Identification of reference scenarios for security attacks to the process industry

Title Page (with Author Details)

Identification of reference scenarios for security attacks to the process industry

Matteo IAIANI, Alessandro TUGNOLI, Valerio COZZANI*

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

(*) Author to whom correspondence should be addressed.
tel. (+39)-051- 20 90240
e-mail: valerio.cozzani@unibo.it

Submitted for publication in:
Process Safety and Environmental Protection

Abstract

The possibility of inducing severe security-related events with damage to people, property, and the environment by deliberate malicious attacks to chemical and process plants handling large quantities of hazardous materials received an increasing attention in recent years. The identification of the credible security scenarios is required by security vulnerability/risk assessment methods. However, the current availability of supporting tools is limited. This may hinder a proper management of the risks, especially in the European context where security threats are only marginally recognized under the Seveso legislation. The present study aims at supporting a harmonized identification of the scenarios triggered by malicious physical attacks to chemical and process plants. An approach based on Bow-Tie formalism is proposed to identify reference security scenarios. The Bow-Tie diagram is used to link the attack modes (Attack Tree) to the relevant release scenarios (Security Events) and to the physical damage scenarios (Event Tree). Reference Bow-Tie diagrams were defined considering substances commonly present in process plants (e.g. flammable substances and oxidising solids). The validation of the reference scenarios (both attack scenarios and physical damage scenarios) was provided by the analysis of more than 20 security-related incidents that occurred in process facilities worldwide in the last 50 years. Application to a case-study proved the effectiveness of the results achieved in supporting SVA/SRA studies and in promoting integration among safety and security management.

Keywords

Major Accident Hazards, Hazardous Substances, Security, Bow-Tie diagram, Scenario Identification

Highlights

- Attack Trees for reference storage installations were developed
- Reference Bow-Ties (Attack + Event Trees) for widely produced chemicals are proposed
- Bow-Ties were validated by information available from past security incidents
- Reference scenarios for a generic facility triggered by malicious acts were identified

List of Acronyms

AM: Attack Mode
ANFO: Ammonium Nitrate Fuel Oil
AT: Attack Tree
BT: Bow-Tie
C&P: Chemical&Petroleum
EQ: relevant hazardous EQuipment
ET: Event Tree
FS: Physical damage scenario
LI: Loss Intensity
LNG: Liquefied Natural Gas
LOC: Loss of Containment
LPG: Liquefied Petroleum Gas
LPI: Loss of Physical Integrity
PPS: Physical Protection System
RAI: Reference Act of Interference
RI: Reference Installation
SE: Security Event
TATP: Triacetone Triperoxide Peroxyacetone
TNT: TriNitroToluene

1. Introduction

Chemical and process plants are highly interconnected and interdependent systems, and vital installations for the society, being part of critical energy and materials supply chains (Landucci and Reniers, 2019). At the same time, they frequently present an inherent hazard due to the processing and storage of hazardous materials (e.g. flammable and toxic materials), that can lead to events with severe consequences on humans, assets, and the environment (Mannan, 2012). These events, the so called "major accidents" in the safety domain, such as loss of containment of hazardous materials, fires, explosions, and toxic dispersions, may be triggered by safety-related causes (e.g. random failure of equipment), but may also be deliberately caused by malicious attacks aiming at interfering with normal operations (Lou et al., 2003; Argenti et al., 2018). For example, in 1993 undefined attackers detonated an explosive device on a side of the middle lift of a gasholder, causing a fireball from the release of natural gas and other fire scenarios in nearby equipment (jet fire and seal fire) (eMARS database, 2021). A number of similar events were recorded in recent years (Casson Moreno et al., 2018; Iaiani et al., 2021a, 2021b), confirming that physical security (security against physical threats) and cybersecurity (security against cyber threats) of chemical and process plants must be considered as a major concern.

Worldwide, regulations addressing the security of installations storing or processing hazardous materials are quite different. In Europe, chemical and process plants handling large quantities of hazardous materials (i.e. Seveso plants) fall under the obligations of the so called "Seveso-III" Directive (Directive 2012/18/EU (European Parliament and Council, 2012)). Mention to deliberate malicious acts may be part of some country-specific transpositions of the Directive, but is not part of its principal aim, that is the control of safety-related major accidents involving dangerous substances. For instance, the Italian transposition of the Directive, i.e. the Legislative Decree 105/2015 (Italian Government and Parliament, 2015), suggests to consider malicious acts and unauthorized accesses in the definition of the internal emergency plan, but no other guidance is provided. For the energy production installations (electricity and Oil&Gas), the European Programme for Critical Infrastructure Protection (EPCIP) (Commission of the European Communities, 2006) promotes the prevention, preparedness and response to terrorist attacks, but no extension is made to the process industry.

In the United States, particular attention to security of chemical and process installations is paid after the "9/11" terrorist attacks. Since these events, policies and legislations aimed at enhancing the preparedness against deliberate malicious attacks were developed (Matteini et al., 2019). In particular, the "Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014" prescribes the Department of Homeland Security to define risk-based security standards for chemical facilities handling large quantities of hazardous materials, i.e. the so called CFATS (Chemical Facility Anti-Terrorism Standards). In this panorama, a great effort in developing Security Vulnerability Assessment (SVA) or Security Risk Assessment (SRA) methodologies, was done. Examples of SVA/SRA methodologies suitable for the chemical and process plants are the CCPS methodology (Center for Chemical Process Safety, 2003), the VAM-CF methodology (Jaeger, 2002), the methodology proposed by API RP 780 (American Petroleum Institute, 2013), the RAMCAP methodology (Moore et al., 2007), and the one developed by the Hazardous Incidents Commission (Störfall-Kommission, 2002).

All SVA/SRA methodologies require the identification of the physical damage scenarios that can be originated through deliberate malicious attacks (Baybutt, 2018). 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 ("Conduct a 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"), and step 3 of the RAMCAP methodology ("Consequence analysis"). 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.

Scenario identification, sometimes exploiting the Bow-Tie concept, is a step required also by the novel and more complex approaches that were recently proposed in the literature 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/faults) to consequences (outcomes in terms of damages 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 (Khakzad et al., 2011). For example, Landucci et al. (2017) 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 (PPS). This requires the definition of the set of attack modes as starting point for the design of the BN. Similarly, attack characterization is an input information for the application of the BN-based model proposed by Argenti at al. (2018) aimed at the assessment of the external threats targeting chemical facilities. Analogously to what was done by Khakzad et al. (2013) 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. (2017) to allow for 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.

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 (Jon et al., 2021)), the Markov modelling is typically used for solving BNs (Markov Chain Monte Carlo framework) (Khakzad et al., 2014b, 2014a; Leoni et al., 2021; Li et al., 2021), or it is coupled to them (e.g. the coupled Continuous-Time Markov Chain – Bayesian Network Model developed by Badr et al. (2021)). 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. (2019) presented a game-theoretic method for optimizing the allocation of defensive resources to protect chemical and process facilities by considering the existence of multiple types of attackers. Similarly, Zhang et al. (2019) and Rezazadeh et al. (2019) 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. Game theory was also adopted in the field of cybersecurity of chemical and process facilities by Hausken (2017), addressing the effects of information sharing between firms and between attackers in order to identify the best defence strategies. Identification of the attack patterns and a proper characterization of the potential outcomes are needed also in these cases.

The consequence-based method including a Dynamic Vulnerability Assessment Graph (DVAG) model proposed by Chen et al. (2019) to integrate safety and security resources for security risk reduction requires identification of primary scenarios (Step 2 in the flowchart of the method) to develop dynamic graphs. Graph theory approach was also adopted by Khakzad and Reniers (2019) and coupled with dynamic Bayesian Network for vulnerability of process plants facing man-made domino effects.

Abdo et al. (2017) proposed a fuzzy logic approach based on integrated Bow-Tie analysis in order to handle vagueness and imprecision in the input parameter frequencies and evaluate likelihood of adverse safety/security scenarios. Finally, it is worth mentioning the alternative semi-quantitative SRA approach developed by Bajpai and Gupta (2007, 2005) which, following the typical steps of a standard SVA/SRA, requires inputs like knowledge of credible threats, plant vulnerabilities and expected consequences.

