.O.)	ME2: SIS device	RM1: signal shutdown	LC1: valve opening
			RM3: function reprogramming	LC1: valve opening
PV003A PV003B LV002 LV003 FV003	RMC2: control valves (F.C)	ME1: BPCS devices (PIC003, LIC002, LIC003, FIC003)	RM1: signal shutdown	LC2: valve closing
			RM2: setpoint change	LC7: increase in valve opening degree
				LC8: decrease in valve opening degree
				LC9: opening-closing cycles of the valve
PA002A	RMC3: mechanical pump and its driver	ME1: BPCS device (FIC004)	RM1: signal shutdown	LC5: stop of the pump
			RM2: setpoint change	LC10: increase of the rotational speed of the pump
				LC11: decrease of the rotational speed of the pump
		ME2: SIS device	RM1: signal shutdown	LC5: stop of the pump
			RM3: function reprogramming	LC5: stop of the pump
				LC10: increase of the rotational speed of the pump
				LC11: decrease of the rotational speed of the pump
				LC12: cycles of increase-decrease of the rotational speed of the pump
				LC13: start of the pump
				LC14: start and stop cycles of the pump

The identification of the critical events (CEs) for all the critical process nodes identified (Step 6 of the methodology) in the Oil&Gas plant was performed through the MIMAH procedure [99]. In this procedure, the type of equipment (as defined by the taxonomy in **Table 10**) is matched with the potential CEs and the physical state of the substance considered (STAT1: solid, STAT2: liquid, STAT3: two-phase, STAT4: gas/vapour). More details on the procedure are reported in ARAMIS D1C – Appendix 3 [191].

When ND_F is considered, the relevant CEs for the units of the node are (**Table 14**): CE5 (start of fire), CE6 (breach on the shell in vapour phase), CE7 (breach on the shell in liquid phase), CE8 (leak from liquid pipe), CE9 (leak from gas pipe), CE10 (catastrophic rupture). It is important to remark that the identification of the reference release modes for each CE (e.g., the size of the holes and the duration of the releases) lays beyond the scope of the PHAROS procedure, since consequence analysis is not carried out and may be a following step of the overall hazard assessment procedure.

The parallel assessment of a nearby node (the second stage compression node, named ND_E) and the available HazOp study evidenced that some mechanisms of action (MAs) for that node can be caused by an abnormal quantity of liquid entering ND_E via the gas outlet pipe of ND_F. This deviation, propagating among different nodes, was tracked adding a “virtual RMC (RMCv)” in the assessment of ND_E (RMCv01: liquid in the gas inlet from ND_F) and considering an “additional CE” in ND_F (CEa01: high liquid fraction in the gas outlet) (**Table 16**).

The credible mechanisms of action (MAs), by means of which an attacker can originate each of the CEs for the ND_F, were identified (Step 7 of the methodology). The identification started from the selection of the categories of MAs following the guidelines provided in **Table 13**, then tailoring the MAs to the process equipment present in the node ND_F. **Table 16** summarizes the results obtained. The table shows that the CE5 (start of fire) cannot be caused by an attack to the control system because it is not possible to give rise to a flammable mixture inside the separator (e.g., adding an oxidizing substance to the system) exclusively by means of remote manipulations, and, even less, to ignite such a mixture. The CE5 was therefore rejected for node ND_F.

The critical events CE6, CE7, CE8, CE9 and CE10 all share the same category of MAs: the direct increase of the internal pressure above the maximum allowed value (MA13), the increase of the liquid level, which results again in the increase of internal pressure (MA16), or a combination of the two (MA13+MA16). MA13 can be further specified as a blockage of the gas outlets (MA13.1) or a connection to an external source of high pressure (MA13.2) (**Table 16**). In the following assessment, no distinction will be made among these CEs. As regards CEa01, instead, in order to have liquid in the outlet gas pipe to node ND_E (second stage compression, see **Figure 37**), only the mechanism of action MA16.1 (more liquid flow at the inlet than at the outlet) is necessary. These MAs will be the basis for the definition of the CMs in the next step.

Table 16 Mechanisms of action (MAs) identified for each CE associated with the node ND_F. Adapted from [101].

CE codes (Step 6)	MA category codes (Step 7)	Mechanisms of actions (Step 7)
CE5: start of fire	MA11 + MA6: addition of an oxidising substance to the system + give rise to a type of ignition	not feasible + not feasible
	MA11 + MA1: addition of an oxidising substance to the system + temperature increase	not feasible + not feasible
CE6: breach on the shell in vapour phase	MA13: give rise to internal overpressure	MA13.1: lock of the gas outlets
		MA13.2: external source of pressure (maximum opening of the inlet valves) + lock of gas the outlets
	MA16: increase in the liquid level (hold up)	MA16.1: more liquid flow at the inlet than at the outlet
	MA13 + MA16: give rise to internal overpressure + increase in the liquid level (hold up)	MA_{13+16}.1: lock of the gas outlets + more liquid flow at the inlet than at the outlet
		MA_{13+16}.2: external source of pressure (maximum opening of the inlet valves) + lock of the gas outlets + more liquid flow at the inlet than at the outlet
CE7: breach on the shell in liquid phase	same as for CE6	same as for CE6
CE8: leak from liquid pipe	same as for CE6	same as for CE6
CE9: leak from gas pipe	same as for CE6	same as for CE6
CE10: catastrophic rupture	same as for CE6	same as for CE6
CEa01: high liquid fraction in the gas outlet	MA16: increase in the liquid level (hold up)	MA16.1: more liquid flow at the inlet than at the outlet

The identification of the combinations of LCs (Step 8 of the methodology) was carried out with the support of the worksheet presented in **Figure 36**. **Table 17** shows an example of the reasoning behind the identification of the relevant RMCs and the selection of the LCs of concern for the mechanism of action MA13.1 (lock of the gas outlet). It can be noted from the table that some RMCs allocated to ND_F are not relevant for the assessed MA, while manipulation of alternative RMCs is possible to achieve the same effect in other cases (e.g., the same effect is achieved by closing shutdown valve SDV007 or by closing PV003B). The complete results obtained for ND_F are reported in **Table 18**: the presence of alternative RMCs for each mechanism of action implies that more than one CM was identified for each MA (see also **Table A.1** in the Appendix of this Chapter).

Table 17 Example of the selection of LCs for the RMCs of node ND_F: MA13.1 was considered. NM: no manipulation of the RMC required. Adapted from [101].

MA category	MA13: give rise to internal overpressure	
MA	MA13.1: lock of the gas outlets (i.e., Stream 5 and Stream 6 in **Figure 38**)	
RMCs	**Does the RMC need to be remotely manipulated?**	**LCs**
SDV003	NO, because the valve is on an inlet stream	NM
SDV004	NO, because the valve is on a liquid outlet stream	NM
SDV005	NO, because the valve is on an inlet stream	NM
SDV006	NO, because the valve is on a liquid outlet stream	NM
SDV007	ALTERNATIVE: it must be closed in order to interrupt the flow or PV003B must be manipulated (partially or completely closed)	LC2 or manipulation on PV003B
BDV003	NO, because it opens in case of fire detection when the PSV cannot manage the gas flow to be discharged	NM
PV003A	YES, it must be closed more (even completely) in order to reduce/interrupt the flow.	LC2 or LC8
PV003B	ALTERNATIVE: it must be closed more (even completely) in order to reduce/interrupt the flow or SDV007 must be manipulated (closed)	LC2/LC8 or manipulation on SDV007
LV002	NO, because the valve is on a liquid outlet stream	NM
LV003	NO, because the valve is on an inlet stream	NM
FV003	NO, because the valve is on an inlet stream	NM
PA002A	NO, because the pump is on a liquid outlet stream	NM

The analysis of the P&ID and of relevant documentation allowed for the identification of the effective safeguards (Step 9 of the methodology), which can block or mitigate the MAs identified for the node. For example, the components of the effective active/procedural safeguards (APSs) relevant for the mechanism MA13.1 of the node ND_F are the high pressure alarms PAH003 and PAHH003, the LSD logic which manages the shutdown valves SDV003 and SDV005, and the position light of shutdown valve SDV007 (ZLL00L). The relevant inherent/passive safeguards (IPSs) for the same node are the pressure safety valve PSV001 and, as a mitigation measure for the liquid spill, the catch basin. **Table 18** reports, for each MA, the complete sets of all the effective safeguards. Since in some cases alternative relevant RMCs exist for the same MA, a given safeguard may not be effective for all of them: the set of effective safeguards for each CM is thus reported in **Table A.1** in the Appendix of this Chapter.

Summarizing the findings from the analysis of ND_F (**Table 18**), the critical events that can be originated through a malicious manipulation of the BPCS and the SIS consist in the loss of containment via a breach on the shell in the liquid and gas phases (CE6 and CE7), the leaks from the gas and liquid pipes (CE8 and CE9), the catastrophic rupture of the three-phase separator (CE10), and the high liquid fraction in the gas outlet (CEa01), which may cause damage in the downstream node. Conventional event tree analysis and consequence simulation can be used to assess the impact originating from the identified critical events. This piece of information is required by the cybersecurity risk assessment of the IT-OT network system (e.g., ISO/IEC 27005 and ISA/IEC 62443).

The increase in internal pressure (also obtained through an increase in the liquid level) was identified as the generic mechanism of action (MA category) to originate the critical events from CE6 to CE10, while the overfilling of the three-phase separator can also result in CEa01. A total of 24 combinations (**Table A.1** in the Appendix of this Chapter) were identified in order to carry out these MAs.

Table 18 Worksheet for node ND_F. NM: no manipulation of the RMC required. The detailed list of all the CMs is reported in **Table A.1** in the Appendix of this Chapter. Adapted from [101].

ND_F						
Critical events (CEs)		CE6, CE7, CE8, CE9, CE10		CE6, CE7, CE8, CE9, CE10, CEa01	CE6, CE7, CE8, CE9, CE10	
Categories of Mechanisms of action		MA13: give rise to internal overpressure		MA16: increase in the liquid level (hold up)	MA13 + MA16: give rise to internal overpressure + increase in the liquid level (hold up)	
Mechanisms of action (MAs)		MA13.1: lock of the gas outlets	MA13.2: maximum opening of the inlet valves + lock of the gas outlets	MA16.1: more liquid flow at the inlet than at the outlet	MA_{13+16}.1: lock of the gas outlets + more liquid flow at the inlet than at the outlet	MA_{13+16}.2: maximum opening of the inlet valves + lock of the gas outlets + more liquid flow at the inlet than at the outlet
Combinations (CMs)		CM1, CM2 (**Table A.1**)	CM3, CM4 (**Table A.1**)	CM5 - CM8 (**Table A.1**)	CM9 - CM16 (**Table A.1**)	CM17 - CM24 (**Table A.1**)
Remotely manipulable components (RMCs)	SDV003	NM	NM	NM	NM	NM
	SDV004	NM	NM	LC2 or manipulation on LV002	LC2 or manipulation on LV002	LC2 or manipulation on LV002
	SDV005	NM	NM	NM	NM	NM
	SDV006	NM	NM	LC2 or manipulation on PA002A	LC2 or manipulation on PA002A	LC2 or manipulation on PA002A
	SDV007	LC2 or manipulation on PV003B	LC2 or manipulation on PV003B	NM	LC2 or manipulation on PV003B	LC2 or manipulation on PV003B
	BDV003	NM	NM	NM	NM	NM
	PV003A	LC2 or LC8	LC2 or LC8	NM	LC2 or LC8	LC2 or LC8

	PV003B	LC2/LC8 or manipulation on SDV007	LC2/LC8 or manipulation on SDV007	NM	LC2/LC8 or manipulation on SDV007	LC2/LC8 or manipulation on SDV007
	LV002	NM	NM	LC2/LC8 or manipulation on SDV004	LC2/LC8 or manipulation on SDV004	LC2/LC8 or manipulation on SDV004
	LV003	NM	LC7	NM	NM	LC7
	FV003	NM	LC7	NM	NM	LC7
	PA002A	NM	NM	LC5/LC11 or manipulation on SDV006	LC5/LC11 or manipulation on SDV006	LC5/LC11 or manipulation on SDV006
	SDV003	NM	NM	NM	NM	NM
Active/Procedural safeguards (APSs)		PAH003, PAHH003, ZLL007, LSD logic activated by PSHH	PAH003, PAHH003, ZLL007, LSD logic activated by PSHH	PAH003, PAHH003, LAH002, LAHH005, LAH004, LAHH006, ZLL004, ZLL006, LSD logics activated by PSHH, interface LSHH and oil LSHH, UA unavailable	PAH003, PAHH003, LAH002, LAHH005, LAH004, LAHH006, ZLL004, ZLL006, ZLL007, LSD logics activated by PSHH, interface LSHH and oil LSHH, UA unavailable	PAH003, PAHH003, LAH002, LAHH005, LAH004, LAHH006, ZLL004, ZLL006, ZLL007, LSD logics activated by PSHH, interface LSHH and oil LSHH, UA unavailable
Inherent/Passive safeguards (IPSs)		PSV001, catch basin	PSV001, catch basin	PSV001, catch basin	PSV001, catch basin	PSV001, catch basin

4.2.2.3. Discussion of the results of the case

From a general perspective, the role of the proposed methodology in the prevention of accidents from malicious manipulations of the control system can be demonstrated through case studies coming from past accident analysis (see Section 3.1.4). For example, in 1982 the manipulations that led to the over-pressurization of the Trans-Siberian gas pipeline and the consequent explosion [142] could have been identified through PHAROS analysis and appropriate countermeasures could have been adopted in order to prevent the major accident (e.g., a proper design of the installed PSVs). In the same way, the intentional burnout of a pump that was induced by attackers by remote manipulations of the control system of a water plant in Springfield, in 2011 [142], would have been identified through the application of this methodology and taken into account for a safer design of both the IT-OT system and the physical plant.

Some general conclusions may also be drawn from the analysis of the results of the case study. In particular, a simplified criticality analysis was carried out to point out the most relevant items (e.g., RMCs) among the ones relevant for a specific issue (e.g., MAs and CMs). It is based on the count of the items relevant to each of the issues considered: the reader is referred to the Appendix reported at the end of this Chapter for details on the procedure applied for simplified criticality analysis. Alternative combinations of RMCs exist for the same MA; the complete list for ND_F is reported in **Table A.1** in the Appendix of this Chapter together with the effective safeguards (both inherent/passive and active/procedural safeguards).

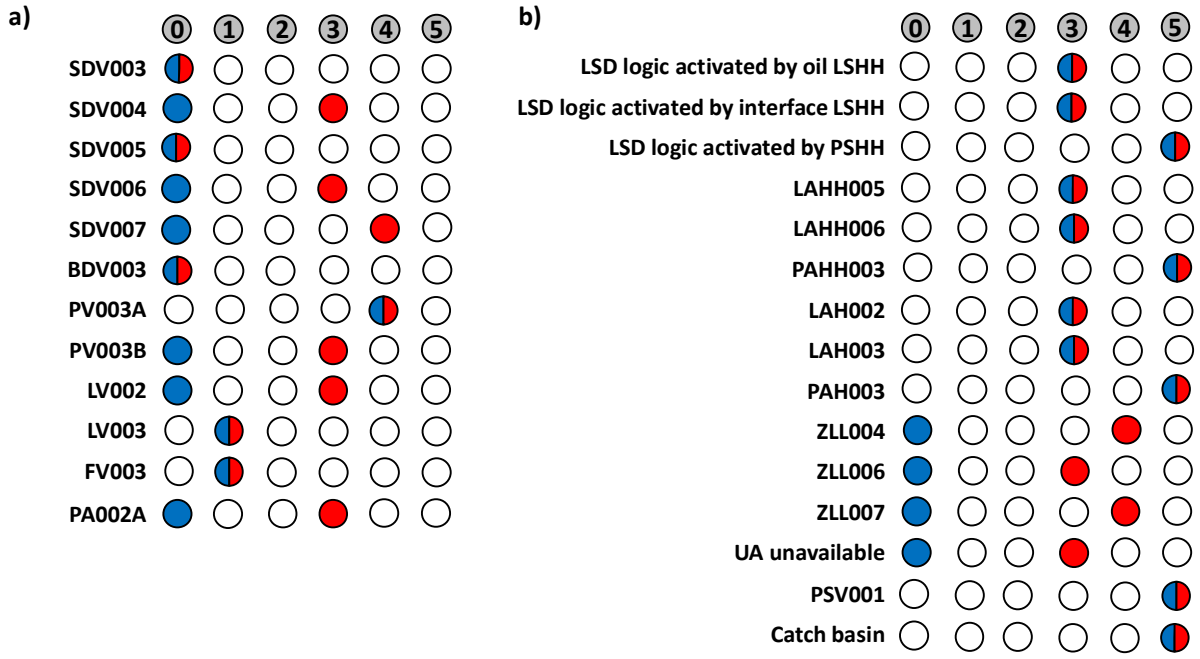

Figure 39 Criticality of the RMCs and of the safeguard components for the MAs of ND_F. a) minimum number (blue colour) and maximum number (red colour) of MAs involving the manipulation of each RMC; b) minimum number (blue colour) and maximum number (red colour) of MAs for which each safeguard component is effective. Adapted from [101].

Figure 39-a shows the results of a criticality analysis addressing the role of the different RMCs allocated to the node ND_F. The figure reports, for each RMC, the number of MAs that involve the manipulation of the RMC. As **Table 18** identified some alternative combinations of RMCs with equivalent effect on the system under assessment (e.g., SDV004 is alternative to LV002 for MA16.1, $MA_{13+16}.1$ and $MA_{13+16}.2$), the criticality analysis of each RMC shows a maximum and a minimum number (respectively in red and blue colours in the figure). The minimum values refer to MAs for which the RMC manipulation is strictly required, while the maximum value refers to all the MAs for which the RMC has a role in at least one combination.

The figure allows, on the one hand, the identification of the more critical components and, on the other hand, the understanding of the minimum number of elements that need to be manipulated to cause a critical event. In the case study analysed, the control valve PA003A is found to be the most critical component of the system, as it needs to be manipulated in four out of five identified MAs (it is not relevant for MA16.1). The blowdown valve BDV003 and the shutdown valves SDV003 and SDV005 result to be the less critical RMCs as they do not need manipulation for any MA. Some other components (e.g., SDV004) can be part of many MAs leading to a CE (i.e., high maximum score), but their protection may not be considered to receive a high priority as there are always alternative RMCs that can be manipulated achieving the same effects (i.e., the minimum criticality score is 0).

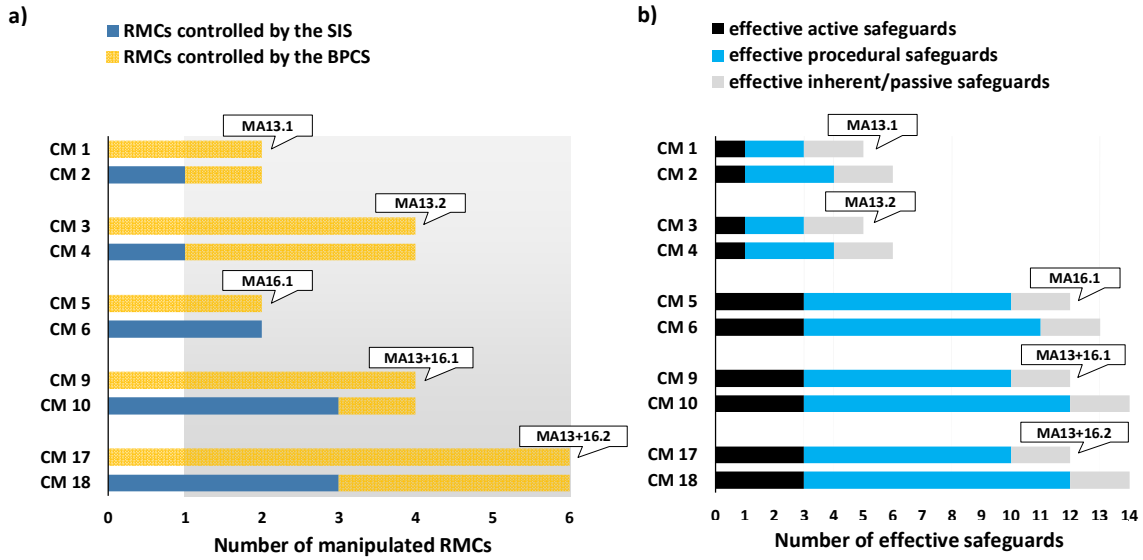

Figure 40 Criticality of the RMCs and of the safeguard components for the MAs of ND_F. a) number of RMCs involved in sample combinations for each MA; b) number of effective safeguard components involved in sample combinations for each MA. See **Table A.1** in the Appendix of this Chapter for definitions of CMs. Adapted from [101].

Figure 40-a shows the number of RMCs allocated to the node ND_F which need to be manipulated to achieve a MA, either by attacking the BPCS or the SIS. As multiple CMs exist for each MA, two sample combinations for each MA were presented (complete list in **Table A.1** in the Appendix of this Chapter). The diagram shows that, for all the considered CMs, the attackers do not always need to affect both the systems in order to be able to successfully impart the necessary manipulations. All the identified MAs may be obtained by infecting only the BPCS, and the mechanism MA16.1 may be also obtained by an action on RMCs controlled exclusively by the SIS. Thus, it may be concluded that in a standard set up, physical components may be in principle manipulated generating critical events only using the BPCS.

However, in order to successfully conduct an attack resulting in a critical event on the process equipment, the attackers have also to bypass the safeguards in place. If active and/or procedural safeguards are present, this also requires the manipulation of the SIS besides the BPCS. This fact is in favour of security, being the BPCS and the SIS typically separated one from the other in the IT-OT network architecture.

In the facility analysed in the case study, that is representative of standard design of process plants in the chemical and process industry, no mechanism of action can be achieved by manipulating only a single RMC (the minimum number of manipulated RMCs required is 2, for mechanisms MA13.1 and MA16.1). A higher complexity of the mechanism of attack is generally regarded in favour of higher security level (e.g., defence in depth).

It should also be remarked that a high level of redundancy of active and procedural safeguards is present, as part of a standard design procedure required by conventional safety management of systems processing relevant amounts of hazardous substances. Nevertheless, some safeguards are more critical, as they are effective on more than one MA. As shown in **Figure 39-b**, the SIS logic activated by the PSHH and the alarms PAHH003 and PAH003 are effective for all the identified MAs, requiring a priority in their maintenance at IT-OT system level (e.g., by the implementation of dedicated cybersecurity countermeasures to the respective zones and conduits in the IT-OT system). Actually, if the attacker aims to originate critical events on the process equipment belonging to node ND_F, they necessarily have to tamper with these safeguards.

Altogether, these findings support cybersecurity risk assessment as described in ISA/IEC 62443, as they link consequences to OT elements. This facilitates the assessment in the definition of the zones and conduits, in the definition of impacts, and in the identification of relevant countermeasures, etc. These pieces of information can also support the identification of the measures for human error reduction to protect the APSs more relevant in preventing a successful cyber-attack to the control system.

Figure 40-b reports the number and the type of effective safeguard components that may contrast each of the selected sample CMs for each MA. For all the reported combinations, there are both effective active/procedural safeguards (APSs) and inherent/passive safeguards (IPSs) in place: this is obviously in favour of a higher security level, especially considering that only the APSs may be made unavailable as a result of an attack. The identification of IPSs is extremely important as they provide a layer of protection independent from the automated control system, whose effectiveness and likelihood of failure has to be taken into account in the cybersecurity risk assessment (e.g., ISA/IEC 62443). For the plant under assessment, two IPSs are present: the catch basin and the pressure safety valve PSV001. The first has only a mitigative function (it limits liquid spreading in case of spill, decreasing the severity of accidental scenarios), while the second may be suitable to block the MAs, potentially making ND_F safe from attacks aimed at the discussed CEs. However, the valve PSV001 is typically sized on the basis of relieving rates that do not include a malicious manipulation scenarios [192]. Hence, the sizing of critical IPS, as safety valves, may be revised taking into account the security cases identified by the present approach and introducing them in the sizing procedure of API 521 RP [192]. In fact, sizing of a safety relief valve is typically based on relieving rates defined according to anomalous process conditions, which do not include malicious manipulation scenarios. A reference standard frequently used is API standard 520 [193].

In case of valve *PSV001*, the design cases from API standard 521 [192] (i.e., safety-related design cases) are closed outlet (blocking of the gas outlet, line 6 in **Figure 38**) and the external fire (venting requirement for generated gas/vapour in case of vessel isolation (shut down) and energy input from an external fire).

For the safety-related design cases the minimum required discharge area for the valve was calculated following the API standard 520, and the actual orifice area was selected according to API standard 526 [194] (see **Table 19**). On the basis of the safety-related cases, the valve is sized for the external fire case, resulting in a required discharge area of 799 mm^2, and a type J orifice (830 mm^2) installed [194].

The analysis carried out with PHAROS identified other five security-related design scenarios, corresponding to manipulations of the identified MAs (see **Table 18**). The required relieving capacity and the minimum area (see **Table 19**) were identified by a trial-and-error procedure based on Aspen HYSYS Dynamics simulation of the manipulations of each MA on a realistic model of the three-phase separator. This allowed to take into account the dynamic effect in the pressurization of the vessel. API standard 520 defines maximum overpressure (i.e., pressure increase over the set pressure of the PSV) of 10% of set pressure for non-fire cases and of 21% for fire cases, but it provides no value for security-related cases. Hence, both values were explored in **Table 19**.

Table 19 shows that, in the specific case of the Three Phase Separator VS003, a PSV001 designed for the external fire case is an effective safeguard also for all the MAs identified by PHAROS. By converse, if the PSV001 valve was sized for the "closed outlets" case, it would not be fully effective for pressurization scenarios deliberately introduced through a malicious manipulation of the automated control and safety systems. Generalizing, this provides a warning on the critical role that a check on the effectiveness of IPSs has in preventing critical events from malicious remote manipulations of BPCS and SIS.

Table 19 Sizing of the pressure safety valve PSV001 [192–194]. Adapted from [101].

Sizing for	Set pressure	Overpressure	Required relieving capacity	A_{min}	$A_{standard}$ orifice	Phase
Safety-related case: closed outlets	22 barg	10%	2244 kg/h	127 mm^2	198 mm^2 (type F)	Gas
Safety-related case: external fire	22 barg	21%	11448 kg/h	799 mm^2	830 mm^2 (type J)	Gas
Security-related case: mechanism of action MA13.1	22 barg	21%	2244 kg/h	115 mm^2	126 mm^2 (type E)	Gas
		10%	2244 kg/h	127 mm^2	198 mm^2 (type F)	Gas
Security-related case: mechanism of action MA13.2	22 barg	21%	4488 kg/h	229 mm^2	325 mm^2 (type G)	Gas
		10%	4488 kg/h	252 mm^2	325 mm^2 (type G)	Gas
Security-related case: mechanism of action MA16.1	22 barg	21%	9280 kg/h	65 mm^2	71 mm^2 (type D)	Gas-liq
		10%	9280 kg/h	108 mm^2	126 mm^2 (type E)	Gas-liq
Security-related case: mechanism of action MA_{13+16}.1	22 barg	21%	31340 kg/h	275 mm^2	325 mm^2 (type G)	Gas-liq
		10%	31340 kg/h	305 mm^2	325 mm^2 (type G)	Gas-liq
Security-related case: mechanism of action MA_{13+16}.2	22 barg	21%	57700 kg/h	500 mm^2	507 mm^2 (type H)	Gas-liq
		10%	57700 kg/h	570 mm^2	830 mm^2 (type J)	Gas-liq

4.3. POROS methodology

4.3.1. Detailed description of the methodology

The POROS methodology consists in nine steps, as shown in **Figure 41**.

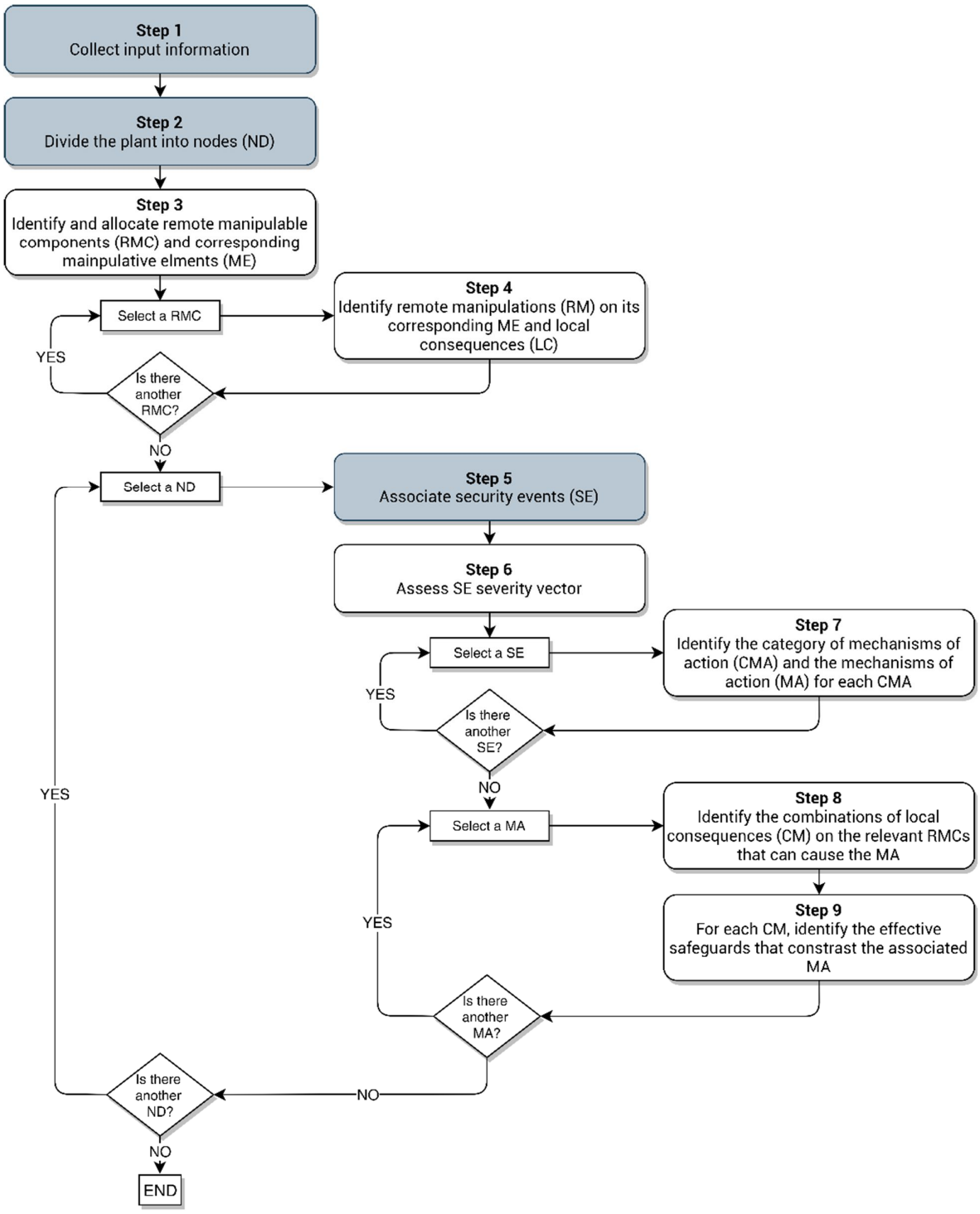

Figure 41 Flowchart of the POROS methodology. Shaded steps can be integrated with conventional safety studies. Adapted from [100].

Step 1 of POROS methodology coincides with Step 1 of PHAROS methodology: the reader is referred to Section 4.2.1 for the sake of brevity.

Step 2, the plant is divided into nodes (NDs). Each node comprises a main process equipment (e.g., storage vessel, column, reactor, etc.), the auxiliary equipment (e.g., pump, drum, etc.), and the pipework. **Table 10** reports the main general categories of plant items based on the classification provided by ARAMIS [99,178]. Unlike PHAROS application, not only the nodes in which hazardous substances are processed or stored are considered in the POROS application: in fact, utilities (e.g., cooling water system, power generation system, instrument air system), if included in the scope of the assessment, are also considered as nodes. The division in nodes is conceptually similar to that adopted in HazOp studies (described by the standard IEC 61882 [97]): if such a study is already available for the same plant, the HazOp nodes can be adopted.

Step 3 of POROS methodology coincides with Step 4 of PHAROS methodology: the reader is referred to Section 4.2.1 for the sake of brevity.

Step 4 of POROS methodology coincides with Step 5 of PHAROS methodology: the reader is referred to Section 4.2.1 for the sake of brevity.

Step 5 consists in associating to each ND the compatible security events[4] (SEs). A SE is an undesired event that affects the operability and/or the physical integrity of the system under investigation. Examples of SE may include loss of containment (LOC) or loss of physical integrity (LPI), stop of plant operations (e.g., activation of shutdown logics), equipment damage (e.g., failure of equipment components), operation out of specification (e.g., product out of specifications, emissions out of limits, waste of raw materials), etc.

The categories of LOCs and LPIs proposed e.g., by the standard API 581 [185], the MIMAH methodology [99] and the "Purple Book" [186], can be used as reference. **Table 20** reports a suggested list of possible SEs. Case specific LOC or LPI emerging from available safety and operability studies (e.g., HazOp [97], failure modes and effect analysis (FMEA) [98], DyPASI [187]), shall be included in the list of CEs for the node. This step is based on the review of the P&IDs, of the list of substances stored or handled and their hazardous properties, of the control philosophies, and of the safety instrumented functions.

[4] They are named "security events" to differentiate them from the "critical events" of PHAROS methodology; in fact, the term "critical event" is typically adopted in the literature in reference to a major accident scenario (e.g., ARAMIS [99]), while POROS methodology addresses also operability issues.

Table 20 Proposed classes for security events (SEs) and related categories of mechanisms of action (MAs). Adapted from [100].

Security events	Category of mechanisms of action	Example
SE01: product out of specification	CMA01: composition/phase out of specification	Contamination of the product
	CMA02: temperature out of specification	Excessive viscosity of the product
	CMA03: pressure out of specification	Steam out of specification
	Other	
SE02: arrest/blockage of a piece of equipment/item	CMA04: valve closure/opening	Production stop by closure of a remotely operated block valve Production stop by opening of a remotely operated valve on bypass line Production stop by opening of a remotely operated depressurization valve
	CMA05: motor or driver arrest	Stop of the electric motor of a pump Stop of the electric motor of a compressor Stop of the electric motor of a conveyor
	CMA06: induce the plugging/packing	Alteration of set point controlling the solid/liquid ratio of a slurry Stop of the agitator
	Other	
SE03: activation of ESD/PSD/LSD logic	CMA07: direct activation of ESD/PSD/LSD logic	Generating a false signal from a manual activation button of ESD/PSD/LSD
	CMA08: temperature exceeding safety limits	Change of operative conditions, inducing a TAHH
	CMA09: pressure exceeding safety limits	Change of operative conditions, inducing a PAHH
	CMA10: level exceeding safety limits	Change of operative conditions, inducing a LALL
	CMA11: composition exceeding safety limits	Change of operative conditions, inducing a decrease of pH Change of a reactant dosage in a highly exothermic reaction system
	CMA12: unavailability of essential services	Stop of instrument air generator Inducing failure of the pilot flame of a flaring system
	Other	
SE04: exceeding design specification for construction materials	CMA13: material damage by temperature	Lowering temperature below brittle point Rising temperature above creep condition
	CMA14: material damage by load	Inducing excessive pressure/vacuum Inducing excessive thermal expansion

		Inducing fatigue failure by load cycles
	CMA15: material damage by chemical incompatibility	Adding corrosive material Adding plasticizer material
	CMA16: material damage by mechanical action	Inducing erosion (excessive solid) Inducing cavitation
	Other	
SE05: damage of moving components/machinery	CMA17: inducing driver failure	Inducing electric motor failure in a pump Inducing membrane actuator failure
	CMA18: inducing component failure of moving systems	Cycling of a valve leading to excessive wearing of seals Stop of lubrication or cooling
	CMA19: exceeding operative limits	Exceeding surge/stonewall limit in a compressor Exceeding low/high flow limits of the pump
	Other	
SE06: loss of containment (LOC) and loss of physical integrity (LPI)	CMA20: induce a thermal or chemical decomposition	Exceeding onset temperature for decomposition
	CMA21: induce an explosion	Mixing incompatible materials
	CMA22: start a fire	Deactivation of inerting system for pyrophoric materials
	CMA23: damage of the construction material of the containment system (see SE04)	See examples in SE04
	CMA24: damage of moving components in the containment system (see SE05)	See examples in SE05
	CMA25: over-filling	Overfilling of an atmospheric storage tank
	Other	
SE07: Other	Other	

In Step 6 a severity level is associated to each SE. A qualitative severity scale is proposed in **Table 21**. The scale is compliant with the guidelines on severity scales outlined by Baybutt [195], and it was developed starting from the process safety metrics proposed by the Center for Chemical Process Safety (CCPS) [196] and the categorization of impacts sketched by Hausken [197]. Four severity levels are considered (1 - minor impact, 2 - medium impact, 3 - major impact and 4 - extensive impact), exploring four types of target values (EC: economic value, IV: influence value, EN: environmental value, HV: human value). In **Table 21**, the loss of economic value is given by the sum of direct costs (e.g., repair or replacement of process equipment) and indirect costs (e.g. loss of profits due to production downtime); loss of human value accounts both for the injuries (e.g., amputations, diseases, physical damages) and/or on-site and/or off-site fatalities following the security event; loss of influence value is associated to the reduction of the symbolic, political and economic prestige of the affected facility and thus it is strongly related to reputation; loss of environmental value is

accounted for the long- or short-term effects on the physical environment (air, water or soil) requiring environmental remediation. A severity vector is defined for each SE reporting the scores for the four target values ([EC, IV, EN, HV]).

Useful information for evaluating the severity score concerns the material balances, the datasheets of tagged items, the list of substances stored/handled and their hazardous properties.

The ranking of SE severity provided supports the evaluations of the worst-case impact scenario as requested in the framework of the ISA/IEC 62443 series of standards (more specifically in step ZCR 5.3 "Determine consequences and impact" of ISA/IEC 62443-3-2 in **Figure 33**).

A high number of SEs is usually identified at Step 5. However, it is recognized that efforts in improvement of preventive and mitigation measures shall target primary the SEs with the higher level of concern for a given context. The application of a cut-off criteria (Step 6) setting a threshold value for the severity level is suggested. The use of threshold values in the analysis of scientific uncertainty related to a threat (i.e., the cyber threat in this case) is customary among the authors in the literature (e.g., see Hausken [198], Bschir [199], and Koch at al. [200]).

A simple cut-off focusing on SE with the highest level of severity (i.e., severity level ≥ 3 for at least one target type) is suggested for general application, based the high risk aversion typically expected for severe scenarios [19].

Nevertheless, other cut-off criteria are possible, especially when well characterised cyber-threat sources are of concern. In facts, the generic cut-off suggested above does not take into account that the goal of the attacker is influenced by factors such as his/her beliefs, preferences, motivations, and capabilities [126,201–203]. For example, while triggering a major event with severe consequences in terms of human value may be a likely goal for a well-equipped and high-motivated terrorist organization, it is not expected to be the case for non-violent activists motivated by pacific rebellion.

While categorization of the goals of the attacker lays beyond the scope of current methodology, it is commonly performed as part of conventional SVA/SRA methods (see e.g., “Identify Threat” step ZCR 5.1 in ISA/IEC 62443-3-2, or “Attacker Identification” step 3.1 in CCPS SVA methodology). The categorization of SEs from Step 5 in terms of severity vector will help the identification of the ones matching the goals of specific attackers. **Table 22** proposes an example of expected ranges for the severity vector values for the SE selection with reference to different types of attacker (classification of attacker adapted from ISO/IEC 27005).

Table 21 Severity scale adopted for severity ranking of the SEs. Adapted from CCPS [196] and Hausken [197].

Severity level		Loss of economic value (EC)		Loss of influence value (IV)	Loss of environmental value (EN)	Loss of human value (HV)
1	MINOR IMPACT	Cost of total losses < $100K	No disruption or possible short disruption of operations/business	No loss of reputation. OR Minor and short-lived impact in the locality. OR Local media coverage.	Short-term remediation to address acute environmental impact. No long-term cost or company oversight.	Injury requiring treatment beyond first aid to employees or contractors (but no lost time injury).
2	MEDIUM IMPACT	Cost of total losses between $100K and $1MM	Medium time/medium change to resume operations/business. Unit repair/replacement needed.	Significant potential damage to the regional reputation. OR Regional media coverage.	Environmental remediation required with cost less than $1MM. No other regulatory oversight required.	Lost time injury to employees or contractors. OR Minor off-site impact with precautionary shelter-in-place
3	MAJOR IMPACT	Cost of total losses between $1MM and $10MM	Long time/major change to resume operations/business. Unit repair/replacement needed.	Serious/permanent damage to the ability of the Company to sustain business position in the location, some broader implications for the Company. OR National media coverage.	Environmental remediation required and cost in between $1MM - $2.5 MM. State government investigation and oversight of process.	On-site fatality employees or contractors; multiple lost time injuries or one or more serious offsite injuries. OR Shelter-in-place or community evacuation.
4	EXTENSIVE IMPACT	Cost of total losses > $10MM	Total loss of operations/business. Revamping necessary to resume the process.	Potential loss of future business position in the location/region and significant broader implications for the Company. OR National media coverage over multiple days.	Environmental remediation required and cost in excess of $2.5 MM. Federal government investigation and oversight of process.	Off-site fatality or multiple on-site fatalities. OR Other significant community impact.

Table 22 Example of classifications of the type of attackers, their motivations, the possible consequences that can be generated, and expected ranges for the severity vector values associated to the possible consequences.

Attacker	Motivations / preferences	Possible consequences	Expected target Severity of impacts (see Table 21)
Hacker, Cracker, Non-violent hacktivist	Challenge, ego, rebellion, status, monetary gain, media coverage	- Hacking - Social engineering - System intrusion, break-ins - Unauthorized system access	EC: minor (1) to extensive (4) IV: medium (2) to extensive (4) EN: minor (1) HV: minor (1)
Insider	Curiosity, ego, intelligence, monetary gain, revenge	- Assault on an employee - Blackmail - Browsing of proprietary information - Computer abuse - Fraud and theft - Information bribery - Input of falsified, corrupted data - Interception - Malicious code - Sale of personal information - System bugs - System intrusion - System sabotage - Unauthorized system access	EC: medium (2) to extensive (4) IV: medium (2) to extensive (4) EN: minor (1) HV: minor (1)
Nation-state State-sponsored organization	Competitive advantage, economic espionage	- Defence advantage - Political advantage - Economic exploitation - Information theft - Intrusion on personal privacy - Social engineering - System penetration - Unauthorized system access	EC: major (3) to extensive (4) IV: major (3) to extensive (4) EN: major (3) to extensive (4) HV: major (3) to extensive (4)
Terrorist, Violent hacktivist, Cyber-criminal	Destruction, exploitation, revenge, political gain, media coverage	- Bomb/terrorism - Information warfare - System attack - System penetration - System tampering	EC: medium (2) to extensive (4) IV: medium (2) to extensive (4) EN: medium (2) to extensive (4) HV: medium (2) to extensive (4)

Step 7 consists in identifying all the mechanisms of action (MAs) that may generate each SE through an attack to the OT system, and thus it is conceptually similar to Step 7 of PHAROS methodology (see Section 4.2.1) The MAs are the physical mechanisms that the attackers may use to initiate the SE (e.g., increase the internal pressure of a vessel by closing the gas outlets). **Table 20** shows reference categories of mechanisms of action (CMAs) for each SE and some examples of MAs. The categories of mechanism of action (CMAs) can support the identification of the MAs by grouping them in conceptually similar categories. As a matter of facts, more than one MA can typically be identified based on the same CMA (e.g., considering a chemical reactor, the category "CMA01: composition/phase out of specification" may be realized through different mechanisms of action: by changing flowrates of reactants, by changing temperature, by changing pressure, by changing residence time, etc.).

Although the CMAs in **Table 20** provide a guideline for the identification of the mechanisms of action, developing MAs tailored to the design features of the ND under assessment is required, as some mechanisms of action may be case specific (e.g., number and arrangement of input/output lines may vary). Therefore, process documentation such as PFDs, P&IDs, control philosophies, and safety instrumented functions, supports the identification of MAs. If a HazOp study or a fault tree analysis are available for the ND, they can complement this step of MA identification, since many of the applicable mechanisms of action are possibly identified by such studies.

If there are no possible MAs for a SE, the SE is removed from those previously associated to the ND under investigation. Some MAs may require actions from a nearby node to occur (i.e., manipulation of RMCs belonging to a nearby node is required). In these cases, the information is propagated from a node to another similarly to deviations propagating among different nodes in a traditional HazOp study.

Step 8 and Step 9 of POROS methodology coincide with steps 8 and 9 of PHAROS methodology: the reader is referred to Section 4.2.1 for the sake of brevity. Clearly, also for POROS application, these two steps can be supported for each ND by the worksheet shown in **Figure 36**.

Similarly to an HazOp study, once all the steps have been performed, a completeness check is required. It consists in verifying that all the NDs have been analysed, and that all the MAs, through which the associated SEs can be originated, were developed as CMs. Particular attention shall be given to completeness check in case of SEs that require manipulations on RMC in more than one ND.

4.3.2. Illustrative case study

4.3.2.1. Set-up of the case study

An offshore Oil&Gas platform for gas compression is considered in the case study.

Figure 42 shows the simplified block diagram of the process, while **Figure 43** shows the simplified P&ID of the section within the scope of the analysis (node ND_1 and node ND_2 in the following). The inlet stream from the sealine is separated by the Slug Catcher SC100. The liquid phase is sent to the liquid treatment section (out of the scope of current study), while the gas phase is sent to a two-stage compression with intermediate cooling by seawater (exchangers HE100 and HE101). The compressors CR100 and CR101 are driven by a gas turbine TR100. The KO drums KD100 and KD101 avoid the presence of liquid in the suction lines of the compressors. More details on the items present in the plant section of interest are reported in **Table 23**.

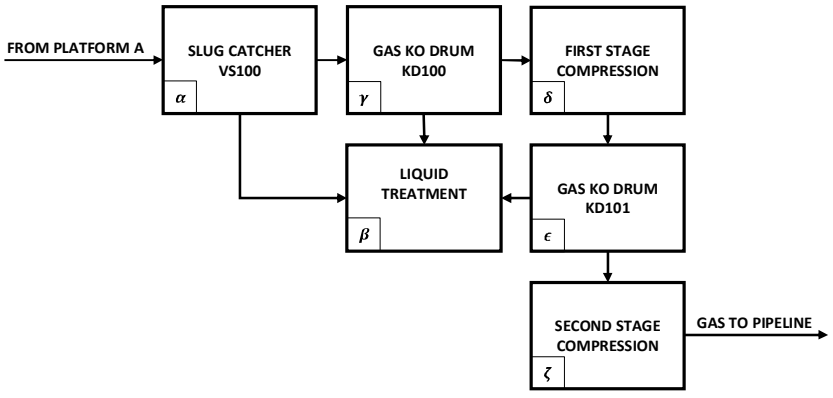

Figure 42 Simplified block diagram of the Oil&Gas platform considered in the case study.