Landucci and Reniers (2019), identify an evident lack of specific procedures and guidelines for the identification of the security scenarios for chemical and process plants in the current practice. In fact, the techniques commonly used in process hazard analysis/identification in the field of process safety, such as HazOp studies (International Electrotechnical Commission, 2016), What if Analysis (Mannan, 2012), Failure Modes and Effects Analysis (FMEA) (International Electrotechnical Commission, 2018), Methodology for the Identification of Major Accident Hazard (MIMAH) (Delvosalle et al., 2006), are not suitable to take into account security aspects. In fact, given the different theoretical foundation of security issues with respect to safety issues (Baybutt, 2017), these techniques developed for safety aspects do not provide for systematic approaches and tools aimed at accounting for the mechanism of deliberate malicious attacks.

Specific hazard identification techniques were recently proposed for the specific field of cybersecurity for plants handling hazardous materials. These include cyber Bow-Tie approaches (Abdo et al. 2018), the CyberPHA method (Cusimano and Rostick 2018), reverse-HazOp methods for attacks to BPCS and SIS (Iaiani et al. 2021c, 2021d), and the toolkit for risk identification suggested by Carreras Guzman et al. (2021). 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.

The definition of sets of reference scenarios for the chemical and process industry is a suitable approach to bridge the gap in the identification of scenarios for security assessments. 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 outcomes (physical damage scenarios). Sets of reference scenarios may be developed with reference to specific types of model installation (e.g. a fixed roof storage tank or a storage warehouse) and can be used by practitioners as a reference starting point to undertake a case specific analysis of the detailed attack patterns. The use of reference scenarios as support to risk identification is well consolidated in the safety management practice, where it provides the baseline for the authorities and practitioners to analyse 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 (Delvosalle et al., 2006), those reported in the "Handbook of Scenarios for Assessing Major Chemical Accident Risks" (Gyenes et al., 2017) aimed to assist the EU Member States and other Seveso implementing countries in land-use planning (LUP), and those proposed for LUP decision making purposes (Tugnoli et al., 2013).

The extension of the approach based on reference scenarios to the domain of physical security of chemical and process plants is deemed to be possible, given the existence of similarities among plant layout elements (fences, access control points, building accesses, internal road network (Garcia, 2007)) 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 (Ylönen et al., 2021a, 2021b). Shared understandings and effective communication provide necessary common ground for jointly asking and answering questions across disciplinary boundaries (Gilligan, 2021). Several authors stress that, in spite of the obvious differences in the origin of the risk, much could be gained by the one adopting the knowledge, understanding, tools and techniques of the other, and vice versa (Brewer, 1993; Eames and Moffett, 1999; Firesmith, 2003). In particular, 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 (Abimbola and Khan, 2019; Bostick et al., 2018; Chen et al., 2021; Cutter et al., 2013; Hausken, 2020). This is of particular relevance, since potential conflicts or inconsistences between requirements defined in isolation by the safety and 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)(Ji et al., 2021; Leveson, 1995; Pietre-Cambacedes and Bouissou, 2013; Sørby, 2003).

In this panorama, the present study introduces a novel set of reference security scenarios (intended as the evolution of events starting from attack scenarios to the physical damage scenarios) and a step-by-step procedure based on Bow-Tie approach for case-specific security scenario identification, aimed at supporting the hazard identification phase of SVA/SRA methodologies, including the most recent quantitative approaches discussed above. The reference security scenarios were 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 formalism. A Bow-Tie diagram 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). Validation of the Bow-Tie diagrams obtained was provided by the analysis of security-related incidents

that occurred in process facilities worldwide in the last 50 years. The potential use of the developed reference Bow-Ties is demonstrated on a case-study.

The paper is organized as follows: in Section 2 the method applied for the development and validation of the proposed reference Attack Modes (AMs), Attack Trees (ATs), and Bow-Ties (BTs) is presented. In Section 3, the validation of AMs, ATs, and BTs is reported. In Section 4, a flow-chart of the step-by-step procedure for the identification of reference security scenarios is described, together with its exemplification by the application to a practical case-study. In Section 5, the results of the case-study are presented. In Section 6 an overall discussion of the results is provided.

2. Method

The present study is aimed at supporting hazard identification phase in SVA/SRA studies providing tools for the identification of security scenarios that may originate in chemical and process plants (from attack scenarios to physical damage scenarios) using the Bow-Tie (BT) formalism (Delvosalle et al., 2006; Mannan, 2012).

An approach based on BT diagrams was selected since, according to Mannan (2012), the BT diagram approach is used 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 (Delvosalle et al., 2006) to support upper-tier Seveso plants in identifying the potential major accident scenarios.

In the present study, reference BTs are 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 SVA/SRA methodologies and other methods 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 1. 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" (American Petroleum Institute, 2013). The Attack Tree (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 (Störfallkommission, 2002)) into a set of possible attack modes (AM). The Event Trees (on the right side of the SE) shows all the possible physical events leading from the SE to the physical damage scenarios (FS).

The development of the reference BTs within the present study consisted of three main phases, namely: i) identification and validation of a reference set of attack modes (AM); ii) definition and validation of Attack Trees (AT) for a set of reference installations; iii) construction and validation of reference BT diagrams. The phases are described in detail in the following.

The proposed sets of reference AMs, ATs, and BTs and their validation are reported in Section 3. The step-by-step procedure for their application in order to identify reference security scenarios is described in Section 4.

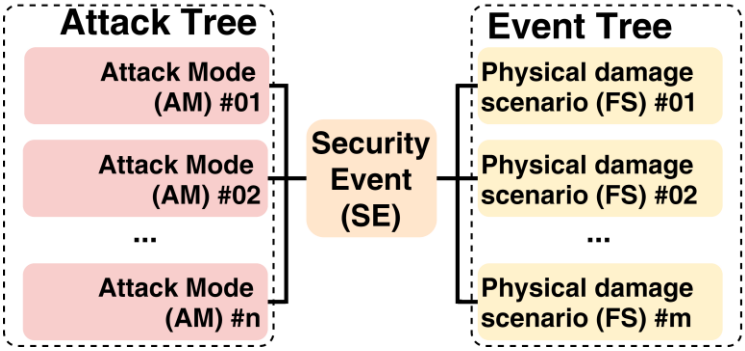

Figure 1. Generic structure of the proposed Bow-Tie (BT) diagram.

2.1 Identification and validation of reference Attack Modes (AM)

The first phase of present study was aimed at the definition of a reference set of Attack Modes (AM) 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 (Abdo et al., 2018; Cusimano and Rostick, 2018; Hashimoto et al., 2013; Iaiani et al., 2021c, 2021d).

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 process plants. Sources analysed include: Störfallkommission (2002), the CCPS methodology (Center for Chemical Process Safety, 2003), the VAM-CF methodology (Jaeger, 2002), the API RP 780 SRA methodology (American Petroleum Institute, 2013), and the RAMCAP methodology (Moore et al., 2007). 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 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 methods suggest for the chemical and process industry (American Petroleum Institute, 2013; Center for Chemical Process Safety, 2003), 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 (2002) for typical deliberate interferences with or without the use of aids, Pert et al. (2006) for incendiary substances, Landucci et al. (2015) 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)(valkyrie.pro, 2019), the standards EN 1063 (European Committee for Standardization, 2019) and EN 1522 (European Committee for Standardization, 1999) for type and characteristics of bullets.

Validation of the AMs was carried out on the basis of the information available in the database populated by Casson Moreno et al. (2018), and updated by Iaiani et al. (2021a), concerning security-related incidents that occurred in the Chemical&Petroleum (C&P) sector. 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 (UNSD, 1999). 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.

2.2 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 (AT) for a set of reference installations. ATs are graphs that represent the security acts (deliberate malicious attacks) leading to a Security Event (SE)(Abdo et al., 2018). In the present study the AT for each reference installation contains three elements: the Attack Modes (AMs), the safety/security barriers and the Security Events (SEs).