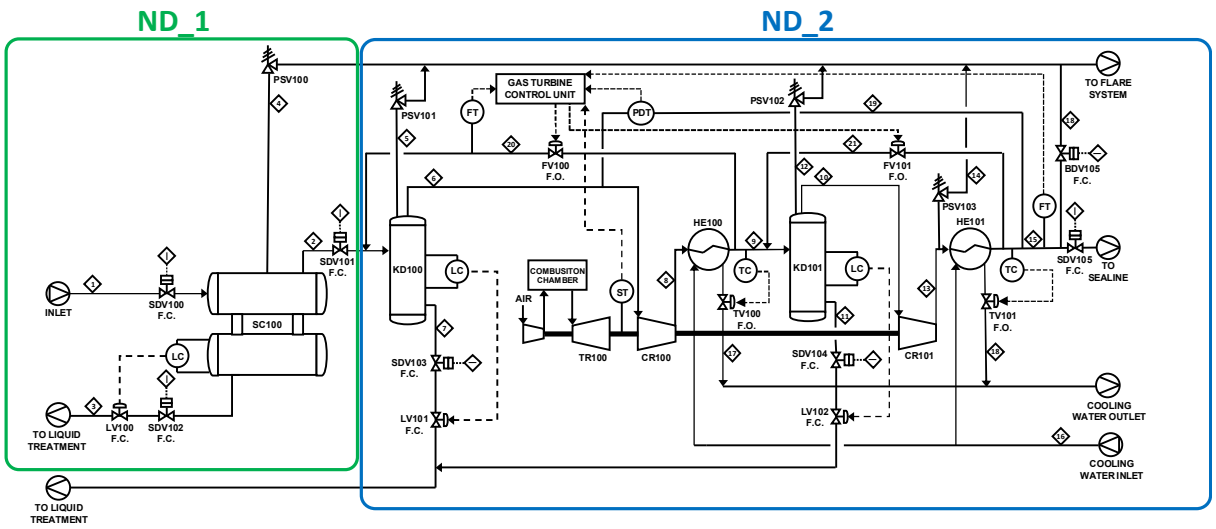

Figure 43 Simplified P&ID of the nodes ND_1 ("Slug Catcher") and ND_2 ("Two-phase compression"). Adapted from [100].

Table 23 Description of the items present in node ND_1 and ND_2 (see also **Figure 43**). Adapted from [100].

EQ codes (Step 2)	Items (Step 2)	Description
EQ1.2	Slug Catcher VS003	Pressurized vessel for the separation of Stream 1 into a gas phase and a liquid phase
	KO drum KD100/1	Pressurized vessel aimed at eliminating liquid traces from Stream 2 and 9 respectively
EQ2.1	Heat Exchanger HE100/1	S&T heat exchanger aimed at cooling down Stream 8 and 13 respectively
EQ7.2	Gas turbine TR100	Combustion engine for compressors CR100/1
EQ5.2	Compressor CR100/1	Centrifugal compressor in Stream 6 and 10 respectively
EQ4.1	Stream 1	Process inlet stream from Platform A
	Stream 2	Process stream (gas phase) from VC100 to KD100
	Stream 3	Process stream (liquid phase) from VC100 to liquid treatment
	Stream 4/5/12/14	Emergency stream (PSV) to HP Flare (gas phase)
	Stream 6	Process stream (gas phase) from KD100 to CR100
	Stream 7	Process stream (liquid phase) from KD100 to liquid treatment
	Stream 8	Process stream (gas phase) from CR100 to HE100
	Stream 9	Process stream (gas phase) from HE100 to KD101
	Stream 10	Process stream (gas phase) from KD101 to CR101
	Stream 11	Process stream (liquid phase) from KD101 to liquid treatment
	Stream 13	Process stream (gas phase) from CR101 to HE101
	Stream 15	Process stream (gas phase) from HE101 to sealine
	Stream 16/17	Utility inlet stream (cooling water) to HE100/1 respectively
	Stream 18/19	Utility outlet stream (cooling water) from HE100/1 respectively
	Stream 20	Instrumentation stream (PDT)
	Stream 21	Recircle stream (gas phase) to KD100
	Stream 22	Recircle stream (gas phase) to KD101

4.3.2.2. Results of the case study

Following the collection of the input data (Step 1 of the methodology), the process under investigation was divided into nodes according to the typical rules of the HazOp study [97] (Step 2 of the methodology). For the sake of brevity, the application of POROS methodology is demonstrated on the process nodes ND_1 and ND_2 (see **Figure 42**): ND_1 includes the slug catcher SC100 and the connected pipework, while ND_2 includes the gas turbine, the KO drums KD100 and KD101, the heat exchangers HE100 and HE101, and the connected pipework.

After the division into NDs, the remote manipulable components (RMCs) which are present in the plant under assessment, and the associated manipulative elements (MEs) were identified following the guidelines provided in **Table 11** (Step 3 of the methodology). The identified RMCs and associated MEs were then allocated to the two nodes (ND_1 and ND_2) in accordance with the rules described in Section 4.2.1 (**Table 24** summarizes the results). In this specific case, the RMCs include emergency valves (blowdown valve and shutdown valves), control valves and a motor-driven gas turbine. The shutdown valves and the blowdown valve are shut-off valves controlled by the SIS by means of controllers such as PLCs (Programmable Logic Controllers), that are the MEs on which an attacker can act. The control valves are controlled by the BPCS by means of controllers such as PIDs (Proportional Integral Derivative), while the gas turbine is controlled by both BPCS and SIS systems.

The remote manipulations (RMs) for the MEs were identified in accordance with the guidelines provided in **Table 11** (Step 4 of the methodology). "Signal shutdown" (code RM1) and "function reprogramming" (code RM3) were considered for the PLCs of the SIS (acting on the shut-off and blowdown valves) and of the BPCS (acting on the gas turbine); "signal shutdown" (code RM1) and "setpoint change" (code RM2) were considered for the PIDs controllers of the BPCS (acting on the control valves).

The local consequences (LCs) on the RMCs that result from the RMs associated to each ME were then identified applying the typical associations of RMs and LCs shown in **Table 11**. This requires the consideration of the fail-safe nature of all the automatic valves [58], the control action of the PID controllers (direct or reverse), the logics of the PLCs and the safety instrumented functions of the SIS.

Table 24 summarizes the remote manipulations (RMs) and the local consequences (LCs) on the total RMCs that are present in the plant under investigation. For example, the control valve LV100 (see **Table 24** and **Figure 43**), as a consequence of a signal shutdown (RM1) to the PID controller by which the valve is managed (i.e. its ME), stops the flow (LC2) as it fails in the closed position.

Table 24 Remote manipulations (RMs) and local consequences (LCs) for each RMC allocated to the nodes ND_1 and ND_2. Adapted from [100].

RMCs (Step 3)	RMC codes (Step 3)	Allocated to (Step 3)	ME codes (Step 3)	RM codes (Step 4)	LC codes (Step 4)
SDV100 SDV101 SDV102 SDV103 SDV104 SDV105	RMC1: shut-off valves (F.C.)	ND_1 ND_1 – ND_2 ND_1 ND_2 ND_2 ND_2	ME2: Safety Instrumented System devices	RM1: signal shutdown RM3: function reprogramming	LC2: valve closing LC2: valve closing
BDV105	RMC1: shut-off valve (F.O.)	ND_2	ME2: Safety Instrumented System devices	RM1: signal shutdown RM3: function reprogramming	LC1: valve opening LC1: valve opening
LV100 LV101 LV102	RMC2: control valves (F.C)	ND_1 ND_2 ND_2	ME1: Basic Process Control System devices (PID controllers)	RM1: signal shutdown RM2: setpoint change	LC2: valve closing LC7: increase in valve opening degree LC8: decrease in valve opening degree LC9: opening-closing cycles of the valve
TV100 TV101 FV100 FV101	RMC2: control valves (F.O)	ND_2 ND_2 ND_2 ND_2	ME1: Basic Process Control System devices (PID controllers)	RM1: signal shutdown RM2: setpoint change	LC1: valve opening LC7: increase in valve opening degree LC8: decrease in valve opening degree LC9: opening-closing cycles of the valve
GAS TURBINE (TR100 + CR100 + CR101)	RMC4: gas turbine (launched by electric motor)	ND_2	ME1: Basic Process Control System device (PLC)	RM1: signal shutdown RM3: function reprogramming	LC5: stop of the gas turbine LC5: stop of the gas turbine LC10: Increase of the rotational speed of the gas turbine LC11: Decrease of the rotational speed of the gas turbine

			LC12: cycles of increase-decrease of the rotational speed of the gas turbine LC13: start of the gas turbine LC14: start and stop cycles of the gas turbine
	ME2: Safety Instrumented System device	RM1: signal shutdown	LC5: stop of the gas turbine
		RM3: function reprogramming	As for RM3 on ME1

The identification of the security events (SEs) for ND_1 and ND_2 was performed in accordance with the guidelines provided in **Table 20**, taking into account the specific features of the physical equipment/components in the assessed process (Step 5 of the methodology). In particular, all the SEs listed in the table were considered applicable for ND_2, while for ND_1 only SE05 (damage of moving machinery/component) was not taken into consideration.

The SEs associated to the two NDs under investigation were scored for their severity according to the scale proposed in **Table 21**. The severity scoring was based on a preliminary estimation of the consequences expected by each SE for the selected node (**Table 25**). For instance, inducing or directly activating an Emergency Shut Down (ESD) leading to the arrest and depressurization of the two compressors (ND_1-SE03 or ND_2-SE03 in **Table 25**) is expected to cause a downtime of the plant (i.e., total amount of time without productivity) of about 6 hours, with no loss of containment or energy release. Hence, no damage to environment, people, and reputation is expected (severity level 1: minor impact). However, considering an average value of production of 1'420'000 $/day, a total cost of losses of about 355'400$ was estimated (i.e., medium impact according to **Table 25**). Therefore, a severity level of 2 was assigned to SE03 for both the nodes in **Table 25**.

Table 25 shows that tangible adverse consequences are expected for most SEs. This further confirms that operability and asset integrity issues induced by remote manipulation of the control system are of interest for facilities as the one analysed in the current case study. However, in this particular case, given e.g., the low potentiality of the plant, the economic losses resulting from short production downtimes (e.g., by stopping compressors with a dedicated command, as in ND_2-SE02) score medium to minor impacts. High severity levels are obtained for cases that trigger permanent damage to the equipment (ND_1-SE04, ND_2-SE04 and ND_2-SE05), which are characterized by longer downtimes and high costs of replacement, as well as by cases leading to loss of containment of flammable gases (SE06 for both nodes). In particular, the high cost of the compressors in ND_2 leads to identify any permeant damage to this equipment as level 4 severity SE for loss of economic value.

In the following, the discussion of the results of the case study will focus on the most severe SEs (at least one element of the severity vector ≥ 3), for which dedicated countermeasures at IT-OT level are a priority. Interestingly enough, the selection criterion matched the one presented for "state-sponsored organization" attacks identified in **Table 22**.

Table 25 Security events (SEs) considered applicable for ND_1 and ND_2 and severity vector assessed according to the severity scale proposed in **Table 21**. Adapted from [100].

Node	Items	SE code (Step 5)	Expected consequences[5] (Step 6)	Severity vector [EC, IV, EN, HV] (Step 6)	Cut-off (Step 6)
ND_1	Slug catcher SC100 Piping	SE01: product out of specification (incomplete separation)	No direct economic effect on ND_1. No damage to people or environment.	[1, 1, 1, 1]	Not selected
		SE02: arrest/blockage of a piece of equipment/item (closing liquid or gas outlet)	Stop of production: recovery follows normal start-up procedures (expected downtime 3h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE03: activation of ESD/PSD/LSD logic	Stop of production: recovery follows normal start-up procedures (expected downtime 6h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE04: exceeding design specification for construction materials	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 2 weeks). No damage to people or environment.	[4, 1, 1, 1]	Selected
		SE06: loss of containment (LOC) and loss of physical integrity (LPI)	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 4 weeks). Resulting fire may damage nearby equipment. No damage to people. Negligible damage to environment.	[4, 2, 1, 1]	Selected
ND_2	KO drum KD100 KO drum KD101 Turbine TR100 Compressor CR100 Compressor CR101	SE01: product out of specification (pressure)	Stop of production: recovery follows abnormal start-up procedures (expected downtime 3h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
		SE02: arrest/blockage of a piece of equipment/item (stop of electric motor)	Stop of production: recovery follows normal start-up procedures (expected downtime 3h).	[2, 1, 1, 1]	Not selected

[5] No damage to people is considered as expected consequence of any SE since the platform is normally unmanned.

Heat exchanger HE100 Heat exchanger HE101 Piping		No damage to people or environment.		
	SE03: activation of ESD/PSD/LSD logic	Stop of production: recovery follows normal start-up procedures (expected downtime 6h). No damage to people or environment.	[2, 1, 1, 1]	Not selected
	SE04: exceeding design specification for construction materials	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 2 weeks). No damage to people or environment.	[4, 1, 1, 1]	Selected
	SE05: damage of moving components/machinery	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 4 weeks). High costs for compressor repair and replacement. No damage to people or environment.	[4, 2, 1, 1]	Selected
	SE06: loss of containment (LOC) and loss of physical integrity (LPI)	Stop of production: recovery requires repair and replacement of equipment (expected downtime of 4 weeks). Resulting fire may damage nearby equipment. No damage to people. Negligible damage to environment.	[4, 2, 1, 1]	Selected

The credible mechanisms of action (MAs) by means of which an attacker can initiate any of the selected SEs for the node ND_2, were identified (Step 7 of the methodology). The identification was based on the applicable categories of mechanisms of action (CMAs) provided in **Table 20**. The list of MAs was generated tailoring the CMAs to the process equipment and items that are present in the node ND_2.

Table 26 summarizes the results obtained from Step 7. For example, MA4 (inducing excessive pressure by closing the gas outlets), MA5 (inducing excessive pressure by increasing the rotation speed of the gas turbine), and a combination of these two (MA6), are some of the MAs that may initiate SE04 (exceeding design specification for construction materials), all related to CMA14 (material damage by load). All the identified MAs will be at the basis of the definition of the combination of local consequences (CMs) in the next step.

The analysis carried out and the results of an available HazOp study evidenced that some CMAs identified can be obtained manipulating the nearby node ND_1. In particular, CMA18 (inducing component failure of moving systems) can be obtained through the mechanism of action MA8 (liquid fraction in the compressor suction line) which needs the manipulation of RMCs on ND_1. This deviation, propagating among the two

nodes, was tracked by re-selecting SE01, i.e., “product out of specification”, and more specifically in this case “liquid fraction in the gas outlet”, for the node ND_1. A “virtual RMC” (vRMC100) was then added to ND_2, representing the RMCs allocated to ND_1 that need to be manipulated in order to initiate such security event (i.e., SDV102 or LV100). Similarly, another virtual RMC (vRMC101), corresponding to the RMCs associated to the cooling system, was included in the list of the node ND_2: in facts, a damage to the construction material of the equipment by temperature in ND_2 (CMA13) is deemed possible through an induced unavailability of the cooling system (mechanism of action MA3). However, the node corresponding to the cooling system was not further developed in the current case study for sake of brevity.

No suitable MA was identified for SE04 and SE06 of node ND_1 (not reported in **Table 26**): the specific features of the equipment present in this node and the processed fluids do not allow many of the mechanisms listed in **Table 20** (e.g., no change of temperature is possible, pressure from upstream lines is always lower than design pressure).

Table 27 shows the results obtained in the assessment of Step 8 (identification of combinations of local consequences, CMs) and Step 9 (identification of effective active/procedural, and inherent/passive safeguards, APSs and IPSs) of the methodology for both the nodes ND_1 and ND_2.

For the sake of brevity, only the RMCs (and virtual RMCs) that need to be manipulated in at least one CM are shown in the table. In some cases, the manipulation of alternative RMCs is possible to achieve the same effect on the physical process (it is generally the case of a control valve and a shutdown valve on the same process stream). For instance, an attacker can increase the outlet temperature from HE100 or HE101 either by closing one or both the control valves TV100 and TV101 (MA2) through the change (increase) of the setpoint of the corresponding controller (with consequent decrease in valves opening degree, LC8), or alternatively, by making unavailable the cooling water system (i.e., manipulation of the virtual component vRMC101, MA3).

With respect to the identification of the effective safeguards (Step 9 of the methodology), taking as an example CM2.5 (see **Table 27**), the APSs that were identified through the revision of the P&IDs and relevant documentation are the LSD/PSD logics activated by PSHHs, the high and very high pressure alarms PAHs, the hand switch (HS) for manual activation of ESD/PSD/LSD logic, the position light for closed position (ZLL) of SDV105, the HS for its manual reset and the anti-surge loop, while the IPSs are the pressure safety valve PSV100, PSV101 and PSV102 (see **Figure 43**).

Table 26 Mechanisms of action (MAs) identified for SE in the nodes ND_1 and ND_2. Names of plant items are referred to **Figure 43** and described in **Table 23**. Adapted from [100].

Node	SE codes	CMA codes (Step 7)	MA codes (Step 7)
ND_1	SE01: product out of specification (liquid fraction in the gas outlet)	CMA25: over-filling	MA1: over-filling of SC100 by closing the liquid outlet
ND_2	SE04: exceeding design specification for construction materials	CMA13: material damage by temperature	MA2: increasing temperature by closing the cooling water line in HE100 and HE101 MA3: increasing temperature by making the cooling water unavailable
		CMA14: material damage by load	MA4: inducing excessive pressure by closing the gas outlet from HE101 MA5: inducing excessive pressure by increasing the rotation speed of the GAS TURBINE MA6: inducing excessive pressure by closing the gas outlet from HE101 + increasing rotation speed of the GAS TURBINE
	SE05: damage of moving components/machinery	CMA18: inducing component failure of moving systems	MA7: start and stop cycles or speed variation cycles of the GAS TURBINE by manipulating the fuel gas feed and the electric starter motor MA8: liquid fraction in CR100 and CR101 suctions by over-filling KD100 and KD101
		CM19: exceeding operative limits (surge limit)	MA4: inducing excessive pressure by closing the gas outlet from HE101 MA5: inducing excessive pressure by increasing the rotation speed of the GAS TURBINE MA6: inducing excessive pressure by closing the gas outlet from HE101 + increasing rotation speed of the GAS TURBINE
	SE06: loss of containment (LOC) and loss of physical integrity (LPI)	CMA23: damage of the construction material of the containment system	MA4: inducing excessive pressure by closing the gas outlet from HE101 MA5: inducing excessive pressure by increasing the rotation speed of the GAS TURBINE MA6: inducing excessive pressure by closing the gas outlet from HE101 + increasing rotation speed of the GAS TURBINE
		CMA24: damage of moving components in the containment system	MA7: start and stop cycles or speed variation cycles of the GAS TURBINE by manipulating the fuel gas feed and the electric starter motor MA8: liquid fraction in CR100 and CR101 suctions by over-filling KD100 and KD101

Table 27 List of combinations (CMs) of local consequences (LCs) on the relevant RMCs for each MA of the nodes ND_1 and ND_2. For each CM, effective active/procedural safeguards (APSs) and inherent/passive safeguards (IPSs) are reported. Adapted from [100].

Node	MA code	CM code (Step 8)	Relevant RMCs and LCs (Step 8)	Effective APSs (Step 9)	Effective IPSs (Step 9)
ND_1	MA1	CM1.1	SDV102 totally closed (LC2)	PSD logic activated by LSHH on SC100 High level alarm LAH on SC100 + HS for manual ESD/PSD/LSD Very high level alarm LAHH on SC100 + HS for manual ESD/PSD/LSD Position light ZLL for SDV105 + HS for manual reset of SDV105	None
		CM1.2	LV100 partially or totally closed (LC8 or LC2)	PSD logic activated by LSHH on SC100 High level alarm LAH on SC100 + HS for manual ESD/PSD/LSD Very high level alarm LAHH on SC100 + HS for manual ESD/PSD/LSD	None
ND_2	MA2	CM2.1	TV100 partially or totally closed (LC8 or LC2)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD	None
		CM2.2	TV101 partially or totally closed (LC8 or LC2)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD	None
		CM2.3	TV100 partially or totally closed (LC8 or LC2) TV101 partially or totally closed (LC8 or LC2)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD	None
	MA3	CM2.4	vRMC101 manipulated (unavailable cooling water)	High temperature alarms TAHs + HS for manual ESD/PSD/LSD Very high temperature alarms TAHHs + HS for manual ESD/PSD/LSD APSs present in the cooling system	None
	MA4	CM2.5	SDV105 totally closed (LC2)	LSD/PSD logics activated by PSHHs and Anti-Surge system High pressure alarms PAHs + HS for manual ESD/PSD/LSD Very high pressure alarms PAHHs + HS for manual ESD/PSD/LSD Position light ZLL for SDV105 + HS for manual reset of SDV105	PSV101 PSV102 PSV103
	MA5	CM2.6	GAS TURBINE with increased rotational speed (LC10)	LSD/PSD logics activated by PSHHs and Anti-Surge system High pressure alarms PAHs + HS for manual ESD/PSD/LSD Very high pressure alarms PAHHs + HS for manual ESD/PSD/LSD	PSV101 PSV102 PSV103
	MA6	CM2.7	SDV105 totally closed (LC2) GAS TURBINE with increased rotational speed (LC10)	LSD/PSD logics activated by PSHHs and Anti-Surge system High pressure alarms PAHs + HS for manual ESD/PSD/LSD Very high pressure alarms PAHHs + HS for manual ESD/PSD/LSD Position light ZLL for SDV105 + HS for manual reset of SDV105	PSV101 PSV102 PSV103
	MA7	CM2.8	GAS TURBINE started and stopped cyclically (LC14)	LSD logic activated by Anti-Surge system GAS TURBINE unavailability alarm UA + HS for manual ESD/PSD/LSD	None

MA8	CM2.9	SDV103 totally closed (LC2) vRMC100 manipulated (see MA1)	PSD logic activated by LSHH on SC100 LSD logic activated by LSHHs on KD100 High level alarms LAHs on SC100 and KD100 + HS for manual ESD/PSD/LSD Very high level alarms LAHHs on SC100 and KD100 + HS for manual ESD/PSD/LSD Position light ZLL for SDV103 + HS for manual reset of SDV103 (if manipulated) Position light ZLL for SDV102 + HS for manual reset of SDV102	None
	CM2.10	LV101 partially or totally closed (LC8 or LC2) vRMC100 manipulated (see MA1)	PSD logic activated by LSHH on SC100 LSD logic activated by LSHHs on KD100 High level alarms LAHs on SC100 and KD100 + HS for manual ESD/PSD/LSD Very high level alarms LAHHs on SC100 and KD100 + HS for manual ESD/PSD/LSD (if manipulated) Position light ZLL for SDV102 + HS for manual reset of SDV102	None

4.3.2.3. Discussion of the results of the case study

Although the results of the case study should not be directly generalized, they demonstrate that, besides inducing a Process Shut Down (PSD) or a production outage, malicious manipulations of the control system may induce more severe scenarios, as equipment damage and/or major accidents. This applies not only to equipment in the process section of the plant, but also to utilities and services (e.g., instrument air, power supply or cooling water). While an induced shutdown of an essential service leads to consequences similar to the shutdown of the process area, inducing damage (e.g., SE04, SE05, SE06) in these units may result in a prolonged downtime of the entire plant, with consequences that exceed the direct repair cost of the damaged units. This may be of particular interest for attackers aiming at causing economic value or influence value losses for the company, characterized by a non-violent belief (i.e., no human value or environmental value losses). Moreover, if shutdown procedures are inhibited by the attacker, the manipulation of utilities may also lead to widespread consequences around the plant. This is the case of manipulations to the cooling water system in the case study, which may lead to compressor damage in node ND_2.

As evidenced by the case study, POROS supports the systematic identification of all the possible SEs, but also the selection of a limited number of SEs for a more in-depth assessment. While generic security and cybersecurity countermeasures (e.g., well-configured firewalls, patched software, presence of AV software, user authentication, network segmentation, etc, see also Section 3.1.4.3) are able to appropriately prevent all the SEs, including those with low severity, specific measures, providing a redundancy and thus increasing the level of protection, can be identified for the high severity SEs. As shown in the case study, the analysis of the MAs for the selected cases allows the identification of RMCs that may require targeted implementation of additional countermeasures and/or a safer plant design (inherent safety).

The guideline tables (**Table 11**, **Table 12**, and **Table 20**) were found adequate for the definition of all the code classes required throughout the POROS application to the case study (SE, RMC, ME, RM, LC, MA), confirming their use to achieve repeatable results and low subjectivity in the assessment of Oil&Gas operations.

As in the application of PHAROS methodology (see Section 4.2.2), **Table 27** also confirms that, in some cases, relatively few remote manipulable components (RMCs) need to be manipulated in order to execute a mechanism of action (MA) that can initiate a high severity security event (SE). Many CMs consist of a single manipulated component: it is the case of 7 out of 12 combinations identified through POROS analysis (**Table 27**). This is obviously not in favour of security since attackers must not carry out a complicated attack pattern in order to affect the operability and/or the physical integrity of the target system.

In the cases where the manipulation of a single RMC is required to carry out a MA, the attacker apparently needs to infect only the BPCS or the SIS for a successful action. For example, in the case study, CM1.1 is obtained by manipulating the PLC connected to the SIS in order to close SDV102, and CM2.1 is achieved by manipulating the PID controller of the BPCS that control the valve TV100. However, SEs as those shown in **Table 20**, are prevented by specific safeguards in the process system. If active and/or procedural safeguards are present, the attacker needs to manipulate the SIS in order to prevent a safe response of the system. This, combined with the presence of CMs involving only RCMs controlled by the SIS, makes the latter system the most critical element of the automation system as regards attacks aiming at severe SEs. This leads to a possible conflict between instrumented safety and security issues, which deserves appropriate assessment. On the other hand, physical safeguards (e.g., pressure safety valves, rupture disks, catch basins, etc.), as they do not contain RCMs, can not be manipulated through an attack to the IT-OT network system and, therefore, they can be considered fully effective in avoiding the SE in case of proper design. Hence, the proper sizing of inherent/passive safeguards must consider security cases that can be generated through the malicious manipulation of the BPCS and the SIS (e.g., considering the cyber-attack scenario in addition to those reported in standard API 521 [192] for the sizing of PSVs). However, as evidenced from the results of the case study, IPSs may be effective only for the prevention and mitigation of some of the MAs (e.g., those involving

pressure or temperature out of design specifications, while no IPSs was identified in other cases, e.g., to prevent the overfill of ND_1).

Procedural safeguards (e.g., manual resets for shut-off valves controlled by the SIS, hand switches for manual stop of operating machines, alarms, position lights, etc.) share with automated safeguards the possibility to be deactivated by an attacker. However, as shown by the results in **Table 27**, a large number of elements belonging to procedural safety exist for each MA, if compared to the active and passive safeguards. This seems to suggest that a high level of complexity of the CMA is needed to deactivate all of them, requiring a detailed knowledge of updated process details, reasonably possible only when the attack involves insiders. Therefore, it can be argued that procedural safeguards may play as well a role in preventing a SE, though they may be negatively affected by human reliability factors.

Table 28 presents how the results of POROS can support the definition of the IT-OT protection requirements for the elements that act on the physical components of the plant (i.e., the manipulative elements, MEs) according to ISA/IEC 62443. The risk assessment described in ISA/IEC 62443-3-2 divides the IT-OT system into separate zones (i.e., grouping of logical or physical assets based upon risk or other criteria [45]) and conduits (i.e., logical grouping of communication channels that share common security requirements connecting two or more zones [45]), and defines for each zone/conduit the security level target required for tolerable risk. The assessment of proposed countermeasures (i.e., safeguards in the IT-OT network system) and the design of additional ones is based on this information. The definition of the security level target also requires an evaluation of "worst-case impact on risk areas as personnel safety, financial loss, business interruption and environment" (ISA/IEC 62443-3-2). The severity level for the SEs triggered by a malicious manipulation of the MEs belonging to a zone can be used to provide such evaluation.

Table 28 shows the SEs than can be triggered by the manipulation of elements in one zone, as identified by POROS. The worst-case SE severity can be taken as a reference severity for the security level target definition of the zone. As discussed above, sometimes manipulation of elements belonging to different zones may be required to cause the worst-case SE, making the attack more complex and, possibly, decreasing likelihood. Thus, the division of the IT-OT network system in smaller zones can be identified as a good strategy to reduce the risks of concern in the current assessment. **Table 28** shows that only a limited number of the SIS elements require high levels of security: the definition of smaller zones with dedicated countermeasures, when possible, may lead to a more effective protection of these parts of the OT system, allowing less stringent requirements to be applied to the rest of the system.

Although the division into zones and conduits of the network system suggested by ISA/IEC 62443 lead to the advantages discussed above, they may affect the operational reliability of the overall system [204]. In fact, when interdependent subsystems are required to work together for maintaining regular operation, the introduction of segregation and barriers may increase the probability of failures, reducing system availability. This can be critical in case of the SIS system since it executes safety functions, where given performances of reliability shall be met (e.g., SIL rating as for IEC 61511). Thus, a cost-benefit analysis of the separation of the network system into smaller zones and conduits that take into account both advantages in terms of system safety/security and disadvantages in terms of system operational reliability is of central importance.

Table 28 Information for ISA/IEC 62443 3-2 (step ZCR 5.8 e 5.12) provided by POROS.

Zones	SEs	Severity vector [EC, IV, EN, HV]	RMCs belonging to the current Zone	Active safeguards belonging to the current Zone	Active safeguards belonging to other Zones
Zone 1: BPCS-1 (gas turbine - control)	ND_2-SE04 (material damaged by load)	[4, 1, 1, 1]	GAS TURBINE	None	LSD/PSD logics activated by PAHHs (Zone 3) LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND_2-SE05 (gas turbine damaged by surge)	[4, 2, 1, 1]	GAS TURBINE	None	LSD/PSD logics activated by PAHHs (Zone 3) LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND_2-SE05 (gas turbine damaged by start/stop cycles)	[4, 2, 1, 1]	GAS TURBINE	None	LSD/PSD logic activated by Anti-Surge (Zone 3)
Zone 2: BPCS-2 (rest of the plant - control)	ND_2-SE04 (material damaged by temperature)	[4, 1, 1, 1]	TV100, TV101	None	None
	ND_2-SE05 (gas turbine damaged by liquid)	[4, 2, 1, 1]	LV100, LV101	None	PSD logic activated by LSHH on SC100 (Zone 4) LSD logic activated by LSHHs on KD100 (Zone 4)
Zone 3: SIS-1 (gas turbine - safety)	ND_2-SE04 (material damaged by load)	[4, 1, 1, 1]	GAS TURBINE	LSD/PSD logic activated by Anti-Surge	LSD/PSD logics activated by PAHHs (Zone 4)
	ND_2-SE05 (gas turbine damaged by surge)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD logic activated by Anti-Surge	LSD/PSD logics activated by PAHHs (Zone 4)
	ND_2-SE06 (ND_2-SE05/ND_2-SE04 + LOC or LPI)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD logic activated by Anti-Surge	LSD/PSD logics activated by PAHHs (Zone 4)
	ND_2-SE05 (gas turbine damaged by start/stop cycles)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD activated by Anti-Surge	None
	ND_2-SE06 (ND_2-SE05 + LOC or LPI)	[4, 2, 1, 1]	GAS TURBINE	LSD/PSD activated by Anti-Surge	None

Zone 4: SIS-2 (rest of the plant - safety)	ND_2-SE04 (material damaged by load)	[4, 1, 1, 1]	SDV105	LSD/PSD logics activated by PAHHs	LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND_2-SE05 (gas turbine damaged by surge)	[4, 2, 1, 1]	SDV105	LSD/PSD logics activated by PAHHs	LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND_2-SE06 (ND_2-SE05/ND_2-SE04 + LOC or LPI)	[4, 2, 1, 1]	SDV105	LSD/PSD logics activated by PAHHs	LSD/PSD logic activated by Anti-Surge (Zone 3)
	ND_2-SE05 (gas turbine damaged by liquid)	[4, 2, 1, 1]	SDV102, SDV103	PSD logic activated by LSHH on SC100 LSD logic activated by LSHH on KD100	None
	ND_2-SE06 (ND_2-SE05 + LOC or LPI)	[4, 2, 1, 1]	SDV102, SDV103	PSD logic activated by LSHH on SC100 LSD logic activated by LSHH on KD100	None

Appendix - Criticality analysis of the role of RMCs and safeguards

In the discussion of the results of PHAROS application (Section 4.2.2.3), a simplified criticality analysis was carried out to point out the most relevant items (e.g., RMCs) among the ones relevant for a specific issue (e.g., MAs, CMs). It is based on the count of the items relevant to each of the issues considered. Alternative combinations of RMCs exist for the same MA; the complete list for ND_F is reported in **Table A.1** together with the effective safeguards (both inherent/passive and active/procedural safeguards). The details on the calculation of the results presented in **Figure 39** and **Figure 40** in Section 4.2.2.3 are reported in the following.

Criticality of the RMCs for the MAs of ND_F: number of MAs involving the manipulation of each RMC (Figure 39-a).

The figure reports, for each RMC allocated to ND_F, the minimum and maximum number of the MAs in which the manipulation of the RMC is required. As in some cases, more than one RMC can be alternatively manipulated to carry out the same MA, both a minimum and maximum number of MAs in which the RMC is involved are defined.

The minimum number of MAs that require the manipulation of a given RMC is calculated as follows:

- If manipulation of the RMC has no alternatives for a given MA, the MA is counted as 1.
- If manipulation of an alternative RMC results in the same contribution to the given MA, the MA is counted as 0.

The maximum number of MAs is calculated as follows:

- If manipulation of the RMC has no alternatives for a given MA, the MA is counted as 1.
- If manipulation of an alternative RMC results in the same contribution to the given MA, the MA is counted as 1.

The greater the number of MAs requiring manipulation of a given RMC, the more critical the RMC is, as its hijacking can be exploited in many ways.

Criticality of the RMCs for the CMs of ND_F: number of RMCs involved in sample combinations for each MA (Figure 40-a).

The figure shows only two sample CMs for each MA. These were generally selected as the ones presenting the lower numbers of manipulated RCMs for each control sub-system (BPCS or SIS system). For these sample CMs, the count of the RMCs that require manipulation is reported.

The count is made with reference to **Table A.1** as follows:

- If manipulation of the RMC is required for a given CM, the RMC is counted as 1.
- If manipulation of the RMC is not required for a given CM, the RMC is counted as 0.

The lower the number of RMCs that require to be manipulated for a CM, the more critical the CM (and the corresponding MA) is, as complexity of the attack is reduced.

As the RMCs in the considered case study are controlled either by the BPCS or by the SIS, the percentage of each type is also reported.

Criticality of the safeguards for the MAs of ND_F: number of MAs for which each safeguard is effective (Figure 39-b).

The figure reports, for each safeguard of ND_F (both inherent/passive and active/procedural safeguards), the count of the MAs in which the safeguard is effective. In some cases, alternative combinations of RMCs exist for the same MA and a given safeguard may not be effective for all of them; hence both a minimum and maximum number of MAs are defined for each safeguard.

The minimum number of MAs is calculated as follows:

- If a safeguard is effective for all the CMs identified for a given MA, the MA is counted as 1.
- If a safeguard is effective only for *m* CMs out of the *s* CMs identified for a given MA and $m < s$, the MA is counted as 0.

The maximum number of CMs is calculated as follows:

- If a safeguard is effective for all the CMs identified for a given MA, the MA is counted as 1.
- If a safeguard is effective only for *m* CMs out of the *s* CMs identified for a given MA and $m < s$, the MA is counted as 1.

The greater the number of MAs for which each safeguard is effective, the more critical availability the safeguard is, as it is effective in negating several patterns of action to the attacker.

Criticality of the safeguards for the CMs of ND_F: number of effective safeguards involved in sample combinations for each MA (Figure 40-b).

The figure shows only two sample CMs for each MA, for which the number of effective safeguards is reported. The sample CMs were the same previously selected for ***Figure 40-a***.

The count of the effective safeguards is made with reference to **Table A.1** as follows:

- If a safeguard is effective for a given CM, the safeguard is counted as 1.
- If a safeguard is not effective for a given CM, the safeguard is counted as 0.

The lower the number of effective safeguards that are required for a CM, the more critical the CM (and the corresponding MA) is, as a lower number of layers of protection preventing the outcomes of the attack is present.

As safeguards can be procedural, active or inherent/passive, the percentage of each type is also reported.

Table A.1 List of the combinations (CMs) which result from manipulating alternative RMCs relevant for each MA of the node ND_F (see **Table 18** in Section 4.2.2.2). Effective safeguards (inherent/passive and active/procedural) are reported for each CM. Adapted from [101].

Combinations		Relevant RMCs	Effective safeguards
MA13.1	CM 1	PV003A partially or totally closed PV003B partially or totally closed	PAH003, PAHH003, LSD logic activated by PSHH, PSV001, catch basin
	CM 2	SDV007 totally closed PV003A partially or totally closed	PAH003, PAHH003, ZLL007, LSD logic activated by PSHH, PSV001, catch basin
MA13.2	CM 3	PV003A partially or totally closed PV003B partially or totally closed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LSD logic activated by PSHH, PSV001, catch basin
	CM 4	SDV007 totally closed PV003A partially or totally closed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, ZLL007, LSD logic activated by PSHH, PSV001, catch basin
MA16.1	CM 5	SDV004 totally closed SDV006 totally closed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL004, ZLL006, LSD logics activated by PSHH, interface LSHH and oil LSHH, PSV001, catch basin
	CM 6	LV002 partially or totally closed PA002A stopped or with decreased rotational speed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
	CM 7	SDV004 totally closed PA002A stopped or with decreased rotational speed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL004, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
	CM 8	LV002 partially or totally closed SDV006 totally closed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin
MA_{13+16}.1	CM 9	PV003A partially or totally closed PV003B partially or totally closed LV002 partially or totally closed PA002A stopped or with decreased rotational speed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
	CM 10	SDV004 totally closed SDV006 totally closed SDV007 totally closed PV003A partially or totally closed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL004, ZLL006, ZLL007, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin
	CM 11	SDV004 totally closed SDV007 totally closed PV003A partially or totally closed PA002A stopped or with decreased rotational speed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL004, ZLL007, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin

	CM 12	SDV004 totally closed SDV006 totally closed PV003B partially or totally closed PV003A partially or totally closed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL004, ZLL006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin
	CM 13	SDV006 totally closed SDV007 totally closed PV003A partially or totally closed LV002 partially or totally closed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL006, ZLL007, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin
	CM 14	SDV007 totally closed PV003A partially or totally closed LV002 partially or totally closed PA002A stopped or with decreased rotational speed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL007, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
	CM 15	SDV004 totally closed PV003A partially or totally closed PV003B partially or totally closed PA002A stopped or with decreased rotational speed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL004, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
	CM 16	SDV006 totally closed PV003A partially or totally closed PV003B partially or totally closed LV002 partially or totally closed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin
$MA_{13+16}.2$	CM 17	PV003A partially or totally closed PV003B partially or totally closed LV002 partially or totally closed PA002A stopped or with decreased rotational speed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
	CM 18	SDV004 totally closed SDV006 totally closed SDV007 totally closed PV003A partially or totally closed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL004, ZLL006, ZLL007, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin
	CM 19	SDV004 totally closed SDV007 totally closed PV003A partially or totally closed PA002A stopped or with decreased rotational speed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL004, ZLL007, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
	CM 20	SDV004 totally closed SDV006 totally closed PV003B partially or totally closed PV003A partially or totally closed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL004, ZLL006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin
	CM 21	SDV006 totally closed SDV007 totally closed PV003A partially or totally closed LV002 partially or totally closed	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZL006, ZLL007, LSD logic activated by PSHH, interface

	LV003 partially or totally opened FV003 partially or totally opened	LSHH and/or oil LSHH, PSV001, catch basin
CM 22	SDV007 totally closed PV003A partially or totally closed LV002 partially or totally closed PA002A stopped or with decreased rotational speed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL007, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
CM 23	SDV004 totally closed PV003A partially or totally closed PV003B partially or totally closed PA002A stopped or with decreased rotational speed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL004, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, UA unavailable, PSV001, catch basin
CM 24	SDV006 totally closed PV003A partially or totally closed PV003B partially or totally closed LV002 partially or totally closed LV003 partially or totally opened FV003 partially or totally opened	PAH003, PAHH003, LAH002, LAH004, LAHH005, LAHH006, ZLL006, LSD logic activated by PSHH, interface LSHH and/or oil LSHH, PSV001, catch basin

5. Development of methods for the identification, quantitative risk assessment, and mitigation of physical security threats to process plants

The studies described in this Chapter are aimed at supporting hazard identification and quantitative assessment in SVA/SRA studies with respect to physical security threats (malicious interferences aimed at causing damage bypassing Physical Protection System – PPS – elements). **Figure 44** shows a schematic synthesis of the link between the methods developed and described in the following and the backbone structure of SVA/SRA methodologies.

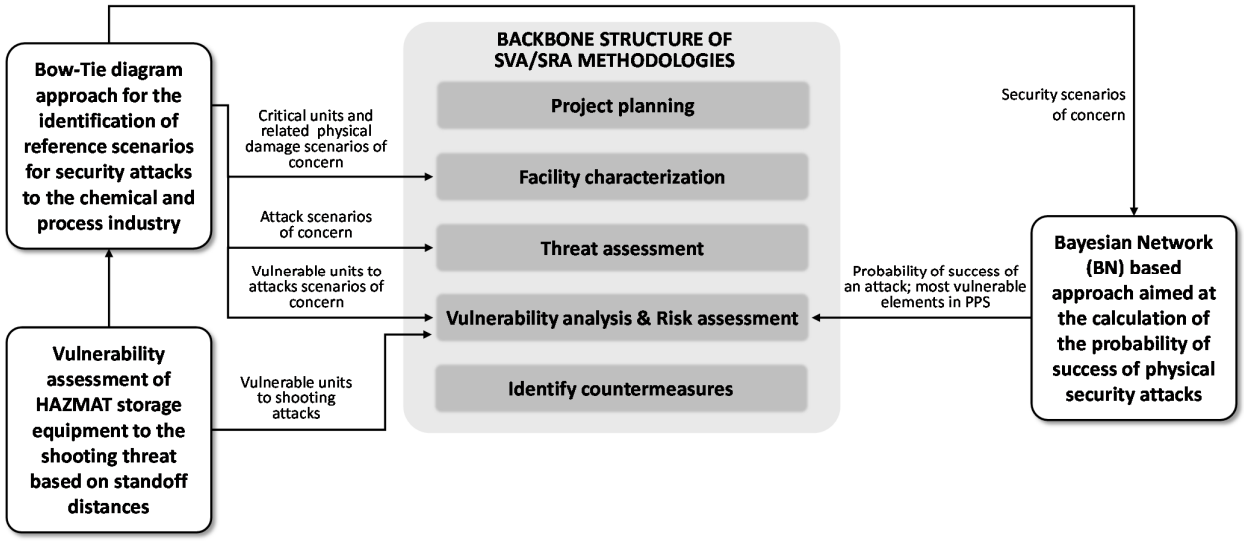

Figure 44 Schematization of the link between the methods developed and link with backbone structure of SVA/SRA methodologies.

5.1. A Bow-Tie diagram approach for the identification of reference scenarios for security attacks to the chemical and process industry

This Section presents a study aimed at the definition of a novel set of reference security scenarios (intended as the evolution of events starting from the attack scenarios to the physical damage scenarios) and of a step-by-step procedure based on Bow-Tie (BT) formalism for the identification of reference security scenarios. Therefore, the results obtained from this study help answer Research Question 1 and Research Question 2 (see Section 2.1 and **Figure 4**), supporting hazard identification phase in SVA/SRA studies. In particular, the reference security scenarios are identified for the more widely used storage units in chemical and process plants and with reference to a general classification of possible attack modes. The results are reported using Bow-Tie (BT) diagrams. The potential use of the developed reference BTs within the proposed step-by-step procedure for the identification of reference scenarios is demonstrated on a case study addressing an atmospheric floating roof storage tank containing a low volatile flammable liquid.

5.1.1. Method

5.1.1.1. Overview

A Bow-Tie (BT) diagram approach was selected since, according to Mannan [19], it allows to identify critical events, build accident scenarios, revise causes of accidents/incidents, and study the effectiveness and influence of safety/security barriers. For instance, the BT diagram approach has been adopted by the ARAMIS methodology [99] to support upper-tier Seveso plants in identifying the potential major accident scenarios.

Reference BTs have been developed to foster an easier identification of the potential attack modes (attack scenarios) and of the consequent likely physical damage scenarios in the context of application of classical SVA/SRA methodologies and other academic proposals for security risk quantification (e.g., models based on dynamic Bayesian Networks or Markov chains). The information on the attack modes and physical damage scenarios coming from the developed reference BTs can also support the identification of further security countermeasures within the physical protection system (PPS) of the facility analysed, with the intent of making some attack patterns more complex and/or mitigate their consequences. Moreover, the output of the BT analysis is qualitatively similar to that obtained from BT application in safety studies (e.g., major accident hazard analysis for Seveso installations), thus allowing the application of shared strategies in the mitigation of consequences and in the planning of emergency responses.

The generic structure of a BT in the field of security is shown in **Figure 45**. At the centre of the BT is the security event (SE), defined as a "malicious release of hazardous materials or energy, which may cause multiple casualties, severe damage, and public or environmental impact" [35]. The Attack Tree (AT, on the left side of the SE) groups the conceivable acts of interference (i.e., the deliberate malicious attacks committed by the attackers with the aim of directly or indirectly causing damage to an asset [44]) into a set of possible attack modes (AM). There are barriers between the attack modes and the security event with the function of preventing or at least mitigating its consequences. In particular, in addition to the physical protection elements in place (e.g., site fences, entry gates with manned reception, etc.), and the security response (e.g., police), the standoff distance is considered among the list of barriers. The latter is an inherent physical barrier defined as the "minimum distance between the asset of interest and the location where an attack takes place without causing any damage" [103]. Thus, standoff distances play a primary role in the protection against such attacks, as they may be able to deny the success of a particular attack mode and prevent/mitigate the resulting SE. Clearly, while the physical protection elements and the security response do not depend on the specific attack mode, the standoff distances are AM-specific and so they can be considered in the development of generic (not facility-specific) reference BT diagrams.

The Event Trees (ET, on the right side of the SE) shows all the possible physical events leading from the SE to the physical damage scenarios (FS) whose consequences can be reduced by mitigation systems and emergency responses which are the same employed in case of safety-related accidents. However, both internal (evacuation plan) and external (population sheltering) emergency response and mitigation plans developed for safety scenarios may be adapted to fully address the security issues (e.g., considering the presence of attackers on site). In perspective, this may provide the chance to develop safety/security requirements in the framework of the integrated management of safety and security risks [122].

The development of the reference BT diagrams consisted of three main phases, namely:

1. identification and validation of a reference set of Attack Modes (AMs);
2. definition and validation of Attack Trees (AT) for a set of reference installations;
3. construction and validation of BT diagrams for reference substances.

Each phase is described in detail in the following.

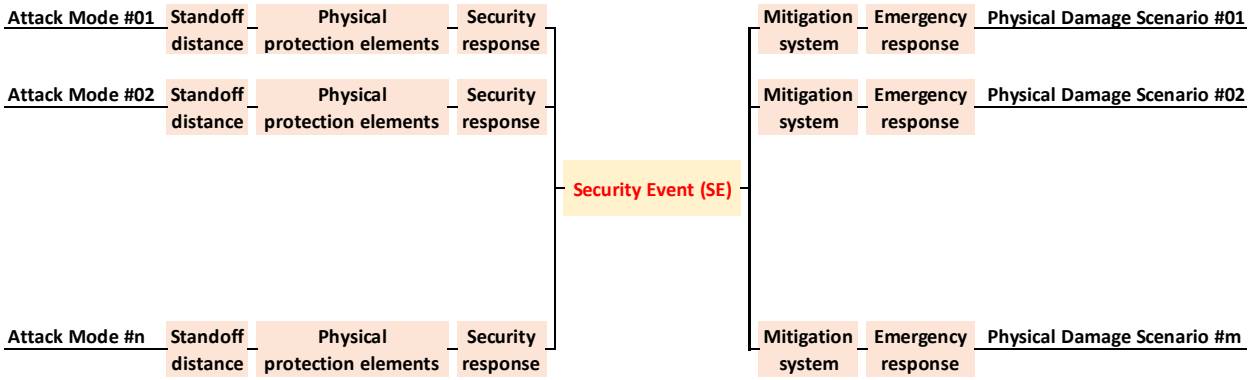

Figure 45 Generic structure of a Bow-Tie diagram in the security domain.

5.1.1.2. Identification and validation of reference Attack Modes (AM)

The first phase of the method applied was aimed at the definition of a reference set of Attack Modes (AMs) perpetrated by the attackers. The reference set of AMs consists in a list of generic but clearly defined types of physical acts of interference to a process plant (process and storage installations), that can be carried out by single individuals or organizations. Cyber-attacks or unauthorized physical accesses to the control room were explicitly considered out of the scope of the assessment. In facts, the mechanism of these attacks strongly depends on the design of the process and control system and a dedicated approach is needed for the analysis of the potential impacts: the reader is referred to Section 4.