The set of Reference Installations (RIs) considered in the present analysis were adapted from those proposed by Delvosalle et al. (2006) and by Tugnoli et al. (2013). 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 (SE) such as a loss of physical integrity (LPI) and/or a loss of containment (LOC) of the hazardous material stored in the reference installation (Delvosalle et al., 2006). In case of LOC of fluids, the classification proposed by the TNO "Purple Book" (Uijt de Haag and Ale, 2005) and adopted by Cozzani et al. (2013) 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. The assessment was based on the definitions of the set of adopted AMs, taking into account the specific features of the attack vectors.

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) sector collected in a specific database (Casson Moreno et al., 2018; Iaiani et al., 2021a). 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.

2.3 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 the reference installations considered in the present study. The generic scheme of a BT (Figure 1) 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 (Delvosalle et al., 2006). 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 definitions of the FSs considered in the present study that are present in the ETs are reported in Appendix A (see Table A1).

The ETs generated for the most frequent families of substances stored and processed in the chemical and process industry (Wiley-VCH, 2011) are reported in Appendix B: flammable liquids (Figure B1), flammable pressurized gasses (Figure B2), flammable gasses (Figure B2), flammable cryogenic liquids (Figure B3), toxic pressurized gasses (Figure B4), pressurized liquefied toxic gasses (Figure B5), and oxidizing solids (Figure B6).

The security-related BTs obtained were validated with the data from Iaiani et al. (2021a), as previously done for the validation of AMs and ATs. More specifically, the occurrence of incidents featuring the consequences reported in the ETs was checked, allowing the validation of specific branches of the ETs. In Section 3, only the BTs for which validation was possible are reported and discussed.

3. Validation of proposed Attack Modes, Attack Trees, and Bow-Tie diagrams

Validation of the proposed AMs, ATs and BTs in the context of process industry was provided by the analysis of past security-related incidents that occurred in relevant facilities in the last 50 years. The incidents were derived from the database developed in the study performed by Casson Moreno et al. (2018) and recently updated by Iaiani et al. (2021a). Elements of the proposed ATs and BT that were recorded at least one time were considered possible to occur again and therefore validated. Since the validation was based on a relatively low number of recorded events (i.e. 51 incidents), care shall be put into assigning any rigorous statistical value to the number of occurrences. However, the use of lessons learnt, even from a limited number of events, is a common practice in cases of rare events and early warnings analysis (Ovidi et al., 2020; Paltrinieri et al., 2012; Paltrinieri and Reniers, 2017; Planas et al., 2015; Skogdalen and Vinnem, 2012; Zhu et al., 2017).

A brief description of the incidents used in the validation of both the ATs for reference installations and the BT diagrams, are reported in Table A1 in Appendix A. Information on the total number of security-related incidents collected for the Chemical&Petroleum sector (including also those reported in Table A1) and used in the validation phase can be found in Iaiani et al., (2021a).

3.1 Validation of the proposed reference Attack Modes

The categories of Attack Modes (AMs) proposed in the present study are defined in Table 1. The categories closely match the acts of interference described by Störfall-Kommission (2002), specifically derived for process and chemical facilities and previously adopted by other authors (Argenti et al., 2018; Landucci et al., 2017), 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 (2002) were joined in the AM#01 category "Deliberate interference with or w/o aids" (see definition in Table 1) 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 (2002) were joined in the AM#02 category "Arson using simple/incendiary means" (see definition in Table 1) 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 1) is not reported in Störfall-Kommission (2002). Nevertheless, references to this attack mode were found in the CCPS SVA methodology, in the API RP 780 SRA methodology, in Argenti et al. (2018), Landucci et al. (2017), and Casson Moreno et al. (2018). 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 (Landucci et al., 2015): these differences lead to different security barriers within the physical protection system (PPS) for the detection and delay of such attacks (Garcia, 2007).
- In the AM#05 "Shooting" defined in the present study (see definition in Table 1), 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 (Mary Lynn Garcia (2007), Landucci et al. (2015), Landucci et al.

(2017), Casson Moreno et al. (2018), and Argenti et al. (2018)) confirmed the suitability of the proposed classification of AMs.

Table 1. Reference AMs adopted in the present study. For each AM, reference tool/substance, attack vector, success criterion and potential loss intensities (LIs) are reported.

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 5.56×45mm NATO cartridge	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	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 in the database developed by Casson Moreno et al. (2018) and updated by Iaiani et al. (2021a) provided a validation for the proposed set of AMs. A total of 51 incidents reported enough information to characterize the AM (Figure 2) as defined in Table 1. The numbers (red-coloured) contained in the tags on each branch displayed in Figure 2 are referred to the count of incidents for which information matching the AM description reported in Table 1 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 A1 (Appendix A) 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) (GTD, 2021). 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 2. 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 for the validation of the approach.

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 1 were validated, presenting at least one past security-related incident matching the description of the AMs. As stated, no incident collected in the Chemical&Petroleum sector (Iaiani et al., 2021a) 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 (Voorhees, 2017) 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 (ARIA database, 2021): 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.

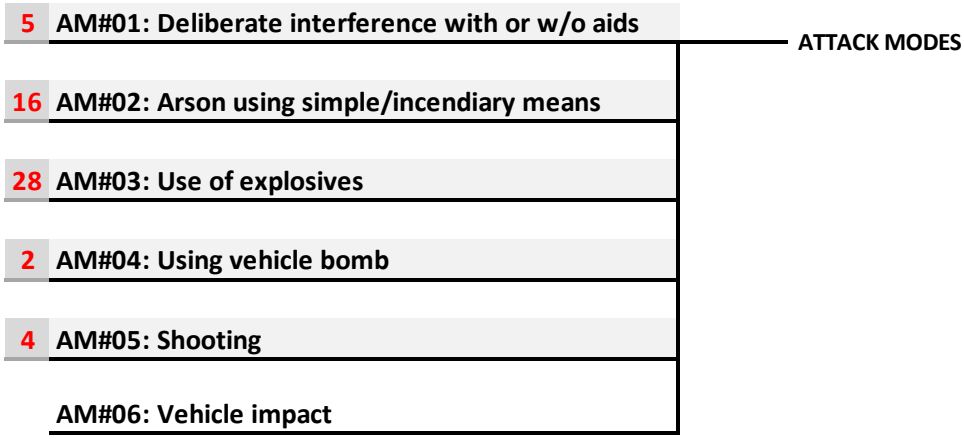

Figure 2. Set of Attack Modes (AMs) considered in the present study. Numbers in tags refer to the number of incidents validating the AM.

Each AM listed in Table 1 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: a 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 1). Even in the case tools are used (as in RAI#01-B), they are, according to the

AM definition (see Table 1), man-portable or present on site. This implies that the attacker has no specific elements of the protection layers 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 (Iaiani et al., 2021c, 2021d). 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 A1). Moreover, gasoline is considered by Pert et al. (2006) 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 1), and the ignition of 1000 L contained inside an IBC tank that is already present onsite (RAI#02-B, see Table 1). In one incident in the database (see incident #18 in Table A1) 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. (2015) 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 1), since it presents the higher explosion energy (2803 kJ/kg) among the candidates and it is therefore the more 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 incident #85 and #100 in Table A1).

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 (Landucci et al., 2015). 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 1). The use of vehicle bombs was found in two incidents (Casson Moreno et al., 2018; Iaiani et al., 2021a).

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. However, a rifle using the 5.56×45mm NATO cartridge was considered in the RAI#05 associated to AM#05: this cartridge is reported in the European standards EN 1063 (European Committee for Standardization, 2019) and EN 1522 (European Committee for Standardization, 1999) on the testing and rating of armoured vehicles and structures. 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 (European Committee for Standardization, 2019, 1999)).

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 1 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 (Cozzani et al., 2013).

3.2 Validation of the proposed Attack Trees for reference installations

In this section, the proposed Attack Trees (ATs) for the reference storage installations considered in the present study (RI1: atmospheric storage installation; RI2: pressurized storage installation; RI3: storage warehouse) are shown and validated. ATs display the credible Attack Modes (AMs) and the safety/security barriers available to prevent a Security Event (SE), intended as a malicious release of hazardous material and/or energy (LOC or LPI).

Among the physical security-related incidents reported for the Chemical&Petroleum sector (Iaiani et al., 2021a), 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. These 21 incidents are all briefly described in Table A1 (Appendix A).

3.2.1 Attack Tree for atmospheric storage installations

Figure 3 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 leading to a mass and/or energy release) involving a RI1 installation. As shown in the figure, there is historical 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 3 are referred to the tags of the incidents described in Table A1 (Appendix A).

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 (ARIA database, 2021). 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 (eMARS database, 2021), 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 collected in the database (Iaiani et al., 2021a) 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 (GTD, 2021). 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 (eMARS database, 2021). In the AT shown in Figure 3, 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 1) is reported. Actually, as explained in Appendix C, 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 (Argenti et al., 2018; Landucci et al., 2015; Woodward, 1978) 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 around these installations. This conclusion is also supported by the lack of recorded incidents featuring this AM.

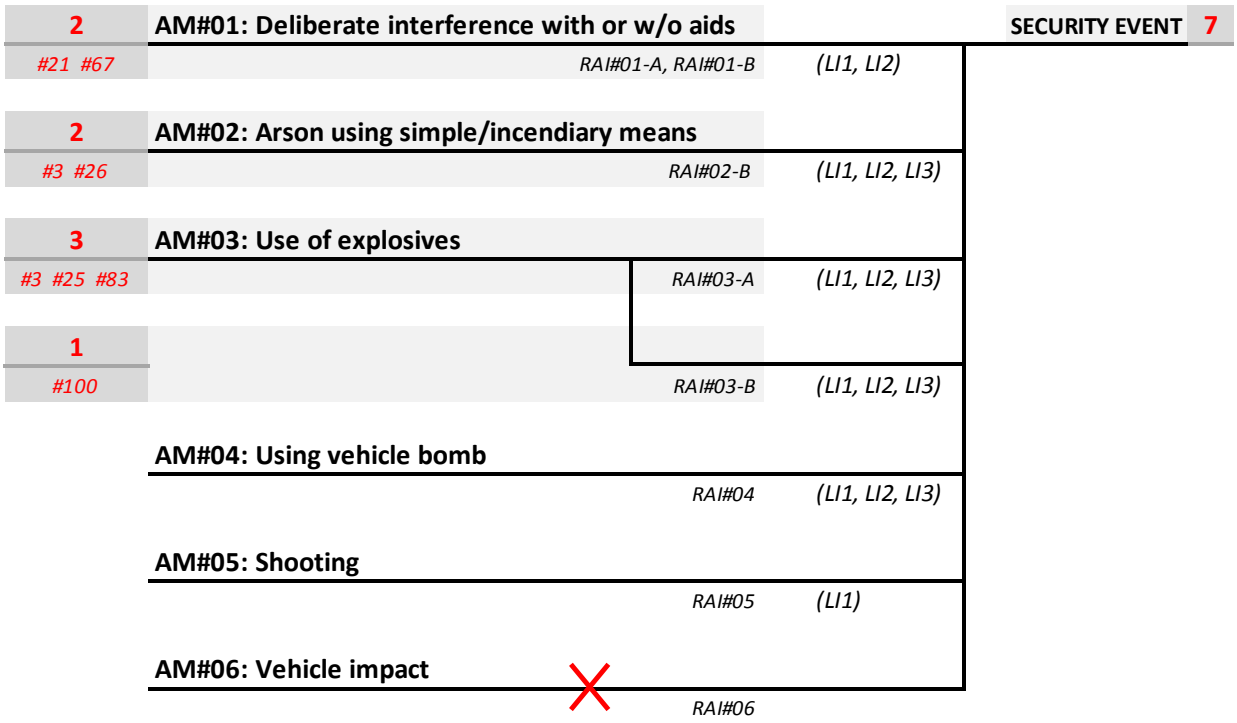

Figure 3. Attack Tree for atmospheric storage installations (RI1). Numbers in tags refer to the number of incidents validating the branch of the AT. Incident codes refer to the incidents described in Table A1; AM#-codes and RAI#-codes are defined in Table 1.

3.2.2 Attack Tree for pressurized storage installations

Figure 4 shows the Attack Tree (AT) for pressurized storage installations (RI2). No incidents collected in the database (Iaiani et al., 2021a) 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 as discussed in Appendix C). 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 (eMARS database, 2021).

Differently from 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).

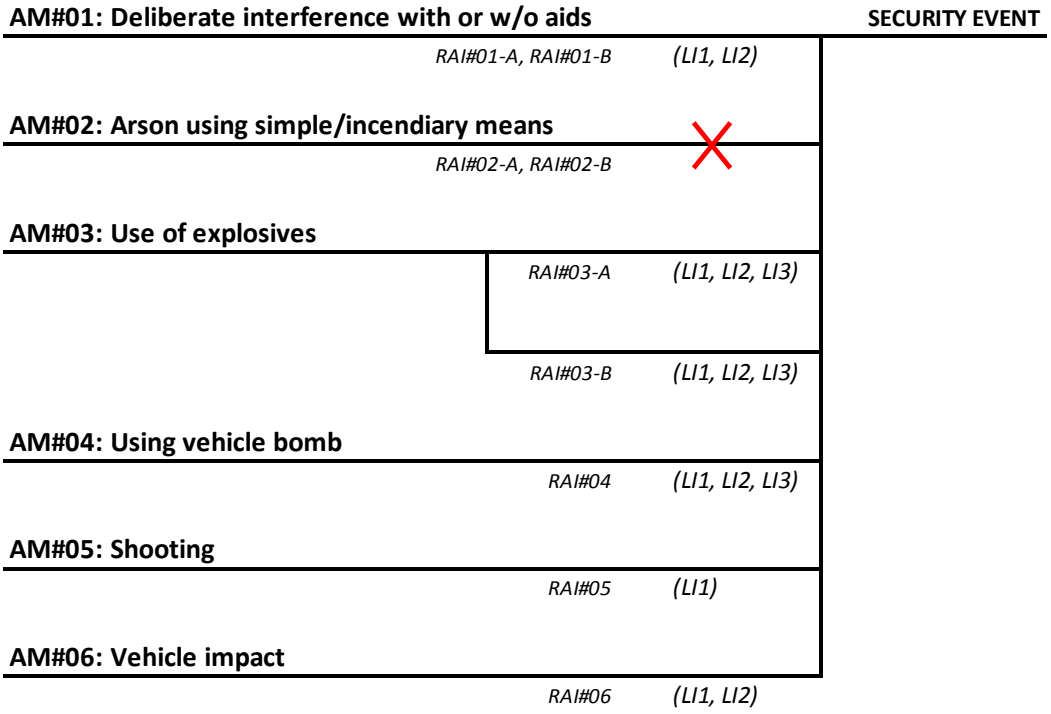

Figure 4. Attack Tree for pressurized storage installations (RI2). AM#-codes and RAI#-codes are defined in Table 1.

3.2.3 Attack Tree for storage warehouses

Figure 5 shows the validated Attack Tree (AT) for storage warehouses (RI3). Fourteen incidents (Iaiani et al., 2021a) 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 5 are referred to the tags of the incidents described in Table A1 (Appendix A).

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 5): 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 (ARIA database, 2021). 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 (ARIA database, 2021). 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 Appendix C).

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 (ARIA database, 2021). 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 (ARIA database, 2021). 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 sentiments (Ackerman et al., 2007).

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.

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, given the low thickness of the typical low-volume containers used for liquids and powders.