The set of attack modes was identified from the analysis of the main Security Vulnerability Assessment (SVA) and Security Risk Assessment (SRA) methodologies, focusing on the applicability in the context of chemical and process plants. Sources analysed include: Störfall-Kommission [44], the CCPS methodology [39], the VAM-CF methodology [40], the SRA methodology proposed by API RP 780 [35], and the RAMCAP methodology [43]. The proposed attack modes represent broad classes which reflect the current experience in the security domain, considering a scope of application that goes even beyond the chemical and process industry. Therefore, they are expected to reasonably include all the credible cases of attack. They are particularly suitable for direct application in “asset-based approach”, which many SVA/SRA methodologies suggest for the chemical and process industry [35,39], where threats and hazards of the assets on site are only broadly described without exploring the specific details of all the possible attack paths.

In order to better support the identification and description of credible attack modes for plant equipment (process and storage installations), one or more Reference Act of Interference (RAI) was defined for each AM. The RAIs are examples of attacks, defined in terms of instruments and/or materials available to the attacker. RAIs were defined considering credible worst-case situations of attack in terms of instruments and/or materials that can be available to the attacker. The reference instruments and/or materials for each AM were defined based on information available in relevant literature: Störfall-Kommission [44] for typical deliberate interferences with or without the use of aids, Pert et al. [205] for incendiary substances, Landucci et al. [103] for types and quantities of explosives that can be potentially carried by a single man or by a vehicle, datasheets of heavy lift drones available in technical catalogues for information about common charges (payloads) [206], the standards EN 1063 [173] and EN 1522 [172] for type and characteristics of projectiles.

Validation of the AMs was carried out on the basis of the information available in the database populated and analysed by Iaiani et al. [2,17], concerning security-related incidents that occurred in the Chemical&Petroleum (C&P) sector (see Section 3.1.3). In particular, the suitable records in terms of relevant information were classified according to the set of proposed AMs. This allowed checking that the set of proposed AMs obtained is an exhaustive and constitutes a structured set of mutually exclusive and well-described categories according to the basic principles of standard statistical classifications defined by the United Nations Statistics Division [153].

The past incidents proved that, for the specific process industry targets, historical evidence of events belonging to the proposed set of attack modes is present. The information available in some of the incidents recorded in the database also allowed the validation of the instruments identified in the RAIs for each AM.

5.1.1.3. Definition and validation of Attack Trees (AT) for reference installations

The same attack mode will result in different damages on the basis of the characteristics of the target (e.g., type of equipment, design pressure) and on the minimum distance from the target installation that the attacker can reach. Thus, the second phase of the present study was aimed at the definition and validation of Attack Trees (ATs) for a set of reference installations. ATs are graphs that represent the security acts (deliberate malicious attacks) leading to a Security Event [58]. In the present study, the AT for each reference installation contains three elements: the Attack Modes (AMs), the standoff distances, the safety/security barriers, and the Security Events (SEs).

The set of Reference Installations (RIs) considered in the present study were adapted from those proposed by Delvosalle et al. [99] and by Tugnoli et al. [121]. They include the more common installations where large amounts of hazardous materials are stored. In particular the following RIs were considered:

- RI1: atmospheric storage installation (e.g., cone roof tank, horizontal cylindrical tank, floating roof tank, gas holder);
- RI2: pressurized storage installation (horizontal cylindrical tank, sphere tank);
- RI3: storage warehouse (storage of solid in small packages, storage of liquid in small containers).

In the BT approach, the attack is considered to cause a Security Event such as a loss of physical integrity (LPI) and/or a loss of containment (LOC) of the hazardous material stored in the reference installation [99]. In case of LOC of fluids, the classification proposed by the TNO “Purple Book” [186] and adopted by Cozzani et al. [207] was used in the characterization of the SE. In particular, three different Loss Intensities (LI) are considered:

- LI1: release from a 10 mm average release diameter;
- LI2: release of the entire vessel inventory in 10 min and full-bore rupture of connected pipework;
- LI3: instantaneous release of the entire vessel content.

In particular, in order to define the ATs for each RI, the possibility of each AM to cause a LOC according to the above-defined LIs, or a LPI, was assessed. From the definitions of the adopted set of AMs, taking into account the specific features of the attack vectors associated to each of them, it follows that the success of the attack primarily depends on the level of penetration reached by the attacker, or, in other words, by the distance reached between the attacker and the point where the target installation is located. This is the reason why standoff distances play a primary role in the protection against deliberate malicious attacks: they may be able to deny the success of a particular attack mode and prevent the resulting SE. Hence, in the present study, standoff distances were considered as a factor that may modify the applicability of a certain AM to a specific AT. This allows to better describe the link between the success or failure of the Physical Protection System (PPS) in place to restrict access to certain areas and the possible SEs resulting from an attack. In the present study, typical values of standoff distances for the reference installations considered, are calculated. These values may support the design of the PPS as regards the location of the physical plant equipment within the industrial site, as well as that of the physical barriers (site fences, gateways, building walls, doors, etc.), evidencing the area that attackers have to reach in order to trigger events with severe consequences.

The calculation of standoff distances for RAIs exploiting overpressure or heat load as attack vector was based on the use of models for characterization of the physical effects as function of distance. The standoff distance corresponds, in this case, to the distance at which the value of the physical effect is lower than a damage threshold value for the target installation. Damage threshold values available in the literature for different types of storage equipment [207–209] were used for the scope. The TNT (trinitrotoluene) equivalence model

proposed by Bounds [210] was used for modelling the peak overpressure caused by detonation of explosive devices. Liquid pool fires originated from incendiary attacks were modelled using the correlations derived by Mudan [211], Raj [212], Bagster and Pitablado [213] reported in the "Yellow Book" of TNO [214].

For attacks based on shooting physical plant equipment, despite the availability in the literature of specific studies on the topic [109–112,114,215–217], the development of adequate damage models for projectile impact on plant equipment is still lacking. Therefore, an extended review and validation of projectile perforation models was carried out in order to identify the most reliable models for the prediction of perforation of atmospheric and pressurized storage equipment [218]: the reader is referred to Section 5.2 for the specific details on the study.

Also in this case, the validation of the ATs was carried out with the support of the information available in the security-related incidents collected for the Chemical&Petroleum (C&P) and described in Section 3.1.3. In particular, the occurrence of incidents featuring the damage to the reference installations considered was checked, allowing the validation of specific branches of the ATs.

5.1.1.4. Construction and validation of Bow-Tie (BT) diagrams for reference substances

The third phase of the present study was aimed at the development and validation of security-related Bow-Tie (BT) diagrams for reference substances stored in the reference installations considered in the present study. The generic scheme of a BT (**Figure 45**) involves two parts: the Attack Tree (AT) on the left side of the Security Event (SE) and Event Tree (ET) on its right side. The ET-part of the BT strongly depends on the acute hazard characteristics and the pre-release operative conditions of the substances contained inside the installation.

Event trees were generated according to the method proposed in step 6 of the MIMAH methodology [99]. The method allows to identify all the events leading from the security event (SE) to the physical damage scenarios (FS) using guiding matrices which express the possible links between the elements of the ETs (e.g., a matrix linking the security events with the secondary events, based on the substance physical state). The FSs considered in the present study that are present in the ETs are (see definitions in **Table 33** in Section 5.1.2.4): jet fire (FS#01), VCE (FS#02), flash fire (FS#03), pool fire (FS#04), flare (FS#05), toxic cloud (FS#06), fireball (FS#07), physical explosion (FS#08), confined chemical explosion (FS#09).

The ETs were generated for the most frequent families of substances stored and processed in the chemical and process industry [219]: flammable liquids, flammable pressurized gasses, flammable gasses, flammable cryogenic liquids, toxic pressurized gasses, pressurized liquefied toxic gasses, and oxidizing solids.

The security-related BTs obtained were validated with the information available in the security-related incidents collected for the Chemical&Petroleum (C&P) and described in Section 3.1.3, as previously done for the validation of AMs and ATs. More specifically, the occurrence of incidents featuring the scenarios reported in the ETs was checked, allowing the validation of specific branches of the ETs. In the following, only the BTs for which validation was possible are reported and discussed.

5.1.2. Proposed Attack Modes, Attack Trees, Bow-Tie diagrams and validation

A brief description of the incidents used in the validation of both the ATs for reference installations and the BT diagrams, is reported in **Table 29**.

Table 29 Details on security-related events with some information available on the chain from attack scenarios to physical damage scenarios. Adapted from [220].

ID	Date	Country	Attack Description	Impact description	Ref
#1	09/08/1965	Uruguay	The political group "Tupamaros" detonated explosive devices in a facility warehouse owned by the chemical and pharmaceutical company Bayer in order to demonstrate anti-US sentiment.	The warehouse suffered damages.	[3]
#2	05/04/1970	USA	Unknown threat actors attacked a warehouse (arson) owned by the American Potash and Chemical Company.	The warehouse suffered damages with economic losses not exceeding $1 million.	[140]
#3	11/04/1970	USA	Unknown threat actors attacked a storage tank at the Dow Chemical Company detonating explosives triggering fires using incendiary devices (gasoline- or alcohol-based).	Five people received minor injuries from flying projectiles and an estimated $250,000 in damages was caused to the facility.	[140]
#9	18/10/1981	France	Unknown threat actors attacked a warehouse (arson) containing chemical products (14 tons of sodium chlorate and 33,000 litres of flammable liquids (alcohol, solvents, etc.)).	A fire broke out and a series of violent confined chemical explosions due to sodium chlorate decomposition occurred. The incident caused 1 fatality and 12 injuries, besides $26 millions of economic losses.	[9]
#18	26/06/1988	Hungary	A former employee crawled into a warehouse storing 23 tons of flammable liquids (paints thinners, white spirit, toluene, xylene) on a rest day, and with a cigarette end he/she ignited the flammable vapours contained inside.	A flash fire occurred and a fire broke out inside the warehouse.	[9]
#20	16/02/1989	Germany	Terrorists attacked a warehouse (arson) containing flammable and toxic pesticides.	A fire broke out and the toxic smokes were dispersed nearby.	[9]
#21	16/05/1989	France	Act of vandalism in an oil recovery company, consisting in a deliberate interference.	Loss of containment of 8000 litres of oil. Environmental impacts followed the event.	[9]
#22	14/09/1989	Pakistan	Deliberate acts using explosive devices on a chemical store.	The chemical store suffered damages.	[140]
#25	26/02/1993	Unknown	An explosive device was placed on a side of the middle lift of a gasholder and then was detonated.	The tanks collapsed and 33 tons of natural gas were released. The gas was immediately ignited resulting in an airborne fireball. The smaller nearby gasholder experienced a seal fire, while the larger gasholder, on the other side of the damaged equipment, was punctured in its third lift resulting in a jet fire.	[8]
#26	18/07/1995	France	Unknown threat actors attacked a warehouse (arson) in a reprocessing plant for industrial waste containing hydrocarbons and oily residues.	A fire broke out in the warehouse, but the two main oil tanks were not damaged.	[9]

#27	12/05/1996	France	Act of vandalism (arson) in a warehouse containing 10 tons of iron oxide (close to a natural gas expansion station) of an asphalts production plant.	A fire broke out in the warehouse and production was shut down for 24 hours.	[9]
#29	19/01/1997	France	Act of vandalism (deliberate interference with or without aids) in a wastewater treatment plant.	Loss of containment of 2000 litres of fuel oil from two tanks contained inside a technical room. Environmental impacts followed the event.	[9]
#31	31/07/1999	Canada	Unknown threat actors attacked a warehouse (arson) containing flammable paint products.	A fire broke out and the toxic smokes were dispersed nearby.	[9]
#60	23/07/2006	France	Unknown threat actors attacked a warehouse (arson) of a facility producing synthetic latex and rubber.	A fire broke out and a toxic smoke was dispersed nearby. The plant was shutdown.	[9]
#65	02/10/2009	France	Act of vandalism (deliberate interference with or without aids) to a warehouse containing paint products (primarily acrylic resins, urethane in ethyl acetate).	Loss of containment of the paint products from the containers onto the ground and pollution of the AIRAINES (Category 1 watercourse) via the stormwater network.	[9]
#67	23/02/2010	Italy	Deliberate act to a storage tank farm at a petrochemical plant consisting in a deliberate interference.	Release of 2600 tons of hydrocarbons (diesel fuel and heavy fuel oil). Environmental impacts followed the event.	[8]
#73	06/10/2013	France	Act of vandalism (arson together with deliberate interference with or without aids) in a warehouse storing paint products.	Loss of containment of the paint products from the containers onto the ground and other machinery. This material was then ignited resulting in fire.	[9]
#82	26/06/2015	France	A certified delivery driver drove his light-duty utility vehicle inside a closed hangar used to fill inert gas bottles under pressure. The vehicle contained flammable gas bottles, opened by the driver prior to entering the hangar. The explosive atmosphere created inside was then ignited.	The confined chemical explosion that occurred as a consequence of the deliberate ignition of the explosive atmosphere triggered a fire inside the hangar causing severe damages.	[9]
#83	14/07/2015	France	Deliberate act using explosive devices placed on a storage tank farm at a petrochemical plant.	Release of 2000 tons of naphtha and 1000 tons of gasoline that resulted in pool fires.	[8]
#85	13/02/2017	Syria	Terrorist attack using drones with explosives to a natural gas production plant.	Release of natural gas that resulted in multiple flares from equipment.	[9]
#100	14/09/2019	Saudi Arabia	Terrorist attack using drones with explosives to the Saudi Aramco oil processing facility.	14 storage tanks were punctured resulting in the release of oil and consequent pool fires. 3 process equipment were also damaged resulting in loss of containment.	Web articles [221,222]

5.1.2.1. Validation of the proposed reference Attack Modes

The categories of Attack Modes (AMs) proposed in the present study are defined in **Table 30**. The categories closely match the acts of interference described by Störfall-Kommission [44], specifically derived for process and chemical facilities and previously adopted by other authors [2,34,51] (see e.g., the attack modes considered in the analysis of past security-related events presented in Section 3.1), with some exceptions:

- The acts of interference "Deliberate misoperation", "Manipulation", "Interference using simple aids", and "Interference using major aids" reported and defined in Störfall-Kommission [44] were joined in the AM#01 category "Deliberate interference with or w/o aids" (see definition in **Table 30**) in the present study. In fact, although they differ in the actions perpetrated by the attackers (e.g., they span from deliberate opening/closing of valves to ramming tanks and pipework with tools), they are expected to result in qualitatively similar damages to the targeted installation (e.g., damage of machinery or equipment unit) and can be described by similar sets of SEs (i.e., LI1/LI2-intensity LOC).
- The acts of interference "Arson using simple means" and "Arson using incendiary devices" listed in Störfall-Kommission [44] were joined in the AM#02 category "Arson using simple/incendiary means" (see definition in **Table 30**) in the present study. In fact, although the means used by the attackers for setting fire are different, both the acts have the same attack vector (i.e., heat load, resulting in same effects expected on the target physical installation) and would result in the same set of SEs (i.e., LI1/LI2/LI3-intensity LOC).
- The AM#04 "Using vehicle bomb" defined in the present study (see definition in **Table 30**) is not reported in Störfall-Kommission [44]. Nevertheless, references to this attack mode were found in the CCPS SVA methodology, in the API RP 780 SRA methodology, in Argenti et al. [51], Landucci et al. [34], and Casson Moreno et al. [15]. This AM was introduced, since, although having the same attack vector of the attack mode AM#03 "Use of explosives" (i.e., overpressure), both the attack mechanism and the total amount of explosive detonated are considerably different [103]: these differences lead to different security barriers within the Physical Protection System for the detection and delay of such attacks [7].
- In the AM#05 "Shooting" defined in the present study (see definition in **Table 30**), the use of military heavy weapons such as missiles, rockets and mortars, was not included since considered unlikely in the context of the European Union and, more in general, when not addressing war zones.

Overall, the review of other SVA/SRA methodologies (CCPS SVA, VAM-CF, API RP 780 SRA, RAMCAP), as well as of other literature on the topic [7,15,34,51,103] confirmed the suitability of the proposed classification of AMs.

Table 30 Reference AMs adopted in the present study. For each AM, reference tool/substance, attack vector, success criterion, and potential loss intensities (LIs) are reported. Adapted from [220].

AM code	Attack Mode	Description	RAI code	Reference Act of Interference	Attack vector	Success criterion	Loss Intensity
AM#01	Deliberate interference with or w/o aids	Deliberate acts involving simple operations without the use of instruments or using tools that are present on site	RAI#01-A	Closing/Opening manual valves	n.a.	Target installation location is reached	LI1, LI2
			RAI#01-B	Ramming installations and/or instrumentation	n.a.	Target installation location is reached	LI1, LI2
AM#02	Arson using simple/incendiary means	Incendiary attacks	RAI#02-A	Ignition of 50 L of gasoline contained in 2x25 L jerrycans	Heat load	Target installation is damaged due to heat load effects of fire	L1, LI2, LI3
			RAI#02-B	Ignition of 1000 L of gasoline contained in an IBC tank with catch basin present in the target facility	Heat load	Target installation is damaged due to heat load effects of fire	L1, LI2, LI3
AM#03	Use of explosive	Use explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	RAI#03-A	Detonation of 50 kg of TATP carried inside a backpack	Overpressure	Target installation is damaged due to overpressure effects of explosion	L1, LI2, LI3
			RAI#03-B	Detonation of 30 kg of TATP lifted by a drone	Overpressure	Target installation is damaged due to overpressure effects of explosion	L1, LI2, LI3
AM#04	Use of vehicle bomb	Use explosives (placed inside a vehicle) to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	RAI#04	Detonation of 50000 kg of AN/dolomite (50/50) + diesel fuel contained inside a vehicle	Overpressure	Target installation is damaged due to overpressure effects of explosion	L1, LI2, LI3

AM#05	Shooting	Interference at close distance, using different types of weapons	RAI#05	Shooting to equipment using 7.62×51mm cartridge (rifle)	Projectile impact	Perforation and/or penetration of target installation due to projectile impact	L1
AM#06	Vehicle impact	Deliberate acts involving vehicles rammed against plant installations.	RAI#06-B	Ramming installations using a large good vehicle (LGV)	n.a.	Target installation location is reached	LI1, LI2

The information from the incident records classified for the Chemical&Petroleum (C&P) sector by Iaiani et al. [2] provided a validation for the proposed set of AMs. A total of 51 incidents reported enough information to characterize the AM (**Figure 46**) as defined in **Table 30**. The numbers (red coloured) contained in the tags on each branch displayed in **Figure 46** are referred to the count of incidents for which information matching the AM description reported in **Table 30** was available on the specific attack pattern carried out. It should be remarked that the numbers in tags add up to 55 since in 4 incidents more than one AM was adopted to target different units on the same site: for example, incident #3 in **Table 29** reports an attack consisting both in the detonation of explosive devices (AM#03) and in the use of alcohol/gasoline-based incendiary weapons (AM#02) [140]. Also the AMs for which a damage to plant installations is not specifically reported (e.g. unsuccessful attacks), were included in the validation count reported in **Figure 46**. Clearly enough, the classes of attack modes are broad, including all applicable attack patterns. Therefore, they are not limited to those occurred in the specific past incidents used in the validation process.

The use of explosive devices (AM#03) resulted the most frequent attack mode. This type of attack is usually carried out by highly capable and well-motivated attackers such as terrorist organizations. Incendiary attacks (AM#02) also resulted a typical attack pattern performed by attackers: the reason behind this is probably related to the fact that this AM does not require the attackers to be highly equipped and well-motivated. Overall, with the exception of AM#06 (vehicle impact), all the other categories of AMs considered in the present study and described in **Table 30** were validated, presenting at least one past security-related event matching the description of the AMs. As stated, no incident collected in the Chemical&Petroleum sector [2] reported an attack consisting in the ramming of plant equipment with a vehicle (truck, lift truck, car, motorcycle, etc.). Nevertheless, although this attack mode is commonly used by terrorists directly against a crowd of people due to the high number of casualties achievable (e.g., the truck ramming attack in Nice (July 2016) caused at least 84 casualties and 256 injuries), it is considered possible even for the chemical and process industry (simple attack pattern and severe damages achievable on plant equipment). For example, in 2013 a motorcycle rammed a natural gas distribution station near a gas pipeline causing a burning gas leak with flames shooting up over 10 m high [9]: although this incident did not occur in a process facility, it demonstrates the potentially severe consequences of a vehicle impact on an industrial infrastructure handling hazardous materials.

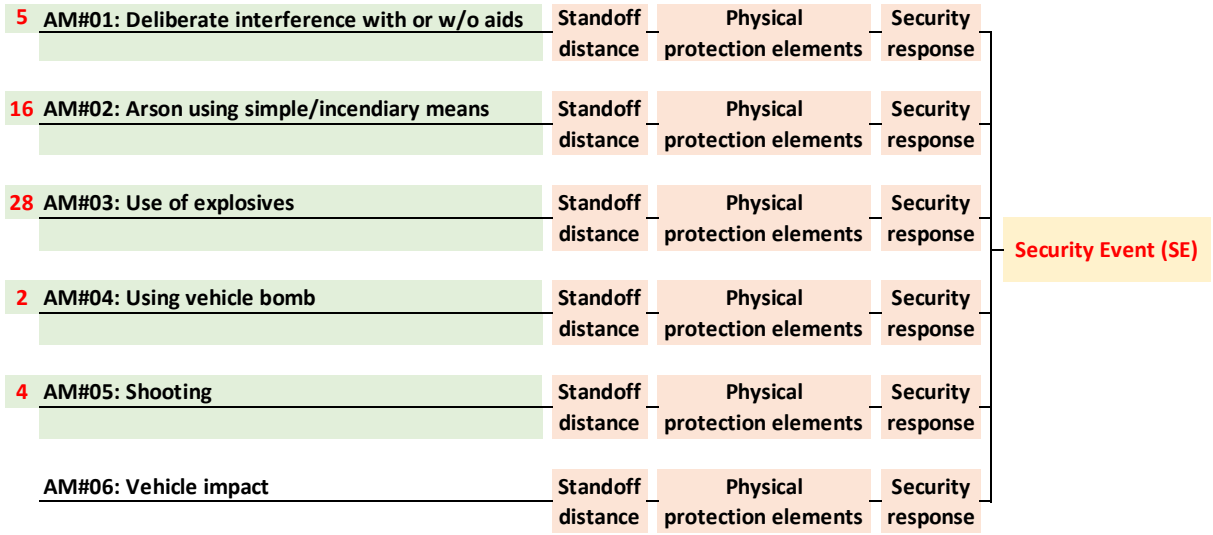

Figure 46 Set of Attack Modes (AMs) considered in the present study. Numbers in tags refer to the number of incidents validating the AM. Adapted from [220].

Each AM listed in **Table 30** was then exemplified in terms of Reference Acts of Interference (RAIs).

In case of deliberate interferences with or without aids (AM#01), two RAIs were considered: the first is representative of a deliberate interference without the use of tools, i.e., RAI#01-A "closing/opening manual valves", and the other is representative of a deliberate interference with the aid of tools, i.e., RAI#0-B "ramming equipment and/or instrumentation". Both these RAIs require the presence of the attacker at the target location (see success criterion in **Table 30**). Even in the case tools are used (as in RAI#01-B), they are, according to the AM definition (see **Table 30**), man-portable or present on site. This implies that the attacker has no specific elements of the PPS to overcome other than those limiting his/her physical access to the installation. As previously stated, deliberate interferences consisting in remote malicious manipulations of the control and safety system (BPCS, Basic Process Control System, and the SIS, Safety Instrumented System) are out of the scope of the present study and have been considered in specific studies [100,101] (see Section 4). Given the nature of this attack, a LI3 release (i.e., instantaneous release of the entire vessel content) is not deemed credible.

In case of incendiary attacks (AM#02), the use of incendiary substances such as alcohol and/or gasoline was explicitly reported in 3 incidents (e.g., see incidents #2 and #3 in **Table 29**). Moreover, gasoline is considered by Pert et al. [205] as one of the most commonly used accelerants (i.e., fluids which facilitate the spread of a fire). Therefore, gasoline was adopted as the reference substance for the definition of the RAIs associated to this AM. As for quantity, two credible attack scenarios were considered: the ignition of 50 L contained in two jerrycans of 25 L each that are carried by the attacker (which is the maximum expected load carried by a man accessing on foot, RAI#02-A, see **Table 30**), and the ignition of 1000 L contained inside an IBC tank that is already present onsite (RAI#02-B, see **Table 30**). In one incident in the database (see incident #18 in **Table 29**) the ignition of flammable material was due to a lit cigarette.

With respect to attacks using explosives (AM#03), two recorded incidents list trinitrotoluene (TNT) and military dynamite as the explosive material used. These are classified as military explosives, and access to large quantities of these materials is usually restricted and therefore less likely outside war zones. A study by Landucci et al. [103] explored Ammonium Nitrate (AN) – Fuel Oil (i.e. ANFO) mixtures and Acetone Peroxide or Triacetone Triperoxide Peroxyacetone (i.e., TATP) as possible homemade explosive materials to be used in attacks involving explosives to process facilities among the substances listed in the US Government Hazardous Substances Database. Based on these sources, TATP was selected as the reference explosive used in the two RAIs considered for AM#03 (i.e., RAI#03-A and RAI#03-B, see **Table 30**), since it presents the higher explosion energy (2803 kJ/kg) among the candidates and it is therefore the most efficient one (worst-case). The two RAIs considered differ in the carrier of the charge, and therefore in the quantity that is expected to be used. RAI#03-A considers a charge of 50 kg of TATP carried by a single man (e.g., contained inside a backpack), while RAI#03-B considers a charge of 30 kg of TATP carried by a heavy lift drone. Use of drones in attacks with explosives is reported in 2 incidents in the database (see incidents #85 and #100 in **Table 29**).

When vehicles are used as explosive carrier (AM#04), transported quantities can reach maximum 50000 kg (two overloaded large goods vehicles). However, such large amounts of TATP are not credible since are too hazardous to produce, transport, and manipulate [103]. Hence, AN/dolomite 50/50 + DF (Ammonium Nitrate 50% / inert dolomite 50% + Diesel Fuel) mixture was considered as reference homemade explosive in the RAI associated to AM#04 (i.e., RAI#04, see **Table 30**). The use of vehicle bombs was found in two incidents [2,15].

In case of shooting attacks (AM#05), in none of the four incidents reporting this AM it is specified the type of firearm used by the attackers. Therefore, among the standardized projectiles reported in the European standards EN 1063 [173] and EN 1522 [172], the 7.62×51mm cartridge (hard-core projectile) was considered in the RAI#05 associated to AM#05 (conservative assumption). Both single and multiple shooting are accounted in RAI#05. In all cases, projectile penetration is expected to create holes in the shell of the target equipment, causing LI1 releases (projectile diameter is typically lower that 10 mm [172,173]).

Finally, as regards attacks consisting in vehicle impacts (AM#06), a single RAI was defined considering large goods vehicles (worst-case) ramming physical storage installations (RAI#06). A LI3 release (i.e., instantaneous release of the entire vessel content) is not deemed credible in this case.

Table 30 also summarises the attack vectors exploited by the attackers to damage the target installation (e.g., heat load, overpressure effects, projectile impact) and the success criteria associated to each AM, and consequently to each of the RAIs defined. In case of deliberate interferences (AM#01) and vehicle impacts (AM#06) the attackers are required to reach the location of the target installation in order to cause a security event, while for AMs that involve triggering fires (AM#02), explosions (AM#03 and AM#04) and shooting (AM#05), this aim is achieved if the physical effects caused by the attacks have a sufficient strength to result in a SE. In case of heat load and overpressure vectors, threshold values above which a damage causing a release from plant equipment is possible may be derived from literature studies concerning domino effect evaluation [207].

5.1.2.2. Validation of the proposed Attack Trees for reference installations

Among the physical security-related incidents reported for the Chemical&Petroleum sector by Iaiani et al. [2] (see Section 3.1.3), only 21 incidents described events related to the release of hazardous material and/or energy involving one of the three reference installations considered in the present study (see **Table 29**).

Attack Tree for atmospheric storage installations

Figure 47 shows the validated Attack Tree (AT) for atmospheric storage installations (RI1). Seven incidents collected in the database reported a security event (loss of physical integrity to a mass and/or energy release) involving a RI1 installation. As shown in the figure, there is historical leading evidence of a SE caused by the majority of the attack modes considered in the present study: branches with tags are those validated by past security-related incidents. The #-codes reported in **Figure 47** are referred to the tags of the incidents described in **Table 29**. The details on the displayed standoff distances are reported in Section 5.1.2.3.

Incidents #21 and #67 prove that for atmospheric storage installations, deliberate interferences with or w/o aids (AM#01) may cause loss of containment of hazardous materials with severe consequences. In particular, in incident #21 (occurred on May 16th, 1989 in France), vandals caused the release of 8000 L of oil which resulted in environmental damages [9]. In incident #67 (occurred on February 23rd, 2010 in Italy), attackers targeted a tank farm of a petrochemical plant inducing the release of 2600 tons of hydrocarbons (diesel fuel and heavy fuel oil) in the rivers Po and Lambro [8], causing damages to the environment. In the two records it is not reported if the attackers made use of tools present on site.

The analysis of the past security-related incidents allowed validating also the branches corresponding to attacks using simple/incendiary means (AM#02) and those using explosive devices (AM#03). As an example, incident #3 (occurred on April 11th, 1970 in the United States) reports that unknown attackers targeted an atmospheric storage tank of the Dow Chemical Company using both explosives and gasoline-based incendiary means [140]. Five people were injured by the flying fragments of the tank and an economic loss of about $250,000 was caused to the company. Another example from the database is incident #25 (occurred on February 2nd, 1993): an explosive device was placed on a side of the middle lift of a gasholder containing natural gas at low pressure. After its detonation, the tank collapsed, and 33 tons of natural gas were released and immediately ignited resulting in an airborne fireball. The detonation also originated a breach on the shell of a nearby gasholder and the resulting gas jet became ignited [8]. In the AT shown in **Figure 47**, in the case of incendiary attacks (AM#02), only the reference act of interference RAI#02-B (ignition of a 1000 L IBC tank containing gasoline, see **Table 30**) is able to cause damage. In fact, as explained in Section 5.1.2.3, no damage is possible when attackers ignite small incendiary devices (RAI#02-A). Differently, in the case of attacks using explosive devices (AM#03), both the detonation of explosives carried by humans (RAI#03-A) and by drones

(RAI#03-B) are able to cause damage (as an example of drone attack, see incident #100 occurred on September 14th, 2019, in Saudi Arabia).

No attacks consisting in the detonation of explosives contained inside vehicles (AM#04) or in shooting (AM#05) were recorded for this RI in the database. However, these attacks are deemed to be potentially able to damage atmospheric storage installations [51,103,223] and were thus included in the AT.

Vehicle impact attacks (AM#06) are not considered credible for atmospheric storage installations due the typical presence of catch basins or bunds (i.e., the physical protection elements (PPE) in place) around these installations. This conclusion is also supported by the lack of recorded incidents featuring this AM.

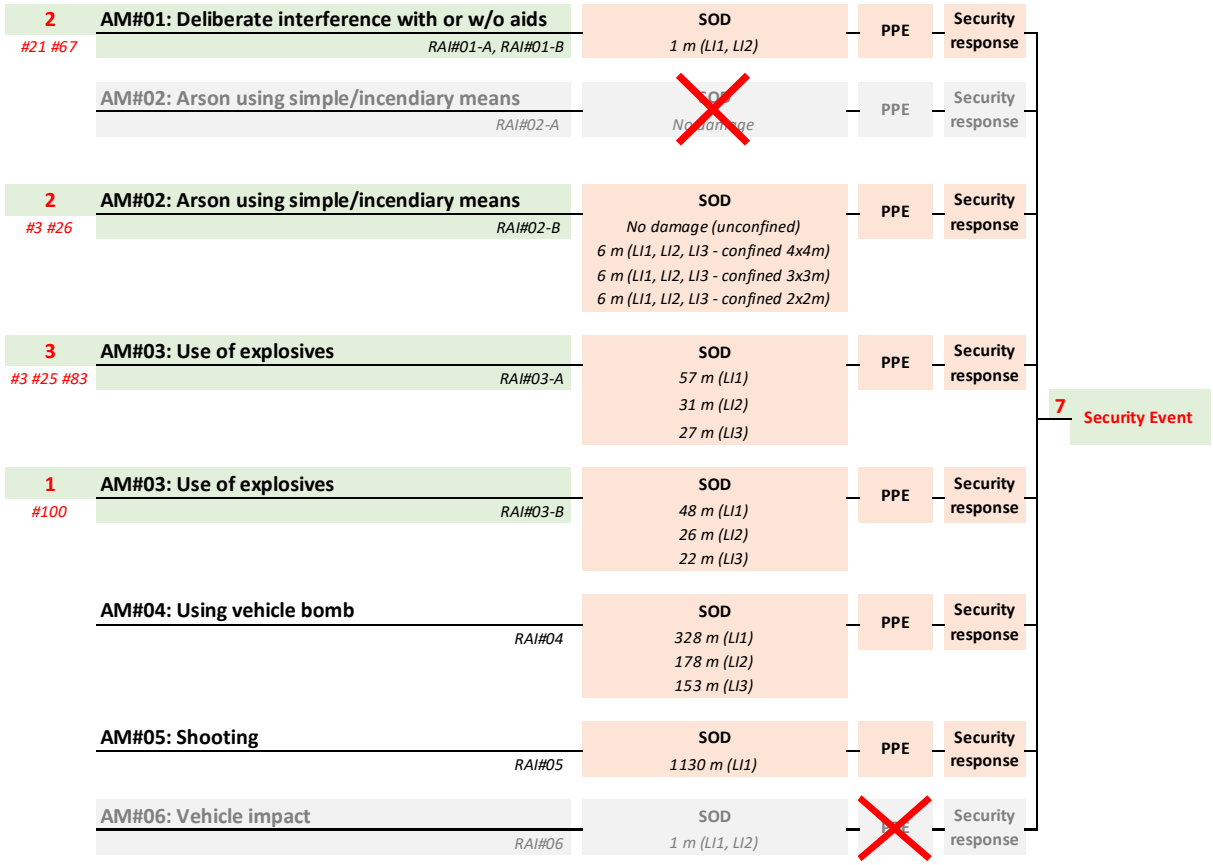

Figure 47 Attack Tree for atmospheric storage installations (RI1). Numbers in tags refer to the number of incidents validating the branch of the AT. Incident codes refer to the incidents described in **Table 29**; AM#-codes and RAI#-codes are defined in **Table 30**. PPE: Physical Protection Element. Adapted from [220].

Attack Tree for pressurized storage installations

Figure 48 shows the Attack Tree (AT) for pressurized storage installations (RI2). No incidents collected in the database occurred in the Chemical&Petroleum sector reported a SE (loss of physical integrity leading to a mass and/or energy release) involving a RI2 installation, and therefore no branch has been validated. However, all the attack modes considered in the present study have the potential to cause damage to pressurized equipment units, with the exception of attacks using simple/incendiary means (AM#02, both the associated RAI#02-A and RAI#02-B, see discussion in Section 5.1.2.3). This is confirmed by the incident that occurred on June 12th, 1987 in Spain, where an equipment under pressure, even if not devoted to storage, was damaged as a consequence of a terrorist attack to the petrochemical plant where it was located. A

significant amount of flammable gas was released in the atmosphere, forming an explosive cloud that was ignited resulting in an explosion [8].

Unlike atmospheric storage installations, in case of pressurized storage installations vehicle impact attacks (AM#06) are considered credible. In fact, bunds may not be present for this type of equipment as the loss of containments that generally occur are gas-phase releases (no pool formation) or two-phase releases (with or without rainout depending on the degree of vaporization).

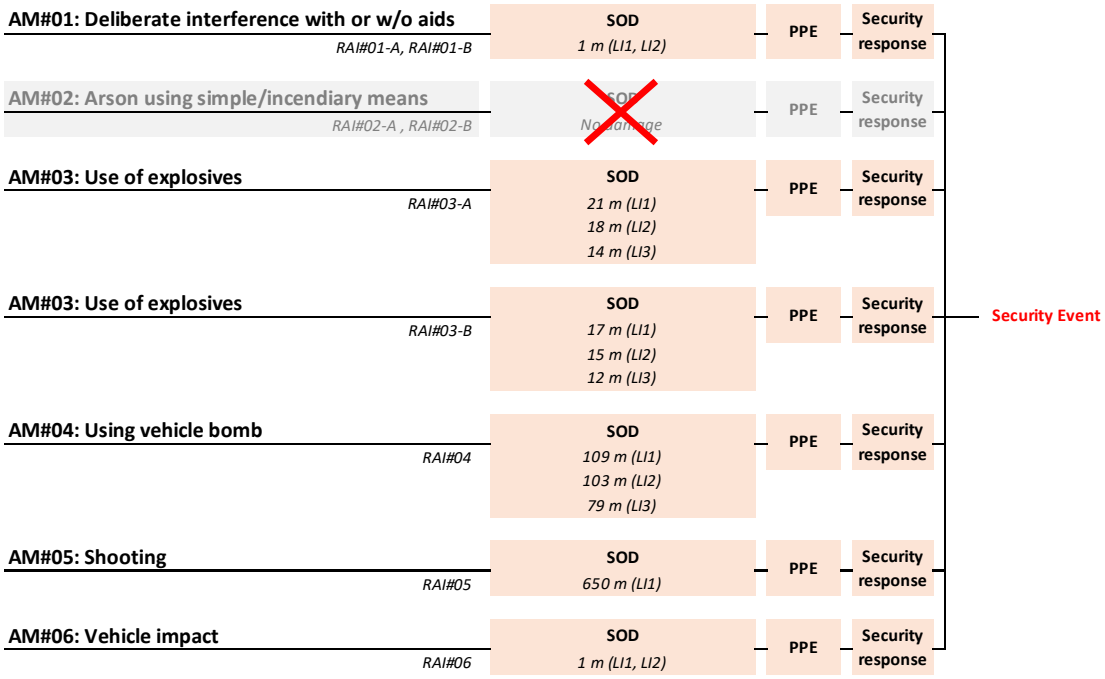

Figure 48 Attack Tree for pressurized storage installations (RI2). AM#-codes and RAI#-codes are defined in **Table 30**. PPE: Physical Protection Element. Adapted from [220].

Attack Tree for storage warehouses

Figure 49 shows the validated Attack Tree (AT) for storage warehouses (RI3). Fourteen incidents collected in the database reported a security event (loss of physical integrity leading to a mass and/or energy release) involving a RI3 installation. As reported in the figure, there is historical evidence of a security event caused by some of the attack modes considered in the present study: branches with tags are those validated by past incidents. The #-codes reported in **Figure 49** are referred to the tags of the incidents described in **Table 29**.

It is important to remark that attacks taking place outside the warehouse (e.g., the detonation of an explosive device outside a storage building) are not accounted in the present study. Therefore, attackers have to reach the interior area in order to accomplish their goals, bypassing the physical barriers in place (e.g., locked doors, vehicle gateways, walls).

The incendiary attack (AM#02) resulted by far the most common AM among all in case of storage warehouses (see validated branches in **Figure 49**): this is probably due to the very frequent presence of flammable materials stored (e.g., paint products, solvents) that can be ignited, resulting in fires, as well as to the presence of solids that can decompose at high temperature causing explosions. For example, in incident #18 (occurred on June 26th, 1988 in Hungary) a former employee crawled into a warehouse where 23 tons of flammable liquids (paints thinners, white spirit, toluene, and xylene) were stored and set fire using a lit cigarette as an ignition source [9]. Another interesting incendiary pattern is that of event #82 (occurred on

June 26th, 2015 in France) where a certified delivery driver drove his light-duty utility vehicle inside a warehouse used to fill inert gas bottles under pressure. The vehicle contained flammable gas bottles that were opened by the driver before entering the site, creating an explosive atmosphere that was ignited resulting in a confined explosion that triggered a fire inside the hangar [9]. Given the different materials of the containers (e.g., rigid plastic, aluminium metal sheet) with respect to the atmospheric and pressurized steel storage tanks (RI1-RI2 installations), both the reference acts of interference RAI#02-A and RAI#02-B are deemed to cause damage (see Section 5.1.2.3).

A deliberate interference with or w/o aids (AM#01) is deemed to be a very common attack mode for storage warehouses. In facts, attackers are required to perform simple actions such as removing caps from containers, opening manual taps or breaking bags. For example, in incident #65 (occurred on October 2nd, 2009 in France) the attackers forced the containers of paint products (primarily acrylic resins and urethane in ethyl acetate) causing their release on the ground and the consequent pollution of a watercourse via the stormwater network [9]. Similarly in incident #73 (occurred on October 6th, 2013 in France), vandals punctured the paint products containers placed inside a warehouse, causing the spill of the flammable content on the ground and on other machinery [9]. Since attackers subsequently set fire by igniting such flammable mixtures, the event was also tagged as arson (AM#02).

The branch corresponding to the detonation of explosive devices (AM#03) carried by the attackers themselves (RAI#03-A) was also validated by past incidents. For example, in incident #1 (occurred on August 9th, 1965 in Uruguay) a warehouse owned by the chemical and pharmaceutical company Bayer was attacked and damaged with explosive devices by the political group “Tupamaros” in order to demonstrate anti-US sentiment [3]. No standoff distance is reported in the branch of the AT corresponding to this RAI as damage is considered certain in case of successful detonation (see Section 5.1.2.3).

On the contrary, the use of explosives (AM#03) lifted by drones (RAI#03-B) was not observed in past incidents involving a storage warehouse: this attack pattern is deemed to be unlikely for RI3 installations due to the fact that storage buildings of hazardous materials are typically enclosed areas and access of drones may be difficult.

Although no incidents collected in the database reported the detonation of a vehicle bomb inside a storage warehouse (AM#04), this AM is deemed to be possible: similarly to what stated for explosive devices, the damage is considered certain in case of successful detonation (see Section 5.1.2.3).

Regarding shooting attacks (AM#05), no validation was possible as no incident reporting this AM was recorded. However, this AM is physically possible, as a perforation of the containers is considered certain for shooters within the interior area of a storage warehouse (no standoff distance reported) given the low thickness of the typical low-volume containers used for liquids and powders (see Section 5.1.2.3).

Similar considerations apply to vehicle impact attacks (AM#06).

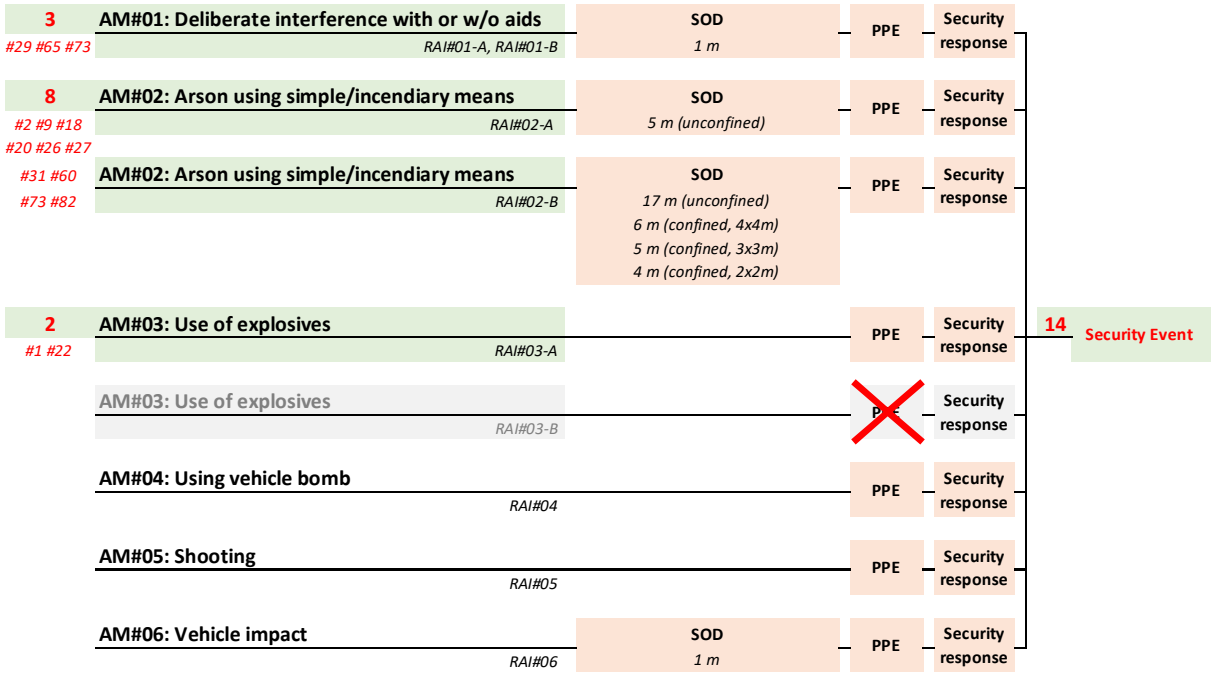

Figure 49 Attack Tree for storage warehouse (RI3). Numbers in tags refer to the number of incidents validating the branch of the AT. Incident codes refer to the incidents described in **Table 29**; AM#-codes and RAI#-codes are defined in **Table 30**. PPE: Physical Protection Element. Adapted from [220].

5.1.2.3. Calculated standoff distances

In the following, calculation of standoff distances for each attack mode (AM) and reference target storage installation (RI) considered in the present study, is discussed. The obtained values of the standoff distances are reported in the AT of **Figure 47**, **Figure 48**, and **Figure 49**. As mentioned above, providing standoff distance values (e.g., by appropriate Physical Protection System) may lead to elimination of the corresponding branch of the AT.

Standoff distances for deliberate interferences with or w/o aids (AM#01)

In case of deliberate interferences with or w/o aids (AM#01), an arbitrary standoff distance of 1 m was defined for all the three categories of target reference storage installations considered in the present study (RI1-RI2-RI3 installations). In fact, according to the success criterion discussed in Section 5.1.2.1, attackers have to reach the target installation in order to cause a security event (mass and/or energy release). This is applicable to both RAI#01-A and RAI#01-B (see **Table 30**).

Standoff distances for arson using simple/incendiary means (AM#02)

In case of incendiary attacks (AM#02), different standoff distances were adopted for the three categories of reference target storage installations (RI).

For the steel-made atmospheric and pressurized target storage installations (i.e., RI1-RI2 installations) the pool fires originated by the ignition of 50 L (RAI#02-A) and 1000 L (RAI#02-B) of gasoline were modelled using the correlations derived by Mudan [211], Raj [212], Bagster and Pitablado [213] reported in the "Yellow Book" of TNO [214]. The radiative heat flux was evaluated as function of the distance and of the duration of the fire. These were compared with the damage criteria provided in a study by Cozzani et al. [209], which correlate heat flux with time to failure (ttf) of atmospheric and pressurized steel-made equipment. Distances for which the ttf was higher than fire duration were considered safe for the target equipment. The standoff

distance was identified as the minimum distance at which the safe condition was satisfied, rounded up at the upper integer. Results are reported in **Table 31**.

In case of a pool fire originated by the ignition of an unconfined 50 L pool of gasoline (RAI#02-A) both the RI1 and RI2 installations resulted safe from the heat load emitted as the duration of the fire was lower than their ttf (fire duration lower than 1 minute).

As regards the ignition of 1000 L of gasoline contained inside IBC tanks (RAI#02-B), different pool sizes were considered since obstacles limiting pool spreading (e.g., curbs, other units, bunds) may be present on the ground. In particular, in addition to the case of unconfined pool, 2x2 m^2, 3x3 m^2, and 4x4 m^2 pools were considered. The results obtained are summarized in **Table 31**. The standoff distances in case of atmospheric storage installations (RI1) are about a few meters (maximum 6 m from the centre of the fire) while no damages were considered credible for pressurized storage installations (RI2) as, from the consequence analysis, IBC tanks should be very close to target equipment (moving IBC tanks to such location would require equipment already considered in AM#01 and AM#06). As it is common in the assessment of fire scenarios [209], it is not possible to discriminate a priori between loss intensities LI1, LI2, and LI3: within the standoff distance, the extension of damage depends on specific features of the target installations and of the attack.

In case of incendiary attacks to storage warehouses (RI3), the hazardous substances are usually stored in rigid plastic containers, thin metal sheet containers or bags. The concept of fuel package, defined as “a group of combustible items whose characteristics and arrangement are such that the ignition of one item can be expected to cause the spread of fire to the remaining items in the group” [224], was adopted in order to define standoff distances. NFPA555 [224] defines conventional separation distances beyond which the items are not considered part of the same fuel package: in particular, a standoff distance of 1 meter from the flame was adopted for RAI#02-A (ignition of 50 L of gasoline – unconfined pool) and for RAI#02-B (ignition of 1000 L of gasoline – unconfined pool).

Table 31 Standoff distances calculated for RAI#02-A and RAI#02-B considering different pool sizes. Thermal radiation for damage at pool fire duration for steel made equipment is calculated according to Cozzani et al. [209]. Adapted from [220].

RAI code	Target Storage Installation	Pool size [m^2]	Pool fire duration [min]	Thermal radiation for damage at pool fire duration [kW/m^2]	Thermal radiation at the flame centre (SEP) [kW/m^2]	Standoff distances from flame centre [m]
RAI#02-A	Atmospheric (RI1)	5 (unconfined on gravel, D=2.5m)	< 1	140	109	No structural damage
	Pressurized (RI2)	5 (unconfined on gravel, D=2.5m)	< 1	>140	109	No structural damage
	Warehouse (RI3)	5 (unconfined on concrete, D=3.5m)	< 1	n.a.	99	5 (1.5 m from flame surface)
RAI#02-B	Atmospheric (RI1)	103 (unconfined on gravel, D=11.5m)	< 1	140	50	No structural damage
		16 (confined, 4x4m)	7	22	90	6 (1.5 m from flame surface)
		9 (confined, 3x3m)	12	15	100	6 (2.6 m from flame surface)
		4 (confined, 2x2m)	27	12	112	6 (3.7 from flame surface)
	Pressurized (RI2)	103 (unconfined on gravel, D=11.5m)	< 1	>140	50	No structural damage
		16 (confined, 4x4m)	7	74	90	In flame
		9 (confined, 3x3m)	12	54	100	3 (1 m from flame surface)
		4 (confined, 2x2m)	27	45	112	2 (0.7 m from flame surface)
	Warehouse (RI3)	201 (unconfined on concrete, D=16m)	< 1	n.a.	38	17 (1 m from flame surface)
		16 (confined, 4x4m)	7	n.a.	90	6 (1.5 m from flame surface)
		9 (confined, 3x3m)	12	n.a.	100	5 (1.6 m from flame surface)
		4 (confined 2x2m)	27	n.a.	112	4 (1.7 m from flame surface)

Standoff distances for the use of explosives (AM#03) and of vehicle bombs (AM#04)

In case of attacks involving explosives (carried by a single man as in RAI#03-A, lifted by drone as in RAI#03-B, or contained inside vehicles as in RAI#04), different standoff distances were adopted for the three categories of reference target storage installations.

For the steel-made atmospheric and pressurized target installations (i.e., RI1-RI2 installations), the effects due to the peak overpressure were modelled using TNT-equivalence model proposed by Bounds [210] and were compared with damage criteria provided Cozzani and Salzano [208]. Damage models allow, in this case, to differentiate between expected loss intensities (LI1, LI2, and LI3). **Table 32** reports the calculated standoff distances in case of detonation of 50 kg (RAI#03-A) and 30 kg (RAI#03-B) of TATP, and of 50,000 kg of AN/dolomite 50/50 + DF (RAI#04). They turned out to be always below 60 m in case of attack using explosives carried by persons or drones (AM#03), and 330 m in case of vehicle bombs (AM#04). In case of pressurized targets, standoff distances are at least 40% lower than for atmospheric counterparts.

In case of storage warehouses (RI3), damage and release from containers may occur with overpressures lower than the threshold values used for RI1 and RI2 installations. Given the order of magnitude of the standoff distances calculated for atmospheric and pressurized storage installations (see **Table 32**), a release is always considered possible in case of successful detonation inside the building (conservative assumption). Therefore, the concept of standoff distances coincides with limitation to warehouse access for RAI#03-A, RAI#03-B, and RAI#04 to RI3-installations.

Table 32 Standoff distances calculated for RAI#03-A, RAI#03-B, RAI#04 considering LI1, LI2, and LI3 loss intensities from steel-made atmospheric and pressurized target storage installations. Adapted from [220].

				Standoff distances [m]		
RAI code	**Target Storage Installation**	**Loss Intensity**	**Threshold value [bar]**	**30 kg TATP (RAI#03-A)**	**50 kg TATP (RAI#03-B)**	**50000 kg AN/dolomite (50/50) + DF (AM#04)**
RAI#03-A, RAI#03-B, RAI#04	Atmospheric (RI1)	LI1	0.07	48	57	328
		LI2	0.16	26	31	178
		LI3	0.2	22	27	153
	Pressurized (RI2)	LI1	0.3	17	21	119
		LI2	0.38	15	18	103
		LI3	0.61	12	14	79

Standoff distances for shooting attacks (AM#05)

Standoff distances for atmospheric and pressurized storage installations with respect to shooting attacks (AM#05) were calculated in the context of the study described in Section 5.2.4.2, to which the reader is referred in order to gain more detailed information on the method adopted and on the results obtained. The final calculated values of standoff distances, considering different families of projectiles, are reported in **Table 44** in Section 5.2.4.2. However, in the context of the current analysis, the higher value obtained for atmospheric vessels (i.e., 1130 m) and that obtained for pressurized vessels (i.e., 650 m) are considered for RAI#05 for conservative reasons (safe-side): these correspond to the ones obtained for the reference projectile “7.62x51 mm”.

Given the low thickness and the materials employed in the containers used in the storage of hazardous materials in warehouses, a release is always considered possible in case of successful shooting inside the building. Therefore, standoff distance coincides with access to the RI3-installation.

Standoff distances for vehicle impact attacks (AM#06)

Analogously to deliberate interferences with or w/o aids (AM#01), also for attacks consisting in the ramming of installations using a large goods vehicle (AM#06), an arbitrary standoff distance of 1 m was defined. In fact, according to the success criterion discussed in 5.1.2.1, attackers have to reach the target installation with the vehicle of choice in order to cause a security event (mass and/or energy release).

This arbitrary standoff distance was applied to pressurized storage installations (RI2) and to storage warehouses (RI3): in fact, in case of atmospheric storage installations (RI1), the AM was already excluded.

5.1.2.4. Validation of the proposed Bow-Tie diagrams for reference substances

Only 12 reports of the incidents collected for the Chemical&Petroleum sector [2] have enough details on the physical damage scenarios following the SE to allow the validation of the BTs developed. Thus, direct validation was only possible for a limited number of cases: flammable liquids stored in an atmospheric storage installation (RI1), flammable liquids stored in a warehouse (RI3), oxidizing solids stored in a warehouse (RI3). Nevertheless, the validation provided earlier concerning the ATs and the consideration that the ET part of the BT is not qualitatively affected by the AM (see also the discussion below on ignition probability), allow a confident use of the ETs reported in **Figure 50** (generated using the MIMAH methodology [99]). It is important to underline that, given the scope of the analysis to identify reference security scenarios (from attack scenarios to physical damage scenarios), the unmitigated ETs are reported. However, such ETs may be updated considering also mitigation systems and emergency response by the aid of safety-specific methods (e.g., the MIRAS methodology [99]). The physical damage scenarios that are displayed in the ETs are described in **Table 33**.

Table 33 Definitions of the physical damage scenarios (FS) considered in the present study, adapted from the "Yellow Book" of TNO [225].

FS code	Physical damage scenario	Description
#01	Jet fire	Combustion of a high-speed release of a flammable gas.
#02	VCE	The explosion resulting from an ignition of a premixed cloud of flammable vapour, gas or spray with air, in which flame acceleration and partial confinement cause the formation of blast wave.
#03	Flash fire	The combustion of a flammable vapour and air mixture in which flame passes through that mixture at less than sonic velocity, such that negligible damaging overpressure is generated.
#04	Pool fire	The combustion of material evaporating from a layer of a flammable liquid.
#05	Flare	The combustion of low-speed release of a flammable gas which mixes with air forming a flammable mixture.
#06	Toxic cloud	Atmospheric dispersion of a gas or aerosol, which is toxic to humans by inhalation.
#07	Fireball	A fire, burning with a diffusive flame and in the presence of lifting effects causing the burning mass to rise into the air.
#08	Physical explosion / BLEVE	The explosion resulting from the sudden failure of a vessel containing a pressurized gas or a pressurized liquid at a temperature well above its normal boiling point (in this case the explosion is commonly called BLEVE - Boiling Liquid Expanding Vapour Explosion). The explosion generates missiles ejection and blast wave.
#09	Confined chemical explosion	An explosion of fuel-oxidant mixture inside a closed system (e.g., a vessel or building). The latter can be generated by a rapid decomposition of the substance contained in the closed system. The explosion generates missiles ejection and blast wave.

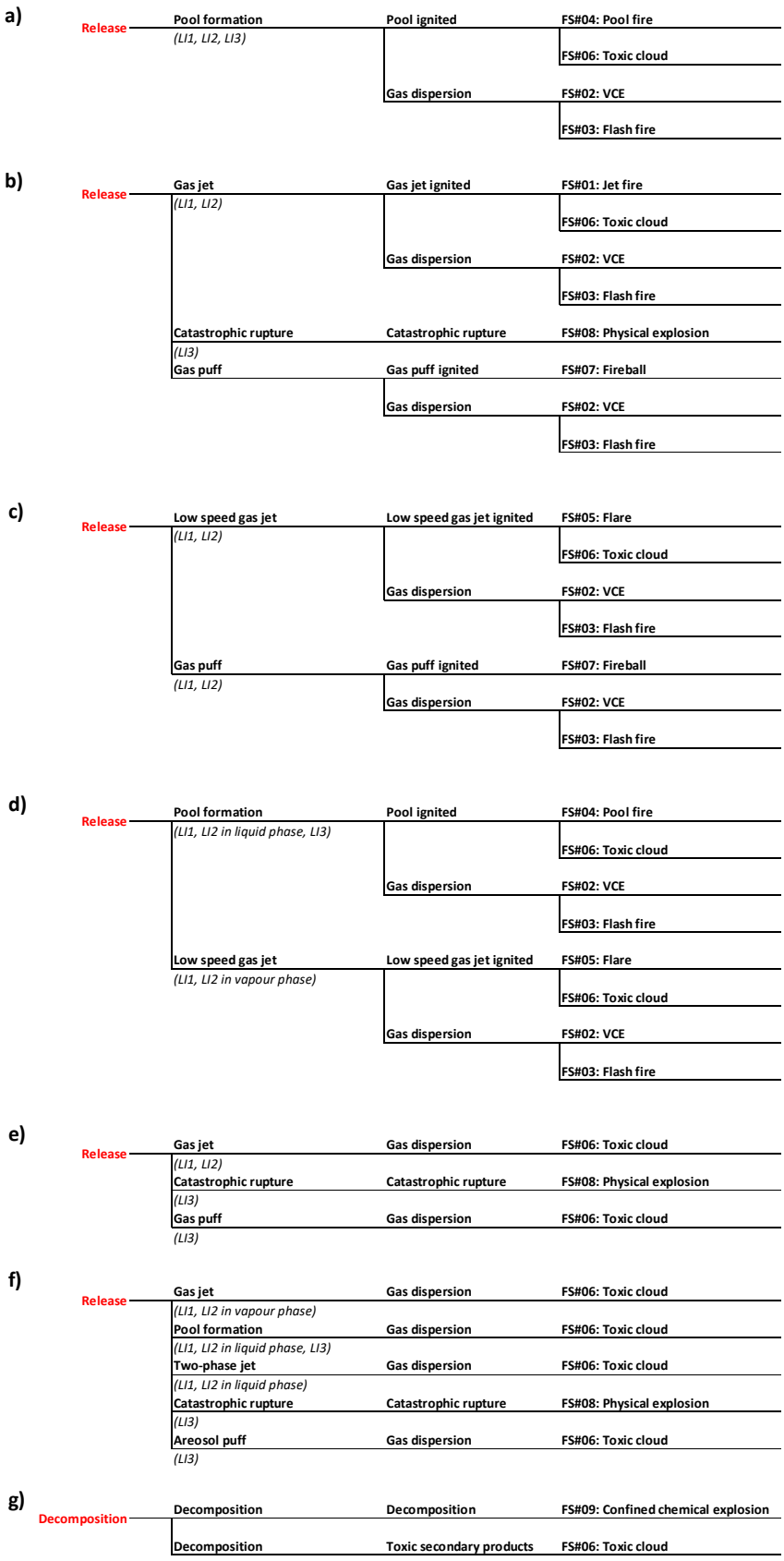

Figure 50 a) ET for flammable liquids; b) ET for flammable pressurized gasses; c) ET for flammable gasses d) ET for flammable cryogenic liquids; e) ET for toxic pressurized gasses; f) ET for oxidizing solids. Adapted from [99].

Bow-Tie diagram for atmospheric storage of flammable liquids

Figure 51 shows the Bow-Tie (BT) diagram obtained for the atmospheric storage of flammable liquids (e.g., oil/hydrocarbon solvents). The AT on the left side of the security event (loss of containment) is the one developed in Section 5.1.2.2 for atmospheric storage installations (RI1), while the Event Tree (ET) was generated with the MIMAH methodology (see **Figure 50-a**). Green-shaded branches are those validated by past security-related incidents.

The only possible primary event is the formation of a pool of the flammable substance, which was validated by four incidents (see tags in **Figure 51** and description in **Table 29**). In two cases this event was caused by deliberate interferences involving simple operations without the use of instruments or using tools that are present on site (AM#01, see incidents #21 and #67 in **Table 29**), while in the other two events it was due to the detonation of explosives (AM#03, see incidents #83 and #100 in **Table 29**).

A pool fire (FS#04) is the physical damage scenario that occurs in case of immediate ignition of the flammable pool. This happened in two of the four incidents available for BT validation. In incident #83 (occurred on July 14th, 2015 in France), 2000 tons of naphtha and 1000 tons of gasoline were released and ignited resulting in pool fires as a consequence of the detonation of explosive devices (AM#03/RAI#03-A see **Table 30**) [8]. Similarly, in incident #100 (occurred on September 14th, 2019 in Saudi Arabia), the Saudi Aramco oil processing facility underwent a drone attack (AM#03/RAI#03-B see **Table 30**) that caused the release of oil from 14 atmospheric storage tanks and other process equipment that resulted in multiple pool fires [221,222,226]. In case combustion conditions produce large amounts of toxic compounds, a toxic cloud (FS#06) is associated to the pool fire, and toxic effects are added to those related to the heat load.

Overall, the formation of a pool is deemed credible for all the AMs considered. However, its ignition (i.e., the occurrence of a pool fire) is highly probable only in case of incendiary attacks. In case of attacks using explosive devices (AM#03 and AM#04), ignition is deemed possible, but not certain. In fact, in the incident that occurred on February 15th, 2018 in Colombia, attackers detonated an explosive device causing a release from an oil pipeline, but no ignition occurred [140]. All the other AMs are not deemed to be able to automatically ignite the flammable pool. Similarly, the gas dispersion and the potential delayed fire scenarios are considered unlikely.

As regards the secondary event “gas dispersion”, it is excluded in case of low volatile liquids, and in case of incendiary attacks (AM#02) given the presence of an immediate source of ignition (i.e., the arson deliberately triggered by the attackers). If a delayed ignition occurs after the gas dispersion, a vapour cloud explosion (VCE, FS#02) or a flash fire (FS#03) may occur depending on several factors such as the reactivity of the substance involved, the turbulence of the gas cloud, the confinement, and the explosive gas mass. Both the gas dispersion and the delayed fire scenarios, though deemed possible, were not validated by past incidents.

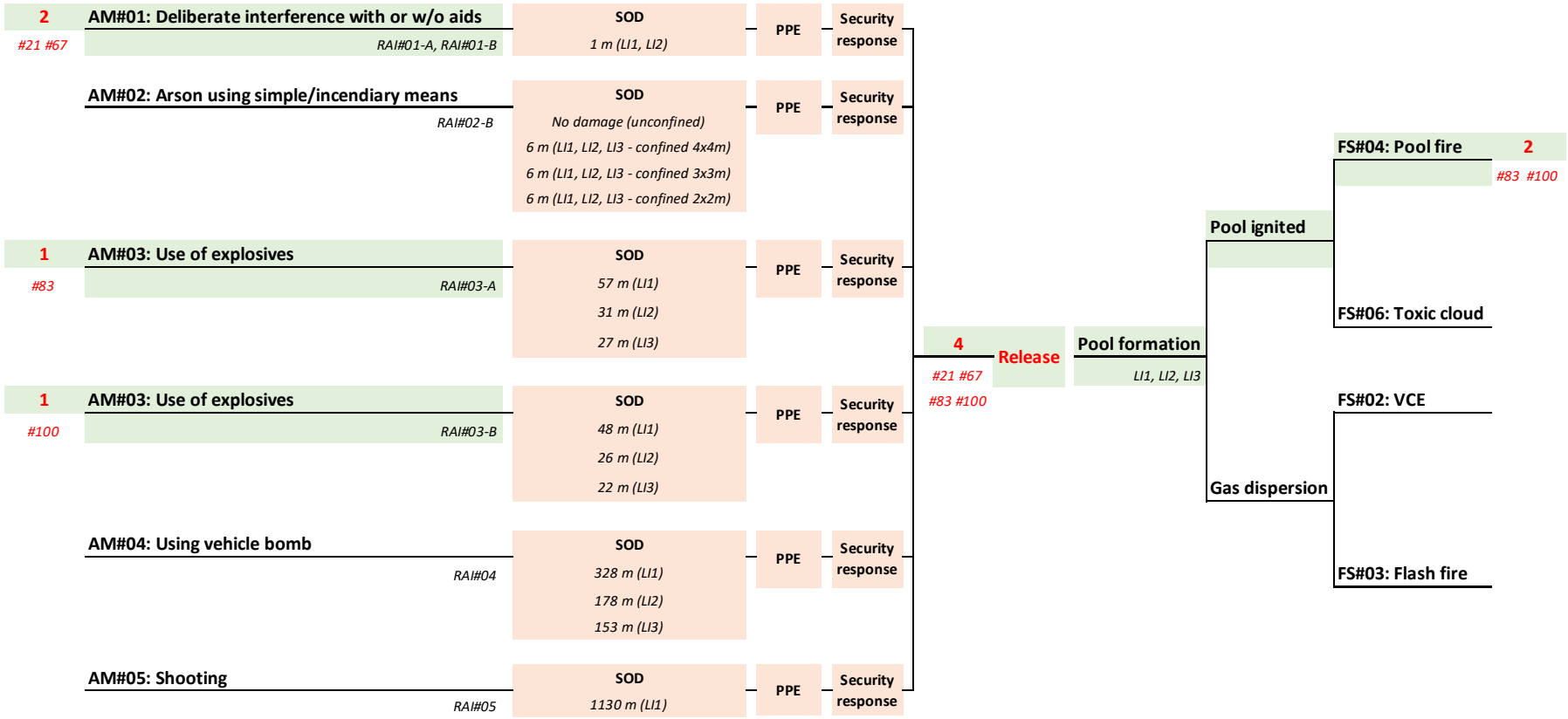

Figure 51 Bow-Tie for atmospheric storage of flammable liquids. Numbers in tags refer to the number of incidents validating the branch of the BT. #-codes refer to the incidents described in **Table 29**; AM#-codes and RAI#-codes are defined in **Table 30**; FS#-codes are described in **Table 33**. Adapted from [220].

Bow-Tie diagram for storage of flammable liquids in a warehouse

Figure 52 shows the Bow-Tie (BT) diagram that was obtained for the storage of flammable liquids (e.g., paint products) in a warehouse. The AT on the left side of the security event (loss of containment) is the one developed in Section 5.1.2.2 for storage warehouses (RI3), while the Event Tree (ET) on the right side was generated with the MIMAH methodology considering flammable liquids. In particular, the ET was adapted from that in **Figure 50-a** considering that warehouses are indoor spaces: vapour cloud explosion (VCE, see FS#02 in **Table 33**) was replaced by confined chemical explosion (see FS#09 in **Table 33**) and flash fire (see FS#03 in **Table 33**) was eliminated. Green-shaded branches are those validated by past incidents.

The results obtained from the analysis of the BT in **Figure 52** are similar to those discussed for the atmospheric storage of flammable liquids. The formation of a pool was validated by 6 incidents collected in the database (see tags in **Figure 52**): deliberate interferences with or without the use of aids (AM#01) and incendiary attacks (AM#02) were the AMs carried out by the attackers to cause such scenario. For example, in incident #29 (occurred on January 19th, 1997 in France) vandals deliberately caused the release of 2000 L of fuel oil in a wastewater treatment plant [9], while in incident #31 (occurred on July 31st, 1999 in Canada) a warehouse containing flammable paint products was set afire causing also the dispersion of toxic smoke [9]. The other attack modes were not validated: however, as previously discussed, they are potentially able to cause a loss of containment (see Section 5.1.2.2).

In 4 out of the 6 incidents, the flammable liquid became ignited, resulting in a pool fire (FS#04) inside the storage warehouse: this happened for all the incidents characterized by an incendiary attack (AM#02), confirming that a pool fire is a very likely physical damage scenario in case of deliberate arsons within warehouses storing flammable liquids. A toxic cloud (FS#06) in addition to the fire scenario was recorded in 3 incidents. This FS results likely in case of liquids such as paint products or pesticides. For example, in incident #20 (occurred on February 16th, 1989 in Germany) the dispersion of toxic smoke was reported as a consequence of the fire of flammable and toxic pesticides caused by a terrorist incendiary attack [9].

As regards the secondary event “gas dispersion”, it is excluded in case of low volatile liquids, and in case of incendiary attacks (AM#02) given the presence of an immediate source of ignition (i.e., the arson deliberately triggered by the attackers). If a delayed ignition occurs after the gas dispersion, a confined chemical explosion (FS#09) may occur. However, this physical damage scenario was not validated by past incidents.

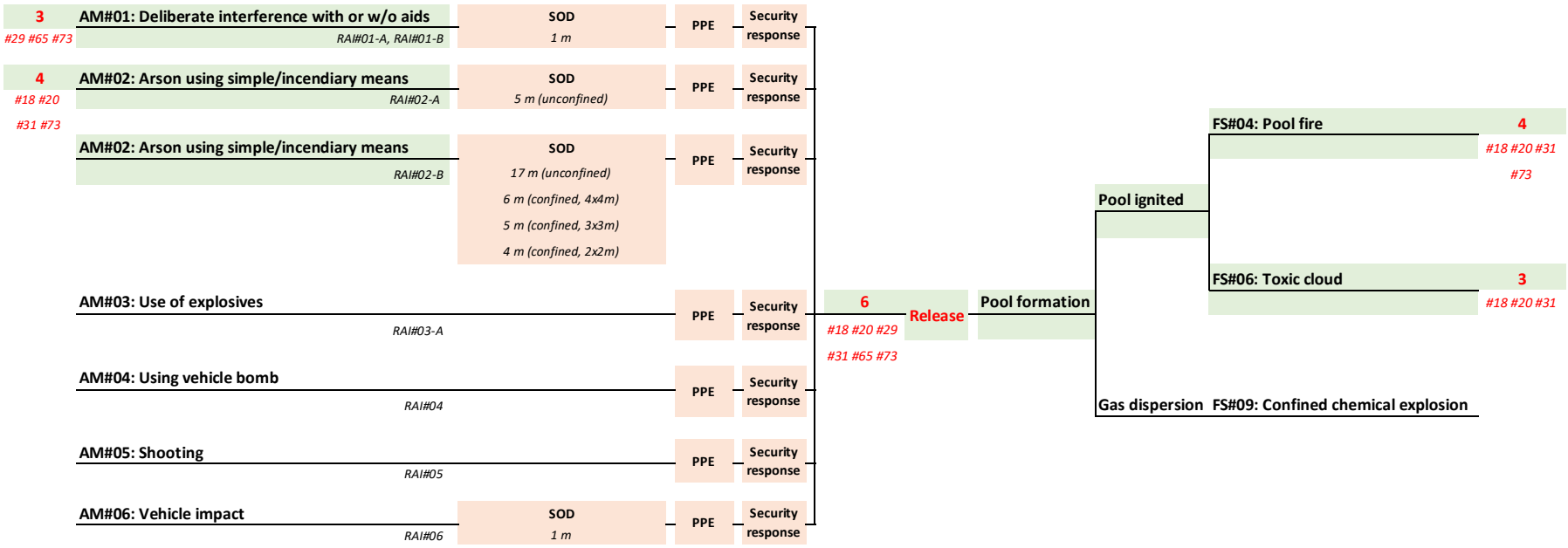

Figure 52 Bow-Tie for storage of flammable liquids in a warehouse. Numbers in tags refer to the number of incidents validating the branch of the BT. #-codes refer to the incidents described in **Table 29**; AM#-codes and RAI#-codes are defined in **Table 30**; FS#-codes are described in **Table 33**. Adapted from [220].

Bow-Tie diagram for storage of oxidising solids with explosion hazards

Figure 53 shows the Bow-Tie (BT) diagram obtained for oxidizing solids with explosive hazards (e.g., ammonium nitrate / sodium chlorate) that are stored in bags inside a warehouse. The AT on the left side of the security event (decomposition, i.e. a change of the chemical state of the substance [99]) is that developed for storage warehouses (RI3) and discussed in Section 5.1.2.2. The ET on the right side of the BT was generated with the MIMAH methodology considering oxidizing solids with explosive hazards (see **Figure 42-g**). Green-shaded branches are those validated by past incidents.

The decomposition of an oxidising solid can be triggered by the action of an energy and/or heat source or by the reaction with an incompatible substance. Therefore, only incendiary attacks (AM#02) and attacks involving explosives (AM#03 and AM#04) are potentially capable to trigger the decomposition of an oxidizing solid due to their respective attack vectors (i.e., heat load and overpressure, see **Table 30**), which leads to a confined explosion in the warehouse. The decomposition may also lead to the formation of secondary toxic products (toxic cloud, FS#06).

Incident #9 (occurred on October 18th, 1981 in France) validated the incendiary attack (AM#02). In the event, this AM led to the decomposition of 14 tons of sodium chlorate (oxidising solid) that resulted in a confined chemical explosion (FS#09) inside a storage warehouse which also contained 33,000 L of flammable liquids. The incident caused one fatality and 12 injuries, and an estimated $26 million of economic losses [9].

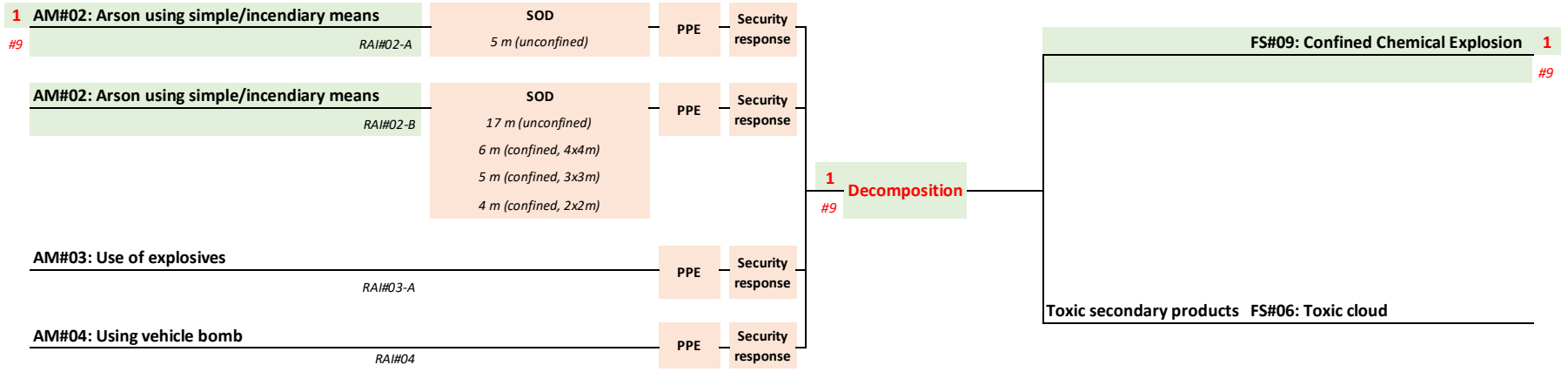

Figure 53 Bow-Tie for storage of oxidising solids with explosion hazards in a warehouse. Numbers in tags refer to the number of incidents validating the branch of the BT. #-codes refer to the incidents described in **Table 29**; AM#-codes and RAI#-codes are defined in **Table 30**; FS#-codes are described in **Table 33**. Adapted from [220].

5.1.3. Method for identification of reference security scenarios: step-by-step approach

5.1.3.1. Overview of the approach

The method described in the present study (see Section 5.1.1) can be generalized, allowing for the development of Bow-Tie diagrams for any other hazardous substance and target installation different from those considered herein. The flowchart of the generalized procedure for the identification of reference security scenarios based on Bow-Tie formalism, is shown in **Figure 54-a**. It consists in 7 steps: starting from the collection of the needed input information, it provides for the selection of the relevant hazardous equipment (EQ) in the plant and the identification of credible Security Events (SE) for each EQ; then, for each SE, it requires to build an Attack Tree (AT) and an Event Tree (ET) and combining them into a Bow-Tie (BT) diagram in order to define reference security scenarios according to specific criteria.

Clearly, in case they are applicable, the set of proposed and validated Attack Modes (AMs), Attack Trees (ATs) for reference installations (RI1: atmospheric storage installations; RI2: pressurized storage installations; RI3: storage warehouses), and Bow-Tie (BT) diagrams for reference hazardous substances (atmospheric storage of flammable liquids, storage of flammable liquids in a warehouse, storage of oxidising solids with explosion hazards in a warehouse) are used respectively in Step 4, Step 6, and Step 7 as direct outputs (see **Figure 54-a**).

The reference security scenarios obtained by the application of the approach sketched in **Figure 54-a** can support hazard identification in SVA/SRA studies with respect to physical threats. For example, support to the SVA developed by the CCPS (see **Figure 54-b**), which is specific for the chemical and process industry, is provided to Step 2 “Facility characterization”, providing the critical assets in the plant (i.e., the relevant hazardous equipment (EQ)), the potential hazards (i.e., the security events (SE)), and the events that can follow the SE (i.e., the physical damage scenarios in the ETs), Step 3 “Threat assessment”, providing the attack scenarios (from the ATs) that can be used by the attackers to generate the SEs, and Step 4 “Vulnerability analysis”, providing the specific cause-consequence chains of events from attack scenarios to physical damage scenarios (i.e., the security scenarios).

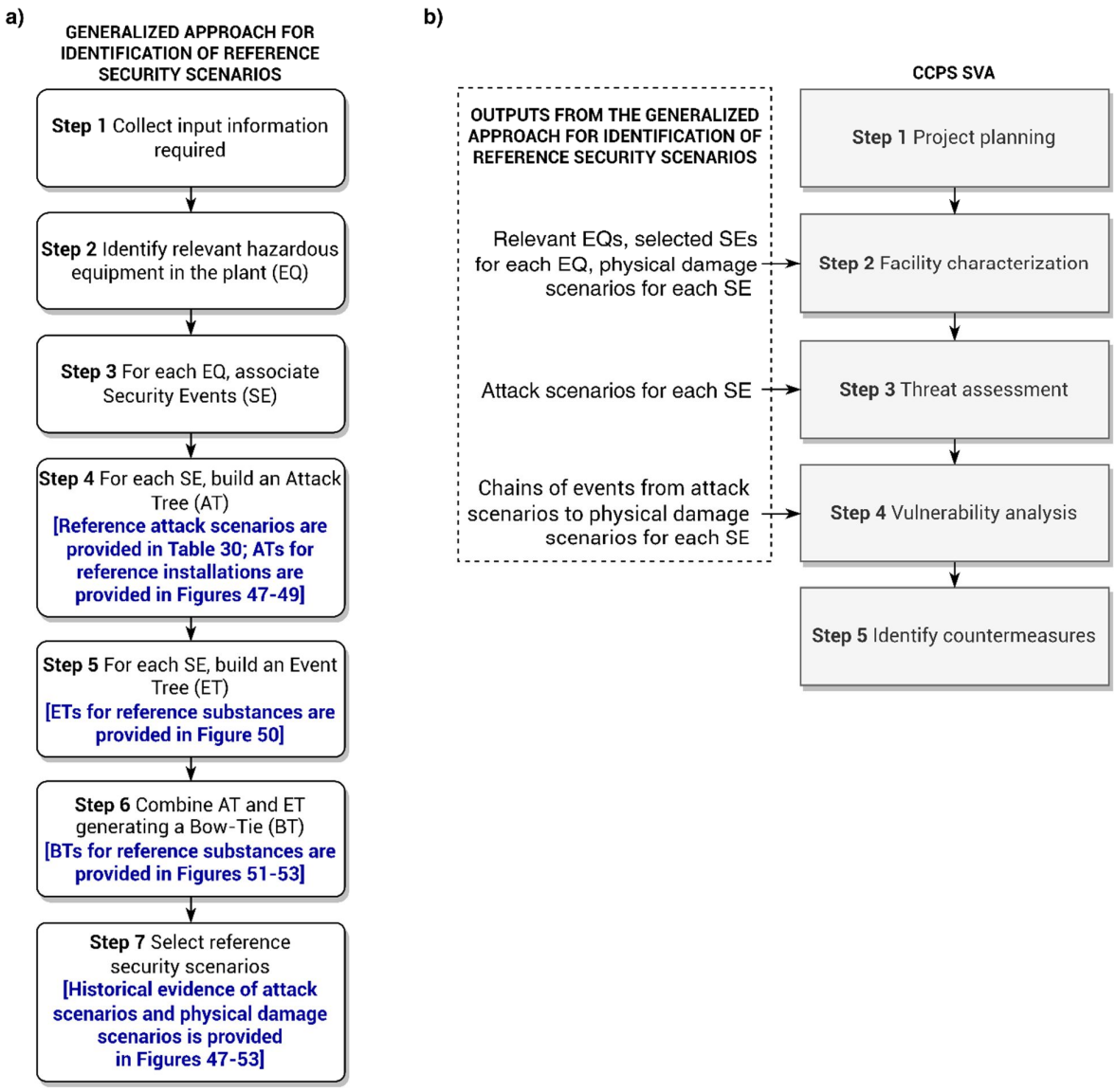

Figure 54 a) Flowchart of the generalized approach for the identification of reference security scenarios; b) Contribution of the results of the approach shown in panel-a) in supporting application of CCPS SVA. Adopted from [220].

5.1.3.2. Detailed description of the approach

The approach for the identification of reference security scenarios consists of 7 steps (see **Figure 54-a**).

In Step 1, the input information needed for the application is collected: the PFD (Process Flow Diagram), the material balances, the list of substances stored or processed and their hazardous properties, the operating conditions of each equipment unit, the data sheets of each equipment unit, and the layout of the plant.

In Step 2, the relevant hazardous equipment (EQ) in the plant (i.e., the ones which participate significantly to the risk created by the plant)) are identified. They shall be selected on the basis of the inherent hazard (potential to originate accident scenarios due to inherent characteristics of the process, such as high inventory of hazardous materials or severe operating conditions). Inherent safety indicators such as UPI by Tugnoli et al. [178], RISI by Rathnayaka et al. [227], and PSI by Shariff et al. [181], can be used for this purpose. Conventional methodologies for the hazard ranking of process units can be used as well such as the Dow F&EI [182], the Mond Index [184], and the threshold-based approach proposed by MIMAH methodology [99],

considering only the hazard factors scoring consequence severity (e.g., penalties for high frequencies of equipment failure are neglected since they are not relevant to security threats).

In Step 3, the compatible Security Events (SE) are associated to each relevant hazardous equipment selected in the previous step. A SE is intended as loss of physical integrity (LPI) and/or a loss of containment (LOC) of the hazardous material stored and/or processed in the equipment unit. The categories of LPIs and LOCs proposed by the standard API RP 581 [185], the MIMAH methodology [99], the TNO "Purple Book" [186], or by Iaiani er al. [101] (see **Table 13** in Section 4.2.1) can be used as reference.

In Step 4, an Attack Tree (AT) is built for each SE selected in the previous step, reporting all the ways through which the relevant hazardous equipment (EQ) under consideration can be attacked (i.e., the Attack Modes (AM)) using the fault tree formalism [228]. The analysis described in the previous sections provides an exhaustive set of validated attack scenarios (AMs and respective RAIs, see Section 5.1.2.1) that can be used to build the AT, obtained from an extended review of the ones proposed in the reference sources of most used SVA/SRA studies suitable for the chemical and process industry. Clearly the AMs shall be tailored considering the specific case: only the ones that can potentially cause the SE under consideration shall be considered in the AT. An AM can be considered or excluded based on the type of attack vector, distance from the target, type of safety/security barriers in place, etc. Moreover, in case the EQ is an atmospheric storage installation, a pressurized storage installation, or a storage warehouse, the analysis carried out provides reference validated ATs (see Section 5.1.2.2) that can be directly used as output of this step.

In Step 5, an Event Tree (ET) is built for each SE selected in Step 3, reporting all the events leading from it to the physical damage scenarios (FS). The method proposed in step 6 of the MIMAH methodology [99] can be used to this purpose, considering the type of SE under consideration, the acute hazard characteristics and the pre-release operative conditions of the substances contained inside the relevant hazardous equipment (EQ) under consideration.

In Step 6, a Bow-Tie (BT) diagram is obtained for each SE combining the AT (left side of BT) and the ET (right side of BT) developed in Step 4 and Step 5 respectively. In the analysis described in the previous sections, validated BTs for reference substances (atmospheric storage of flammable liquids, storage of flammable liquids in a warehouse, storage of oxidising solids with explosion hazards in a warehouse) are provided (see Section 5.1.2.4), and can be directly used as output of this step. Clearly, in the latter case, steps 4 and 5 are bypassed and the case-specific considerations regarding the tailoring of the AMs and of the physical damage scenarios shall be done in this step.

In Step 7, reference security scenarios (event sequence starting from the attack scenarios and ending with the physical damage scenarios) are selected. This can be done using the worst-case criterion: for each AM in the AT, the physical damage scenario with the most severe consequences (i.e., the worst-case physical damage scenario) on humans, assets, and the environment, is selected. Qualitative severity scales as those provided by Iaiani et al. [100] (see **Table 21** in Section 4.3.1) or expert judgment may be used to identify worst-case scenarios.

Alternatively, reference security scenarios may be identified on the basis of accidents/incidents that have occurred in the past. The proposed AMs (see Section 5.1.2.1), ATs (see Section 5.1.2.2), and BTs (see Section 5.1.2.4) were validated using past security-related incidents. Thus, all the validated security scenarios can be selected as reference security scenarios.

5.1.4. Illustrative case study

5.1.4.1. Set-up of the case study

The use of the results of the present study in the framework of security hazard identification is demonstrated with reference to a tank in a storage section of a petrochemical plant. **Figure 55** shows an atmospheric floating roof storage tank (TA01) containing a low volatile flammable liquid. A catch basin surrounded by a concrete wall is present around the tank. The minimum distance between the concrete wall and the tank is 15 m. The minimum distance between the tank and the fence of the site is 60 m. Three alternative potential locations reached by the attacker were considered (see **Figure 55**). In the first one (P1), the attack takes place from position P1 outside the site fence (at 60 m from TA01). In the second case (P2), the attacker enters the plant internal road network, but is outside the catch basin of TA01. In the third case (P3), the attack takes place in close proximity of TA01, inside the catch basin.

Figure 55 Layout of the site considered for the case study showing the atmospheric storage tank TA01, the catch basin (continuous yellow line), the site fence (black and grey dashed line), and the positions P1, P2, and P3. Adopted from [220].

5.1.4.2. Results of the case study

The required input information (PFD, material balances, hazardous properties of the substances involved, equipment data sheets, etc.) was collected as requested by Step 1 of the approach described in Section 5.1.3.

As the substance involved in the storage section considered in the case study is a flammable liquid, the Dow F&EI [182] was deemed suitable for the estimation of the inherent potential hazard of the storage tanks present in the layout and it was therefore used for the selection of the relevant hazardous equipment (EQs) as required by Step 2. For the sake of brevity, among all the tanks with the highest scores, tank TA01 (see **Figure 55**) was selected for further assessment. Its inherent hazard is due to the large inventory of flammable liquid stored that can potentially be released (24,000 m^3).

The security events (SEs) suggested by the TNO "Purple Book" [186] for atmospheric tanks were considered applicable for TA01 (Step 3):

- continuous release from a hole with an effective diameter of 10 mm (LI1);
- continuous release of the complete inventory in 10 min at a constant rate of release (LI2);
- instantaneous release of the complete inventory (LI3).

Once the SEs have been selected, the approach provides for the construction of an Attack Tree (AT) for each of them (Step 4), grouping all the attack modes that can generate such SEs. As the tank TA01 in the case study is an atmospheric storage installation, the AT shown in **Figure 47**, developed in the present study, is applicable to all the three SEs considered above. However, case-specific considerations shall be done in order to identify which AMs among those appearing in such AT are capable of generating the selected SEs at each position P1, P2, and P3 considered in the case study (see **Figure 55** and the following discussion of results from the application of Step 6).

Step 5 of the described approach provides for the creation of the event tree (ET) for each selected SE. As the ET for flammable liquids reported in **Figure 50-a** is applicable to all the three SEs considered for tank TA01, it can be adopted as direct output of Step 3 with some modifications due to the case-specific hazardous properties and storage conditions of the flammable liquid contained inside TA01 (see the following discussion of results from the application of Step 6).

Step 6 requires the creation of a Bow-Tie (BT) diagram for each selected SE, combining the already developed AT (Step 4) and ET (Step 5). However, the BT for the atmospheric storage of flammable liquids reported in **Figure 51** is applicable to all the three SEs considered for tank TA01, allowing to bypass steps 4 and 5. Thus, tailoring of AMs taking into account the three different positions P1, P2, and P3 reachable by the attackers (see **Figure 55**), and tailoring of physical damage scenarios are done in this step as explained in the description of the proposed approach (see Section 5.1.3.2).

In particular, the hazardous properties and storage conditions of the flammable liquid exclude the possibility of a large vapor cloud formation from evaporation of spilled pools. Thus, VCE (FS#02) and flash fire (FS#03) displayed in the BT in **Figure 51** are excluded. Outdoor uncontrolled combustion is not expected to create large clouds of acute toxic compounds, thus toxic cloud (FS#06) is also excluded.

A damage caused by deliberate interferences with or without the use of aids (RAI#01-A and RAI#01-B) is only possible from position P3 due to the fact that the attacker has to reach TA01 according to the succession criterion associated to this AM (see **Table 30**). While worst-case loss intensity (i.e., a LI2 release loss intensity, see **Table 30**) is supposed to be achieved in case of use of tools (e.g., disc grinder, cutting torch), only small diameter sample valves are present on TA01: thus in the latter case, only a LI1 release loss intensity is expected.

As discussed in sections 5.1.2.2 and 5.1.2.3, arson is able to damage atmospheric tanks only in case of an incendiary device involving large quantities of flammable material (e.g., 1000 L of gasoline contained inside an IBC tank as in RAI#02-B): thus RAI#02-A may reasonably be excluded. However, RAI#02-B in position P3 requires to move IBC tanks within the catch basin area, where they are not normally present, thus requiring special equipment (e.g., a crane) to move the gasoline load across the wall of the catch basin. The same RAI (RAI#02-B) from position P1 and position P2 is not expected to cause damage: pool fire modeling (see discussion on standoff distances in Section 5.1.2.3) reveals that for distances approximately higher than 5 m from the flames this RAI is not able to cause damage to atmospheric tanks. Therefore, the incendiary attack (AM#02) is excluded from the potential AMs able to cause damage to TA01 at any of the considered positions.

On the contrary, in case of attacks involving explosives (AM#03), damage is potentially possible from two of the three positions considered. In particular, the detonation of 50 kg of TATP (RAI#03-A) is deemed to cause

damage at a distance of less than about 57 m, while in case of detonation of 30 kg of TATP (RAI#03-B) at a distance less than 48 m (see discussion on standoff distances in Section 5.1.2.3). Therefore, no releases are expected to be started by a detonation of the reference amounts of TATP in position P1, while they are possible in positions P2 and P3. Unlike deliberate interferences with or without the use of aids (AM#01), a loss intensity LI3 is achievable by this AM from both the two positions.

Similar considerations apply to the detonation of a vehicle bomb (AM#04) from both the positions accessible to vehicles (P1 and P2 in **Figure 55**, since vehicle access to P3 is prevented by the presence of the catch basin), resulting a very critical attack pattern. In fact, in the case of detonation of 50000 kg of AN/dolomite (50/50) + diesel fuel inside a vehicle (RAI#04), the effects of the peak overpressure are able to cause damage at a distance of about 150 m (see Section 5.1.2.3), far farther than the distance between P1 and TA01 (60 m).

In case of shooting attacks (AM#05), a perforation is reasonably possible from each of the three positions considered. In fact, even the distance from P1 and TA01 (the largest of the three) is two orders of magnitude less than the calculated standoff distance (i.e., 1030 m, see Section 5.1.2.3). However, only a release loss intensity LI1 is expected in this case (the diameter of the hole is nearly the same as that of the bullet [229]).

Finally, the presence of the catch basin, makes the vehicle impact attacks (AM#06) not able to cause damage to the tank TA01.

The last step of the proposed approach (Step 7) provides for the identification of reference security scenarios among the ones identified through the developed BT diagram. In particular, the worst-case criterion was used to identify reference security scenarios for TA01. Given the specific properties of the substance stored inside tank TA01, the pool fire is the worst-case FS among the ones present in the ET part of the BT of **Figure 51**. In case of deliberate interferences with or without the use of aids (AM#01), the attacker has to ignite the spilled liquid from tank TA01 in order to generate a pool fire, while for attacks involving the use of explosives (AM#03 and AM#04) and the shooting attacks (AM#05), the ignition is possible according to the characteristics of the respective attack vectors (see **Table 30**).

Table 34 summarizes the results obtained in the case study in terms of reference security scenarios for each potential position that can be reached by the attackers (P1, P2, and P3 in **Figure 55**).

Table 34 Reference security scenarios suggested for the case study on tank TA01. The maximum release loss intensity (LI) achievable through each AM is reported. N/A: not applicable. Adapted from [220].

AM code	Attack Mode	RAI code	P1 (50m from TA01)	P2 (15m from TA01)	P3 (1m from TA01)
AM#01	Deliberate interference with or w/o aids	RAI#01-A	N/A	N/A	Pool fire (L1)
		RAI#01-B	N/A	N/A	Pool fire (L2)
AM#02	Arson using simple/incendiary means	RAI#02-A	N/A	N/A	N/A
		RAI#02-B	N/A	N/A	N/A
AM#03	Use of explosive	RAI#03-A	N/A	Pool fire (L3)	Pool fire (L3)
		RAI#03-B	N/A	Pool fire (L3)	Pool fire (L3)
AM#04	Use of vehicle bomb	RAI#04	Pool fire (LI3)	Pool fire (LI3)	N/A
AM#05	Shooting	RAI#05	Pool fire (LI1)	Pool fire (LI1)	Pool fire (LI1)
AM#06	Vehicle impact	RAI#06	N/A	N/A	N/A

5.1.4.3. Discussion of the results of the case study

The present study provides tools based on Bow-Tie formalism aimed at the identification of reference security scenarios (from attack scenarios to physical damage scenarios) that can be used in the context of SVA/SRA studies as baseline information for the further calculation of the security risk of chemical and process plants. The validation of the proposed set of Attack Modes (AMs), Attack Trees (ATs) for reference installations, and Bow-Tie (BT) diagrams for reference hazardous substances with past security-related incidents, allowed to prove that there is historical evidence of part of the events belonging to the chain of security scenarios proposed.