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

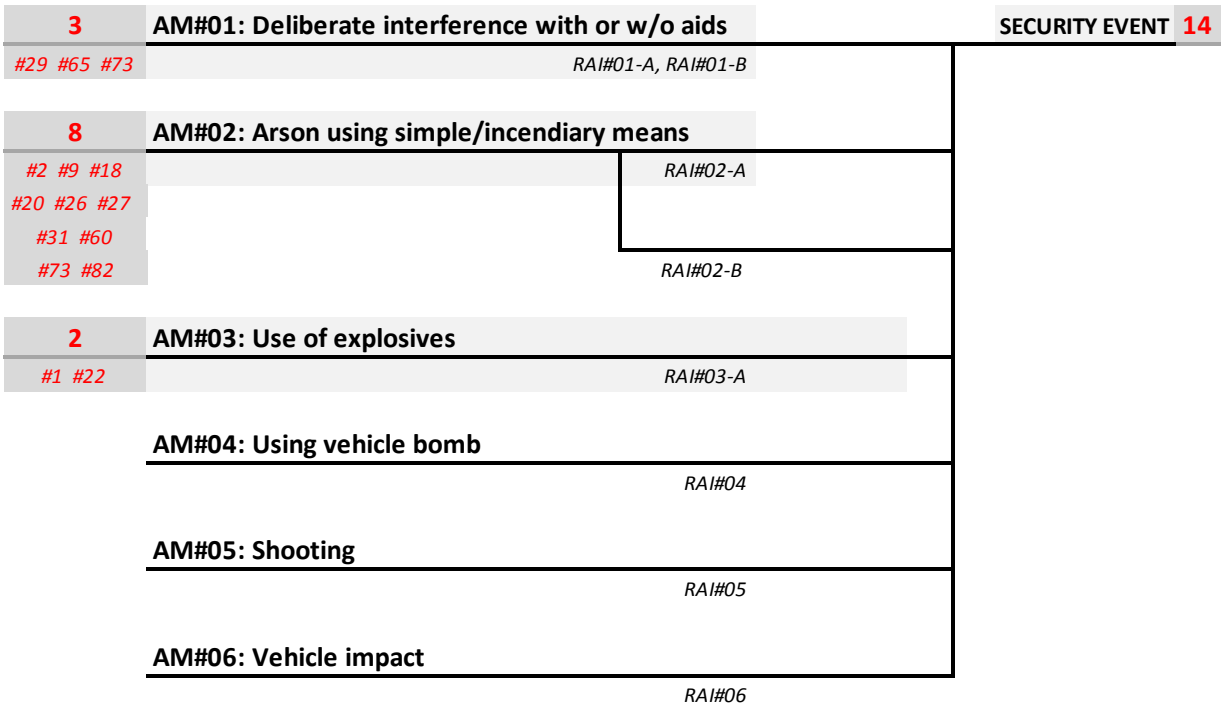

Figure 5. Attack Tree for storage warehouse (RI3). Numbers in tags refer to the number of incidents validating the branch of the AT. The incident #-codes refer to the tags of the incidents described in Table A1; AM#-codes and RAI#-codes are defined in Table 1.

3.3. Validation of the proposed Bow-Tie diagrams

Figures 6 to 8 report the proposed reference Bow-Tie (BT) diagrams that were obtained from the combination of the Attack Trees (ATs) validated above (see Section 3.2) with the Event Trees (ETs) applicable for the stored material (see Appendix B).

Only 12 incident files present in the database (Iaiani et al., 2021a) 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 Appendix B.

3.3.1 Bow-Tie diagram for atmospheric storage of flammable liquids

Figure 6 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 3.2.1 for atmospheric storage installations (RI1), while the Event Tree (ET) was generated with the MIMAH methodology (see Figure B1 in Appendix B). Grey-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 6 and description in Table A1). 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 A1), while in the other two events it was due to the detonation of explosives (AM#03, see incidents #83 and #100 in Table A1).

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 1) (eMARS database, 2021). 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 1) that caused the release of oil from 14 atmospheric storage tanks and other process equipment (bbc.com, cnbc.com, nytimes.com) that resulted in multiple pool fires. 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 (GTD, 2021). 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.

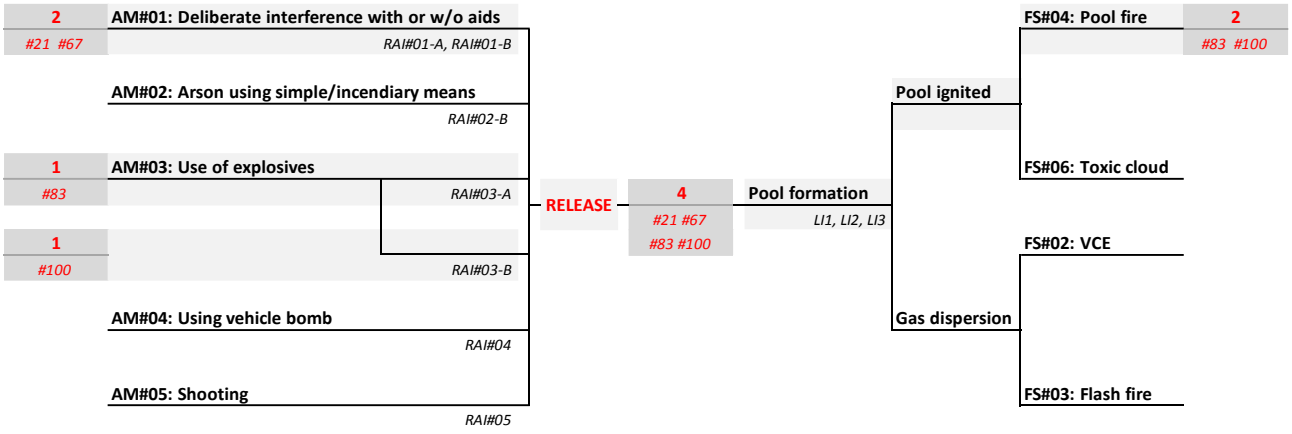

Figure 6. Bow-Tie for atmospheric storage of flammable liquids. Numbers in tags refer to the number of incidents validating the branch of the BT. #-codes refer to the incidents described in Table A1; AM#-codes and RAI#-codes are defined in Table 1; FS#-codes are described in Table B1.

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

Figure 7 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 3.2.3 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 B1 (Appendix B) considering that warehouses are indoor spaces: vapour cloud explosion (VCE, see FS#02 in Table B1) was replaced by confined chemical explosion (see FS#09 in Table B1) and flash fire (see FS#03 in Table B1) was eliminated. Grey-shaded branches are those validated by past incidents.

The results obtained from the analysis of the BT in Figure 7 are similar to those discussed in the previous section (atmospheric storage of flammable liquids). The formation of a pool was validated by 6 incidents collected in the database (see tags in Figure 7): 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 (ARIA database, 2021), 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 (ARIA database, 2021). The other attack modes were not validated: however, as previously discussed, they are potentially able to cause a loss of containment (see Section 3.2.3).

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 (ARIA database, 2021).

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.

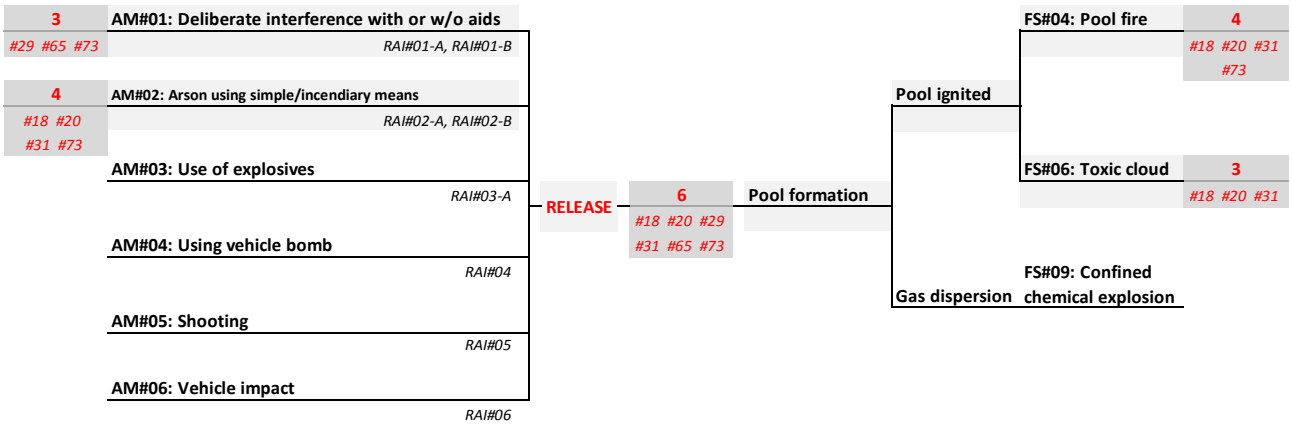

Figure 7. Bow-Tie for storage of flammable liquids in a warehouse. Numbers in tags refer to the number of incidents validating the branch of the BT. #-codes refer to the incidents described in Table A1; AM#-codes and RAI#-codes are defined in Table 1; FS#-codes are described in Table B1.

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

Figure 8 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 (Delvosalle et al., 2006)) is that developed for storage warehouses (RI3) and discussed in Section 3.2.3. The ET on the right side of the BT was generated with the MIMAH methodology considering oxidizing solids with explosive hazards (see Figure B7 in Appendix B). Grey-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 1), 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 (ARIA database, 2021).

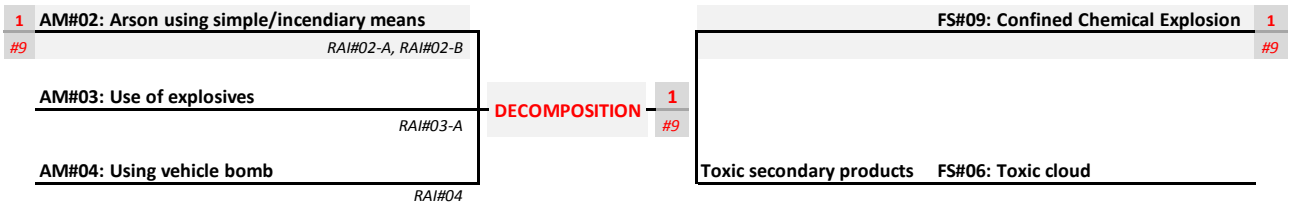

Figure 8. Bow-Tie for storage of oxidising solids with explosion hazards in a warehouse. Numbers in tags refer to the number of incidents validating the branch of the BT. #-codes refer to the incidents described in Table A1; AM#-codes and RAI#-codes are defined in Table 1; FS#-codes are described in Table B1.

4. Procedure for identification of reference security scenarios: step-by-step approach and illustrative case-study

4.1 Procedure for identification of reference security scenarios

The flowchart of the procedure proposed for the identification of reference security scenarios based on Bow-Tie formalism is shown in Figure 9-(a). It consists in 7 steps: starting from the collection of the input information required, it provides 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 to combine them into a Bow-Tie (BT) diagram in order to define reference security scenarios. In Steps 4, 6 and 7, the set of proposed and validated Attack Modes (AMs), Attack Trees (ATs) for reference installations, and Bow-Tie (BT) diagrams for reference hazardous substances introduced in section 3 may be used (see Figure 9-(a)).

The reference security scenarios obtained by the application of the procedure in Figure 9-(a) may be used to support the hazard identification step in SVA/SRA studies. As an example, the output of the present methodology provide the identification of 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) needed to support to Step 2 “Facility characterization” of the CCPS SVA, which is specific for the chemical and process industry (see Figure 9-(b)). The ATs obtained may support the definition of the attack scenarios that may be used by the attackers to generate the SEs needed in Step 3 “Threat assessment” of CCPS SVA. Moreover, the identification of the specific cause-consequence chains of events from attack scenarios to physical damage scenarios (i.e. the security scenarios) required in Step 4 “Vulnerability analysis” of the same methodology may be derived from the BTs obtained in the present study.

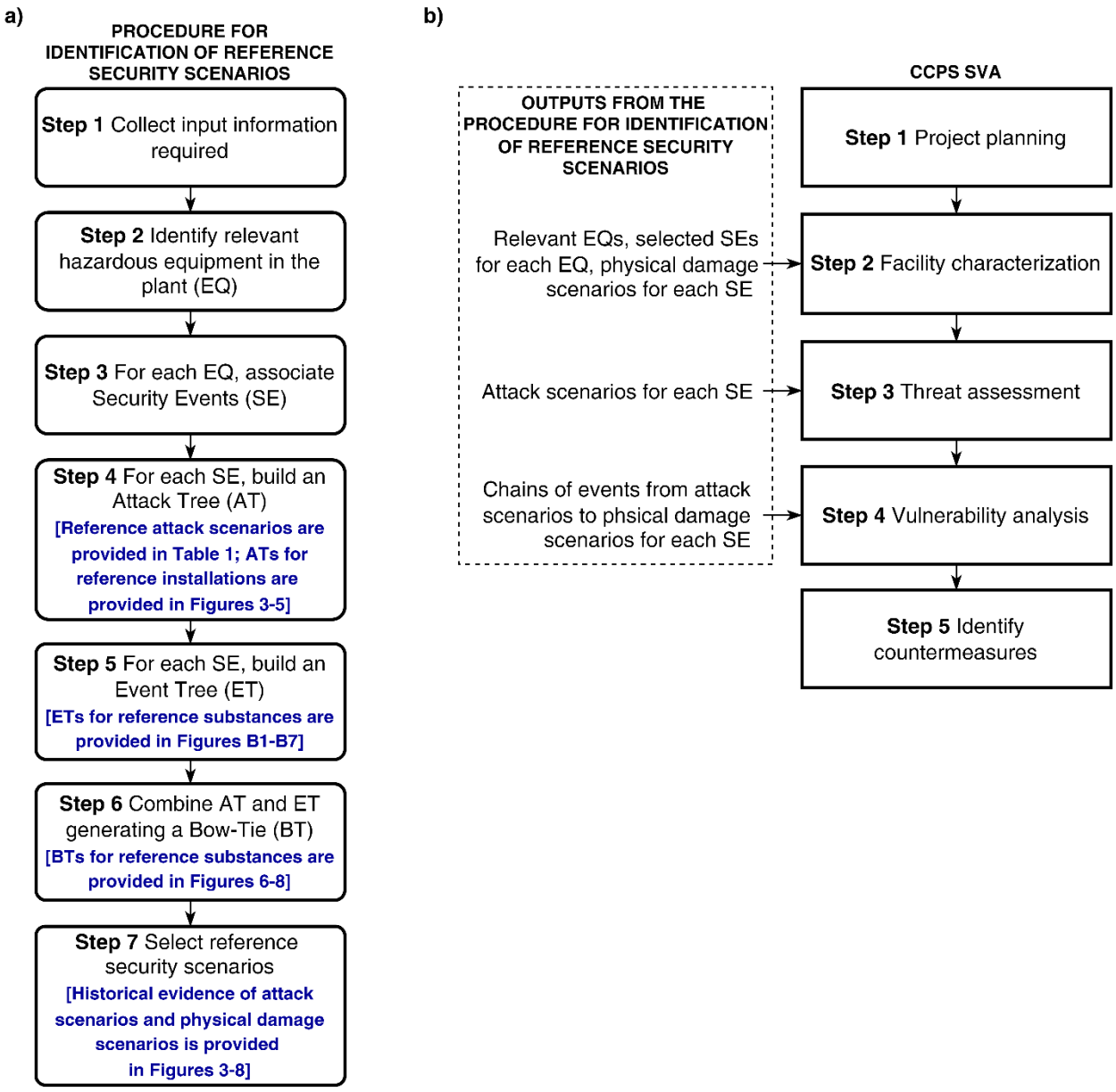

Figure 9. (a) Flowchart of the procedure proposed for the identification of reference security scenarios; (b) Contribution of the proposed procedures in supporting application of CCPS SVA.

4.2 Illustrative 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 10 shows an atmospheric floating roof storage tank (TA01) containing a low-volatility 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 35 m. Three alternative potential locations reached by the attacker were considered (see Figure 10). In the first case (P1), position P1 is outside the site fence (at 50 m from TA01). In the second case (P2), the attacker should enter the plant internal road network, but the attack takes place from position P2 that is outside the catch basin of TA01. In the third case (P3), the attack takes place from position P3 that is in close proximity of TA01, inside the catch basin.