The step-by-step applicative use of the proposed AMs, ATs, and BTs (Section 5.1.4) to the atmospheric tank storing a low volatile flammable liquid considered in the case study (i.e., tank TA01 in **Figure 55**), proved the quality of the results that can be achieved in supporting SVA/SRA studies. In particular, the security scenarios identified in the case study (summarized in **Table 34**) are requested in the application of SVA/SRA methodologies suitable for the security assessment of chemical and process facilities such as the one developed by the CCPS (see flowchart in **Figure 54-b**). In fact, application of Step 2 “Facility characterization”, Step 3 “Threat assessment”, and Step 4 “Vulnerability analysis” of the CCPS SVA require the identification of the relevant hazardous equipment in the plant, the potential security events (LPIs and/or LOCs) that can occur in such equipment, the attack scenarios by which the SEs can be generated, and the physical damage scenarios that follow the SEs so that their consequences for humans, the assets, and the environment can be evaluated. All this information is provided by the reference security scenarios identified through the procedure described in Section 5.1.3 based on Bow-Tie formalism.

It is important to underline that, while the proposed AMs are applicable to any equipment unit, the use of the developed and validated ATs is limited to storage equipment units only, and that of BTs to the storage of flammable liquids (in atmospheric tanks or in storage warehouses), and of oxidizing solids with explosion hazards. However, the step-by-step procedure described in Section 5.1.3 for the identification of reference

security scenarios is applicable to any type of equipment unit and hazardous substance processed or stored, allowing to assess both the process and the storage sections of a plant. Future developments can therefore be aimed at providing ATs for process and transportation equipment units and of BTs for a broader set of hazardous substances.

The security scenarios listed in **Table 34** can also support the identification of security countermeasures (intended as elements of the physical protection system (PPS), i.e., the physical protection elements (PPE) with functions of delaying, deterring and/or detecting). For example, the potential severity of the physical damage scenarios associated to AM#03 (use of explosive devices) suggests enforcing adequate monitoring of suspicious truck traffic on the road outside the fence perimeter in order to increase the probability of attackers to be detected, e.g., by adding video surveillance (closed-circuit television, CCTV). It is important to underline that also the identification of security countermeasures is requested in the application of SVA/SRA methodologies (e.g., steps 4 and 5 of CCPS SVA).

The identified security scenarios (**Table 34**) may be compared to those considered in safety assessments in order to yield a more broad understanding of risk and to integrate in a single set the management of safety and security requirements [122].

The safety-related Bow-Tie diagram developed for the tank TA01 in the context of a Safety Report (**Figure 56**) reports physical damage scenarios that match those identified using the reference security-related BT of **Figure 51**. Therefore, emergency response and mitigation plans, both internal (evacuation plan) and external (population sheltering), developed for safety scenarios, may be adapted to address the security issues. Thus, the response to safety scenarios can be adapted to consider specific issues arising from security threats (e.g., possible presence of attackers on site may require specific checks and communications on available evacuation routes) and security-specific physical damage scenarios can be included in the plan (e.g., catastrophic rupture of TA01 is deemed very unlikely in the safety assessment). This provides the chance to develop integrated Safety Reports that consider both safety and security scenarios, in the framework of the integrated management of safety and security risks [58,122,230,231].

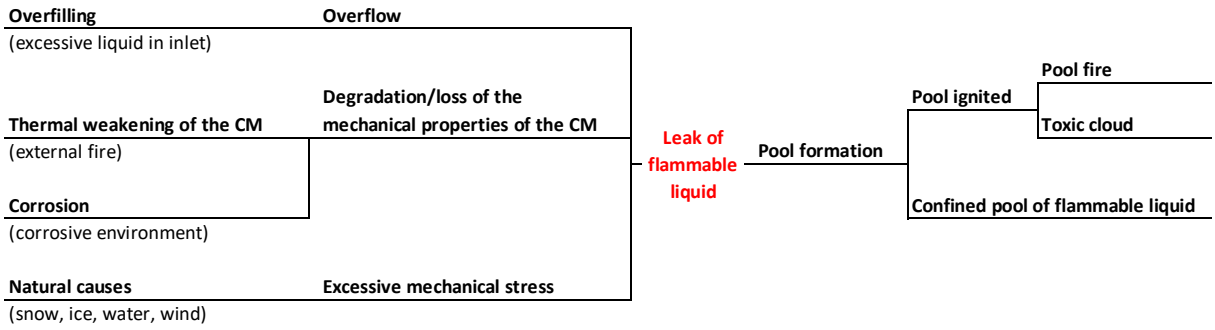

Figure 56 Safety-related Bow-Tie diagram developed considering a leak of flammable liquid from TA01 as critical event. CM: Construction material. Adapted from [220].

5.2. Evaluation of standoff distances for shooting attacks to atmospheric and pressurized storage tanks

This Section presents a study aimed at providing generic standoff distances for the shooting threat (i.e., minimum distance between the target asset and the location of the attacker that will not cause any significant damage to it) for atmospheric and pressurized storage equipment considering a set of standardized handgun and rifle projectiles (according to EN 1522 and EN 1063) that can be used to investigate the conditions for a successful attack and to support the design of passive protection barriers within the Physical Protection System (PPS) of a facility. Moreover, this study paves the way for the definition of quantitative approaches for the assessment of the shooting threat in facilities processing and/or storing hazardous materials. Therefore, the results obtained from this study help answer Research Question 2 and Research Question 3 (see Section 2.1 and **Figure 4**). An extended review and validation of projectile perforation models is also part of the study given their need in the calculations and the lack in the literature of specific damage models for projectile impact on equipment items storing relevant quantities of hazardous materials. The obtained standoff distances are used within the reference Bow-Tie diagrams developed in the context of study described in Section 5.1 of this Chapter.

5.2.1. Method

The method applied for the calculation of the standoff distances for shooting attacks to atmospheric and pressurized storage installations containing hazardous materials (e.g., flammable, toxic, and explosive materials) is summarized in the flowchart shown in **Figure 57**.

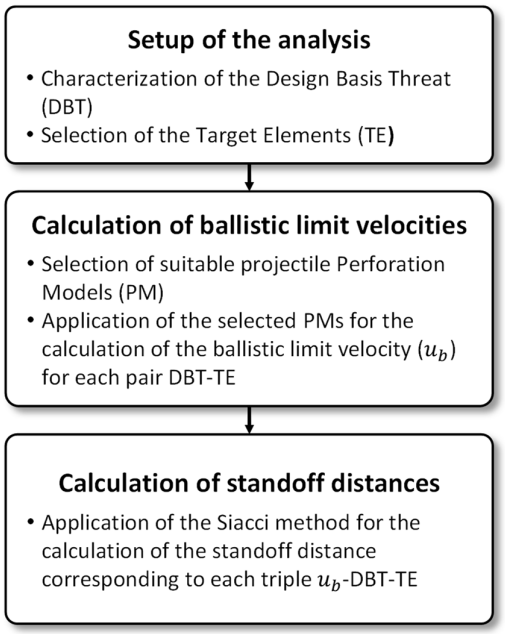

Figure 57 Flowchart of the method applied for the calculation of the standoff distances for atmospheric and pressurized storage installations.

In particular, in the first step of the method applied, the Design Basis Threat (DBT) and the Target Elements (TE) of the shooting attacks are defined (see **Figure 57** and **Figure 58**).

In the context of SVA/SRA, the DBT is intended as the characterization of the attacker in terms of its characteristics and capabilities [7,35,39]. In particular, given the aim of the present study, the DBT is here restricted to shooting attacks with small/light weapons (e.g., handguns and rifles). However, given the great variety of firearms and projectiles (shape, type, material) that may potentially be used by the shooter, this study proposes the use of a reference set of projectiles and weapons, derived from the classification present in EN 1522 [172] and EN 1063 [173] which are the most common standards used in Europe for ballistic protection.

According to the scope of the Bow-Tie approach presented in Section 5.1 to which the present study refers, steel-made atmospheric and pressurized storage vessels were considered as the Target Elements (TEs). In fact, these units have wide usage in refineries and chemical process industries to safely store hazardous materials [219] and are known to significantly contribute to the hazard profile of an installation [19]. Also in this case, a reference set of vessels was considered in the analysis: in particular, the design data of such vessels (i.e., volume, diameter, height/length, shell thickness) and the mechanical properties of the used steel materials, were based on standard API 650 [232] and Section VIII of ASME Boiler & Pressure Vessel Code [233].

The second step of the method applied in the present study (see **Figure 57**) is devoted to the calculation of the ballistic limit velocity (u_b) for each possible pair of reference projectile considered in the DBT and each TE. The ballistic limit velocity is defined as the minimum projectile velocity required to perforate a particular target (i.e., the selected TEs) at normal incidence [234]. Ballistic valocities were calculated by suitable projectile perforation models (PMs). Therefore, given the lack in literature of studies on damage models for projectiles [218], an extended review of available projectile perforation models (PMs) and their validation with data from experimental tests of shooting attacks was carried out.

First, the PMs were retrieved. The search was extended to academic articles, books, and technical reports available in scientific journals and on the web. A perforation model is intended as multi-parameter correlation allowing for the prediction of the perforation of a specific target element. It is important to stress that perforation models differ from penetration models: perforation provides for the creation of an opening from the attack face to the rear face of the target element, while penetration may not affect its entire thickness [173].

The retrieved perforation models were classified according to model type (empirical (E), analytical (A), numerical (N)), projectile shape (pointed conical or ogival projectiles (P), projectiles with a round nose (RN), flat nose projectiles (FN) also referred to as “blunt” projectiles, and spherical projectiles (S); see **Figure 59-a**), and projectile type (soft-core (SC, generally lead or mild steel, commonly referred to as “ball” rounds) and hard-core (HC, generally hardened steel or tungsten carbide, commonly referred to as “armour-piercing (AP) projectiles; see **Figure 59-b**).

Second, data from relevant perforation tests were retrieved. According to the standards EN 1063 [173] and EN 1523 [235], a perforation test consists in the shooting at a certain distance (named “test range”) of a target element (named “test piece”) characterized in terms of shape, size and material, with a specific projectile. Particular attention was paid to identify perforation tests on materials with mechanical properties similar to those typically used for industrial storage tanks.

Third, validation of the collected perforation models using the experimental data of perforation tests, was carried out. It shall be noted that, for most of the models, this provided for testing them beyond the data used for their original validation, allowing to confirm or even to extend the range of application. The validation was performed considering the ballistic limit velocity of the projectile: in particular, the ballistic limit velocity measured experimentally and those predicted by the perforation models were compared. Quantitative comparison was based on the following statistical performance measures:

- Mean Absolute Percentage Error (MAPE) defined as:

$$MAPE = \frac{1}{N}\sum_{i=1}^{N}\left|\frac{x_{exp,i} - x_{cal,i}}{x_{exp,i}}\right| \cdot 100 \quad (3)$$

- Mean Percentage Error (MPE) defined as:

$$MPE = \frac{1}{N}\sum_{i=1}^{N}\frac{x_{exp,i} - x_{cal,i}}{x_{exp,i}} \cdot 100 \quad (4)$$

- Root Mean Square Deviation (RMSD):

$$RMSD = \sqrt{\frac{\sum_{i=1}^{N}\left(x_{exp,i} - x_{cal,i}\right)^2}{N}} \quad (5)$$

where $x_{exp,i}$ is the experimental value, $x_{cal,i}$ is the calculated value, and N is the total number of values.

MAPE and MPE both compute the average of percentage errors by which predictions of a model differ from experimental data. However, MPE makes use of actual percentage errors, rather than the absolute percentage errors considered in MAPE, allowing positive and negative errors to compensate each other. Therefore, MAPE is a measure of the prediction accuracy of a model in relative terms, while MPE is a measure of the bias in the predictions (i.e., tendency in providing values systematically lower or higher than experiments).

RMSD computes the square root of the average of squared errors and thus it is a measure of the accuracy of a model in absolute error terms, as it is not scaled to experimental data as MAPE. RMSD is used to compare forecasting errors of different models for a particular set of experimental data, but it is not suitable for the comparison of model performance between different datasets, as the MAPE, since it is scale-dependent.

The closer the MAPE, MPE, and RMSD are to zero, the better the perforation model predicts perforation experimental data. Overall, the assessment of the selected statistical parameters allows the identification of the most suitable perforation models for each of the validation datasets, concerning different classes of projectile shape and type.

Fourth, the selected most suitable PMs were used to calculate the ballistic limit velocity for the TEs selected in the present study (atmospheric and pressurized storage tanks). It is pragmatically assumed that successful perforation occurs when the projectile penetrates the target until the remaining non-penetrated thickness is equal or lower than the minimum thickness required to sustain the mechanical stress by design (t_d). In other words, perforation is considered to occur if t_{max} calculated as for the applicable PM exceeds the "effective thickness" (t_{eff}) defined as:

$$t_{eff} = t - t_d \quad (6)$$

where t is the actual shell thickness and t_d is the shell design thickness value required to withstand the design internal pressure or hydrostatic load.

The assumption above is justified by the current lack of data and models for the analysis of penetration of loaded plates. Advancements in this field can be achieved by further advanced numerical studies of penetration (e.g., Scazzosi et al. [236] and Holmen et al. [237]), or by carrying out specific experimental tests. From the practical point of view, the assumption is expected to yield safe-side results (i.e., overestimation of the thickness that can be perforated by a projectile) as it practically assumes not-existent the portion of shell thickness corresponding to t_d.

The shell design thickness (t_d) for the pressurized cylindrical vessels is calculated applying the Von Mises criterion considering a planar stress state [238], while for atmospheric cylindrical storage vessels, it is calculated considering the hydrostatic load according to the method reported in standard API 650 [232].

In last step of the method applied in the present study (see **Figure 57**), the standoff distances for the selected TEs and projectiles considered in the DBT, were calculated. The calculation required the modelling of the projectile trajectory in order to evaluate the decay of the horizontal component of the projectile velocity as a function of the downrange distance (i.e., the horizontal distance travelled by the projectile from the muzzle of the weapon to the target). The standoff distance for shooting attacks corresponds to the downrange distance associated with a horizontal component of the impact velocity of the projectile that equals the ballistic limit velocity calculated in the previous step (see the graphical representation in **Figure 58**).

The evaluation of the downrange distances, and thus of the standoff distances, require the solution of differential equations describing the projectile trajectory, which are commonly solved with approaches based on simplified assumptions (e.g., constant atmospheric density, departure angle less than about 15°) [239]. In particular, in the current study, the *Siacci* method [239] was adopted.

Generic and conservative (safe-side) standoff distances were then identified for atmospheric and for pressurized targets for each reference projectile by considering the highest standoff distance from those calculated. These values are proposed as generic standoff distances to be used in the context of a SVA or SRA. Clearly enough the procedure described above can be used, as well, for the definition of case-specific standoff distances if data for a specific TE is used in the application.

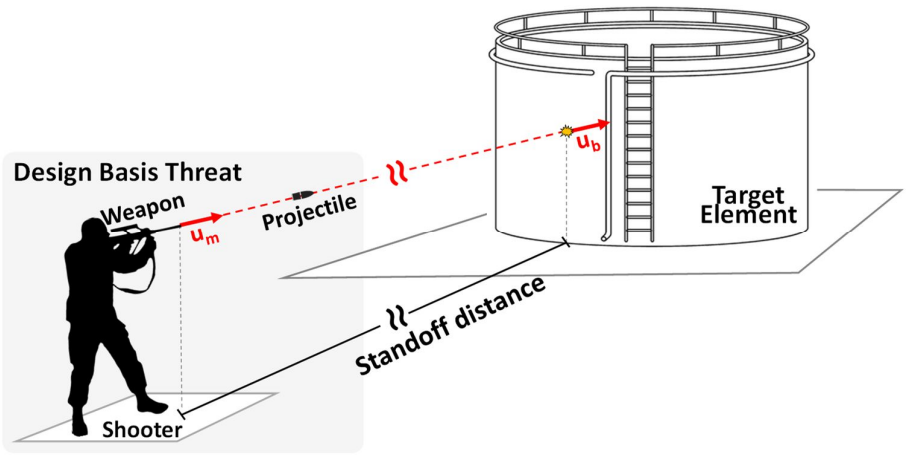

Figure 58 Schematization of the shooting attack: Design Basis Threat (DBT), Target Element (TE), and standoff distance. u_m: muzzle velocity; u_b: ballistic limit velocity.

5.2.2. Setup of the analysis

5.2.2.1. The Design Basis Threat

The characterization of the Design Basis Threat (DBT) consists in the definition of the characteristics and capabilities of the attacker. In the present study, this means selecting a set of projectiles which are fired by a shooter (see **Figure 58**). Characteristics of the shooter such as skills and motivations are not considered in the current study, assuming a highly skilled and well-motivated attacker (worst-case scenario).

Classification of projectiles based on shape and type is shown in **Figure 59** (panel-a and panel-b respectively).

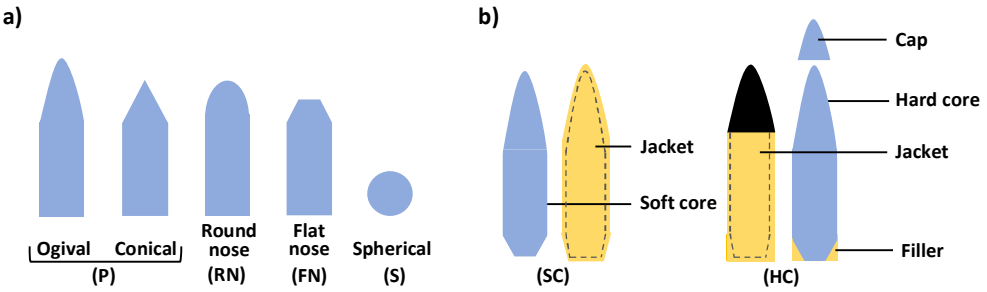

Figure 59 Classification considered in the current study for projectiles, based on (a) shape and (b) type. Adapted from [218].

The set of projectiles considered in the DBT was retrieved from the standards EN 1522 [172] and EN 1063 [173] which define the requirements and classification that windows, doors, shutters and, blinds must satisfy when tested according to EN 1523 [235] against bullets fired by hand guns, rifles, and shotguns. Both EN 1522 and EN 1063 classify target resistance to perforation according to protection classes (FB codes) which are in turn associated to different projectile families for performance testing. Seven different protection classes are identified in the standards: from FB1 (the lowest) to FB7 (the highest). Test conditions in the shooting tests through which protection classes are assigned, are specified in terms of the test range (i.e., the distance between the muzzle of the firearm and the attack face of the test specimen), type, shape, calibre, mass, and muzzle velocity (i.e., the velocity of a projectile as it exits the muzzle of a firearm, indicated as u_m in **Figure 58**) of the projectiles.

Five reference projectiles were selected in the DBT, whose relevant information is summarized in **Table 35**. The code name used in the table (FB code) refers to the original specification in EN 1522 and EN 1063. It shall be noted that in case of FB7 projectiles, data in **Table 35** refer to the core diameter and mass, as jacket and lead cap have minor influence on penetration by armour piercing projectiles as demonstrated by the studies of Børvik et al. [240], Chen et al. [241], and Hazell [217].

The five reference projectiles selected allowed to cover a wide set of projectiles with different performances as FB2 and FB4 are handgun projectiles while FB5, FB6 and FB7 are rifle projectiles.

Table 35 Selected reference projectiles from [172,173]. RN=Round nose, SC=Soft-core (lead), FN=Flat nose, P=Pointed, SCP1=Soft-core (lead) with steel penetrator, HC=Steel hard-core (steel, hardness more than 63 HRC). *FB7 data reported refer to the hard-core of the projectile.

Protection Class	Type of weapon	Reference projectile	Projectile type	d (mm)	m (g)	u_m(m/s)
FB2	Handgun	9 mm Luger	RN/SC	9	8	400
FB4	Handgun	44 Rem. Mag.	FN/SC	11	15.6	440
FB5	Rifle	5.56x45	PB/SC	5.56	4	950
FB6	Rifle	7.62x51	P/SC	7.62	9.5	830
FB7	Rifle	7.62x51	FP/HC	6.06*	3.7*	820

d: projectile diameter; m: projectile mass; u_m: muzzle velocity.

5.2.2.2. The Target Elements

HAZMAT steel-made atmospheric and pressurized storage vessels were chosen as the Target Elements (TEs) in the present study.

In particular, a study from Cozzani et al. [209] provided the specific sets of equipment used as reference TEs in the current study: **Table 36** reports the set of atmospheric cylindrical storage vessels (a-codes), while **Table**

37 provides the set of pressurized cylindrical storage vessels (p-codes). Both the tables also report the main design parameters for each equipment item such as design pressure, volume, diameter, and shell thickness. The latter parameter, which plays a key role in the context of material perforation, shows large variability within the practical applications as it depends on design (e.g., design pressure, use of variable thickness with height) and operative requirements (e.g., corrosion allowance). High diameter atmospheric vessels (e.g., codes from a.5 to a.10 in **Table 36**) are characterized by a decreasing shell thickness with height (e.g., different hydrostatic load). The thicknesses reported in the original source for the lower section of the shell are considered. The effective thickness (t_{eff}) calculated for each vessel is also reported in the two tables below.

Table 36 Set of atmospheric cylindrical storage vessels selected in the present study. Adapted from [209].

ID	V (m^3)	D (mm)	t (mm)	t_d (mm)	t_{eff} (mm)
a.1	25	2700	5	0.3	4.7
a.2	100	4400	5	0.7	4.3
a.3	250	6700	5	1.2	3.8
a.4	750	10500	7	2.3	4.7
a.5	1000	15000	9	2.1	6.9
a.6	2500	16000	13	4.9	8.1
a.7	5200	25000	19	6.5	12.5
a.8	10000	30000	20.5	10.4	10.1
a.9	13390	34130	20	12.1	7.9
a.10	17480	39000	23	13.8	9.2

Table 37 Set of pressurized cylindrical storage vessels selected in the present study. Adapted from [209].

ID	P_d (MPa)	V (m^3)	D (mm)	t (mm)	t_d (mm)	t_{eff} (mm)
p.1	1.5	5	1000	11	3.2	7.8
p.2	1.5	10	1200	11	3.8	7.2
p.3	1.5	20	1500	12	4.8	7.2
p.4	1.5	25	1700	15	5.4	9.6
p.5	1.5	50	2100	17	6.7	10.3
p.6	1.5	100	2800	18	8.9	9.1
p.7	1.5	250	3800	24	12.0	12.0
p.8	2	5	1000	14	4.2	9.8
p.9	2	10	1200	14	5.1	8.9
p.10	2	20	1500	16	6.3	9.7
p.11	2	25	1700	20	7.2	12.8
p.12	2	50	2100	23	8.9	14.1
p.13	2	100	2800	24	11.8	12.2
p.14	2	250	3800	32	16.1	15.9
p.15	2.5	5	1000	17	5.3	11.7
p.16	2.5	10	1200	17	6.3	10.7
p.17	2.5	20	1500	20	7.9	12.1
p.18	2.5	25	1700	24	9.0	15.0
p.19	2.5	50	2100	29	11.1	17.9
p.20	2.5	100	2800	30	14.8	15.2
p.21	2.5	250	3800	40	20.1	19.9

As regards the properties of the construction material of the target elements selected, the steel with the lowest strength (coded as A 285M-C steel) from the list present in standard API 650 [232] and Section VIII of ASME Boiler & Pressure Vessel Code [233] was considered for both atmospheric and pressurized storage vessels. This choice yields safe-side results (overestimation of ballistic limit velocity compared to other steel materials). The mechanical properties were retrieved from standard API 650 [232], the hardness was evaluated using the correlation reported in Callister and Rethwisch [242], while other parameters that will be required in the application of the selected projectile perforation models (particularly G, τ and K, see Section 2.4) were taken from Zukas [243]. All this information is here summarized: ρ_t=7850 kg/m^3, E=200 GPa, σ_T=205 MPa, σ_R=380 MPa, BHN_t=110, G=80 GPa, τ_s=220 MPa, K=158 GPa, ν=0.3.

5.2.3. Calculation of ballistic limit velocities

5.2.3.1. The projectile perforation models

The analysis of the literature allowed the collection of 17 perforation models (PMs in the following) relevant in the context of the current study. The relevant information of each PM (i.e., model name, reference, model type, applicable projectile shape, applicable projectile type, applicable target material, model parameters and their applicability range) is summarized in **Table 38**, while the complete set of model equations is provided in Table S.1 in the Supplementary Material of Iaiani et al [218].

A PM may be generalized as follows:

$$u_b = f(d, m, t, \rho_p, \rho_t, \sigma_T, Y, BHN_p, BHN_t, E, f, \tau_S, K, G, \alpha, \nu, C_n, C_v) \quad (7)$$

Where, u_b is the ballistic limit velocity, and the model parameters are: projectile diameter (d), projectile mass (m), projectile density (ρ_p), target density (ρ_t), projectile hardness (BHN_p), target hardness (BHN_t), target yield stress (σ_T), target Young's modulus (E), target bulk modulus (K), target shear modulus (G), friction coefficient (f) between the target and the projectile, Poisson ratio (υ), half-angle of conical nose of the projectile (α), target dynamic yield stress (Y), target static shear strength (τ_S), target thickness (t), and projectile model-specific parameters (C_n, C_v).

The ballistic limit velocity u_b is the minimum required projectile striking velocity needed to perforate (i.e., complete penetration) a particular target element of thickness t at normal incidence [217]. In the current study it is assumed that all output velocities provided by the PMs are ballistic limit velocities. Actually, some of the considered PMs were originally developed to calculate other velocity outputs such as u_{50} (P#01, P#03, P#04, P#06, P#07), defined as the striking velocity required for a particular projectile to perforate a particular piece of material in 50% of the tests [244], and u_0 (P#08, P#12, P#16), also called "protection velocity", defined as the highest striking velocity for which the probability of perforation is zero [245]. These velocities are based on a stochastic concepts as they refer to the statistical outcomes of experimental tests using criteria such as the "six round ballistic limit" [244], whereas the ballistic limit velocity is a deterministic, theoretical concept. Nevertheless, assimilating u_{50} and u_0 to u_b is expected to introduce a limited error for the purposes of the current study, as the dispersion between striking velocities for which penetration or perforation occurs in experimental tests on steels used for industrial storage tanks is typically in the order of few tens of m/s, which is at least one order of magnitude lower than corresponding ballistic limit velocities (between 400 m/s and 900 m/s) [236,240].

Table 38 shows that most of the PMs (11 out of 17) are empirical models, obtained by best fitting of experimental data of perforation tests, while others five PMs are analytical models, obtained solving the equation of motion under specific assumptions (e.g., target of finite thickness) and specific initial conditions (e.g., initial position and velocity of the projectile). A perforation model (P#11 in **Table 38**) was based on data coming from a broad set of numerical simulations [215]. Generally, empirical PMs consider only a limited number of input parameters (such as d, m, and t) and are specified for a limited applicability range (see **Table 38**). On the other hand, analytical PMs require more input parameters, which imply a more extensive characterization of the projectile and target material for their application. The classification and applicability of the PMs take also into account the shape and type of projectiles, as well as the specific material of the target element (see **Table 38**).

As discussed above, the shape of projectiles considered by the PMs was classified according to **Figure 59-a**, while the types of projectiles according to **Figure 59-b** [173]. It is worth mentioning that model P#08 has been originally developed for steel fragments impacting on metallic materials rather than actual bullets [217,245,246]. However, the experimental data used for model development and validation were actually obtained from fragments in the shape of short cylinders and cube-on-cylinders made of compact steel SAE 1020 (BHN about 131, typical of mild steel). The application of the model was thus considered suitable in the context of the current study and its performance in predicting perforation was investigated for both flat nose SC projectiles (BHN typically lower than 131) and flat nose HC projectiles (BHN typically higher than 131).

With respect to the material of the target element, not all the PMs provide parameters that take material properties into account. Moreover, some PMs only consider targets of specific steel materials (e.g., P#08 discussed above). As mentioned earlier, analytical PMs are typically able to take into account more extensively the parameters describing the mechanical properties of the material of the target element (e.g., P#10 in **Table 38** counts for the Young's modulus (E) and the yield stress (σ_T) of the material).

Table 38 Summary of the perforation models (PMs) considered in the current study. Model type codes: E=Empirical, A=Analytical, N=From numerical simulations. Projectile shape codes: P=Pointed, RN=Round nose, FN=Flat nose, S=Spherical. Projectile type codes: SC=Soft-core, HC=Hard-core. N.D.: Not defined. Adapted from [218].

Code	Model Name	Reference	Model Type	Projectile shape	Projectile type	Target Material	Model parameters	Applicability range
P#01	BRL	[247]	E	N.D.	N.D.	Steel	d, m, u, t	N.D.
P#02	Stronge	[248,249]	E	S/FN	N.D.	Steel	d, m, u, t	6.35<d<12.7 mm 1.04<m<8.32 g 1.23<t<3 mm
P#03	De Marre	[250,251]	E	N.D.	N.D.	Steel	d, m, u, t	7<t<30 mm
P#04	BRL	[252]	E	Any	Any	Steel	d, m, u, t	N.D.
P#05	Lees'	[19]	E	FN	SC	Steel	m, u, t	u<1000 m/s m<1 kg
P#06	Baker	[253,254]	E	Any	SC	Metallic	$d, u, t, \rho_p, \rho_t, \sigma_T$	t/d < 1.1
P#07	Modified De Marre	[217,252]	E	FN	SC	Steel	m, u, t	u<600 m/s BHN_p=200/300
P#08	THOR	[217,245,246]	E	FN (tests with cylinders and cube-on-cylinders)	N.D.	Steel	m, u, t	0.8<t<25.4 mm 0.3<m<53 g 183<u<3658 m/s ϑ< 70° BHN_t=≈150 BHN_p=≈134
P#09	Yarin	[112,255]	A	RN (can be extended to P)	HC	Metallic	$m, u, t, r, \rho_t, Y, G_t$	N.D.
P#10	Recht	[112,217,243]	A	P	HC	Metallic	$d, m, u, t, E, \sigma_T, f, \rho_t, \tau_s, K, \alpha$	1<CRH<8
P#11	Rosenberg	[215]	N	P	HC	Metallic	d, m, u, t, Y, ρ_p	t/d<5
P#12	UFC	[115]	E	Any (from the reference)	Any (from the reference)	Steel	d, m, u, t, BHN_t	d<12 mm
P#13	Cavity expansion theory	[223,246,256]	A	Any	HC	Metallic	d, m, u, t, σ_T	N.D.
P#14	Woodward	[223,246,257]	A	FN/P	HC	Metallic	d, m, u, t, Y	N.D.
P#15	Forrestal	[258]	A	P	HC	Metallic	d, m, u, t, E, Y	N.D.

P#16	Healey and Weissman/ConWep	[246,259–261]	E	RN	SC	Steel	m, u, t, BHN_t	N.D.
P#17	Recht	[243]	E	FN/P	SC/HC	Steel	d, m, u, t, L, ρ_t	BHN_t=300

d: projectile diameter; m: projectile mass; t: perforation thickness; u: ballistic limit velocity; ρ_p: projectile density; ρ_t: target density; σ_T: yield stress; τ_S: static shear strength; Y: dynamic yield stress; BHN_p: projectile Brinell's hardness number; BHN_t: target Brinell's hardness number; E: Young's modulus; f: friction coefficient; υ: Poisson ratio; K: bulk modulus; G_t: target shear modulus; ϑ: angle of obliquity; CRH: caliber radius head.

5.2.3.2. Experimental data of perforation tests

A perforation test consists in the shooting, from a fixed distance (named "test range"), of a target element (named "test piece") characterized in terms of shape, size and material, with a specific projectile [173,235]. The open literature, specific publications and the web were screened to retrieve experimental data from perforation tests. Given the scope of the current study (atmospheric and pressurized storage tanks as target elements), only tests on steel-made targets were considered.

The experimental data retrieved and considered in the current study are reported in **Table 39**. The collected dataset contains a total of 34 experimental perforation tests, all characterized in terms of shape and type of the projectile used, type of target material (e.g., mechanical properties such as the Young's modulus (E), the Brinell's hardness (BHN_t), and the yield stress (σ_T)), and size and shape of the target element. It is worth mentioning that E#34 was actually retrieved from the results of numerical models based on FE (Finite Element) and SPH (Smoothed Particle Hydrodynamics). However, since the models were calibrated using experimental results concerning the high-velocity impact of soft-core (lead core) projectiles on monolithic steel plates [236] not reported in the literature, the model results were considered as a proxy of the experimental data used for the model validation and were considered to extend the dataset for SC projectiles.

The majority of the experimental test set-ups applied standardized test procedures (e.g., see [173,235,262]). These tests adopt firearms capable of shooting the projectile at the specified velocity range against a standardized target element. The target element, usually a standardized steel plate according to [235,263], is secured on a support with the impact side perpendicular to the line-of-flight of the projectile. A given number of shoots are fired at specified test conditions (e.g., humidity, temperature, distance, etc.) and the impact velocities are measured with specific devices. Finally the ballistic limit velocity is calculated as the arithmetic mean of an equal number of the highest partial and the lowest perforation impact velocities [262]. In some of the older datasets concerning experimental perforation tests (E#16, E#17, E#18 in **Table 39**), the test procedure slightly differed from the standard: e.g., Woodward [223] obtained values of perforation velocity adjusting the charge weight incrementally until the target element was perforated. The experimental velocities of these tests were however considered as ballistic limit velocities for the validation of the perforation models, as they refer to a damage on the target element similar to that considered in the standardized tests.

In all the tests, the effects of the penetration on the target plate were only local, extending no more than three projectile diameters from the impact point. No reinforcement or support on the plate was present within 30 times the projectile diameter. The steels of the target elements considered in the experimental tests reported in **Table 39** present a range of mechanical properties wider than the steels commonly used as construction material for atmospheric storage tanks as reported in standard API 650 [232] (e.g., steels of E#01-14, E#20-25, and E#34 have higher strength than steels listed in API 650 (range of 205-415 MPa), steels of E#17-18 are similar to lower strength steels reported in it, while steels of E#15-16, E#19, and E#26-33 to higher strength steels listed). Nevertheless, also higher strength steels were included in order to provide a broader validation range for PMs. The thickness range used for the validation is comprised between 4.7 mm and 12 mm, thus including the range of shell thicknesses adopted for the majority of atmospheric storage tanks (see section 5.1), while only a single test reported data for higher thicknesses (20 mm in E#16).

Considering a range of validation wider than that of the applicability is a practice used by other authors. For example, Schonberg and Ryan [116] validated the nine perforation models retrieved for target materials, thicknesses, projectile responses, and impact conditions which did not always match to valid/validated conditions of the original models. Thus, the results of the evaluation should not be taken as an indictment on the quality of the original models. Rather, the results should act as a guide to facilitate the selection of a

model(s) that can be used to predict the perforation of steel targets against different projectiles across a wide range of velocities.

Clearly, the availability of experimental data of ballistic tests on actual storage tanks (or at least on target plates obtained with the same materials and thicknesses in the range of those used for the shell of atmospheric storage tanks) would provide more accurate results in the final identification of optimal perforation models and inherent safety thickness thresholds. Moreover, following the approach adopted by Schonberg and Ryan [117], the availability of such experimental data can pave the way to future developments aimed at improving the selected perforation models (e.g., by introducing empirical adjustments) not with the goal of derive a new, analytically-based perforation model, but to present simple modifications to the existing models to facilitate their broad application across the breadth of impact conditions contained within the dataset of experimental data for use in rapid, first-order performance evaluations in terms of perforation prediction of industrial atmospheric storage tanks.

Nevertheless, in the absence of experimental data of ballistic tests on actual storage tanks, the present study is based on a set of representative experimental data, most of which refer to projectiles that can commonly be fired in the context of a shooting attack to atmospheric and pressurized storage tanks and to materials with similar characteristics to those used in the construction of the tanks.

Table 39 Experimental data from perforation tests (t: perforated target thickness; u_{exp}: experimental ballistic limit velocity; P: Pointed; FN: Flat nose; SC: Soft-core; HC: Hard-core). For hard-core projectiles, only the hard-core of the projectile was considered. Adapted from [218].

Code	Source	Projectile	Parameters of projectile	Target	Parameters of target	t (mm)	u_{exp} (m/s)
E#01	[240]	P/SC: Ball 7.62	d=7.8 mm m=9.5 g	Steel: Weldox 500E	E=210 GPa σ_T=605 MPa BHN_t=200 ρ_t=7850 kg/m^3	6	596.0
E#02	[240]	P/SC: Ball 7.62	d=7.8 mm m=9.5 g	Steel: Weldox 700E	E=210 GPa σ_T=819 MPa BHN_t=250 ρ_t=7850 kg/m^3	6	666.0
E#03	[240]	P/SC: Ball 7.62	d=7.8 mm m=9.5 g	Armour steel: Hardox 400	E=210 GPa σ_T= 1148 MPa BHN_t=400 ρ_t=7850 kg/m^3	6	762.0
E#04	[240]	P/SC: Ball 7.62	d=7.8 mm m=9.5 g	Armour steel: Domex 500	E=210 GPa σ_T=1592 MPa BHN_t=500 ρ_t=7850 kg/m^3	6	886.0
E#05	[240]	P/SC: Ball 7.62	d=7.8 mm m=9.5 g	Armour steel: Armox 560T	E=210 GPa σ_T= 1711 MPa BHN_t=520 ρ_t=7850 kg/m^3	6	918.0
E#06	[240]	P/HC: 7.62 mm APM2	d =6.1 mm m =5 g	Steel: Weldox 500E	E =210 GPa σ_T= 605 MPa BHN_t=200 ρ_t=7850 kg/m^3	12	624.0
E#07	[240]	P/HC: 7.62 mm APM2	d =6.1 mm m =5 g	Steel: Weldox 700E	E =210 GPa σ_T= 819 MPa BHN_t=250 ρ_t=7850 kg/m^3	12	675.0
E#08	[240]	P/HC: 7.62 mm APM2	d =6.1 mm m =5 g	Armour steel: Hardox 400	E=210 GPa σ_T= 1148 MPa	12	741.0

					BHN_t=400 ρ_t=7850 kg/m^3		
E#09	[240]	P/HC: 7.62 mm APM2	d =6.1 mm m =5 g	Armour steel: Domex 500	E=210 GPa σ_T=1592 MPa BHN_t=500 ρ_t=7850 kg/m^3	12	837.0
E#10	[240]	P/HC: 7.62 mm APM2	d =6.1 mm m =5 g	Armour steel: Armox 560T	E=210 GPa σ_T= 1711 MPa BHN_t=520 ρ_t=7850 kg/m^3	12	871.0
E#11	[264]	FN/HC	d =20 mm m =197 g	Steel: Weldox 460 E	E =210 GPa σ_T= 490 MPa BHN_t=170 ρ_t=7850 kg/m^3	6	145.5
E#12	[264]	FN/HC	d =20 mm m =197 g	Steel: Weldox 460 E	E =210 GPa σ_T= 490 MPa BHN_t=170 ρ_t=7850 kg/m^3	8	154.3
E#13	[264]	FN/HC	d =20 mm m =197 g	Steel: Weldox 460 E	E =210 GPa σ_T= 490 MPa BHN_t=170 ρ_t=7850 kg/m^3	10	165.3
E#14	[264]	FN/HC	d =20 mm m =197 g	Steel: Weldox 460 E	E =210 GPa σ_T= 490 MPa BHN_t=170 ρ_t=7850 kg/m^3	12	184.0
E#15	[265]	P/HC: 7.62 mm APM2	d =6.1 mm m =5 g	Steel: Weldox NVE36	E =210 GPa σ_T= 355 MPa BHN_t=190 ρ_t=7850 kg/m^3	12	592.0
E#16	[112]	P/HC: 7.62x5mm M61 AP	d =6 mm m =3.7 g	Steel: Grade 350 MPa	E =200 GPa σ_T= 355 MPa BHN_t=152 ρ_t=7850 kg/m^3	20	775.1

E#17	[223]	P/HC	d =4.76 mm m =2.83 g	Mild steel	E =210 GPa σ_T= 250 MPa BHN_t=135 ρ_t=7850 kg/m^3	4.7	375.0
E#18	[223]	P/HC	d =6.35 mm m =3.03 g	Mild steel	E =210 GPa σ_T= 250 MPa BHN_t=135 ρ_t=7850 kg/m^3	4.7	442.0
E#19	[266]	P/HC: 7.62 mm APM2	d =6.1 mm m =5 g	Steel: Weldox NVE36	E =210 GPa σ_T= 355 MPa BHN_t=190 ρ_t=7850 kg/m^3	12	579.0
E#20	[267]	P/H**C**	d =20 mm m =197 g	Steel: Weldox 460 E	E =210 GPa σ_T= 499 MPa BHN_t=170 ρ_t=7850 kg/m^3	12	295.9
E#21	[267]	P/H**C**	d =20 mm m =197 g	Steel: Weldox 700 E	E =210 GPa σ_T= 859 MPa BHN_t=250 ρ_t=7850 kg/m^3	12	318.1
E#22	[267]	P/H**C**	d =20 mm m =197 g	Steel: Weldox 900 E	E =210 GPa σ_T= 992 MPa BHN_t=300 ρ_t=7850 kg/m^3	12	322.2
E#23	[267]	P/HC	d=20 mm m =197 g	Steel: Weldox 460 E	E =210 GPa σ_T= 499 MPa BHN_t=170 ρ_t=7850 kg/m^3	12	290.6
E#24	[267]	P/HC	d=20 mm m =197 g	Steel: Weldox 700 E	E =210 GPa σ_T= 859 MPa BHN_t=250 ρ_t=7850 kg/m^3	12	335.0
E#25	[267]	P/HC	d=20 mm m =197 g	Steel: Weldox 900 E	E =210 GPa σ_T= 992 MPa	12	340.0

					BHN_t=300 ρ_t=7850 kg/m^3		
E#26	[268]	P/HC: 7.62 x 39mm	d =7.62 mm m =8 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	5	547.8
E#27	[268]	P/HC: 7.62 x 39mm	d =5.59 mm m =3.56 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	6	585.3
E#28	[268]	P/HC: 7.62 x 39mm	d =5.59 mm m =3.56 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	6	588.6
E#29	[268]	P/HC: 7.62 x 39mm	d =5.59 mm m =3.56 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	7	653.1
E#30	[268]	P/HC: 7.62 x 39mm	d =5.59 mm m =3.56 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	7	678.2
E#31	[268]	P/HC: 7.62 x 39mm	d =5.59 mm m =3.56 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	7	660.8
E#32	[268]	P/HC: 7.62 x 39mm	d =5.59 mm m =3.56 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	8	727.4
E#33	[268]	P/HC: 7.62 x 39mm	d =5.59 mm m =3.56 g	Steel: AH 36	E =206 GPa σ_T= 350 MPa BHN_t=160 ρ_t=7850 kg/m^3	8	719.4

E#34	[236]	P/SC: .308 Winchester	d = 7.81 mm m = 9.6 g	Armour steel: Ramor 500	E = 201.38 GPa σ_T= 1450 MPa BHN_t=570 ρ_t=7850 kg/m^3	6.74 mm	1030.0

d: projectile diameter; m: projectile mass; t: perforation thickness; u: ballistic limit velocity; ρ_t: target density; σ_T: yield stress; BHN_t: target Brinell's hardness number; E: Young's modulus.

5.2.3.3. Validation of the perforation models

Validation of the PMs reported in **Table 38** was performed based on the ballistic limit velocity (u_b) of the projectile using the experimental data from perforation tests listed in **Table 39**. The ballistic limit velocity measured experimentally in the perforation tests and that calculated by the PMs are compared in the parity plots shown in **Figure 60**, **Figure 61**, and **Figure 62**. **Table 40** reports the values calculated for the statistical parameters adopted to assess model performance.

Since the PMs are usually applicable only to specific types of projectiles, separate parity plots were obtained, organizing the results from perforation tests in three groups: i) soft-core projectiles (SC) (**Figure 60**); ii) pointed hard-core projectiles (P/HC) (**Figure 61**); and iii) flat nose hard-core projectiles (FN/HC) (**Figure 62**). The experimental perforation tests considered for each group of projectiles are listed in **Table 40**.

All the parity plots report the experimental ballistic limit velocity on the vertical axis (y-axis) and the ballistic limit velocity calculated by PMs on the horizontal axis (x-axis). Dotted lines show the percentage error ($\pm\ 10\%, 20\%, 30\%$). In case the points are above the bisector, the PM provides an underprediction of u_b (which is considered conservative, or safe-side from the point of view of the protection of the target element as the calculated ballistic limit velocity is lower than the experimental one).

Eleven (11) PMs were deemed applicable to the group of soft-core (SC) projectiles (P#01, P#02, P#03, P#04, P#05, P#06, P#07, P#08, P#12, P#16, P#17). Available experimental perforation data for this group are limited to pointed (P) projectiles (E#01-05 and E#34 in **Table 39**). However, also PMs originally developed for SC projectiles but with a flat nose (FN) or round nose (RN) rather than conical or ogival (P) such as P#02, P#05, P#07, P#08, and P#16 (see **Table 38**) have been applied on the available experimental data in order to investigate their performance also for P/SC projectiles.

Moreover, it is important to remark that all the PMs listed above were tested on the totality of experimental data of SC projectiles even if some of them would be applicable only to a subset of data according to the PM applicability range (see **Table 38**, e.g., P#08 and P#17 were originally developed on experimental tests using steel target elements with Brinell's hardness of 150 and 300 respectively, but they were tested on the range of BHN of 200-570).

Figure 60 shows the parity plot for soft-core (SC) projectiles. The specific PMs tested and the experimental perforation data used for their validation are reported in **Table 40**. The error shown by perforation model P#06 (light blue crosses) is the more limited, being always under the 10%-error dotted line. However, all the points are under the bisector, meaning that this PM provides for non-conservative estimations of the ballistic limit velocity from the point of view of target protection from perforation. For this reason, in the context of the current study, model P#06 can be excluded a priori from the list of most suitable PMs for SC projectiles. This behaviour of model P#06, is spite of an application within the declared applicability range (target: metallic; projectile: SC; $t/d < 1.1$), is possibly due to the empirical nature of the PM and the initial goal to provide an estimation of u_{50} rather than a safe side prediction of protection velocity. Among the other PMs, models P#07 (dark green triangles) and P#08 (black dots) seem to better predict the ballistic limit velocity, especially at velocities lower than 800 m/s (all results except one fall below the 20%-error dotted line). The behaviour of these two PMs is also conservative, since the results are all above the bisector, with the exception of a single results for P#07, which is however very close to it. Hence, both the PMs are identified as the more suitable candidates for the prediction of ballistic limit velocity in case of soft-core projectiles. On the other hand, perforation models P#01 (light blue dots), P#02 (red dots), P#03 (violet triangles), P#04 (black crosses), and P#16 (pink diamonds) seem to be overconservative in predicting perforation, with ballistic limit velocities that are more than 30% smaller than those in experimental tests. This is possibly due to the fact that the perforation models P#01, P#02, P#03, and P#04 were not specifically developed for SC projectiles, and P#16 is applicable to round nose (RN) projectiles rather than pointed (P) projectiles as the ones shot in

the experimental data retrieved from literature. Moreover, for both the models P#02 and P#03, validation is beyond the originally specified range of target thicknesses (t is greater than 3 mm and lower than 7 mm) in all the experimental data used for validation.

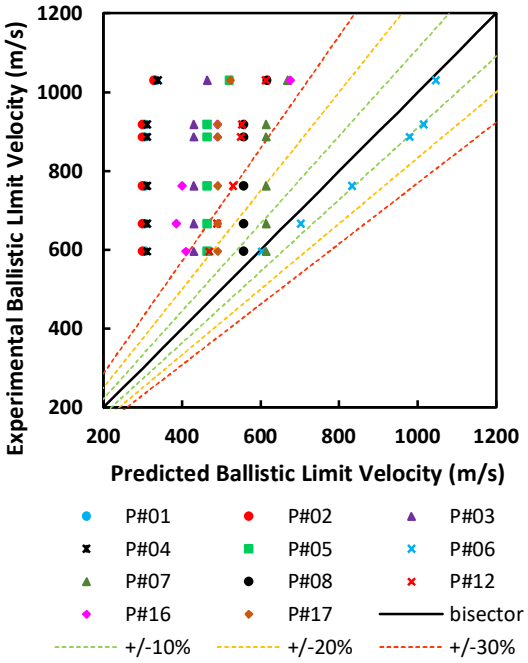

Figure 60 Parity plot comparing experimental (y-axis) and calculated (x-axis) values of the ballistic limit velocity (u_b) in case of soft-core (SC) projectiles. P#-codes are defined in **Table 38**. Adapted from [218].