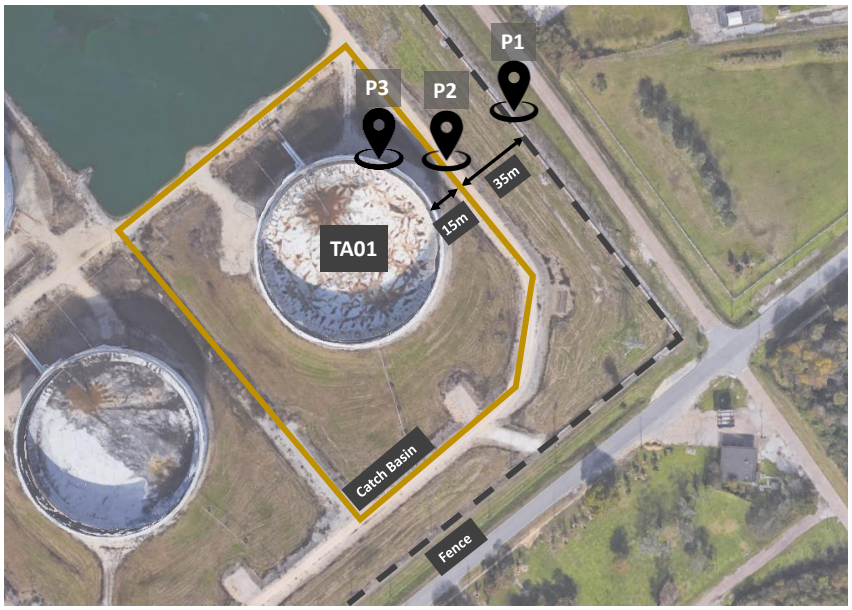

Figure 10. Layout of the site considered for the case-study showing the atmospheric storage tank TA01, the catch basin (continuous yellow line), the site fence (black and grey dashed line), and the positions P1, P2, and P3.

4.3 Step-by-step application of the procedure

The procedure for the identification of reference security scenarios consists of 7 steps (see Figure 9-(a)).

In Step 1, the input information needed for the application of the method 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 (see Section 4.2).

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. (2012), RISI by Rathnayaka et al. (2014), and PSI by Shariff et al. (2012), 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 (Dow Chemical Company, 1994), the Mond Index (Tyler, 1985), and the threshold-based approach proposed by MIMAH methodology (Delvosalle et al., 2006), 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 the present approach,

Since the substance involved in the storage section considered in the case-study is a flammable liquid, the Dow F&EI 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 this step. For the sake of brevity, among all the tanks with the highest scores, tank TA01 (see Figure 10) was selected for further assessment. Its inherent hazard is due to the large inventory of flammable liquid stored that can be potentially be released (24000 m^3).

In Step 3, the compatible Security Events (SE) are associated to each relevant hazardous equipment selected. A SE is intended as loss of physical integrity (LPI) and/or a loss of containment (LOC) of the hazardous material stored in the equipment unit. The categories of LPIs and LOCs proposed by the standard API RP 581 (American Petroleum Institute, 2016), the MIMAH methodology (Delvosalle et al., 2006) and the TNO "Purple Book" (Uijt de Haag and Ale, 2005) can be used as reference. In the present approach, the SEs suggested by the TNO "Purple Book" for atmospheric tanks were considered for tank TA01: 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).

In Step 4, an Attack Tree (AT) is built or selected for each SE. The AT should report all the routes through which the relevant hazardous equipment (EQ) under consideration can be attacked (i.e. the Attack Modes (AM)) using the fault tree formalism (International Electrotechnical Commission, 2021). The present study provides an exhaustive set of validated attack scenarios (AMs and respective RAIs, see Section 3.1) that can be used to build a case-specific AT, obtained from an extended review of those 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 those 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 a storage installation or a warehouse, the present study provides reference validated ATs (see Section 3.2) that can be directly used as output of this step. In the present case-study, the AT shown in Figure 3 is applicable to all the three SEs considered above. If necessary, case-specific considerations shall be introduced in order to exclude AMs among those appearing in Figure 3 which are deemed not credible in generating the SEs considered (see Figure 10 and discussion of Step 6 of the methodology).

In the case-study analyzed, 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 1). While worst-case loss intensity (i.e. a LI2 release loss intensity, see Table 1) is supposed to be achieved in case of use of aids (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 Section 3.2.1, 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 Appendix C) 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. Information on the effects of the peak overpressure (originated by the detonation of explosive devices) on atmospheric equipment is present in Landucci et al. (2015). In particular, the detonation of 50 kg of TATP (RAI#03-A) is deemed to cause damage at a distance of less than about 25 m, while in case of detonation of 30 kg of TATP (RAI#03-B) at a distance less than 20 m. 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.

Similar considerations apply to the detonation of a vehicle bomb (AM#04) from both the positions accessible to vehicles (P1 and P2 in Figure 9, 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 (Landucci et al., 2015b), far farther than the distance between P1 and TA01 (50 m).

In case of shooting attacks (AM#05), a perforation is reasonably possible from each of the three positions considered. Actually, according to Nammo (2022) the armour piercing cartridge 5,56x45mm NATO (the one considered in the RAI#05) can penetrate up to 12 mm of AISI 1020 steel plate at a distance of 100 m, and, according to API 650 standards, shell thickness of atmospheric fixed roof storage installations is about 5-7 mm. However, only a L1 loss intensity release is expected in this case, since the diameter of the hole is nearly the same as that of the bullet (Gupta and Madhu, 1997).

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

In Step 5, an Event Tree (ET) is built for each SE, reporting all the events leading to the physical damage scenarios (FS). The method proposed in step 6 of the MIMAH methodology (Delvosalle et al., 2006) 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 the present case-study, the ET for flammable liquids reported in Figure B1 in Appendix B, is applicable to all the three SEs considered for tank TA01. Nevertheless, also in this case, specific considerations based on hazardous properties and storage conditions of the flammable liquid may be introduced to exclude some physical damage scenarios (see discussion of Step 6). In the present case-study, 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 6 are excluded. Outdoor uncontrolled combustion is not expected to create large clouds of acute toxic compounds, thus toxic cloud (FS#06) is also excluded.

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 present study, validated BTs for reference substances (atmospheric storage of flammable liquids, storage of flammable liquids in a warehouse, storage of oxidising solids with explosion hazards) are also provided in Section 3.3. When reference BTs are available, steps 4 and 5 may be bypassed and the tailoring of the AMs and of the physical damage scenarios are carried out directly in the present 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 (2021d) or expert judgment may be used to identify worst-case scenarios.

Alternatively, reference security scenarios may be identified on the basis of past accidents that have occurred in the past. The proposed AMs (see Section 3.1), ATs (see Section 3.2), and BTs (see Section 3.3) were validated using past events. Thus, all the security scenarios identified from the BT obtained in Step 6 can be selected as reference security scenarios.

With reference to the illustrative case-study, the worst-case criterion was used to identify reference security scenarios. Given the specific properties of the substance stored inside tank TA01, the pool fire is the worst-case FS among those present in the ET (right part of the BT) in Figure 6. 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 1).

The results obtained from the application of the methodology to the illustrative case-study are reported in section 5.2

5. Results

5.1 Reference Attack Modes, Attack Trees and Bow-Tie diagrams

The validated set of proposed Attack Modes (AMs) is reported in Figure 2. In particular, those deemed credible for the chemical and process industry are deliberate interferences with or without the use of aids (AM#01), arson using simple/incendiary means (AM#02), use of explosives (AM#03), using vehicle bomb (AM#04), shooting (AM#05), vehicle impact (AM#06). They are all defined in Table 1 together with reference examples for each of them, i.e. the Reference Acts of Interference (RAIs) that can be used as a basis for tailoring AMs with respect to specific cases.