Eleven (11) PMs were deemed applicable to the group of pointed hard-core (P/HC) projectiles (P#01, P#03, P#04, P#09, P#10, P#11, P#12, P#13, P#14, P#15, P#17). As in the case of SC projectiles, P#17, originally proposed for steel targets with Brinell's hardness of 300, was validated considering also softer and harder steels in order to explore the applicability to a wider set of steels. Therefore, also for this projectile category all the suitable PMs were applied to the total dataset of experimental tests of P/HC projectiles (E#06-10, E#13-33 in **Table 39**).

The parity plot obtained for P/HC projectiles is reported in **Figure 61**. It clearly shows that perforation models P#11 (light grey diamonds), P#12 (red crosses), and P#13 (dark grey triangles), systematically provide incorrect estimates for the experimental data considered, whether they are conservative or not conservative from the point of view of target protection from perforation. This behaviour can be justified for models P#12 and P#13 considering that they were not originally specified for P projectiles, while in case of P#11 it may arise from the model development based exclusively on numerical simulations.

Model P#09 can be also excluded from the set of most suitable PMs for P/HC projectiles as its behaviour is clearly non-conservative (almost the totality of the points is below the bisector), possibly due to its original analytical development for RN projectiles. All the other PMs provide results closer to the bisector, generally providing both underpredictions and overpredictions. However, perforation model P#15 (light green diamonds) appears as a good candidate for P/HC projectiles as it provides accurate estimates of the ballistic limit velocity with most of the points on the bisector or between the ±10% error region (the remaining ones are between the ±30% error region). This is not surprising as the model was specifically developed for P/HC projectiles [258].

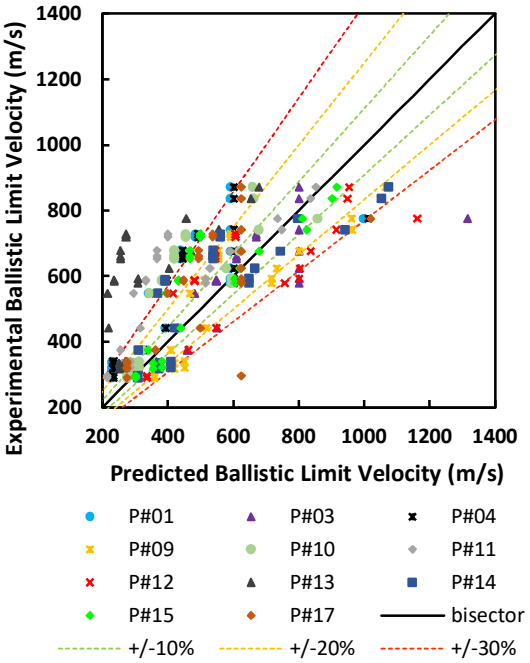

Figure 61 Parity plot comparing experimental (y-axis) and calculated (x-axis) values of the ballistic limit velocity (u_b) in case of pointed hard-core (P/HC) projectiles. P#-codes are defined in **Table 38**. Adapted from [218].

Only a limited number of PMs (seven) are applicable to flat nose hard-core (FN/HC) projectiles (P#01, P#02, P#03, P#04, P#08, P#13, P#14). Also available experimental perforation tests reported a limited number of data points for this group of projectiles (E#11-14 in **Table 39**). The seven PMs were applied to the entire dataset of experimental tests of FN/HC projectiles, similarly to what has been done for the other two projectile categories.

The parity plot obtained, shown in **Figure 62**, clearly identifies the perforation model P#13 (dark grey triangles) as the only PM with errors always lower than 10%. All the other PMs provide ballistic limit velocities with higher errors (also higher than 30%), with several cases of overprediction (non-conservative estimates) of u_b if compared to the experimental values. This outcome may be justified by the generic nature of models P#01, P#03 and P#04 for which the features of FN/HC projectiles and the mechanical properties of the target can not be accounted. Also in case of model P#02, the mechanical properties of the target are not considered among model parameters, and the application in current validation is beyond the originally specified range of target thicknesses (t is greater than 3 mm) and projectile diameter (d is greater than 12.7 mm) in all the experimental data used for validation.

As discussed earlier, model P#08 is an empirical model originally developed for perforation from fragments and not from FN/HC projectiles. Probably due to the behaviour of HC projectiles (hardness typically greater than 134 BHN considered in the original development of the PM) model P#08 provided clear overprediction of ballistic limit velocities. Furthermore, the result is consistent with the good performance demonstrated by P#08 in predicting ballistic limit velocities for SC projectiles (higher ballistic limit velocities are expected from SC projectiles than from HC projectiles for the same target).

On the other hand, both P#13 and P#14 are analytical models able to consider the mechanical properties of the target, but the overprediction of experimental values seems to be higher, for the points available, in the latter model.

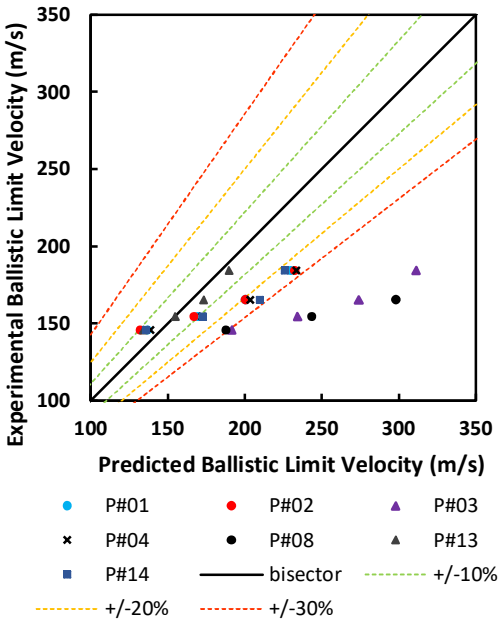

Figure 62 Parity plot comparing experimental (y-axis) and calculated (x-axis) values of the ballistic limit velocity (u_b) in case of flat nose hard-core (FN/HC) projectiles. P#-codes are defined in **Table 38**. Adapted from [218].

As discussed above, although parity plots allowed the preliminary identification of the most suitable PM candidates as reference perforation models in the evaluation of vulnerability to perforation of atmospheric and pressurized storage tanks (scope of the current study), a more quantitative evaluation of model performance of the PMs was based on the statistical parameters defined in Section 5.2.1 (MAPE, MPE and RMSD). The results are shown in **Table 40**.

As expected from the analysis of the parity plot of soft-core (SC) projectiles, perforation model P#06 provided the best results among all the other PMs applicable for this projectile category (MAPE=6.5, MPE=-6.5, RMSD=64.7 m/s). However, as already discussed, this PM provides non-conservative predictions of the ballistic limit velocity (negative MPE) and therefore it is not suitable for the purposes of the current study.

Models P#07 (MAPE=21.5, MPE=21.5, RMSD=231.1 m/s) and P#08 (MAPE=27.7, MPE=27.7, RMSD=278.0 m/s) showed good estimates as well. Model P#07 was originally developed for SC bullets impacting steel targets. However, it shall be pointed out that the good performance of P#07 is demonstrated in spite of the absence of input parameters describing target characteristics, along with the fact that most of the experimental data used for validation fall outside the applicability range of the model as concerns ballistic limit velocity.

As regards model P#08, which was originally developed for fragments in the shape of cylinders and cube-on-cylinders made of mild steel (SAE 1020) [245], the choice to explore validation in case of SC projectiles provided very good results, possibly due to the similarity in size and hardness of the considered SC projectiles and original test fragments (see Section 5.2.3.1). Also in this case, it was found that the model provides a good fit of experimental data on a broader range of hardness values (from 250 BHN of E#01 to 570 BHN of E#34) than the original one (the model was developed for steel targets with Brinell's hardness of 150).

Furthermore, it is important to remark that for both models P#07 and P#08, the points with the smallest errors are those that refer to experimental tests where the targets are made of Weldox 500E (E#01) and Weldox 700E (E#02), which are the most similar to the typical steels used in the construction of industrial storage tanks. The target elements in tests E#03-05 and E#34 are instead made of armour steel.

Table 40 Performance of PMs with respect to the three categories of experimental datasets considered for validation based on the different types of projectiles used in experimental tests (SC, P/HC, FN/HC). MAPE: Mean Absolute Percentage Error; MPE: Mean Percentage Error; RMSD: Root Mean Square Deviation. P#-codes are defined in **Table 38**; E#-codes are defined in **Table 39**; P: Pointed; FN: Flat nose; SC: Soft-core; HC: Hard-core. Adapted from [218].

Perforation model	Experimental data used for validation	MAPE	MPE	RMSD (m/s)
		SC		
P#01	E#01-05, E#34	60.2	60.2	518.3
P#02	E#01-05, E#34	61.2	61.2	525.1
P#03	E#01-05, E#34	44.3	44.3	399.4
P#04	E#01-05, E#34	59.6	59.6	513.8
P#05	E#01-05, E#34	39.6	39.6	362.4
P#06	E#01-05, E#34	6.5	-6.5	64.7
P#07	E#01-05, E#34	21.5	21.5	231.1
P#08	E#01-05, E#34	27,7	27.7	278.0
P#12	E#01-05, E#34	32.7	32.7	294.4
P#16	E#01-05, E#34	41.0	41.0	343.5
P#17	E#01-05, E#34	36.6	36.6	343.9
		P/HC		
P#01	E#06-10, E#15-33	24.0	22.0	165.3
P#03	E#06-10, E#15-33	14.8	-6.7	142.4
P#04	E#06-10, E#15-33	23.9	20.9	161.1
P#09	E#06-10, E#15-33	21.2	-10.8	125.7
P#10	E#06-10, E#15-33	18.1	16.9	151.2
P#11	E#06-10, E#15-33	25.0	24.9	177.1
P#12	E#06-10, E#15-33	20.2	-8.0	140.2
P#13	E#06-10, E#15-33	42.4	42.4	277.6
P#14	E#06-10, E#15-33	17.8	0.8	124.8
P#15	E#06-10, E#15-33	13.9	6.3	114.0
P#17	E#06-10, E#15-33	21.8	7.7	148.2
		FN/HC		
P#01	E#11-14	15.5	-12.5	30.2
P#02	E#11-14	16.2	-11.6	31.3
P#03	E#11-14	54.6	-54.6	95.5
P#04	E#11-14	16.5	-14.2	32.6
P#08	E#11-14	64.6	-64.6	117.8
P#13	E#11-14	4.0	-0.1	7.5
P#14	E#11-14	17.1	-13.7	32.3

A high level of underprediction of experimental data was found for perforation models P#01, P#02, P#03, P#04, P#05, P#12, P#16, and P#17, as shown by the respective MPE values (i.e., 60.2, 61.2, 44.3, 59.6, 39.6, 32.7, 41.0, 36.6 respectively). This was actually expected only for P#12 and P#16, as the PMs provide the evaluation of the protection velocity u_0 [115] which is inherently conservative, while perforation model P#17 should have provided an overestimation of the experimental ballistic limit velocity as it was proposed specifically for 300 BHN steel target elements, which are harder than some materials used in the experimental tests considered (e.g., steels of E#01 and E#02 having respectively 200 and 250 BHN).

Based on the above discussion, perforation models P#07 and P#08 were chosen as reference PMs for SC projectiles. However, since the two models lack in the possibility to account for the mechanical properties of the target element, their use shall be limited to the range of target hardness for which validation is explored

in the current study and that provided errors below 30% (i.e., 200 < BHN < 400). In any case, for Brinell's hardness higher than 400, both the models provide values of ballistic limit velocity in the side of underprediction which is acceptable in the context of the current study, as already remarked.

In the case of pointed hard-core (P/HC) projectiles, as shown in **Table 40**, perforation model P#15 provided the best statistical measures, with MAPE=13.9, MPE=6.3 and RMSD=114.0 m/s. The model was specifically developed for P/HC projectiles and, despite the range of applicability is not declared in [258], it is able to account for the properties of the target such as the dynamic yield stress (Y) and the Young's modulus (E).

Also perforation model P#14 provides accurate estimates (MAPE=17.8, MPE=0.8, RMSD=124.8 m/s). Similarly to P#15, it is aimed at use for P/HC projectiles and can account for the dynamic yield stress (Y) of the target. Nevertheless, the MPE close to zero indicates that both underpredictions and overpredictions are obtained from P#14, which is not considered a desirable behavior in the present framework.

Perforation model P#10 also provides accurate estimates (MAPE=18.1, MPE=16.9, RMSD=151.2 m/s), with the added feature that the results are mostly underestimated in comparison to experimental data (positive MPE and almost equal to MAPE), which is on the safe side for model application in target protection assessments. The model is able to take into account the specific features of the projectiles through shape-related constants (C_v and C_n), the projectile half-angle of conical nose (α), the projectile density (ρ_p), as well as the properties of the target (Young's modulus (E), static yield stress (σ_T), shear stress (τ_S), Poisson ratio (υ), friction coefficient (f), bulk modulus (K)).

In spite of the good performances on MAPE and RMSD, perforation models P#03, P#09, and P#12 predict slightly higher ballistic limit velocities than experiments (MPE of -6.7, -10.8, and -8.0 respectively), thus they were not further considered.

Hence, perforation models P#15 and P#10 are considered as a reference for the further analysis of the vulnerability of industrial storage tanks, with P#10 providing results slightly more conservative than P#15. As mentioned earlier, both models were originally specified for P/HC projectiles and can be tuned on the basis of specific projectile-related and target-related parameters.

For flat nose hard-core (FN/HC) projectiles, the validation was limited to the use of the 4 experimental data reported by Børvik et al. [264]. As already discussed in the analysis of the parity plot in **Figure 62**, all the seven PMs applicable to this projectile category resulted mostly in overpredictions of the experimental values (MPE of -12.5, -11.6, -54.6, -14.2, -64.6, -0.1, -13.7 for P#01, P#02, P#03, P#04, P#08, P#13, and P#14 respectively). However, among them, model P#13 is the only with MPE close to zero (MPE=-0.1), indicating that it provides results with a slight prevalence towards overprediction. Moreover, model P#13 resulted the most accurate with MAPE of 4.0 and RMSD of 7.5 m/s, and it was therefore selected as the reference PM. Model P#13 is an analytical model based on the cavity expansion theory [223,246,256], making it a sound model to predict the case of FN/HC projectiles. According to its constitutive nature, it provides a lower bound value for ballistic limit velocities, which is in line with the underprediction demonstrated for P/HC projectiles where effects of target deformation and friction, not accounted by the model, play a greater role in the definition of ballistic limit velocity.

The selected PMs for SC, P/HC, and FN/HC projectiles are summarized in **Table 41**, which also includes the specific model equations.

Table 41 Selected reference PMs for SC, P/HC, and FN/HC projectiles. The specific correlations provided by each PM for the calculation of ballistic velocity (u_b), are also reported. P#-codes are defined in **Table 38**. Adapted from [218].

Projectile type	PM	Ref	Parameters	Correlation	Applicability
SC	P#07	[217,252]	u (m/s), t (m), m (kg)	$t = 5.42 \cdot 10^{-6} \cdot {u_b}^{4/3} \cdot m^{1/3}$	$u < 600$ m/s $BHN_p \cong 200/300$
	P#08	[217,245,246]	u (ft/s), t (in), m (grains), ϑ (rad)	$u = 10^{4.608} \cdot t^{0.906} \cdot m^{-0.359} \cdot (sec\theta)^{1.286}$	0.8<t<25.4 mm 0.3<m<53 g 183<u<3658 m/s ϑ< 70° $BHN_t \cong 150$ $BHN_p \cong 134$
P/HC	P#10	[112,217,243]	d (m), u (m/s), t (m), m (kg), E (Pa), σ_T (Pa), f, ρ_t (kg/m^3), τ_s (Pa), K (Pa), α (rad)	$t = \frac{4\left(\frac{m}{\pi d^2}\right)}{C_n b}\left[u - \frac{a}{b}\ln\left(\frac{a+bu}{a}\right)\right]$ $a = 2\tau_s \ln(2Z_m) \cdot \left(1 + \frac{f}{\tan(\alpha)}\right)$ $b = C_v\sqrt{K\rho_t}\left(1 + \frac{f}{\tan(\alpha)}\right)\sin(\alpha)$ $Z_m = \frac{E}{\sigma_T}\left(1 + 2\frac{E}{\sigma_T}\right)^{-0.5}$	1<CRH<8
	P#15	[258]	d (m), m (kg), u (m/s), t (m), E (Pa), Y (Pa)	$u = \left(\frac{2\pi r^2 t \sigma_S}{m}\right)^{1/2}$ $\sigma_S = \frac{Y}{\sqrt{3}}\left\{1 + \ln\left[\frac{1}{\sqrt{3}}\left(\frac{E}{Y}\right)\right]\right\}$	
FN/HC	P#13	[223,246,256]	d (m), m (kg), u (m/s), t (m), σ_T (Pa)	$u = \sqrt{\frac{2 \cdot \pi \cdot r^2 \cdot t \cdot A \cdot \sigma_T}{m}}$	

d: projectile diameter; m: projectile mass; t: perforation thickness; u: ballistic limit velocity; ρ_t: target density; σ_T: yield stress; τ_S: static shear strength; Y: dynamic yield stress; BHN_t: target Brinell's hardness number; E: Young's modulus; f: friction coefficient; υ: Poisson ratio; K: bulk modulus; G_t: target shear modulus; ϑ: angle of obliquity.

5.2.3.4. Calculated ballistic limit velocities vs effective thickness of the target elements

Among the identified most suitable projectiles perforation models, the *Modified De Marre* model (P#07) and the *Recht* model (P#10) were applied to calculate the ballistic limit velocity (u_b) for each standardized projectile selected in the DBT (see **Table 35**) with reference to a range of target effective thicknesses (t_{max}). The results of the calculation are shown in **Figure 63**. For each projectile, the higher the thickness of the TE, the higher the ballistic limit velocity required for perforation (the curves are monotonically increasing). Each curve in the figure is represented as a continuous line till the point in which the ballistic limit velocity matches the muzzle velocity (u_m, also reported in **Figure 63**). This point represents the maximum velocity at which a projectile can impact the target element (i.e., muzzle of the firearm next to the external surface of the TE). As perforation is no longer possible if u_b is higher than u_m (dashed curves in **Figure 63**), this sets a limit to the effective thickness that can be perforated by each projectile, defining an inherently safe region for thicknesses higher than the ones corresponding to the muzzle velocity [269]. This occurs for effective thicknesses of 3.2 mm, 4.5 mm, 8 mm, 8.9 mm, and 19.8 mm for FB2, FB4, FB5, FB6, and FB7 projectiles respectively.

These results highlight a big variation in the perforable thickness between handgun projectiles (FB2 and FB4 in **Table 35**) and rifle projectiles (FB5, FB6, and FB7 in **Table 35**). In fact, an attacker who shoots with a handgun will not be able to perforate TEs with a thickness greater than 4.5 mm, while, on the other hand, greater thicknesses can be perforated in case the attacker using rifles. This proves that a higher level of threat may be associated to shooting attacks with rifles with respect to those with handguns. This aspect will be better addressed in the discussion of standoff distances (Section 5.2.4).

Overall, the curves reported in **Figure 63** can be used to easily assess the minimum value of ballistic limit velocity for which perforation of the storage vessels reported in **Table 36** and **Table 37** is possible: the results are reported in **Table 42** and **Table 43** in the next section.

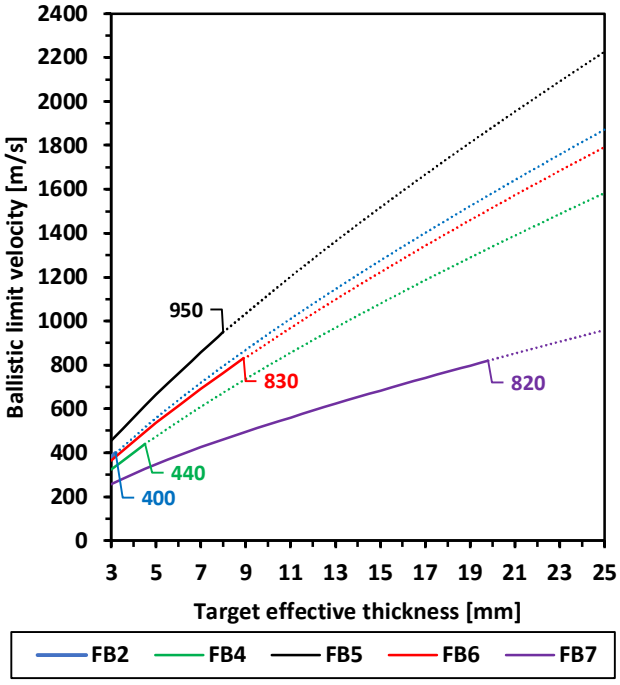

Figure 63 Ballistic limit velocity (m/s) vs target effective thickness (mm) calculated for FB2, FB4, FB5, FB6, and FB7 projectiles (FB-codes defined in **Table 35**). Muzzle velocities (m/s) are reported for each FB class. TE made of Steel A 285M – C.

5.2.4. Calculation of standoff distances

5.2.4.1. Calculated standoff distances vs effective thickness of the target elements

The *Siacci* method [239] was applied to calculate the standoff distances (SOD) for each standardized projectile selected in the DBT (see **Table 35**) with respect to given values of the ballistic limit velocity at the instant the projectile impacts the TE and obtained in the previous step. These results, combined with the information from **Figure 63**, allows to correlate the standoff distances with the effective thickness of the TE. Results are reported in **Figure 64**.

The figure shows a clear distinction between standoff distances obtained for handgun projectiles (i.e., FB2 and FB4) and rifles projectiles (i.e., FB5, FB6 and FB7). In fact, taking as an example the target effective thickness of 3 mm, the standoff distance is almost four times higher moving from FB2 (SOD equal to 10 m) and FB4 handgun projectiles (SOD equal to 143 m) to FB5 rifle projectiles (SOD equal to 540 m), or even more in case of FB6 and FB7 projectiles (SOD equal to 870 m and 1409 m respectively). This trend is maintained also for each of the other thicknesses considered.

These results support specific choices in the design of passive protection barriers within the Physical Protection System (PPS) and in the definition of internal and external response plans for chemical and process plants. For example, effective shell thicknesses equal to 11 mm, which are typical of the higher diameter atmospheric storage tanks or of horizontal pressurized storages (e.g., see the ones reported in **Table 36** and **Table 37**), can be perforated from 400 metres if hit by FB7 projectiles: therefore, shooters may be able to successfully perforate the target even if they are positioned outside the plant boundaries, requiring specific exterior security arrangements in order to increase the probability of detection and of interruption of the attack (e.g., external Closed-Circuit Television (CCTV) system).

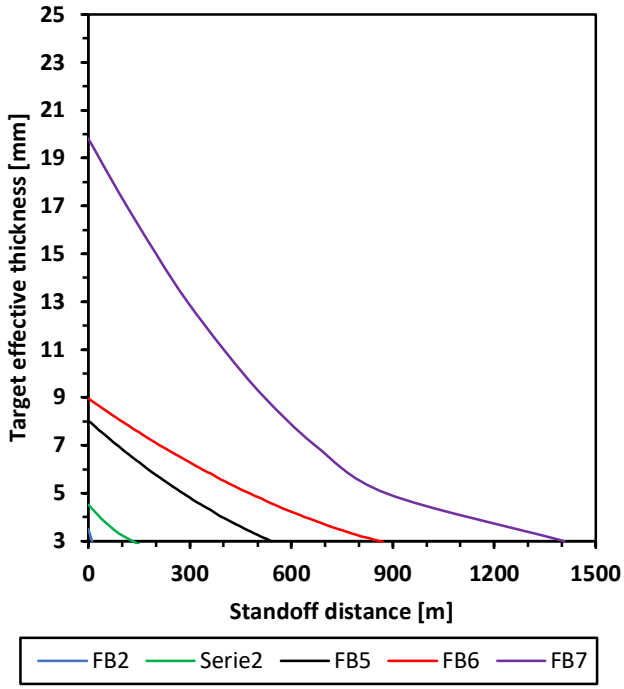

Figure 64 Standoff distances (m) in x-axis vs target effective thickness (mm) in y-axis calculated for FB2, FB4, FB5, FB6, and FB7 projectiles (FB-codes defined in **Table 35**). TE made of Steel A 285M – C.

5.2.4.2. Generic standoff distances for atmospheric and pressurized storage tanks

The results shown in **Figure 63** and **Figure 2** were used to develop generic standoff distances for atmospheric and pressurized cylindrical storage tanks.

Table 42 and **Table 43** report respectively the values of ballistic limit velocity (u_b) and standoff distance (SOD) for the atmospheric and pressurized storage vessels selected as target elements in the present study (see **Table 36** and **Table 37**).

Table 42 Ballistic limit velocities (u_b) and standoff distances (SOD) evaluated for the selected atmospheric storage tanks (**Table 36**). FB-codes defined in **Table 35**; IS: target is inherently safe. TE made of Steel A 285M – C.

ID	t_{eff} (mm)	FB2 $u_m = 400\ m/s$		FB4 $u_m = 440\ m/s$		FB5 $u_m = 950\ m/s$		FB6 $u_m = 830\ m/s$		FB7 $u_m = 820\ m/s$	
		u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)
a.1	4.7	534	IS	452	IS	635	307	512	522	335	930
a.2	4.3	500	IS	423	6	594	360	479	589	318	1000
a.3	3.8	456	IS	386	IS	542	420	436	683	296	1130
a.4	4.7	534	IS	452	IS	635	307	512	522	335	930
a.5	6.9	713	IS	603	IS	847	94	683	225	421	680
a.6	8.1	804	IS	680	IS	956	IS	770	90	465	580
a.7	12.5	1113	IS	942	IS	1323	IS	1066	IS	609	320
a.8	10.1	948	IS	803	IS	1128	IS	908	IS	532	450
a.9	7.9	789	IS	667	IS	938	15	756	112	457	600
a.10	9.2	884	IS	748	IS	1052	IS	847	IS	502	510

With reference to **Table 42**, atmospheric storage vessels a.1-10 resulted to be inherently safe from a shooting attack with a FB2 handgun projectile as the ballistic limit velocity required is higher than the muzzle velocity of the projectile (u_m= 400 m/s). The same outcome was found for FB4 handgun projectiles with the exception of vessel a.2 for which a SOD of 6 m was calculated: this implies that the shooter has to reach the interior area of the site where the tank is located (more complex attack path within the PPS) in order to generate the release of the hazardous substance contained inside.

On the other hand, much higher standoff distances (order of hundreds of meters) were obtained considering rifle projectiles (FB5, FB6, and FB7) reaching about 1000 metres or more in case of a FB7 hard-core projectile fired against a small diameter tank (vessels a.1-3). Clearly, given the extension of these SODs, the shooter is not expected to reach the interior area of the industrial site in order to generate a release (more severe threat due to the low probability of detection of the attack and simplicity of the attack path within the PPS). However, while all the considered atmospheric storage vessels can be perforated by a FB7 projectile fired at a certain distance (lower than the calculated SOD), some of them are inherently safe from a shooting attack carried out with a FB5 projectile (a.6-8 and a.10) and a FB6 projectile (a.7-8 and a.10).

The totality of pressurized storage vessels considered in the present study resulted inherently safe against shooting attacks with handgun projectiles (FB2 and FB4) as reported in **Table 43**. Due to the greater shell thickness compared to that of atmospheric storage tanks, most of the pressurized vessels are inherently safe also from impacts with FB5 (p.4-21) and FB6 (p.4-8 and p.10-21) projectiles. Only vessel p.21 is even safe from a shooting attack which takes use of a FB7 projectile.

Overall, the standoff distances obtained for the pressurized storage vessels are lower than the ones calculated for the atmospheric tanks: in case of FB5 projectiles (SODs are in the order of tens of meters), the attackers are expected to enter the site area, while on the contrary, in case of FB7 projectiles (SODs in the order of hundreds of meters) they are expected to perform the shooting attacks from outside the site fence. For FB6 projectiles, the shooters are required to enter the site boundaries or not depending on the extension of the industrial site as the calculated SODs are around 190 meters.

Table 43 Ballistic limit velocities (u_b) and standoff distances (SOD) evaluated for the selected pressurized storage tanks (**Table 37**). FB-codes defined in **Table 35**; IS: target is inherently safe. TE made of Steel A 285M – C.

ID	t_{eff} (mm)	FB2 $u_m = 400\ m/s$		FB4 $u_m = 440\ m/s$		FB5 $u_m = 950\ m/s$		FB6 $u_m = 830\ m/s$		FB7 $u_m = 820\ m/s$	
		u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)	u_b (m/s)	SOD (m)
p.1	7.8	781	IS	661	IS	929	23	748	120	454	605
p.2	7.2	736	IS	623	IS	875	70	705	190	432	650
p.3	7.2	736	IS	623	IS	875	70	705	190	432	650
p.4	9.6	913	IS	773	IS	1086	IS	875	IS	516	485
p.5	10.3	962	IS	814	IS	1144	IS	922	IS	539	440
p.6	9.1	877	IS	742	IS	1043	IS	840	IS	499	515
p.7	12.0	1079	IS	913	IS	1283	IS	1034	IS	593	350
p.8	9.8	927	IS	785	IS	1103	IS	888	IS	522	470
p.9	8.9	863	IS	730	IS	1026	IS	826	5	492	530
p.10	9.7	920	IS	779	IS	1094	IS	881	IS	519	480
p.11	12.8	1133	IS	959	IS	1347	IS	1085	IS	618	305
p.12	14.1	1218	IS	1031	IS	1448	IS	1167	IS	657	240
p.13	12.2	1093	IS	925	IS	1299	IS	1047	IS	599	335
p.14	15.9	1333	IS	1128	IS	1585	IS	1277	IS	710	160
p.15	11.7	1059	IS	896	IS	1259	IS	1014	IS	584	360
p.16	10.7	990	IS	838	IS	1178	IS	949	IS	552	420
p.17	12.1	1086	IS	919	IS	1291	IS	1040	IS	596	340
p.18	15.0	1276	IS	1080	IS	1517	IS	1222	IS	684	200
p.19	17.9	1457	IS	1233	IS	1732	IS	1395	IS	767	75
p.20	15.2	1289	IS	1090	IS	1532	IS	1234	IS	690	190
p.21	19.9	1577	IS	1335	IS	1876	IS	1511	IS	823	IS

Generic and conservative standoff distances are proposed for each standardized projectile considering the highest standoff distance between those obtained in **Table 42** and **Table 43** (rounded up to the higher ten) for the analysed set of atmospheric and pressurized storage vessels. These values are reported in **Table 44** and can be taken as reference standoff distances to be used by authorities and practitioners in the context of a SVA/SRA to assess shooting attacks to atmospheric and pressurized storage tanks. Clearly enough, application of the procedure described in Section 5.2.1 to the geometry of a specific tank allows for definition of case-specific standoff distances, in case a more rigorous analysis is required by targets with high impact potential.

Table 44 Generic standoff distances (m) proposed for steel atmospheric and pressurized storage tanks considering different classes of projectiles. FB-codes defined in **Table 35**.

SODs [m]	FB2	FB4	FB5	FB6	FB7
Atmospheric storage tank	No perforation	10	420	690	1130
Pressurized storage tank	No perforation	No perforation	70	190	650

5.3. Method for the calculation of the probability of success of malicious physical attacks based on the Bayesian Network (BN)

This Section presents a study aimed at providing a systematic quantitative method based on the Bayesian Network (BN) modelling for the calculation of the probability of success of physical deliberate malicious attacks to industrial physical infrastructures. The method takes into account both preventive and mitigative security intervention strategies. Therefore, the results obtained from this study help answer Research Question 3 (see Section 2.1 and **Figure 4**), supporting the quantitative evaluation of the security risk of a facility. The method is applied in the context of the offshore Oil&Gas industry; however, given its generic nature, the proposed method can be customized and applied to a wider range of critical infrastructures (e.g., security of airports, chemical and process industry). The potential use of the proposed method is demonstrated on a case study addressing an offshore fixed Oil&Gas platform.

5.3.1. Bayesian Network (BN) modelling: key information

According to Baybutt [36] and Nguyen et al. [270], security risk analysis is subjected to a form of uncertainty that is not present for accidents generated by safety-related causes and is difficult to address, namely, the behavior of attackers. In fact, while the consequences of a security attack (e.g., terrorist attack or act of sabotage) may be predicted with some accuracy, the attack itself is subject to large uncertainty [271]. The latter is defined by Aven and Renn [271] as "the difficulty of predicting the occurrence of events and/or their consequences based on incomplete or invalid databases, possible changes of the causal chains and their context conditions, extrapolation methods when making inferences from experimental results, modeling inaccuracies, or variations in expert judgments".

Many authors agree that the Bayesian Network (BN) is a flexible tool for knowledge elicitation and reasoning under uncertainty [54,133], allowing a convenient procedure for a multitude of problems in which one wants to come to conclusions that are not warranted logically but, rather, probabilistically [88,134]. In fact, the capability for bidirectional interferences, combined with a rigorous probabilistic foundation, makes the BN modeling a suitable technique for accident analysis and more importantly, for the design and evaluation of protective measures (i.e., the security barriers in the security domain), replacing earlier ad hoc rule-based schemes [135]. As a matter of fact, BNs are increasingly used nowadays to construct system reliability models, risk management, and safety/security analysis based on probabilistic and uncertain knowledge [88]. For this reason, the BN modelling has been adopted in the proposed quantitative procedure to deal with the uncertainty posed by deliberate malicious attacks to offshore Oil&Gas installations, as well as by the intrusion detection, assessment, and communication aspects. Moreover, the ability of BNs of being applied to forward and backward reasoning through evidence propagation along the network and probability updating, perfectly fits with the need of investigating the role of existing and new security barriers on the final probability of attack success.

BNs consist of both qualitative and quantitative parts. In particular, BNs are directed acyclic graphs (DAGs) in which the nodes represent variables, arcs signify direct dependencies (e.g., causal relationships, sequential order, etc.) between the linked nodes, and the conditional probability tables (CPTs) assigned to the nodes specify how strongly the linked nodes influence each other [272]. The nodes with arcs directed from them are called parents, while the ones with arcs directed into them are called children. The nodes with no parents are also called root nodes, whereas the nodes with no children are known as leaf nodes.

Considering the conditional dependencies of variables, BN represents the joint probability distribution $P(U)$ of variables $U = \{G_1, \dots, G_n\}$ as [273]:

$$P(U) = \prod_{i=1}^{n} P(G_i|Pa(G_i)) \quad (8)$$

where $Pa(G_i)$ is the parent set of variables G_i in the BN.

Accordingly, the probability of variable G_i is calculated as:

$$P(G_i) = \sum_{U \setminus G_i} P(U) \quad (9)$$

where the summation is taken over all the variables except G_i.

BNs take advantage of Bayes theorem to update the prior probabilities of variables given new observations, called evidence E, rendering the updated or posterior probabilities as [273]:

$$P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \quad (10)$$

Overall, the popularity of BNs lies in the fact that they benefit from both qualitative modeling techniques (i.e., representation of dependencies within the set of variables through a network graphical structure) and quantitative modeling techniques based on the computation of CPT of every node [274].

5.3.2. Attacker Sequence Diagram (ASD) modelling: key information

Attackers accomplish their objective by moving along a path through a facility and defeating elements of the Physical Protection System (PPS) encountered along the path [7]. The Attacker Sequence Diagram (ASD) is a graphic representation that is used to help evaluate the effectiveness of the PPS at a facility (see the generic ASD shown in **Figure 65**). It identifies the paths which attackers can follow to accomplish sabotage or theft [7].

The ASD models a PPS by identifying the path elements (PEs) which compose protection layers between adjacent physical areas (see **Figure 65**). Thus PEs are the basic building blocks of a PPS such as personnel and vehicle gateways, emergency exits, shipping/receiving doorways, etc. Path segments (see **Figure 65**) model the entries and the exits between physical areas through the PEs.

The basic concept for an ASD is shown in **Figure 65**: attackers attempt to defeat a path element in each protection layer as they move along a path through the facility to the target. Clearly, in a typical facility, there are usually hundreds of alternative paths an attacker might take to reach a target, and further, each path can be traveled in many ways using force, deceit, or stealth tactics to defeat the various detection and delay components located along a path. Thus, each path consists of a specific set of attacker actions that, if accomplished, will result in the achievement of the attacker objective.

In order to create a site-specific ASD, three main steps have to be followed:

1. modeling the facility by separating it into adjacent physical areas separated by a protection layer controlling movement between areas;
2. defining path elements that make up the protection layers between the adjacent physical areas;
3. assign probability of detection (p_D) and delay time (t_D) for each path element and each physical area.

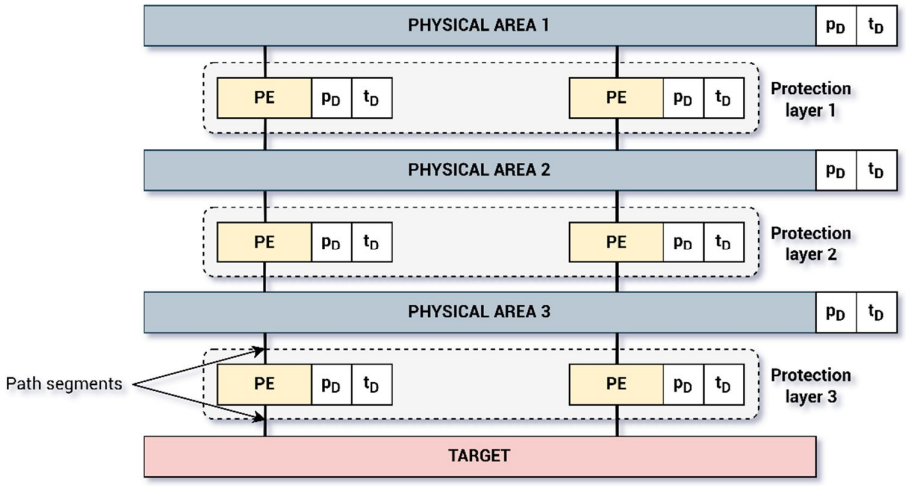

Figure 65 Generic scheme of an ASD. PE: Protection Element; p_D: probability of detection; t_D: delay time.

5.3.3. Proposed quantitative method based on Bayesian Network

5.3.3.1. Overview

The quantitative method based on Bayesian Network proposed in the present study (see flowchart in **Figure 66**) is aimed at estimating the probability of successful execution of a physical attack given the attack attempt (P_2). The method takes into account multiple security intervention strategies (both preventive and mitigative security intervention strategies). Therefore, it provides one element for the estimation of the overall security risk of a facility (see eq. (2) in Section 1.3.1) and provides useful information for the vulnerability assessment phase of SVA/SRA methodologies.

The core mechanism of the proposed method is that of the EASI (Estimate of Attacker Sequence Interruption) model, developed in the context of the security of nuclear power plants (see **Figure 67**) [7]: once a physical intrusion takes place (i.e., an attacker begins his/her task), there is timely execution of a security intervention strategy (preventive or mitigative) in case of the attacker task time remaining after the first detection (ATTr) which results in a correct assessment and communication, is higher than the response time (RT, i.e., the sum of the assessment, communication, and security intervention time (SIT)). The SIT is defined as the time required by the security response to intervene after communication, and it is generally the most significant contribution to the response time (assessment and communication times are often neglected). Similarly to what has been assumed in other vulnerability assessment studies [34,51], also the present study is based on the assumption that in case of the timely intervention of a preventive security strategy, the attack is assumed to be interrupted (i.e., the probability of attack neutralization is considered equal to 1).

Overall, the proposed method consists in the application of 6 steps (see the flowchart shown in **Figure 66**), each described in the next sub-section.

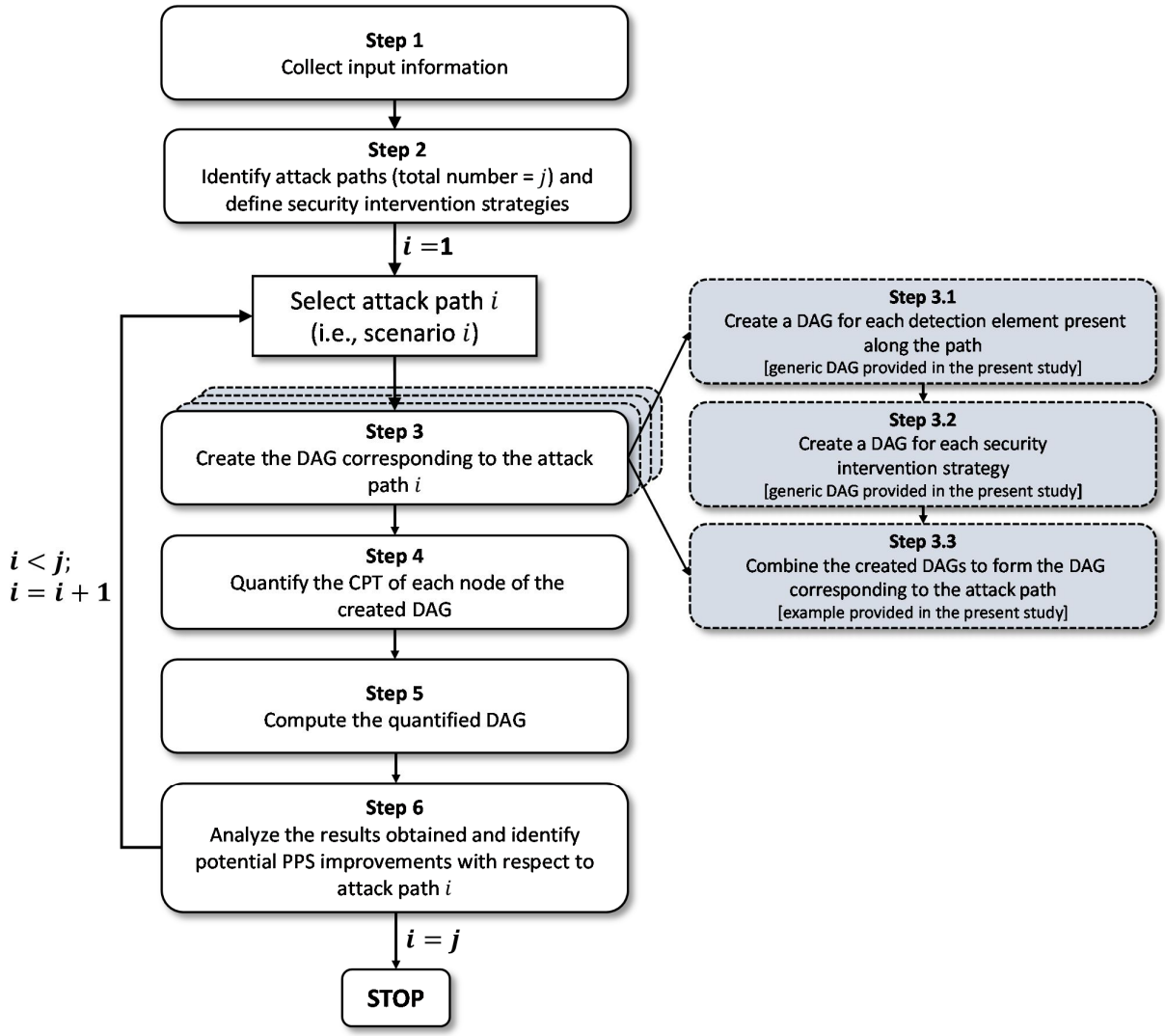

Figure 66 Flowchart of the proposed systematic quantitative method based on Bayesian Network. Adapted from [275].

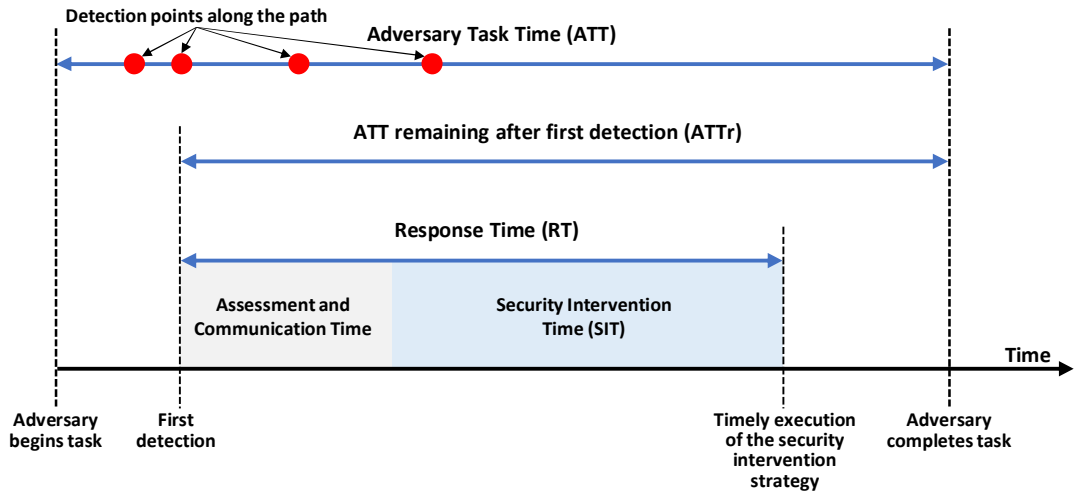

Figure 67 Timing model of EASI (Estimate of Attacker Sequence Interruption) [7]. Adapted from [275].

5.3.3.2. Detailed description of the method

In Step 1 of the proposed method, the input information needed for the application is collected:

- the layout of the PPS of the system analyzed (i.e., detection elements, physical barriers, and physical areas);
- the attack paths, i.e., the specific sequence of physical actions that the attacker has to carry out to overcome the PPS;
- the security intervention strategies (preventive and/or mitigative) which are potentially effective against each attack path considered and the respective SITs;
- quantitative data on probabilities of detection, of correct assessment, of alarm communication for the detection, assessment, and communication elements present in the system analyzed;
- delay times for physical barriers and physical areas.

Step 2 of the proposed method consists of the identification of the potential attack paths, i.e., the specific sequence of physical actions that the attacker has to carry out within the PPS in order to accomplish his/her task (e.g., detonating explosives). The Attacker Sequence Diagrams (ASD) tool described in Section 5.3.2 is suggested for this purpose, since in a previous study by Iaiani et al. [276] its suitability for attack path identification in facilities different from nuclear power plants (in particular the offshore Oil&Gas industry) has been proved.

Moreover, this step provides for the definition of the security intervention strategies available in the system under assessment for the prevention and/or mitigation of each attack path identified. It is essential to underline that a security intervention strategy may be effective against an attack path, but not for another. Therefore, they shall be tailored considering the features of each attack path.

Steps from 3 to 6 of the proposed method (see flowchart in **Figure 66**) shall be carried out for each attack path identified in Step 2.

In particular, Step 3 consists of the creation of the DAG corresponding to the attack path under consideration (i.e., attack path i). To support the systematic application of this step, it has been detailed into 3 sub-steps. The first one (Step 3.1) consists in the creation, for each detection element along the attack path under consideration, of a DAG as the one provided in **Figure 68-a** which is intended for direct application after tailoring with the specific case under assessment. Such DAG is formed by the detection node (D-node in the following), the assessment node (A-node in the following), both with or without their influencing factors (i.e.,

elements that influence the performance of the nodes to which they are connected), and the nodes corresponding to the timely intervention of each security intervention strategy available when detection occurs through the detection element under consideration (SD-node in the following).

Similarly, Step 3.2 consists of the creation, for each security intervention strategy (preventive and/or mitigative) available and potentially effective against the attack path under consideration, of a DAG as the one provided in **Figure 68-b** which is intended for direct application after tailoring with the specific case under assessment. Such DAG is formed by the communication node (C-node in the following) with or without its influencing factors, and the node corresponding to the timely intervention of the security intervention strategy under consideration (S-node in the following).

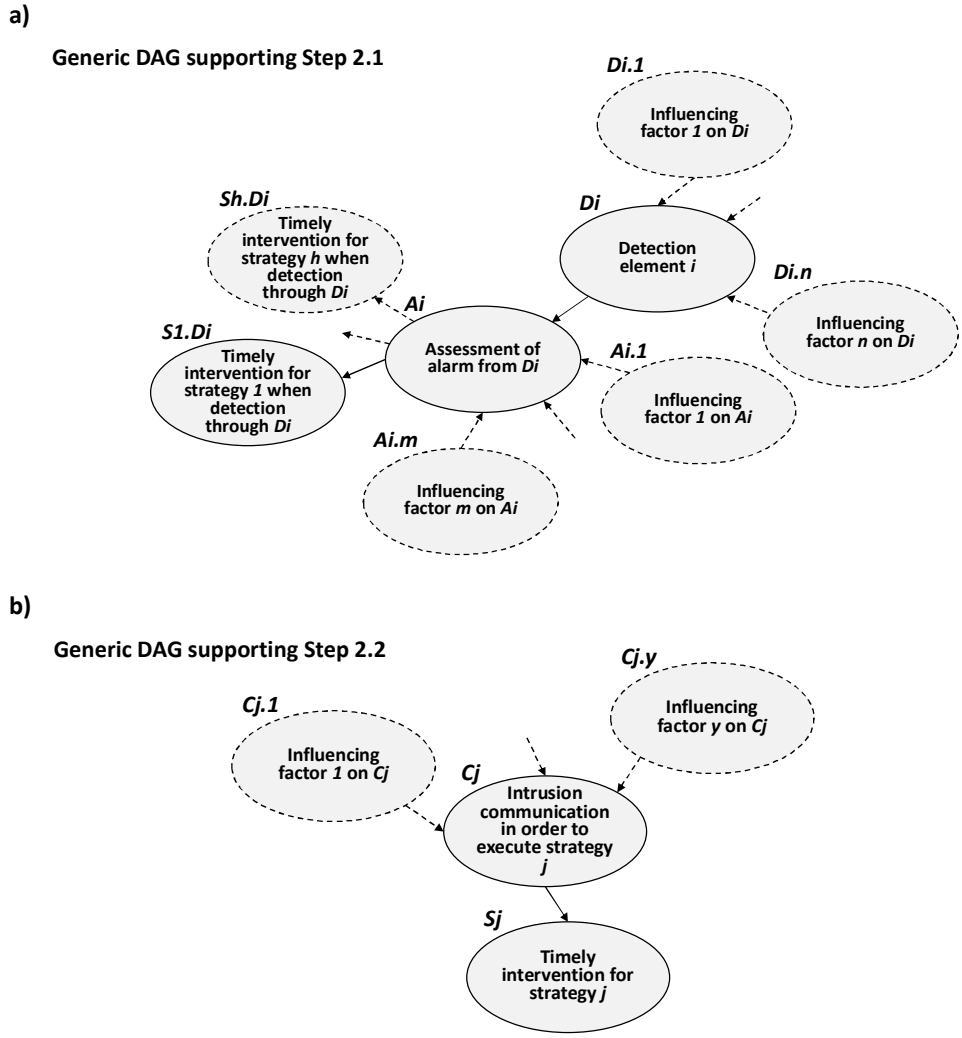

Figure 68 a) Generic DAG supporting application of Step 3.1 of the proposed method (see **Figure 66**); b) Generic DAG supporting Step 3.2 of the proposed method (see **Figure 66**). Adapted from [275].

Finally, Step 3.3 provides for the combination of the DAGs created in the two previous sub-steps to form the required DAG for the attack path under consideration. **Figure 69** reports an example of the output of this step. In particular, the figure shows a DAG which is the result of the combination of four DAGs (blue DAG is referred to detection point 1, green DAG is referred to detection point 2, violet DAG is referred to security intervention strategy 1, yellow DAG is referred to security intervention strategy 2).

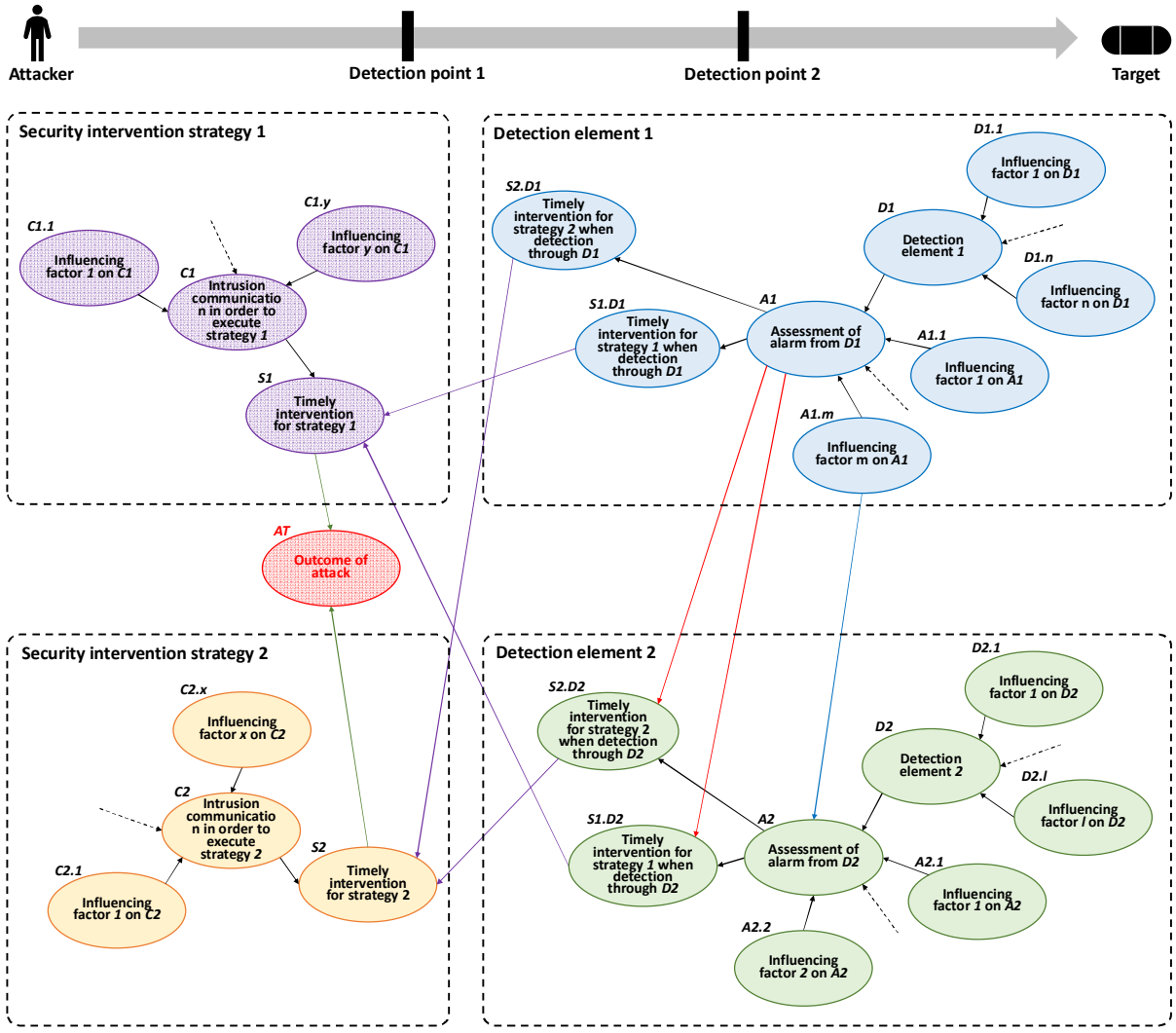

Figure 69 Example of output of Step 3.3: combined DAG with two detection points along the attack path and two security intervention strategies potentially effective against it. Adapted from [275].

In order to support the application of this step, the following guidelines are provided:

- the node corresponding to the outcome of the attack (AT-node in the following) shall be created (red node in **Figure 69**);
- each S-node shall be connected to the AT-node (green arcs in **Figure 69**);
- each SD-node shall be connected to its corresponding S-node (violet arcs in **Figure 69**);
- each A-node referred to a detection element shall be connected to any SD-node referred to a detection element located in a spatially subsequent point along the attack path under consideration (red arcs in **Figure 69**). This is done as the probability of timely intervention of a given security intervention strategy depends only on the first point along the physical path with successful detection and assessment.

Clearly, in addition to the above-required connections, case-specific dependencies may be present due to particular features of the PPS analyzed. Thus, they shall be appropriately represented with arcs within the DAG (e.g., some nodes may share the same influencing factors, blue arc in **Figure 69**).

Each node created in Step 3, except for the AT node, has two states, one corresponding to the favorable condition and the other to the unfavorable condition. The AT-node has 2 states (i.e., *successful*, *not successful*) in case there are no mitigative security intervention strategies and 3 states (i.e., *successful without mitigated consequences*, *successful with mitigated consequences*, *not successful*) in case the latter are present.

Step 4 of the proposed method is aimed at the quantification of the CPT of each node of the DAG developed in Step 3, which means providing marginal probabilities for the root nodes and conditional probabilities for the non-root nodes.

In order to support the application of this step, the following guidelines are provided:

- marginal probabilities of influencing factors can be retrieved from experience-based judgments (expert elicitation), performance data (from tests, data from the vendor, etc.), and/or from an intelligence agency;
- CPT of a D-node, A-node, C-node, and SD-node can be completed according to the following equation [51]:

$$P = P_0 \prod_{h=1}^{Q} (X_h r_h) \tag{11}$$

where:

Q: number of influencing factors and variables that (independently) affect the performance of the element under assessment; P_0: baseline conditional probability representing the probability of the element under assessment successfully performing its function given that all influencing factors are in the favorable state (i.e., given that most favorable conditions to success are present); r_h: measure of the unfavorable impact on the baseline conditional probability P_0 from changing the state of the h-th influencing factor from the favorable state to the unfavorable state and assuming all other influencing factors are still in the favorable state; $X_h = 1$ if the h-th influencing factor is in its unfavorable state, while $X_h = 1/r_h$ if the h-th influencing factor is in its favorable state.

- P_0 for a D-node, A-node, and C-node can be retrieved from experience-based judgments (expert elicitation), performance data (from tests, data from vendor, etc.), and/or from an intelligence agency;

- P_0 for a SD-node can be obtained according to the following equation (normal distribution for time parameters is assumed) which is at the basis of the EASI model [7]:

$$P_0 = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] dx \quad (12)$$

$$x = ATTr - RT \quad (13)$$

where:

$ATTr$: Attacker Task Time remaining after detection in a given detection element; RT: Response Time referred to a given security intervention strategy.

- CPT of a S-node can be completed with 1-values when at least one SD-node is in its favorable state, with 0-values otherwise;
- CPT of the AT-node can be completed with 1-values when at least one S-node is in its favorable state, with 0 values otherwise.

In order to use the EASI model [7] as effectively as possible, and thus to solve eq. (12), some knowledge of standard deviation (SD) is required, both for the security intervention time (SIT) and the delay times for physical areas and barriers. In fact, the use of the SD for the SIT and delay times, allows consideration of the fact that guards and/or operators will not always respond in exactly the same time, and that attackers may take more or less time to crossing physical areas and penetrate physical barriers. Clearly, the SDs shall be as accurate as possible since they influence the total results obtained in terms of probabilities of the states of the AT-node.

SD values can be obtained from experimental tests or measurements (e.g., collecting response intervention time data over several months), or from tabulated values reported in technical reports (e.g., the Hypothetical facility Exercise Handbook developed by Hypothetical Atomic Research Institute (HARI) [277]). However, as an alternative, tests at Sandia National Laboratories have shown that the standard deviation of delay times and SITs can be conservatively estimated at 30% of the mean and, therefore, if there have not been enough tests to establish a statistically significant SD, it is suggested to use 30% of the estimated mean [7].

Step 5 of the proposed method consists of computing the quantified DAG obtained from the previous step to calculate the probabilities of the nodes of interest, based on different evidence set in the graph. This is typically done using software for BN modelling. In particular, the software GeNIe Academic has been adopted in the present study.

Finally, Step 6 of the proposed method e is aimed at the analysis of the results obtained in Step 5 in terms of the vulnerability of the facility analyzed against the attack path under consideration. Possible PPS improvements (e.g., implementation of new countermeasures) are identified and proposed in this step.

5.3.4. Illustrative case study

5.3.4.1. Set-up of the case study

A hypothetical fixed offshore Oil&Gas fluid production platform anchored directly to the seabed with jacket is considered in the illustrative case study. The platform (see **Figure 70**) is surrounded by a protected area (radius of 500 m) where free traffic is not allowed and by a monitored area (radius of 3 km) that is the largest area to be monitored by a long-range radar located on the platform, able to detect ships and other objects over the seabed. Floating barriers (i.e., floating booms suspended between buoys equipped with a net extending above and below the seawater surface) separate the two areas with the exception of a section

dedicated to the passage of authorized ships (ship portal). The shore is located at a minimum distance of 5 km from the platform. Access to the landing deck of the platform (equipped with a video motion system for intrusion detection) is guaranteed by a docking point where ships can moor, and personnel can climb up through a ladder. Stairs allow access to the other four decks: cellar deck (with filters and safety systems), main deck (with utilities, control cabinets, control room, and main equipment such as separators and wellheads), auxiliary deck (with resting rooms for personnel), and helideck for helicopter landing.

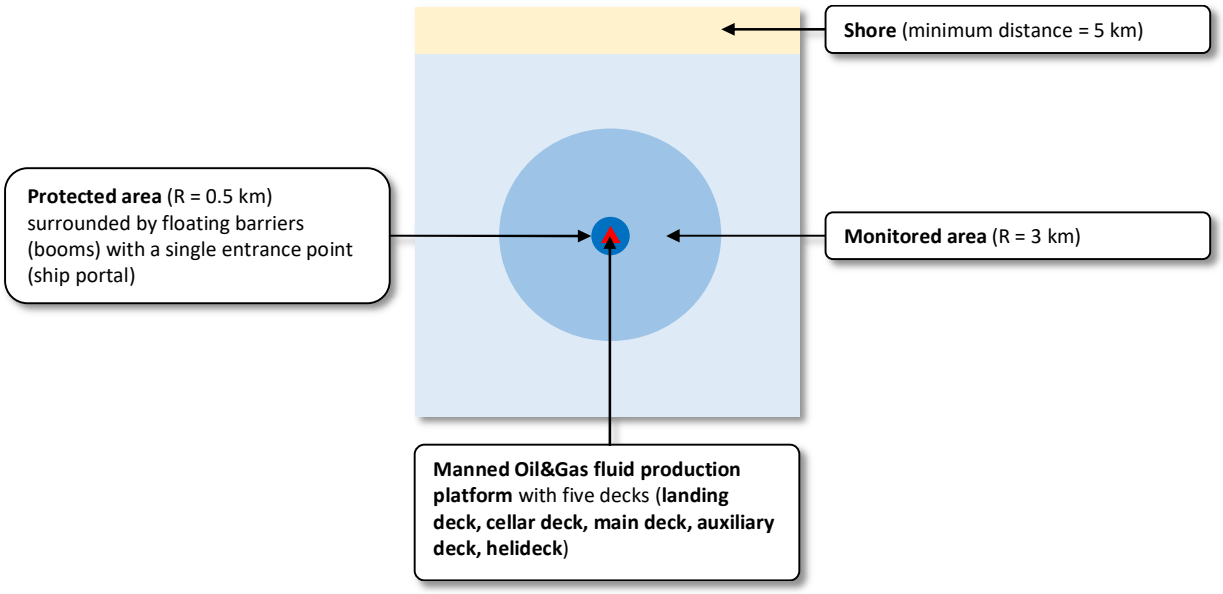

Figure 70 The layout of the offshore Oil&Gas fluid production platform considered in the case study. Adapted from [275].

5.3.4.2. Results of the case study

The required input information (PFD, material balances, hazardous properties of the substances involved, equipment data sheets, etc.) was collected as requested by Step 1 of the method described in Section 5.3.3.

Step 2 of the proposed method (see Section 5.3.3) requires the identification of the possible attack paths that can be carried out by an attacker and the definition of the available security intervention strategies that can prevent it, or at least mitigate its consequences.

For the sake of brevity, the proposed method is applied to a single attack path in order to illustrate its application and to demonstrate the quality of the results that can be achieved. The attack path considered is one of those identified in a previous work [278] using the Attacker Sequence Diagram (ASD) tool [7] to which the reader is referred for more information. In particular, it consists of three main actions that have to be accomplished by an attacker:

1. leaving from the shore and crossing monitored area and protected area by boat;
2. mooring the boat and climbing onto the landing deck through the docking point;
3. reaching the gas/liquid separators section in the main deck, planting and detonating 50 kg of homemade explosive (TATP).

The long-range radar, the video motion system, and the employees present on board are the three detection elements present along the attack path described above.

According to Vasilev [279], an attack making use of explosives is very common for all spectrum of offshore constructions (thus including offshore Oil&Gas platforms) and is able to cause massive damage and loss of life. Moreover, the quantity of 50 kg contained inside a backpack was considered a credible attack scenario for a single attacker according to the study described in Section 5.1 (Bow-Tie diagram approach for the identification of reference security scenarios [220]) to which the reader is referred.

The Coast Guard, with a station located 15 km away from the platform, can intervene in case of intrusion communication in order to interrupt the attack (preventive security intervention strategy). Moreover, as for security policy, in case of intrusion communication, the platform is also forced to shutdown (mitigative security intervention strategy) providing emergency closure of the producing conduits by closing the subsurface safety valves (SSSV).

The combined DAG obtained from the application of Step 3 of the proposed method (see Section 5.3.3), corresponding to the attack path described above, is shown in **Figure 71**.

The DAGs in blue, green, and gray colors are the ones obtained as outputs of Step 3.1, respectively for the long-range radar, the video motion system, and the employees on the platform. Similarly, the ones in violet and yellow colors are those obtained as outputs of Step 3.2, respectively referred to Coast Guard communication and timely intervention, and to communication to the control room operators and timely shutdown activation. Connections between the nodes have been made according to the guidelines provided in the description of Step 3.3 (see Section 5.3.3).

While maintenance and inspection of the radar (node D1 in **Figure 71**) and the video motion system (node D2) have been reasonably considered independent (two separate nodes, D1.1 and D2.2), the node corresponding to meteorological conditions (node D1.2) is shared between the two detection elements, with the video motion system being also influenced by the coverage of intrusion area (node D2.1). Similarly, the intrusion detection by employees (node D3) is influenced by the presence of employees where the intrusion occurs (node D3.1) and by the level of security training of employees (node D3.2), with the latter also influencing the intrusion assessment made by employees (node A3).

The operator level of training (node A1.1), and whether or not the operator is looking at the monitor (node A1.2) influence the assessment through the video system of the alarm from both (shared nodes) the radar and the video motion system (respectively nodes A1 and A2).

The communication to the Coast Guard (node C1) is influenced by the level of training of personnel in external communication procedures (node C1.1) and by the reliability of coverage (node C1.2). Similarly, the communication to the operators in the control room (node C2) is influenced by the level of training of personnel in internal communication procedures (node C2.1).

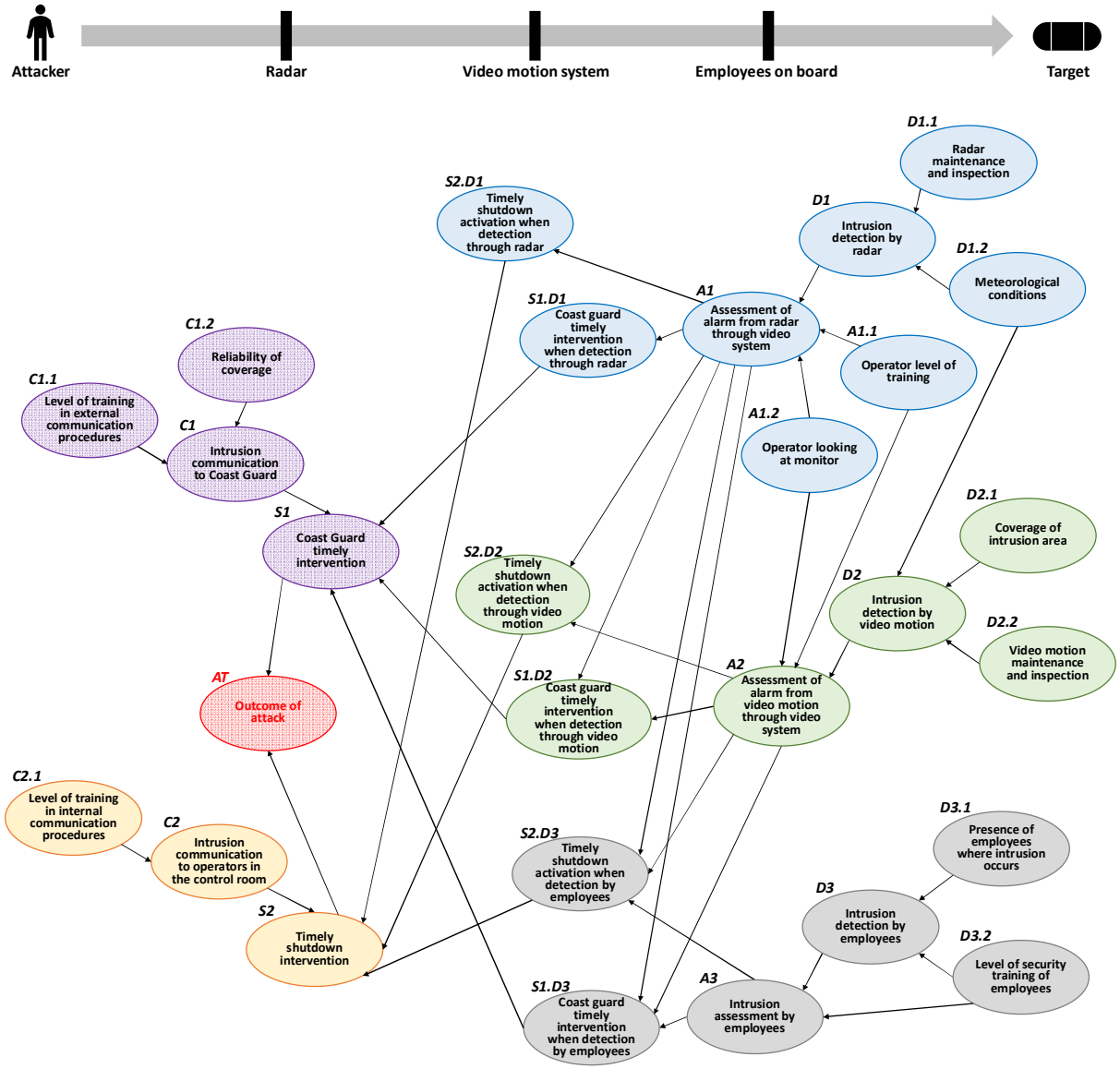

Figure 71 Combined DAG obtained from the application of Step 3. Adapted from [275].

For the sake of clarity, the states that have been considered for each node displayed in the DAG of **Figure 71**, are reported in **Table 45**.

Table 45 List of the states adopted for each node (for node IDs refer to **Figure 71**). Adapted from [275].

Node ID	State 1	State 2	State 3
D1, D2, D3	Detection	No detection	
D1.1, D2.2	Sufficiently frequent	Not sufficiently frequent	
D1.2	Favorable	Unfavorable	
D2.1	Complete	None	
A1, A2, A3	Assessed detection	No assessed detection	
A1.1, D3.2, C1.1, C2.2, C2.1	High	Low	
A1.2, D3.1	Yes	No	
S1.1, S1.2, S1.2, S2.2, S1.3, S2.3, S1, S2	Timely	Not timely	
C1, C2	Communication	No communication	
A	Successful without mitigated consequences	Successful with mitigated consequences	Not successful

Each CPT was filled (Step 4 of the proposed method) according to the equations reported in Section 5.3.3.2 using quantitative input data retrieved from the following sources:

- marginal probabilities for influencing factors and P_0 of D-nodes, A-nodes, and C-nodes were retrieved from Argenti et al. [280] who provide performance data of physical security countermeasures that have been elicited from the consultation of experts, and by the Hypothetical facility Exercise Handbook [277];
- delay times for physical barriers in place were retrieved from the Hypothetical Facility Exercise Data Handbook [277];
- the typical range of speed of commercial boats was retrieved from McKenna et al. [281];
- the typical range of speed of attacker by feet was retrieved from Wadoud et al. [282]

It is important to remark that, according to the guidelines provided by Garcia [7] and summarized in section 5.3.3.2, a standard deviation (SD) of 30% was assumed for the SIT and for the delay times of barriers for which an estimated value was not reported in the literature analyzed.

As an example, **Table 46** reports the input data and the calculations that have been carried out in order to fill the CPT of node D1 ''Intrusion detection by radar''.

Table 46 Example of data and method applied for the quantification of the CPT of node D1 (see **Figure 71**). Numerical data were retrieved from [280] and [277]; the equation used is (11) [51]. Adapted from [275].

Input data for quantification of CPT of node D1				
Node ID	**Node**	**Variable ID**	**Variable**	**Median of elicited values**
D1.1	Radar maintenance and inspection	$MP_{1.1}$	Marginal probability of carrying out adequate maintenance and inspection	0.875
		$r_{1.1}$	Measure of negative impact on the probability of having detection from changing the maintenance and inspection to the unfavorable state and assuming that meteorological conditions remain in a favorable state	0.2
D1.2	Meteorological conditions	$MP_{1.2}$	Marginal probability of meteorological conditions being favorable to detection	0.85
		$r_{1.2}$	Measure of negative impact on the probability of having detection from changing the meteorological conditions to the unfavorable state and assuming that radar maintenance and inspection remain in a favorable state	0.7
D1	Intrusion detection by radar	CP_1	Conditional probability of successful detection given radar maintenance and inspection, and meteorological conditions are in favorable state	0.1

Calculations for quantification of CPT of node D1				
Radar maintenance and inspection	Sufficiently frequent		Not sufficiently frequent	
Meteorological conditions	Favorable	Unfavorable	Favorable	Unfavorable
Detection	CP_1	$CP_1 \cdot r_{1.2}$	$CP_1 \cdot r_{1.1}$	$CP_1 \cdot r_{1.1} \cdot r_{1.2}$
No detection	$1- CP_1$	$1- CP_1 \cdot r_{1.2}$	$1- CP_1 \cdot r_{1.1}$	$1- CP_1 \cdot r_{1.1} \cdot r_{1.2}$

CPT of node D1 quantified				
Radar maintenance and inspection	Sufficiently frequent		Not sufficiently frequent	
Meteorological conditions	Favorable	Unfavorable	Favorable	Unfavorable
Detection	0.1	0.07	0.02	0.014
No detection	0.9	0.93	0.98	0.986

The computing (Step 5 of the proposed method) of the quantified DAG shown in **Figure 71** was performed using the software GeNIe Academic.

The probabilities obtained for the non-root nodes of the DAG in case no evidence was set in the network, are reported in **Table 47**. It is important to underline that for the considered attack path, the damage of the gas/liquid separator is deemed to be certain, according to the standoff distances (i.e., the minimum distance

from the asset of interest and the location where the attack takes place without causing damage) calculated within the study described in Section 5.1. In fact, a damage is always possible at 0 m from an equipment (whether it is an atmospheric vessel, pressurized vessel, or a pressurized horizontal vessel) in case of successful detonation of 50 kg of TATP, and it can be assumed to be the one of maximum extent (worst-case scenario, i.e., release loss intensity LI3: instantaneous release of the entire vessel content). Therefore, for the case study, a successful attack means having a specific loss of containment (LOC) from the gas/liquid separator, and thus the obtained probabilities for the AT-node are actually a combination of P_2 and C in eq. (2) of Section 1.3.1.

Table 47 Results of the quantitative analysis of the developed BN with no evidence set. Only probabilities of main nodes are reported (for node IDs see **Figure 71**). Adapted from [275].

Node ID	States	Probability
D1	Detection	9%
	No detection	91%
A1	Assessed detection	6%
	No assessed detection	94%
D2	Detection	83%
	No detection	17%
A2	Assessed detection	59%
	No assessed detection	41%
D3	Detection	67%
	No detection	33%
A3	Assessed detection	57%
	No assessed detection	43%
C1	Communication	89%
	No communication	11%
C2	Communication	93%
	No communication	7%
S1	Timely	0%
	Not timely	100%
S2	Timely	29%
	Not timely	71%
A	Successful without mitigated consequences	71%
	Successful with mitigated consequences	29%
	Not successful	0%

In order to investigate the effect on the probabilities of the states of the AT-node (*Successful without mitigated consequences, Successful with mitigated consequences, Not successful*) of having a successful detection at sea (i.e., by the long-range radar), at the docking point (i.e., by the video motion system), or on the platform (i.e., by the employees on board) with consequent correct assessment of the alarm, as well the effect of each influencing factor taken in its unfavorable state, different evidence in the DAG has been set. In particular, all these elements were investigated separately, i.e., only one evidence has been set at a time.

The results of each computing, taking into consideration all the cases just mentioned, are shown in **Figure 72**, whose analysis (Step 6 of the proposed method) is part of the discussion section.

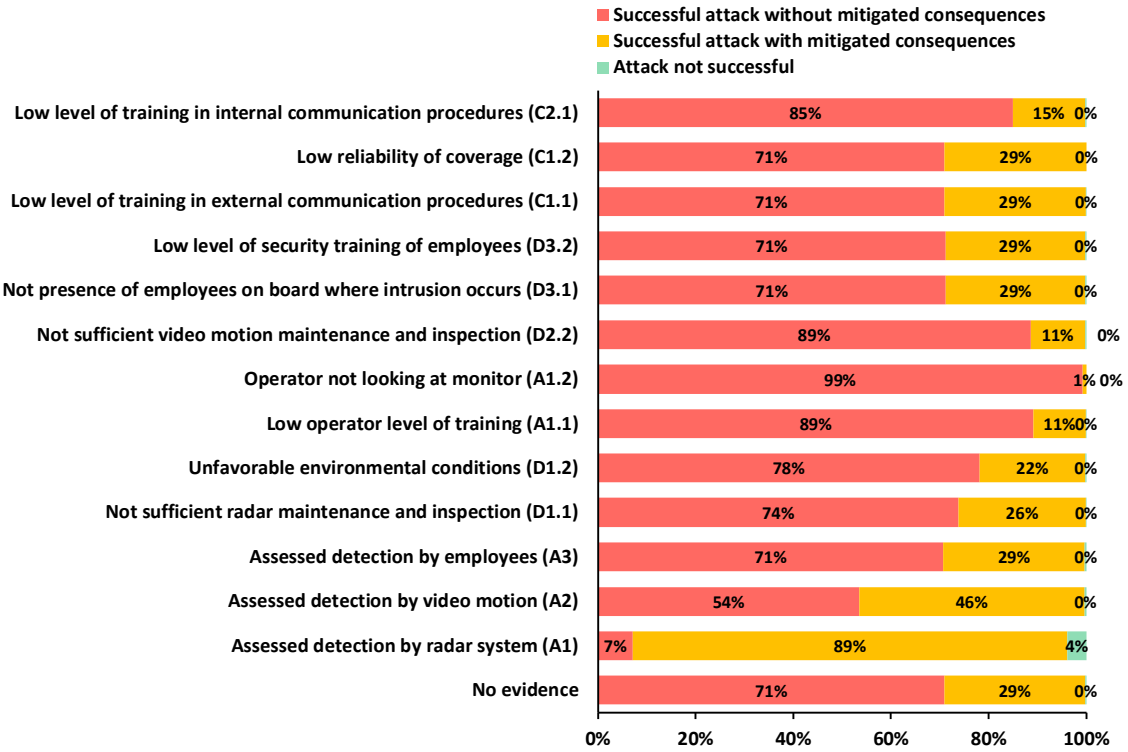

Figure 72 Probabilities of the states of the AT-node obtained by the computing of the developed DAG with different evidence set. Adapted from [275].

5.3.4.3. Discussion of the results of the case study

The present study proposes a systematic quantitative method based on Bayesian Network (BN) for the calculation of the probability of success of physical malicious deliberate attacks given an attempt (P_2 in eq. (2), see Section 1.3.1), taking into assessment both preventive and mitigative security intervention strategies. The method fills the existing gap in the availability of systematic quantitative methods able to accounts for security issues in offshore Oil&Gas facilities, providing the reader with guidelines for the case-specific BN construction. However, given its generic nature, the proposed method can be customized and applied to a wider range of critical infrastructures (e.g., security of airports).

The application of the proposed method to the hypothetical fixed offshore Oil&Gas fluid production platform considered in the illustrative case study proved the quality of the results that can be achieved in supporting the application of the vulnerability assessment phase within SVA/SRA, providing important insights on the degree of vulnerability of the platform assessed, as well as information on the most critical weaknesses present in its Physical Protection System (PPS) thanks to the probability update feature of BNs.

In particular, with reference to **Table 47**, the interruption of attack considered (i.e., reaching the platform by boat and detonating explosives planted on the gas/liquid separators located in the main deck) by the intervention of the Coast Guard resulted in being not possible (probability of state *Attack not successful* of the AT-node is 0%). This is due to the much higher time required by the Coast Guard to intervene (RT of 1080 s) if compared to the total time required by the attackers to accomplish the attack (ATT of 494 s), calculated from the first point where they can potentially be detected, i.e., from the beginning of the monitored area, even considering possible deviation from the mean values (standard deviation of 30% was assumed).

Therefore, the attack path considered resulted in being very critical for the platform analyzed, making mitigation of its consequences (e.g., through platform emergency shutdown and blowdown activation) of paramount importance to reduce the extent of the outcomes in terms of damage to people, to the environment, and to the other assets (potential for man-made cascading events [55,283,284]). Actually, a timely activation of the emergency shutdown system (ESD) is possible even if with a relatively low probability (around 29%, see **Table 47**): in fact, the much lower time required for activating the platform ESD (RT of 120 s) compared to that of Coast Guard intervention (1080 s), makes the execution of this intervention strategy more likely.

Clearly, no security intervention is possible if no detection occurs, and thus, intrusion detection plays a fundamental role in preventing and mitigating deliberate malicious attacks. Among the detection elements present along the attack path considered, the video motion system present in the docking point of the platform is the most effective in detecting the attackers (success probability of 83%, see **Table 47**), followed by the detection by employees (success probability of 67%), and finally the long-range radar (success probability of 9%). However, the role that a detection element has on the final outcome of an attack does not depend only on its absolute probability of detection, but also on the specific point along the path where it is able to detect the attackers: in fact, it influences the time remaining to the attacker to accomplish the attack. For this reason, it is interesting to analyze the effect on the outcomes of the attack considering that each detection element and related assessment have. This was possible thanks to the probability update feature of BNs. In particular, with reference to **Figure 72**, in case the attacker is detected by the radar system and the alarm is correctly assessed, there is a non-zero probability of attack interruption (around 4%), and a probability of having mitigated consequences through timely platform ESD activation, of about 89% (this means that the probability of successful attack is around 7%). Similarly, when the attacker is detected by the video motion system and the alarm is correctly assessed, the probabilities of attack interruption, attack mitigated, and attack successful are 0%, 46%, and 54% respectively, while in the case of intrusion detection and assessment by employees these probabilities are 0%, 29%, and 71% respectively. This result clearly evidences the importance of the detection of attackers in the sea, and in particular when they enter the monitored area: in fact, this leads to a very high probability of mitigation of attack consequences through the activation of the platform ESD and a non-zero probability of Coast Guard timely intervention for attack interruption. For this reason, the radar turned out to be a very important detection element in the prevention and mitigation of the attack path considered for the hypothetical platform in case of successful detection. However, as already stated, the probability of detection through the radar system and that of the correct assessment of the produced intrusion alarm are around 9% and 6%, respectively (see **Table 47**), meaning that the chances of detection at sea are low. Therefore, efforts and resources should be spent on the adoption of more reliable intrusion detection systems in the sea as they may deeply decrease the security risk of the platform analyzed against the attack assessed herein.

As remarked above, the detection element which mainly influences the outcome of the attack is the video motion system, given its much higher probability of detection (83%). The detection occurs in a position where the shutdown activation can still be timely. This is why an insufficient maintenance of the video system (i.e., the influencing factor of the node D2 taken in its unfavorable state) strongly affects the probabilities calculated for the AT node (probability of unmitigated attack of 89% vs. the 71% calculated in case of no evidence set). Clearly, an operator who does not look at the monitor makes the assessment of the detection by the radar and the video motion impossible, and thus no prevention and mitigation can occur (probability of unmitigated attack of 99% vs. the 71% calculated in case of no evidence set).

On the contrary, the detection of attackers by employees on board, despite having a relatively high probability of success (67%), turned out to be quite ineffective, as the time remaining for the attackers to accomplish their actions when they are already on board is lower or comparable (considering a standard deviation of 30%) to the less-time-requiring shutdown activation. This is why a poor level of security training

for employees, as well as the absence of employees where the intrusion occurs (i.e., the influencing factors associated to node D3 taken in their unfavorable states) do not affect the probabilities calculated for the AT-node (see **Figure 72**).

Clearly, the communication of the assessed intrusion detection to the port captaincy and/or to operators in the control room is essential in order to initiate the execution of the respective security intervention strategy, i.e., the intervention of the Coast Guard and the platform shutdown activation. With reference to **Figure 72**, a low level of training in internal communication procedures deeply affects the outcome of the attack as it indirectly affects the platform shutdown activation, which turned out to be the only effective security intervention strategy against the attack considered (probability of unmitigated attack of 85% vs the 71% calculated in case of no evidence set). On the contrary, a low level of training in external communication procedures and low reliability of coverage (i.e., the influencing factors of the communication to port captaincy taken in their unfavorable state) do not influence the outcome of the attack as a timely intervention of the Coast Guard was found to be unlikely also in case of detection at sea.

It is important to point out that despite the above discussion is specific for the results obtained from the analysis of a single physical attack path (the one described in Section 5.3.4.2), they can be in part generalized. In fact, the probability of timely intervention of the Coast Guard will be almost zero for any other type of attack that requires a shorter time to be accomplished by an attacker (e.g., an attack consisting of the shooting of gas/liquid separators from long distance, such as from the inside of the monitored area). Moreover, attacks that do not involve physical access to the platform are also critical since only the radar system (probability of detection of 9%) is potentially able to detect attackers, making intrusion detection and security intervention extremely unlikely.

Overall, the results that can be obtained through the application of the proposed method help decision-makers to prioritize resources and help companies achieve continuous improvement in security performance, allowing them to identify, assess and address vulnerabilities, prevent or mitigate deliberate malicious attacks, enhance training and response capabilities, and maintain and improve relationships with key stakeholders and authorities. However, the proposed procedure may be demanding in terms of time and resources required for its application if a large number of attack paths is credible for the assessed facility. Nevertheless, the modular nature of the steps of the procedure allows in perspective the possibility of automatization by software tools. Notably, the sub-steps from 3.1 to 3.3 may benefit from the future development of specific data libraries. As already stated, the application of the procedure is currently restricted to the scope of physical security attacks. Cyber-attacks to the IT-OT network of the assessed facility are not considered due to inherent differences in the attack path. Future developments may also address the analysis of multiple attack paths, including cyber-attacks, in the context of a probabilistic security vulnerability assessment of an offshore Oil&Gas facility.

6. Conclusions and future challenges

The present 3-year research contributed to the development of new knowledge on the cause-consequence relationship between the deliberate malicious attacks to industrial plants (chemical industry, process industry, Oil&Gas critical infrastructures, etc.), the impacts of such attacks, and the safety/security preventive or mitigative barriers present in the attacked facility. The activities carried out provided hazard identification and quantitative risk assessment methods suitable for supporting application of existing Security Vulnerability Assessment (SVA) and Security Risk Assessment (SRA) methodologies in industrial critical infrastructures (e.g., CCPS SVA, API RP 780 SRA, VAM-CF, RAMCAP, SFK, and the novel quantitative methods proposed in recent years). The different nature of cyber-attacks (interferences aimed at causing damage through the IT (Information Technology) and OT (Operational Technology) systems) compared to that of physical attacks (interferences aimed at causing damage bypassing PPS (Physical Protection System) elements) in terms of systems affected and attack paths carried out by the attackers, resulted in the development of methods suitable for the cybersecurity domain and the physical security domain characterized by differences in the core-mechanism.

In the following, the main research findings as well as the novel scientific contributions are listed:

- The synergic structured analysis of the two novel developed databases (one collecting 373 security-related events affecting onshore industrial process facilities and one collecting 2222 security-related events affecting offshore Oil&Gas industrial facilities) confirmed the relevance of security attacks in the chemical, process, and Oil&Gas sectors, and their potential severity in damaging people, property, and the surrounding environment. The analysis allowed obtaining a set of novel information providing a holistic description of the security threats and scenarios affecting industrial sectors where relevant quantities of hazardous materials are handled. The data obtained can be used to support SVA/SRA studies regarding the phase of attractiveness assessment and those concerning the identification of vulnerabilities, threat scenarios, final outcomes, and security countermeasures, providing a clear picture, based on past events, of the most credible reference scenarios involved in a deliberate malicious attack. Details are reported in Section 3.1 and Section 3.2.
- The two developed systematic rigorous methodologies PHAROS (Process Hazard Analysis of Remote manipulation through the cOntrol System) and POROS (Process Operability analysis of Remote manipulations through the cOntrol System) aimed at the security assessment of the link between malicious manipulations of the BPCS (Basic Process Control System) and the SIS (Safety Instrumented System), and the major accident scenarios (PHAROS) and the production outage scenarios (POROS) that can affect the operability and/or system integrity of the target facility, filled the lack in literature of systematic approaches for cyber-risk identification. The application of PHAROS and POROS methodologies to case studies evidenced that the cyber threat to the chemical, process, and Oil&Gas industry is not only limited to conventional impacts common to all services and sectors (e.g., data theft or corruption), but also to specific and potentially more severe impacts, as induced major events and production outages (confirmed by historical evidence) when the attackers succeed in affecting the BPCS and the SIS systems of the target facility. The results obtained in the case studies remark the importance of taking into account security issues as well as safety issues when designing both the network architecture and the process plant (e.g., considering cybersecurity scenarios in the design of passive safeguards such as Pressure Safety Valves (PSVs)) in order to implement effective “defense-in-depth” strategies for these threats. Overall, the outcomes obtained confirmed that PHAROS and POROS methodologies can support the identification of consequences and impacts associated with cyber threats, as well as the definition of the protection requirements and

countermeasures for the manipulative elements of the plant (e.g., controllers and logics) according to international standards (e.g., ISA/IEC 62443). Details are reported in Chapter 4.

- The novel set of reference physical security scenarios developed (cause-consequence chain from attack scenarios to physical damage scenarios) and the step-by-step procedure based on Bow-Tie formalism for the case-specific identification of reference security scenarios filled the existing gap in the literature regarding the availability of practical tool supporting scenario identification in the context of SVA/SRA studies. These scenarios can also be used as a basis to foster the integration of a list of major accident scenarios into the Safety Report of upper-tier European Union Seveso plants (Seveso Directive 2012/18/EU) in order to yield a more complete understanding of risk and to define a single set of safety/security requirements. Details are reported in Section 5.1.
- The unprecedented extended review and validation of available projectile perforation models (PM) using experimental data from perforation tests allowed to identify suitable damage models for projectile impact on HAZMAT industrial storage vessels that can be used to assess the vulnerability to perforation of these equipment in the context of a shooting attack. The baseline standoff distances for atmospheric and pressurized storage vessels, previously unavailable in the open literature, that were calculated using the identified PMs together with exterior ballistics models, were proved to support several activities in the context of SVA/SRA such as the design of the Physical Protection System (PPS), the identification of credible shooting scenarios, and the assessment of target vulnerability. Details are reported in Section 5.2.
- The developed quantitative procedure based on the Bayesian Network modelling for the calculation of the conditional probability of success of intentional malicious physical attacks overcomes some of the limitations of the available quantitative approaches addressing security risks. The developed procedure is in fact systematic, attack-path dependent, applicable to a wide range of critical infrastructures (e.g., security of airports), and considers both preventive (e.g., response of the security force) and mitigative (e.g., emergency shutdown activation) security intervention strategies in the assessment. The application of the procedure to case studies proved its ability in supporting the application of vulnerability assessment phase of SVA/SRA methodologies as regards the calculation of one of the three contributions to the value of the security risk of a facility, the identification of the most critical attack path (i.e., the one with the lowest probability of interrupted and/or mitigated attack) which determine the overall effectiveness of the PPS, the identification of the vulnerabilities present in the PPS that can facilitate the adversaries to accomplish their tasks, and the definition of potential design improvements towards a more secure PPS. Details are reported in Section 5.3.

Overall, the results of this research support the identification, mitigation, and quantitative risk assessment of chemical and process plants, allowing a deeper understanding of risk and supporting informed decision making in the management of risks from security attacks (cyber and physical deliberate malicious attacks). The proposed methods recognize the multi-faceted nature of the cyber and physical security improvement problem and take into account the interactions with the domains of safety, reliability and cost-effectiveness. They will help companies achieve continuous improvement in security performance using a risk-based approach to identify, assess and address vulnerabilities, prevent or mitigate malicious adverse scenarios, enhance training and response capabilities, and maintain and improve relationships with key stakeholders and authorities.

The results obtained will be also the starting point for future developments aimed at expanding the scope of the proposed methods, at the probabilistic assessment and modeling of the dynamics of IACS (Industrial Automation and Control Systems such as BPCS and SIS) when targeted by cyber-attacks, and at the assessment of system resilience (the ability to plan and prepare for, absorb, recover from, and more

successfully adapt to disruptive events) against deliberate malicious attacks to chemical, process, and Oil&Gas facilities.

References

[1] Landucci G, Reniers G. Preface to special issue on quantitative security analysis of industrial facilities. Reliab Eng Syst Saf 2019;191:106611. https://doi.org/10.1016/j.ress.2019.106611.

[2] Iaiani M, Casson Moreno V, Reniers G, Tugnoli A, Cozzani V. Analysis of events involving the intentional release of hazardous substances from industrial facilities. Reliab Eng Syst Saf 2021;212. https://doi.org/10.1016/j.ress.2021.107593.

[3] Ackerman G, Abhayaratne P, Bale J, Bhattacharjee A, Blair C, Hansell L, et al. Assessing Terrorist Motivations for Attacking Critical Infrastructure. 2007.

[4] Nolan DP. Safety and securiy review for the process industries 2008.

[5] U.S. Department of Justice. Department of justice assessment of the increased risk of terrorist or other criminal activity associated with posting off-site consequence analysis information on the internet 2000.

[6] North America Oil & Gas Pipelines. Discussing the Role of Cyber Security in Oil and Gas Pipelines 2013.

[7] Garcia ML. The Design and Evolution of Physical Protection Systems. 2nd ed. Butterworth-Heinemann; 2007.

[8] eMARS database 2022. https://emars.jrc.ec.europa.eu/en/emars/content (accessed December 23, 2020).

[9] The ARIA Database - La référence du retour d'expérience sur accidents technologiques 2022. https://www.aria.developpement-durable.gouv.fr/the-barpi/the-aria-database/?lang=en (accessed December 8, 2020).

[10] Lee RM, Assante MJ, Conway T. ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack. 2014.

[11] Bing C, Kelly S. Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed | Reuters. Reuters 2021. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ (accessed October 13, 2022).

[12] Robertson J, Turton W. Colonial Hackers Stole Data Thursday Ahead of Shutdown - Bloomberg. Bloom News 2021. https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown (accessed October 13, 2022).

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

[14] Thomas HW, Day J. Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process. 49th Annu. Loss Prev. Symp. 2015, LPS 2015 - Top. Conf. 2015 AIChE Spring Meet. 11th Glob. Congr. Process Saf., 2015, p. 360–78.

[15] Casson Moreno V, Reniers G, Salzano E, Cozzani V. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf Environ Prot 2018;116:621–31. https://doi.org/10.1016/j.psep.2018.03.026.

[16] Iaiani M, Musayev N, Tugnoli A, Macini P, Cozzani V, Mesini E. Analysis of Security Threats for Offshore Oil&gas Operations. Chem Eng Trans 2021;86:319–24. https://doi.org/10.3303/CET2186054.

[17] Iaiani M, Moreno VC, Tugnoli A, Cozzani V. Analysis of security-related events in the chemical and process industry. Proc. 30th Eur. Saf. Reliab. Conf. 15th Probabilistic Saf. Assess. Manag. Conf., 2020.

https://doi.org/10.3850/978-981-14-8593-0_5761-cd.

[18] Responsible Care®: Driving Safety & Industry Performance n.d. https://www.americanchemistry.com/chemistry-in-america/responsible-care-driving-safety-industry-performance (accessed September 7, 2022).

[19] Mannan S. Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control. 4th ed. UK: Butterworth-Heinemann: Elsevier; 2012.

[20] Schierow L. CRS Report RL31530, Chemical Facility Security. 2006.

[21] Department of Homeland Security. Chemical Facility Anti-Terrorism Standards (CFATS) 2017.

[22] European Council. Council directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. Off J Eur Union 1997;L010/97:1–38.

[23] European Parliament and Council. Directive 2003/105/EC of the European Parliament and of the Council of 16 December 2003 amending council directive 96/82/EC on the control of major-accident hazards involving dangerous substances. Off J Eur Union 2003;L345:97–105.

[24] European Parliament and Council. Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing council directive 96/82/EC text with EEA relevance. Off J Eur Union 2012;L197:1–37.

[25] Commission of the European Communities. Communication from the Commission on a European Programme for Critical Infrastructure Protection. 2006.

[26] Department of Homeland Security. Homeland Security Act of 2002. Public Law 107–296—Nov 25 2002.

[27] European Council. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of Eurpean critical infrastructures and the assessment of the need to improve their protection. Off J Eur Commun 2008;L345:75–82.

[28] European Parliament and Council. Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC. Off J Eur Commun 2013;L178:66–106.

[29] Matteini A, Argenti F, Salzano E, Cozzani V. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab Eng Syst Saf 2019;191:106083. https://doi.org/10.1016/j.ress.2018.03.001.

[30] Landoll D. Security risk assessment handbook: a completeguide for performing security risk assessments. 2nd ed. CRC Press; 2011.

[31] Anthony L, Cox T. Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. Risk Anal 2008;28:1749–61. https://doi.org/10.1111/J.1539-6924.2008.01142.X.

[32] Amundrud Ø, Aven T, Flage R. How the definition of security risk can be made compatible with safety definitions. J Risk Reliab 2017;231:286–94. https://doi.org/10.1177/1748006X17699145.

[33] Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y. A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst Saf 2015;139:156–78. https://doi.org/10.1016/J.RESS.2015.02.008.

[34] Landucci G, Argenti F, Cozzani V, Reniers G. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf Environ Prot 2017;110:102–14. https://doi.org/10.1016/j.psep.2017.06.019.

[35] American Petroleum Institute (API). API RP 780 - Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries 2013.

[36] Baybutt P. Issues for security risk assessment in the process industries. J Loss Prev Process Ind 2017;49:509–18. https://doi.org/10.1016/J.JLP.2017.05.023.

[37] Einarsson S, Rausand M. An Approach to Vulnerability Analysis of Complex Industrial Systems. Risk Anal 1998 185 1998;18:535–46. https://doi.org/10.1023/B:RIAN.0000005928.84074.E4.

[38] Department of Homeland Security. Vulnerability Assessment Methodologies Report. Washington: Office for Domestic Preparedness: 2003.

[39] Center of Chemical Process Safety (CCPS). Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. New York: Wiley/AIChE; 2003.

[40] Jaeger CD. Vulnerability assessment methodology for chemical facilities (VAM-CF). Chem Heal Saf 2002;9:15–9. https://doi.org/10.1016/S1074-9098(02)00389-1.

[41] American Petroleum Institute (API). API RP 70 - Security for Offshore Oil and Natural Gas Operations 2010.

[42] American Petroleum Institute (API). API RP 70I - Security for Worldwide Offshore Oil and Natural Gas Operations 2012.

[43] Moore DA, Fuller B, Hazzan M, Jones JW. Development of a security vulnerability assessment process for the RAMCAP chemical sector. J Hazard Mater 2007;142:689–94.

[44] Störfall-Kommission (SFK). SFK–GS–38 - Combating Interference by Unauthorised Persons 2002.

[45] International Society of Automation (ISA) and International Electrotechnical Commission (IEC). ISA/IEC 62443-3-2: Security for industrial automation ando control systems 2020.

[46] Bajpai S, Gupta JP. Site security for chemical process industries. J. Loss Prev. Process Ind., vol. 18, Elsevier; 2005, p. 301–9. https://doi.org/10.1016/j.jlp.2005.06.011.

[47] Bajpai S, Gupta JP. Terror-proofing chemical process industries. Process Saf Environ Prot 2007;85:559–65. https://doi.org/10.1205/psep06046.

[48] van Staalduinen MA, Khan F, Gadag V, Reniers G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. Reliab Eng Syst Saf 2017;157:23–34. https://doi.org/10.1016/j.ress.2016.08.014.

[49] Talarico L, Reniers G, Sörensen K, Springael J. MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. Reliab Eng Syst Saf 2015;138:105–14. https://doi.org/10.1016/J.RESS.2015.01.022.

[50] Argenti F, Landucci G, Spadoni G, Cozzani V. The assessment of the attractiveness of process facilities to terrorist attacks. Saf Sci 2015;77:169–81. https://doi.org/10.1016/j.ssci.2015.02.013.

[51] Argenti F, Landucci G, Reniers G, Cozzani V. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. Reliab Eng Syst Saf 2018;169:515–30. https://doi.org/10.1016/j.ress.2017.09.023.

[52] Rezazadeh A, Talarico L, Reniers G, Cozzani V, Zhang L. Applying game theory for securing oil and gas pipelines against terrorism. Reliab Eng Syst Saf 2019;191:106140. https://doi.org/10.1016/J.RESS.2018.04.021.

[53] Feng Q, Cai H, Chen Z. Using game theory to optimize the allocation of defensive resources on a city scale to protect chemical facilities against multiple types of attackers. Reliab Eng Syst Saf 2019;191:105900. https://doi.org/10.1016/j.ress.2017.07.003.

[54] Misuri A, Khakzad N, Reniers G, Cozzani V. A Bayesian network methodology for optimal security management of critical infrastructures. Reliab Eng Syst Saf 2019;191:106112. https://doi.org/10.1016/j.ress.2018.03.028.

[55] Chen C, Reniers G, Khakzad N. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach. Reliab Eng Syst Saf 2019;191:106470. https://doi.org/10.1016/j.ress.2019.04.023.

[56] Khakzad N, Reniers G. Low-capacity utilization of process plants: A cost-robust approach to tackle man-made domino effects. Reliab Eng Syst Saf 2019;191:106114. https://doi.org/10.1016/J.RESS.2018.03.030.

[57] Zhang L, Reniers G, Qiu X. Playing chemical plant protection game with distribution-free uncertainties. Reliab Eng Syst Saf 2019;191:105899. https://doi.org/10.1016/J.RESS.2017.07.002.

[58] Abdo H, Kaouk M, Flaus JM, Masse F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. Comput Secur 2018;72:175–95. https://doi.org/10.1016/j.cose.2017.09.004.

[59] Hashimoto Y, Toyoshima T, Yogo S, Koike M, Hamaguchi T, Jing S, et al. Safety securing approach against cyber-attacks for process control system. Comput Chem Eng 2013;57:181–6. https://doi.org/10.1016/j.compchemeng.2013.04.019.

[60] Cusimano J, Rostick P. If It Isn't Secure, It Isn't Safe: Incorporating Cybersecurity into Process Safety. AIChE Spring Meet Glob Congr Process Saf 2018.

[61] Baybutt P. On the completeness of scenario identification in process hazard analysis (PHA). J Loss Prev Process Ind 2018;55:492–9. https://doi.org/10.1016/J.JLP.2018.05.010.

[62] Kashubsky M. A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975 – 2010. Perspect Terror 2011;5:139–67.

[63] Karmon E. The Risk of Terrorism Against Oil and Gas Pipelines in Central Asia 2002 2002.

[64] Cisco. Cisco 2018 Annual Cybersecurity Report 2018.

[65] Vaidya T. 2001-2013: Survey and Analysis of Major Cyberattacks 2015:1–25.

[66] Ogie R. Cyber Security Incidents on Critical Infrastructure and Industrial Networks. Proc 9th Int Conf Comput Autom Eng 2017:254–8. https://doi.org/https://doi.org/10.1145/3057039.3057076.

[67] Miller B, Rowe DC. A survey of SCADA and critical infrastructure incidents. RIIT'12 - Proc. ACM Res. Inf. Technol., 2012, p. 51–6. https://doi.org/10.1145/2380790.2380805.

[68] Lezzi M, Lazoi M, Corallo A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Comput Ind 2018;103:97–110. https://doi.org/10.1016/J.COMPIND.2018.09.004.

[69] Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of cyber-warfare. Comput Secur 2012;31:418–36. https://doi.org/10.1016/j.cose.2012.02.009.

[70] Pollutions B for A of IR and P (BARPI). Cybersecurity in industry - ARIA report. 2016.

[71] Willems E. Cyber-terrorism in the process industry. Comput Fraud Secur 2011;2011:16–9. https://doi.org/10.1016/S1361-3723(11)70032-X.

[72] Kjaerland M. A taxonomy and comparison of computer security incidents from the commercial and government sectors. Comput Secur 2006;25:522–38. https://doi.org/10.1016/j.cose.2006.08.004.

[73] Churchwell JS, Zhang KS, Saleh JH. Epidemiology of helicopter accidents: Trends, rates, and covariates. Reliab Eng Syst Saf 2018;180:373–84. https://doi.org/10.1016/j.ress.2018.08.007.

[74] Konstandinidou M, Nivolianitou Z, Kefalogianni E, Caroni C. In-depth analysis of the causal factors of incidents reported in the Greek petrochemical industry. Reliab Eng Syst Saf 2011;96:1448–55. https://doi.org/10.1016/j.ress.2011.07.010.

[75] Lam CY, Tai K. Network topological approach to modeling accident causations and characteristics: Analysis of railway incidents in Japan. Reliab Eng Syst Saf 2020;193:106626. https://doi.org/10.1016/j.ress.2019.106626.

[76] Milch V, Laumann K. The influence of interorganizational factors on offshore incidents in the Norwegian petroleum industry: Challenges and future directions. Reliab Eng Syst Saf 2019;181:84–96. https://doi.org/10.1016/j.ress.2018.09.002.

[77] Tauseef SM, Abbasi T, Abbasi SA. Development of a new chemical process-industry accident database to assist in past accident analysis. J Loss Prev Process Ind 2011;24:426–31. https://doi.org/10.1016/j.jlp.2011.03.005.

[78] Jung S, Woo J, Kang C. Analysis of severe industrial accidents caused by hazardous chemicals in South Korea from January 2008 to June 2018. Saf Sci 2020;124:104580. https://doi.org/10.1016/j.ssci.2019.104580.

[79] Gunasekera MY, de Alwis AAP. Process industry accidents in Sri Lanka: Analysis and basic lessons learnt. Process Saf Environ Prot 2008;86:421–6. https://doi.org/10.1016/j.psep.2008.05.002.

[80] Sales J, Mushtaq F, Christou MD, Nomen R. Study of major accidents involving chemical reactive substances analysis and lessons learned. Process Saf Environ Prot 2007;85:117–24. https://doi.org/10.1205/psep06012.

[81] Fu G, Xie X, Jia Q, Tong W, Ge Y. Accidents analysis and prevention of coal and gas outburst: Understanding human errors in accidents. Process Saf Environ Prot 2020;134:1–23. https://doi.org/10.1016/j.psep.2019.11.026.

[82] Zhang J, Cliff D, Xu K, You G. Focusing on the patterns and characteristics of extraordinarily severe gas explosion accidents in Chinese coal mines. Process Saf Environ Prot 2018;117:390–8. https://doi.org/10.1016/j.psep.2018.05.002.

[83] Byres EJ, Franz M, Miller D. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. Proc Int Infrastruct Surviv Work 2004.

[84] Gertman D, Folkers R, Roberts J. Scenario-based approach to risk analysis in support of cyber security. Proc 5th Int Top Meet Nucl Plant Instrum Control Hum Mach Interface Technol 2006.

[85] Beggs C, Warren M. Safeguarding Australia from Cyber-terrorism : A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption Keywords. Proc 10th Aust Inf Warf Secur Conf Ed Cowan Univ Perth West Aust 2009. https://doi.org/10.4018/978-1-4666-0197-0.ch021.

[86] Song JG, Lee JW, Lee CK, Kwon KC, Lee DY. A cyber security risk assessment for the design of L&C systems in nuclear power plants. Nucl Eng Technol 2012;44:919–28. https://doi.org/10.5516/NET.04.2011.065.

[87] Guan J, Graham J, Hieb J. A digraph model for risk identification and mangement in SCADA systems. Proc. 2011 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2011, 2011. https://doi.org/10.1109/ISI.2011.5983990.

[88] Khakzad N, Khan F, Amyotte P. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliab Eng Syst Saf 2011;96:925–32. https://doi.org/10.1016/J.RESS.2011.03.012.

[89] Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into

Bayesian network. Process Saf Environ Prot 2013;91:46–53. https://doi.org/10.1016/J.PSEP.2012.01.005.

[90] Jon MH, Kim YP, Choe U. Determination of a safety criterion via risk assessment of marine accidents based on a Markov model with five states and MCMC simulation and on three risk factors. Ocean Eng 2021;236:109000. https://doi.org/10.1016/J.OCEANENG.2021.109000.

[91] Leoni L, BahooToroody A, Abaei MM, De Carlo F, Paltrinieri N, Sgarbossa F. On hierarchical bayesian based predictive maintenance of autonomous natural gas regulating operations. Process Saf Environ Prot 2021;147:115–24. https://doi.org/10.1016/J.PSEP.2020.08.047.

[92] Khakzad N, Khan F, Paltrinieri N. On the application of near accident data to risk analysis of major accidents. Reliab Eng Syst Saf 2014;126:116–25. https://doi.org/10.1016/J.RESS.2014.01.015.

[93] Khakzad N, Khakzad S, Khan F. Probabilistic risk assessment of major accidents: application to offshore blowouts in the Gulf of Mexico. Nat Hazards 2014;74:1759–71. https://doi.org/10.1007/s11069-014-1271-8.

[94] Li Z, Hu S, Gao G, Yao C, Fu S, Xi Y. Decision-making on process risk of Arctic route for LNG carrier via dynamic Bayesian network modeling. J Loss Prev Process Ind 2021;71:104473. https://doi.org/10.1016/J.JLP.2021.104473.

[95] Badr A, Yosri A, Hassini S, El-Dakhakhni W. Coupled Continuous-Time Markov Chain–Bayesian Network Model for Dam Failure Risk Prediction. J Infrastruct Syst 2021;27:04021041. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000649.

[96] Hausken K. Security Investment, Hacking, and Information Sharing between Firms and between Hackers. Games 2017;8:23. https://doi.org/10.3390/g8020023.

[97] International Electrotechnical Commission (IEC). IEC 61882 standard: Hazard and operability studies (HAZOP studies) - Application guide 2016.

[98] International Electrotechnical Commission (IEC). IEC 60812 standard: Failure modes and effects analysis (FMEA and FMECA). 2018.

[99] Delvosalle C, Fievez C, Pipart A, Debray B. ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. J Hazard Mater 2006;130:200–19. https://doi.org/10.1016/J.JHAZMAT.2005.07.005.

[100] Iaiani M, Tugnoli A, Macini P, Cozzani V. Outage and asset damage triggered by malicious manipulation of the control system in process plants. Reliab Eng Syst Saf 2021;213:107685. https://doi.org/10.1016/J.RESS.2021.107685.

[101] Iaiani M, Tugnoli A, Bonvicini S, Cozzani V. Major accidents triggered by malicious manipulations of the control system in process facilities. Saf Sci 2021;134:105043. https://doi.org/10.1016/J.SSCI.2020.105043.

[102] Carreras Guzman NH, Kozine I, Lundteigen MA. An integrated safety and security analysis for cyber-physical harm scenarios. Saf Sci 2021;144:105458. https://doi.org/10.1016/J.SSCI.2021.105458.

[103] Landucci G, Reniers G, Cozzani V, Salzano E. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliab Eng Syst Saf 2015;143:53–62. https://doi.org/10.1016/j.ress.2015.03.004.

[104] Dusso A, Grimaz S, Salzano E. Quick assessment of fire hazard in chemical and pharmaceutical warehouses. Chem Eng Trans 2016;48:325–30. https://doi.org/10.3303/CET1648055.

[105] Li Y, Jiang J, Yu Y, Wang Z, Xing Z, Zhang Q. Fire resistance of a vertical oil tank exposed to pool-fire heat radiation after high-velocity projectile impact. Process Saf Environ Prot 2021;156:231–43.

https://doi.org/10.1016/j.psep.2021.10.013.

[106] Li X, Liao K, He G, Zhao J. Influence of blunt-nose and conical fragment on domino accident probability in spherical-tank area. Process Saf Environ Prot 2021;146:800–10. https://doi.org/10.1016/j.psep.2020.12.014.

[107] Scarponi GE, Tugnoli A, Cozzani V. 5. Projectile (missile) driven domino effect. In: Khan F, editor. Domino Eff. Its Predict. Prev. 1st ed., Academic Press; 2021.

[108] Chen XW, Li QM. Deep penetration of a non-deformable projectile with different geometrical characteristics. Int J Impact Eng 2002;27:619–37. https://doi.org/10.1016/S0734-743X(02)00005-2.

[109] Anderson CE. Analytical models for penetration mechanics: A Review. Int J Impact Eng 2017;108:3–26. https://doi.org/10.1016/j.ijimpeng.2017.03.018.

[110] Chen XW, Huang XL, Liang GJ. Comparative analysis of perforation models of metallic plates by rigid sharp-nosed projectiles. Int J Impact Eng 2011;38:613–21. https://doi.org/10.1016/j.ijimpeng.2010.12.005.

[111] Kohout A, Jain P, Dick W. Review, identification and analysis of local impact of projectile hazards in the LNG industry. J Loss Prev Process Ind 2019;57:304–19. https://doi.org/10.1016/j.jlp.2018.07.018.

[112] Stewart MG, Netherton MD. Statistical variability and fragility assessment of ballistic perforation of steel plates for 7.62 mm AP ammunition. Def Technol 2020;16:503–13. https://doi.org/10.1016/j.dt.2019.10.013.

[113] Goldsmith W. Non-ideal projectile impact on targets. Int J Impact Eng 1999;22:95–395. https://doi.org/10.1016/S0734-743X(98)00031-1.

[114] Backman ME, Goldsmith W. The mechanics of penetration of projectiles into targets. Int J Eng Sci 1978;16:1–99. https://doi.org/10.1016/0020-7225(78)90002-2.

[115] US Department of Defense. UFC 4-023-07. Design to resist Direct Fire weapons effects. 2017.

[116] Schonberg W, Ryan S. Predicting metallic armour performance when impacted by fragment-simulating projectiles – model review and assessment. Int J Impact Eng 2021;158:104025. https://doi.org/10.1016/j.ijimpeng.2021.104025.

[117] Schonberg W, Ryan S. Predicting metallic armour performance when impacted by fragment-simulating projectiles – Model adjustments and improvements. Int J Impact Eng 2022;161:104090. https://doi.org/10.1016/j.ijimpeng.2021.104090.

[118] Lecysyn N, Dandrieux A, Heymes F, Aprin L, Slangen P, Munier L, et al. Ballistic impact on an industrial tank: Study and modeling of consequences. J Hazard Mater 2009;172:587–94. https://doi.org/10.1016/j.jhazmat.2009.07.086.

[119] Lecysyn N, Bony-Dandrieux A, Aprin L, Heymes F, Slangen P, Dusserre G, et al. Experimental study of hydraulic ram effects on a liquid storage tank: Analysis of overpressure and cavitation induced by a high-speed projectile. J Hazard Mater 2010;178:635–43. https://doi.org/10.1016/j.jhazmat.2010.01.132.

[120] Gyenes Z, Wood MH, Struckl M. Handbook of Scenarios for Assessing Major Chemical Accident Risks, EUR 28518. 2017. https://doi.org/10.2760/884152.

[121] Tugnoli A, Gyenes Z, Van Wijk L, Christou M, Spadoni G, Cozzani V. Reference criteria for the identification of accident scenarios in the framework of land use planning. J Loss Prev Process Ind 2013;26:614–27. https://doi.org/10.1016/j.jlp.2012.12.004.

[122] Ylönen M, Tugnoli A, Oliva G, Heikkilä J, Nissilä M, Iaiani M, et al. Integrated management of safety

and security in Seveso sites - sociotechnical perspectives. Saf Sci 2022;151. https://doi.org/10.1016/j.ssci.2022.105741.

[123] Gilligan JM. Expertise Across Disciplines: Establishing Common Ground in Interdisciplinary Disaster Research Teams. Risk Anal 2021;41:1171–7. https://doi.org/10.1111/RISA.13407.

[124] Chen C, Yang M, Reniers G. A dynamic stochastic methodology for quantifying HAZMAT storage resilience. Reliab Eng Syst Saf 2021;215:107909. https://doi.org/10.1016/J.RESS.2021.107909.

[125] Abimbola M, Khan F. Resilience modeling of engineering systems using dynamic object-oriented Bayesian network approach. Comput Ind Eng 2019;130:108–18. https://doi.org/10.1016/J.CIE.2019.02.022.

[126] Hausken K. Cyber resilience in firms, organizations and societies. Internet of Things 2020;11:100204. https://doi.org/10.1016/j.iot.2020.100204.

[127] Bostick TP, Connelly EB, Lambert JH, Linkov I. Resilience science, policy and investment for civil infrastructure. Reliab Eng Syst Saf 2018;175:19–23. https://doi.org/10.1016/j.ress.2018.02.025.

[128] Cutter SL, Ahearn JA, Amadei B, Crawford P, Eide EA, Galloway GE, et al. Disaster Resilience: A National Imperative. Environ Sci Policy Sustain Dev 2013;55:25–9. https://doi.org/10.1080/00139157.2013.768076.

[129] Leveson N. SafeWare: System safety and computers. Reading (USA): Addison-Wesley; 1995.

[130] Pietre-Cambacedes L, Bouissou M. Cross-fertilization between safety and security engineering. Reliab Eng Syst Saf 2013;110:110–26. https://doi.org/10.1016/j.ress.2012.09.011.

[131] Sørby K. Relationship between security and safety in a security-safety critical system: Safety consequences of security threats. MSc Thesis 2003.

[132] Ji Z, Yang SH, Cao Y, Wang Y, Zhou C, Yue L, et al. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Saf Environ Prot 2021;148:1279–91. https://doi.org/10.1016/j.psep.2021.03.004.

[133] Pearl J. Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann; 1988. https://doi.org/10.1016/C2009-0-27609-4.

[134] Charniak E. Bayesian Networks without tears. Artif Intell Mag 1991;12:50–63.

[135] Fenton N, Neil M. Risk Assessment and Decision Analysis with Bayesian Networks. 2nd ed. CRC Press/Taylor & Francis Group; 2019.

[136] Rathnayaka S, Khan F, Amyotte P. SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. Process Saf Environ Prot 2011;89:151–64. https://doi.org/10.1016/j.psep.2011.01.002.

[137] Dechema ProcessNET 2022.

[138] Concawe 2022. https://www.concawe.eu/ (accessed December 23, 2020).

[139] E.U. EGIG 2022. https://www.egig.eu/about-egig (accessed December 23, 2020).

[140] Global Terrorism Database (GTD) 2020. https://start.umd.edu/data-tools/global-terrorism-database-gtd (accessed December 8, 2020).

[141] Deutsch Umwelt Bundesamt. Infosis ZEMA 2022. https://www.infosis.uba.de/index.php/de/site/12981/zema/index.html (accessed December 23, 2020).

[142] The Repository of Industrial Security Incidents (RISI) 2015. https://www.risidata.com/Database (accessed December 8, 2020).

[143] United States Department of Transportation (U.S. DoT). PHMSA database 2022. https://www.phmsa.dot.gov/ (accessed December 23, 2020).

[144] Significant Cyber Incidents | Center for Strategic and International Studies n.d. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed December 8, 2020).

[145] Tukey JW. Exploratory Data Analysis. Addison-Wesley; 1977.

[146] Greenacre M. Correspondence Analysis in Practice. 3rd ed. New York: Chapman and Hall/CRC; 2017.

[147] Lorenzo-Seva U, van de Velden M, Kiers HAL. Car: A MATLAB package to compute correspondence analysis with rotations. J Stat Softw 2009;31:1–14. https://doi.org/10.18637/jss.v031.i08.

[148] Paltrinieri N, Tugnoli A, Bonvicini S, Cozzani V. Atypical Scenarios Identification by the DyPASI Procedure: Application to LNG. Icheap-10 10th Int Conf Chem Process Eng Pts 1-3 2011;24:1171–6. https://doi.org/Doi 10.3303/Cet1124196.

[149] Wilson PF, Dell LD, Anderson GF, Gaylord F. Root Cause Analysis: A Tool for Total Quality Management. Milwaukee: Wisconsin: ASQ Quality Press; 1993.

[150] International Electrotechnical Commission (IEC). IEC 62740: Root Cause Analysis (RCA) 2015.

[151] Safe Work Australia. Incident Reporting 2008.

[152] Health and Safety Executive (HSE). RIDDOR - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 2003.

[153] UNIDO - United Nations Industrial Development Organization. INDSTAD 2 2019, ISIC Revision 3 database 2019.

[154] Center for Chemical Process Safety (CCPS). Guidelines for investigating chemical process incidents 2003.

[155] Hubbard B, Karasz P, Reed S. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. New York Times 2019.

[156] Ethical Hacking - Phases of Hacking. Comput Sci n.d. http://cybersecurity.jhigh.co.uk/ethicalHacking/attackPhases.html (accessed July 18, 2019).

[157] FootPrinting-First Step Of Ethical Hacking. EhackingNet n.d. https://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html (accessed July 18, 2019).

[158] Peter T. Snowden confirms NSA created Stuxnet with Israeli aid 2013.

[159] Appelbaum J, Potras L. The NSA and Its Willing Helpers. Edward Snowden Interview. 2013.

[160] Equation = NSA? Researchers Uncloak Huge “American Cyber Arsenal” n.d. https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber-tool-treasure-chest/?sh=11266ddb417f (accessed December 9, 2020).

[161] Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets | CISA n.d. https://us-cert.cisa.gov/ncas/alerts/aa20-296a (accessed December 9, 2020).

[162] Winnti. More than just a game | Securelist n.d. https://securelist.com/winnti-more-than-just-a-game/37029/ (accessed December 9, 2020).

[163] PARK JIN HYOK — FBI n.d. https://www.fbi.gov/wanted/cyber/park-jin-hyok (accessed December 9,

2020).

[164] Paulsen C, Byers R. NISTIR 7298 Rev. 3: Glossary of Key Information Security Terms 2019. https://doi.org/10.6028/NIST.IR.7298r3.

[165] Rouse M. Definition: privilege escalation attack. SearchSecurity n.d. https://searchsecurity.techtarget.com/definition/privilege-escalation-attack.

[166] Boudriga N. Security of mobile communications. Boca Raton: CRC Press.; 2010.

[167] Falliere N, O Murchu L, Chien E. W32.Stuxnet Dossier 2011.

[168] Iaiani M, Tugnoli A, Cozzani V. Cyber Threats Affecting the Process Industry and Similar Sectors. Proc 31th Eur Saf Reliab Conf 2021.

[169] Maritime Safety Information (MSI) 2021. https://msi.nga.mil/Piracy (accessed February 24, 2021).

[170] Jin M, Shi W, Lin KC, Li KX. Marine piracy prediction and prevention: Policy implications. Mar Policy 2019;108:103528. https://doi.org/10.1016/j.marpol.2019.103528.

[171] Peters BC. Nigerian piracy: Articulating business models using crime script analysis. Int J Law, Crime Justice 2020;62:100410. https://doi.org/10.1016/j.ijlcj.2020.100410.

[172] European Committee for Standardization (CEN). BS EN 1522: Windows, doors, shutters and blinds - Bullet resistance - Requirements and classification 1999.

[173] European Committee for Standardization (CEN). EN 1063: Glass in building - Security glazing - Testing and classification od resistance against bullet attack 2019.

[174] DIN VDE V 0831-104: Electric signalling systems for railways - Part 104: IT Security Guideline based on IEC 62443. 2015.

[175] Iaiani M, Tugnoli A, Salzano E, Cozzani V, Landucci G. A systematic procedure for the identification of major accident hazards induced by malicious manipulations of the control and safety instrumented systems. Proc. 30th Eur. Saf. Reliab. Conf. 15th Probabilistic Saf. Assess. Manag. Conf., 2020. https://doi.org/10.3850/978-981-14-8593-0_5338-cd.

[176] Iaiani M. Obiettivi, fasi e modalità di un attacco cibernetico ai sistemi di controllo e si-curezza automatizzati. Metodologia sistematica per l'analisi di cyber secu-rity degli impianti di processo. Alma Mater Studiorum - University of Bologna, 2019.

[177] Taiola M. Cybersecurity in impianti dell'industria di processo. Alma Mater Studiorum - University of Bologna, 2021.

[178] Tugnoli A, Landucci G, Salzano E, Cozzani V. Supporting the selection of process and plant design options by Inherent Safety KPIs. J Loss Prev Process Ind 2012;25:830–42. https://doi.org/10.1016/j.jlp.2012.03.008.

[179] Tugnoli A, Cozzani V, Landucci G. A consequence based approach to the quantitative assessment of inherent safety. AIChE J 2007;53:3171–82. https://doi.org/10.1002/aic.11315.

[180] Khan FI, Husain T, Abbasi SA. Safety weighted Hazard Index (SWeHI). A New, User-Friendly Tool for Swift yet Comprehensive Hazard Identification and Safety Evaluation in Chemical Process Industries. Process Saf Environ Prot 2001;79:65–80. https://doi.org/10.1205/09575820151095157.

[181] Shariff A, Leong CT, Zaini D. Using process stream index (PSI) to assess inherent safety level during preliminary design stage 2012;50:1098–103. https://doi.org/10.1016/j.ssci.2011.11.015.

[182] Dow Chemical Company. Fire & explosion index hazard classification guide. 7th ed. New York:: American Insitute of Chemical Engineers (AIChE): 1994.

[183] ICI Mond Division. The Mond Index. 2nd ed. Winnington, Nortwich, Cheshire, UK: Imperial Chemical Industries Plc, Explosion Hazards Section, Technical Department: 1985.

[184] Tyler BJ. Using the Mond Index to Measure Inherent Hazards. Plant/Operations Prog 1985;4:172–5. https://doi.org/doi:10.1002/prsb.720040313.

[185] American Petroleum Institute (API). API standard 581: Risk-Based Inspection Technology 2016.

[186] Uijt de Haag PAM, Ale BJM. Guidelines for quantitative risk assessment (TNO Purple Book). The Hague (NL): Committee for the Prevention of Disasters; 2005.

[187] Paltrinieri N, Tugnoli A, Buston J, Wardman M, Cozzani V. Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. J Loss Prev Process Ind 2013;26:683–95. https://doi.org/https://doi.org/10.1016/j.jlp.2013.01.006.

[188] Delvosalle C, Fiévez C, Pipart A. ARAMIS D1C - Appendix 4: Generic fault trees. 2004.

[189] Kletz T. Process Plants: A Handbook for Inherent Safer Design. 2nd ed. Philadelphia, PA: 1998.

[190] Meier F, Meier C. Valve fail action 2008.

[191] Delvosalle C, Fiévez C, Pipart A. ARAMIS D1C - Appendix 3: Method to associate critical events and relevant hazardpus equipment. 2004.

[192] American Petroleum Institute (API). Pressure-Relieving and Depressuring Systems (API standard 521) 2014.

[193] American Petroleum Institute (API). Sizing, Selection, and Installation of Pressure-relieving Devices (API standard 520) 2013.

[194] American Petroleum Institute (API). Flanged Steel Pressure-relief Valves (API standard 526) 2017.

[195] Baybutt P. Guidelines for designing risk matrices. Process Saf Prog 2018;37:49–55. https://doi.org/10.1002/prs.11905.

[196] Center for Chemical Process Safety (CCPS). Process Safety Leading and Lagging Metrics. “You don’t improve rhat you don’t measure”. 2011.

[197] Hausken K. A cost–benefit analysis of terrorist attacks. Def Peace Econ 2018;29:111–29. https://doi.org/10.1080/10242694.2016.1158440.

[198] Hausken K, Levitin G. Minmax defense strategy for complex multi-state systems. Reliab Eng Syst Saf 2009;94:577–87. https://doi.org/10.1016/j.ress.2008.06.005.

[199] Bschir K. Risk, Uncertainty and Precaution in Science: The Threshold of the Toxicological Concern Approach in Food Toxicology. Sci Eng Ethics 2017;23:489–508. https://doi.org/10.1007/s11948-016-9773-2.

[200] Koch FH, Yemshanov D, McKenney DW, Smith WD. Evaluating critical uncertainty thresholds in a spatial model of forest pest invasion risk. Risk Anal 2009;29:1227–41. https://doi.org/10.1111/j.1539-6924.2009.01251.x.

[201] Hausken K. The precautionary principle as multi-period games where players have different thresholds for acceptable uncertainty. Reliab Eng Syst Saf 2021;206:107224. https://doi.org/10.1016/j.ress.2020.107224.

[202] Cullen A, Armitage L. A human vulnerability assessment methodology. 2018 Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, CyberSA 2018, Institute of Electrical and Electronics Engineers Inc.; 2018. https://doi.org/10.1109/CyberSA.2018.8551371.

[203] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27005: Information technology - Security techniques - Information security risk management 2018.

[204] Center for Chemical Process Safety (CCPS). CCPS Process Safety Glossary 2022. https://www.aiche.org/ccps/resources/glossary.

[205] Pert AD, Baron MG, Birkett JW. Review of Analytical Techniques for Arson Residues. J Forensic Sci 2006;51:1033–49. https://doi.org/10.1111/j.1556-4029.2006.00229.x.

[206] valkyrie.pro. VALKYRIE HEAVY PRO New 2019 - datasheet 2019. https://www.valkyrie.pro/ (accessed July 13, 2021).

[207] Cozzani V, Tugnoli A, Bonvicini S, Salzano E. Threshold-Based Approach. Domino Eff. Process Ind. Model. Prev. Manag., Elsevier B.V.; 2013, p. 189–207. https://doi.org/10.1016/B978-0-444-54323-3.00009-9.

[208] Cozzani V, Salzano E. Threshold values for domino effects caused by blast wave interaction with process equipment. J Loss Prev Process Ind 2004;17:437–47. https://doi.org/10.1016/j.jlp.2004.08.003.

[209] Cozzani V, Gubinelli G, Salzano E. Escalation thresholds in the assessment of domino accidental events. J Hazard Mater 2006;129:1–21. https://doi.org/10.1016/j.jhazmat.2005.08.012.

[210] Bounds W. Design of blast resistant buildings in petrochemical facilities. Reston, VA, USA: ASCE Publications; 1997.

[211] Mudan KS. Thermal radiation hazards from hydrocarbon pool fires. Prog Energy Combust Sci 1984;10:59–80. https://doi.org/10.1016/0360-1285(84)90119-9.

[212] Raj PK. LNG fires: A review of experimental results, models and hazard prediction challenges. J Hazard Mater 2007;140:444–64. https://doi.org/10.1016/j.jhazmat.2006.10.029.

[213] Bagster D, Pitablado R. Thermal hazards in the process industry. Chem Eng Prog 1989;85:69–75.

[214] Van Den Bosh, C.J.H. Weterings RAPM. Methods for the calculation of physical effects (Yellow Book). 3rd ed. The Hague (NL): Committee for the Prevention of Disasters; 2005.

[215] Rosenberg Z, Dekel E. Terminal ballistics. 2nd ed. Springer; 2016. https://doi.org/10.1007/978-3-030-46612-1.

[216] Crouch IG. The Science of Armour Materials 2017.

[217] Hazell PJ. Armour: Materials, Theory, and Design. CRC Press; 2015.

[218] Iaiani M, Sorichetti R, Tugnoli A, Cozzani V. Projectile perforation models for the vulnerability assessment of atmospheric storage tanks. Process Saf Environ Prot 2022;161:231–46. https://doi.org/10.1016/j.psep.2022.03.025.

[219] Ullmann's Encyclopedia. Ullmann's Encyclopedia of Industrial Chemistry. 7th ed. Wiley-VCH; 2011.

[220] Iaiani M, Tugnoli A, Cozzani V. Identification of reference scenarios for security attacks to the process industry. Process Saf Environ Prot 2022;161:334–56. https://doi.org/10.1016/j.psep.2022.03.034.

[221] bbc.com. Drone strikes set Saudi oil facilities ablaze 2019. https://www.bbc.com/news/world-middle-east-49699429 (accessed November 6, 2020).

[222] cnbc.com. Satellite photos show extent of damage to Saudi Aramco plants 2019. https://www.cnbc.com/2019/09/17/satellite-photos-show-extent-of-damage-to-saudi-aramco-plants.html (accessed November 6, 2020).

[223] Woodward RL. The penetration of metal targets by conical projectiles. Int J Mech Sci 1978;20:349–59. https://doi.org/10.1016/0020-7403(78)90038-3.

[224] National Fire Protection Association (NFPA). NFPA 555 - Methods for Evaluating Potential for Room Flashover. 2007.

[225] Engelhard WFJM. Heat flux from fires – Chapter 6 of the "Yellow Book." The Hague (NL): Committee for the Prevention of Disasters; 2005.

[226] nytimes.com. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran 2019. https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html (accessed November 24, 2020).

[227] Rathnayaka S, Khan F, Amyotte P. Risk-based process plant design considering inherent safety. Saf Sci 2014;70:438–64. https://doi.org/10.1016/J.SSCI.2014.06.004.

[228] International Electrotechnical Commission (IEC). IEC 61025: Fault Tree Analysis (FTA) 2021.

[229] Gupta NK, Madhu V. An experimental study of normal and oblique impact of hard-core projectile on single and layered plates. Int J Impact Eng 1997;19:395–414. https://doi.org/10.1016/s0734-743x(97)00001-8.

[230] Brewer D. Applying security techniques to achieving safety. London: Springer; 1993.

[231] Firesmith D. Common concepts underlying safety security and survivability engineering 2003.

[232] American Petroleum Institute (API). API standard 650: Welded Tanks for Oil Storage. 13th ed. 2021.

[233] ASME. ASME Boiler and Pressure Vessel Code, Section VIII, Part C. 2013.

[234] Carlucci DE, Jacobson SS. Ballistics: theory and design of guns and ammunition. CRC Press/Taylor & Francis Group; 2008.

[235] European Committee for Standardization (CEN). EN 1523: Windows, doors, shutters and blinds - Bullet resistance - Test method 1999.

[236] Scazzosi R, Giglio M, Manes A. Experimental and numerical investigation on the perforation resistance of double-layered metal shields under high-velocity impact of soft-core projectiles. Eng Struct 2021;228:111467. https://doi.org/10.1016/j.engstruct.2020.111467.

[237] Holmen JK, Børvik T, Hopperstad OS. Experiments and simulations of empty and sand-filled aluminum alloy panels subjected to ballistic impact. Eng Struct 2017;130:216–28. https://doi.org/10.1016/J.ENGSTRUCT.2016.09.057.

[238] Harvey JF. Pressure Vessel Design: Nuclear and Chemical Applications. Van Nostrand Company; 1963.

[239] McCoy RL. Modern Exterior Ballistics. The Launch and Flight Dynamics of Symmetric Projectiles. Schiffer Publishing Ltd.; 2012.

[240] Børvik T, Dey S, Clausen AH. Perforation resistance of five different high-strength steel plates subjected to small-arms projectiles. Int J Impact Eng 2009;36:948–64. https://doi.org/10.1016/j.ijimpeng.2008.12.003.

[241] Chen X, Gao Y, He L. Analysis on the perforation of ductile metallic plates by APM2 bullets. Int J Prot Struct 2013;4:65–78. https://doi.org/10.1260/2041-4196.4.1.65.

[242] Callister WD, Rethwisch DG. Materials science and engineering. An indroduction. vol. 10th Editi. 2018. https://doi.org/10.1016/0025-5416(74)90116-5.

[243] Zukas J a. High Velocity Impact Dynamics 1990.

[244] Zook JA, Frank K, Silsby GF. Terminal Ballistics Test and Analysis Guidelines for the Penetration Mechanics Branch, BRL-MR-3960. 1992.

[245] Ballistic Research Laboratories. Project THOR Technincal Report No.46: The resistance of various metallic materials to perforation by steel fragments; empirical relationships for fragment residual velocity and residual weight. 1961.

[246] Crouch IG. Woodhead Publishing in Materials The Science of Armour Materials Edited by. Elsevier; 2017.

[247] Neilson AJ. Empirical equations for the perforation of mild steel plates. Int J Impact Eng 1985;3:137–42. https://doi.org/10.1016/0734-743X(85)90031-4.

[248] Stronge WJ. Impact and Perforation of cylindrical shells by blunt missiles - Metal Forming and Impact Mechanics 1985:289–302.

[249] HSE. OTI 92603 Analysis of Projectiles. vol. 148. 1992.

[250] US Naval Ordnance Laboratory. Explosion Effects Data Sheets NavOrd Report 2986. 1955.

[251] Franzoni A, Rastello L. Sollecitazioni Impulsive su Strutture di un Impianto Nucleare: Studio e Realizzazione di un Acceleratore Pneumatico per un Programma Sperimentale. Tesi di Laurea in Ing. Nucleare. Università di Pisa, 1986.

[252] Brown SJ. Energy release protection for pressurized systems. Part II. Rewiew of studies into impact/terminal ballistics. Appl Mech Rev 1986;39:177–201. https://doi.org/10.1115/1.3143704.

[253] Baker WE, Kulesz J, Ricker R, Bessey RL, Westline PS. Workbook for predicting pressure wave and fragment effects of exploding propellant tanks and gas storage vessels. Undefined 1975.

[254] Baker WE. Explosion hazards and evaluation 1983:807.

[255] Yarin AL, Rubin MB, Roisman I V. Penetration of a rigid projectile into an elastic-plastic target of finite thickness. Int J Impact Eng 1995;16:801–31. https://doi.org/10.1016/0734-743X(95)00019-7.

[256] Hill R. XCI. Plastic distortion of non-uniform sheets. London, Edinburgh, Dublin Philos Mag J Sci 1949;40:971–83. https://doi.org/10.1080/14786444908561367.

[257] Woodward RL, Cimpoeru SJ. A study of the perforation of aluminium laminate targets. Int J Impact Eng 1998;21:117–31. https://doi.org/10.1016/S0734-743X(97)00034-1.

[258] Børvik T, Forrestal MJ, Hopperstad OS, Warren TL, Langseth M. Perforation of AA5083-H116 aluminium plates with conical-nose steel projectiles - Calculations. Int J Impact Eng 2009;36:426–37. https://doi.org/10.1016/j.ijimpeng.2008.02.004.

[259] Department of the Army. TM 5-855-1: Fundamentals of Protective Design for Conventional Weapons 1986:3–9.

[260] Ben-Dor G, Dubinsky A, Elperin T. High-Speed Penetration Dynamics: Engineering Models and Methods. World Scientific; 2013.

[261] Healey, J., Weissman, S., Werner, H., Dobbs, N., Price P. Primary fragment characteristics and impact effects on protective barriers. Technical Report No. 4903. 1975.

[262] US Department of Defense. Mil-Std-662F Test Method Standard V 50 Ballistic Test for Armor 1997.

[263] Law Enforcement Standards Laboratory of the National Bureau of Standards. NIJ Standard 0108.01 - Ballistic Resistant Protective Materials. 1985.

[264] Børvik T, Hopperstad OS, Langseth M, Malo KA. Effect of target thickness in blunt projectile

penetration of Weldox 460 E steel plates. Int J Impact Eng 2003;28:413–64. https://doi.org/10.1016/S0734-743X(02)00072-6.

[265] Lou DC, Solberg JK, Børvik T. Surface strengthening using a self-protective diffusion paste and its application for ballistic protection of steel plates. Mater Des 2009;30:3525–36. https://doi.org/10.1016/j.matdes.2009.03.003.

[266] Holmen JK, Solberg JK, Hopperstad OS, Børvik T. Ballistic impact of layered and case-hardened steel plates. Int J Impact Eng 2017;110:4–14. https://doi.org/10.1016/j.ijimpeng.2017.02.001.

[267] Dey S, Børvik T, Hopperstad OS, Leinum JR, Langseth M. The effect of target strength on the perforation of steel plates using three different projectile nose shapes. Int J Impact Eng 2004;30:1005–38. https://doi.org/10.1016/j.ijimpeng.2004.06.004.

[268] Shin Y ho, Chung J hoon, Kim JH. Test and estimation of ballistic armor performance for recent naval ship structural materials. Int J Nav Archit Ocean Eng 2018;10:762–81. https://doi.org/10.1016/j.ijnaoe.2017.10.007.

[269] Cozzani V, Tugnoli A, Salzano E. Prevention of domino effect: From active and passive strategies to inherently safer design. J Hazard Mater 2007;139:209–19. https://doi.org/10.1016/J.JHAZMAT.2006.06.041.

[270] Nguyen TH, Sinha A, Tambe M. Conquering adversary behavioral uncertainty in security games: An efficient modeling robust based algorithm. AAAI Conf. Artif. Intell., Phoenix (AZ): 2016.

[271] Aven T, Renn O. The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. Risk Anal 2009;29:587–600. https://doi.org/10.1111/J.1539-6924.2008.01175.X.

[272] Torres-Toledano JÉG, Sucar LE. Bayesian Networks for Reliability Analysis of Complex Systems. Lect Notes Comput Sci (Including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) 1998;1484:195–206. https://doi.org/10.1007/3-540-49795-1_17.

[273] Jensen FV, Nielsen TD. Bayesian networks and decision graphs. 2nd ed. New York: Springer; 2007.

[274] Khakzad N, Khan F, Amyotte P, Cozzani V. Domino effect analysis using Bayesian networks. Risk Anal 2012;33:292–306. https://doi.org/10.1111/J.1539-6924.2012.01854.X.

[275] Iaiani M, Tugnoli A, Cozzani V, Reniers G, Yang M. Evaluation of the probability of success of security attacks on offshore O&G installations: a Bayesian network-based approach. Ocean Eng 2022.

[276] Iaiani M, Tugnoli A, Macini P, Mesini E, Cozzani V. Assessing the Security of Offshore Oil&Gas Installations using Adversary Sequence Diagrams. Chem Eng Trans 2022;91:385–90. https://doi.org/10.3303/CET2291065.

[277] Hypothetical Atomic Research Institute (HARI). Hypothetical Facility Exercise Data Handbook. 2013.

[278] Iaiani M, Tugnoli A, Macini P, Mesini E, Cozzani V. Assessing the Security of Offshore Oil&Gas Installations using Adversary Sequence Diagrams. Chem Eng Trans 2022;91.

[279] Vasilev VS. Some specifics of reducing the IED risk in offshore security environment. “Micea Cel Batran” Nav Acad Sci Bull 2016;19:116–27.

[280] Argenti F, Landucci G, Cozzani V, Reniers G. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Saf Sci 2017;94:181–96. https://doi.org/10.1016/J.SSCI.2016.11.022.

[281] McKenna MF, Katz SL, Condit C, Walbridge S. Response of Commercial Ships to a Voluntary Speed Reduction Measure: Are Voluntary Strategies Adequate for Mitigating Ship-Strike Risk? Coast Manag

2012;40:634–50. https://doi.org/10.1080/08920753.2012.727749.

[282] Wadoud AA, Adail AS, Saleh AA. Physical protection evaluation process for nuclear facility via sabotage scenarios. Alexandria Eng J 2018;57:831–9. https://doi.org/10.1016/J.AEJ.2017.01.045.

[283] Reniers G, Cozzani V. Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier; 2013. https://doi.org/10.1016/C2011-0-00004-2.

[284] Iaiani M, Tugnoli A, Cozzani V. Risk of cascading effects in digitalized process systems. In: Faisal K, Pasman H, Yang M, editors. Methods Chem. Process Safety, Vol. 6 Methods to Assess Manag. Process Saf. Digit. Process Syst., Elsevier; 2022, p. 353–88. https://doi.org/https://doi.org/10.1016/bs.mcps.2022.04.010.