Starting from the AMs and RAIs, the Attack Trees (AT) for reference installations were developed and validated. In particular, Figure 3 reports the obtained AT for atmospheric storage installations, Figure 4 the one obtained for pressurized storage installations, and Figure 5 that for storage warehouses. The Security Event (SE) in all the ATs is the loss of physical integrity (LPI) and/or a loss of containment (LOC) of the hazardous material contained inside the reference installation. In case of atmospheric and pressurized installations storing hazardous fluids, three LOCs have been considered, each characterized by a different loss intensity (LI): 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).

The Event Trees (ETs) generated using the method proposed in step 6 of the MIMAH methodology (Delvosalle et al., 2006) for the most frequent families of substances stored and processed in chemical and process plants are reported in Appendix B: flammable liquids (Figure B1), flammable pressurized gasses (Figure B2), flammable gasses (Figure B2), flammable cryogenic liquids (Figure B3), toxic pressurized gasses (Figure B4), pressurized liquefied toxic gasses (Figure B5), and oxidizing solids (Figure B6).

The Bow-Tie (BT) diagrams were obtained combining the proposed ATs and the generated ETs. For the sake of brevity, only those for which validation was possible were discussed: atmospheric storage of flammable liquids (Figure 6), storage of flammable liquids in a warehouse (Figure 7), and storage of oxidising solids with explosion hazards (Figure 8).

Overall, the set of proposed AMs, ATs, and BTs can be used to easily integrate the Bow-Tie approach proposed for the identification of reference security scenarios (chains from attack scenarios to physical damage scenarios). The approach is summarized in Section 4.1 (flowchart reported in Figure 9-(a)), and described step-by-step in Section 4.3.

5.2 Results of the case-study

The case-study is described in Section 4.2: it addresses an atmospheric tank (TA01 in the layout reported in Figure 10) storing a low volatile flammable liquid. Application of the Bow-Tie approach and use of reference AMs, ATs, BTs to the case-study is described in Section 4.2.

Table 4 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 10).

Table 4. 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.

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

6. Discussion

The present study provides tools based on the 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 shows that there is historical evidence at least of part of the events in the sequences identified for the security scenarios proposed.

The step-by-step applicative use of the proposed AMs, ATs, BTs (Section 4.3) to the atmospheric tank storing a low volatile flammable liquid considered in the case-study proved the quality of the results that can be achieved in supporting SVA/SRA. In particular, the security scenarios identified in the case-study (summarized in Table 4) are requested in the application of SVA/SRA methodologies suitable for the security assessment of chemical and process facilities such as that developed by the CCPS (see flowchart in Figure 9-(b)). Actually, application of Step 2 "Facility characterization", Step 3 "Threat assessment", and Step 4 "Vulnerability analysis" of the CCPS SVA requires the identification of the relevant hazardous equipment in the plant, of the potential security events (LPI and/or LOCs) that can occur in such equipment, of the attack scenarios by which the SEs can be generated, and of 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 4.1 based on the Bow-Tie formalism.

It is important to remark 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, and that of BTs to the storage of flammable liquids (in atmospheric tanks or in storage warehouses) and of oxidizing solids having explosion hazard. However, the step-by-step procedure described in Section 4.1 for the identification of reference security scenarios is applicable to any type of equipment unit and hazardous substance, allowing the assessment of both process and storage sections of a plant. Future developments can therefore be aimed at developing specific ATs and BTs for a broader set of process equipment and hazardous substances.

The security scenarios listed in Table 4 can also support the identification of security countermeasures (intended as elements of the physical protection system (PPS) with functions such as delay, detection, and/or response). For example, the potential severity of the physical damage scenarios associated to AM#03 (use of explosive devices) suggests to enforce 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 remark that also the identification of security countermeasures is requested to apply SVA/SRA methodologies (e.g. steps 4 and 5 of CCPS SVA).

The identified security scenarios (Table 4) 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 (Ylönen et al., 2021a, 2021b).

The safety-related Bow-Tie diagram developed for tank TA01 in the context of a Safety Report is shown Figure 11. The BT includes physical damage scenarios that match those identified using the reference security-related BT in Figure 6. Therefore, both internal (evacuation plan) and external (population sheltering) emergency response and mitigation plans developed for safety scenarios may be adapted to address the security issues. This also suggests that the response to safety scenarios can be adapted to consider specific issues arising from security threats and security-specific physical damage scenarios can be included in the plan. In perspective, this may provide 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 (Abdo et al., 2018; Brewer, 1993; Firesmith, 2003).

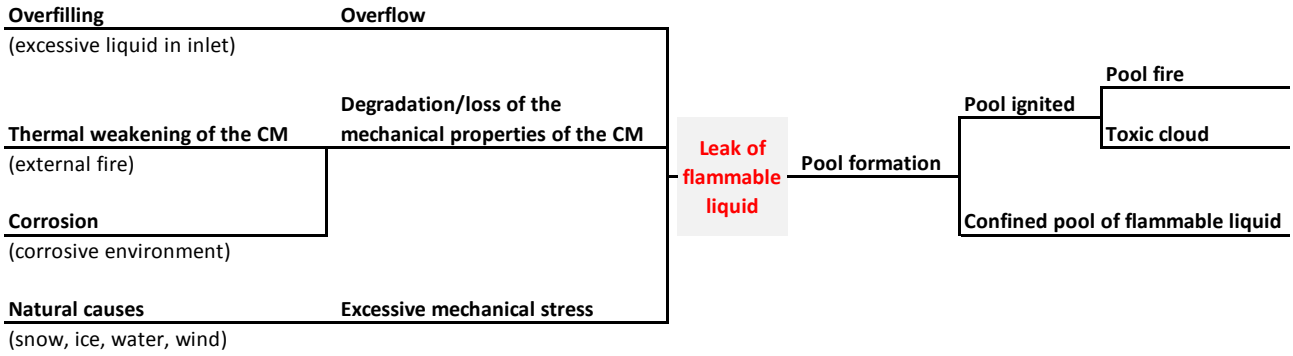

Figure 11. Safety-related Bow-Tie diagram developed considering a leak of flammable liquid from TA01 as critical event. CM: Construction material.

7. Conclusions

The present study provides a reference set of validated Attack Modes (AMs), Attack Trees (ATs) for reference installations, and Bow-Tie (BT) diagrams for reference hazardous substances that can be used for the identification of reference security scenarios that can originate in chemical and process plants. Validation was carried out using security-related incidents that occurred worldwide in the chemical and process industry in the last 50 years.

A step-by-step application of the proposed AMs, ATs, and BTs on a case-study addressing an atmospheric tank storing a low volatile flammable liquid allowed confirming the quality of the results that can be achieved in supporting scenario identification in the context of Security Vulnerability Assessment (SVA) and Security Risk Assessment (SRA) studies (e.g. VAM-CF, CCPS SVA, API RP 780 SRA, RAMCAP, SFK, and the novel quantitative methods proposed in recent years).

Besides their importance for SVA/SRA studies, security scenarios can also be used as a basis to foster the integration of security related events within major accident scenarios included in the Safety Reports of upper-tier European Union Seveso plants (Seveso Directive 2012/18/EU) in order to yield a more complete understanding of major accident hazard and to define a single set of safety/security requirements. Thus, the results achieved in the present study allow stepping forward in developing synergies and promoting integration among safety and security management.

Acknowledgments

The present study was carried out within the 4-STER project funded by INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) for in the framework of the 4th SAF€RA call.

References

Abdo, H., Kaouk, M., Flaus, J.M., Masse, F., 2018. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. Comput. Secur. 72, 175–195. https://doi.org/10.1016/j.cose.2017.09.004

Abdo, Houssein, Flaus, Jean-Marie, Masse, François, Abdo, H, Flaus, J.-M, Masse, F, 2017. Fuzzy semi-quantitative approach for probability evaluation using Bow-Tie analysis. HAL Arch. 2597–2605.

Abimbola, M., Khan, F., 2019. Resilience modeling of engineering systems using dynamic object-oriented Bayesian network approach. Comput. Ind. Eng. 130, 108–118. https://doi.org/10.1016/J.CIE.2019.02.022

Ackerman, G., Abhayaratne, P., Bale, J., Bhattacharjee, A., Blair, C., Hansell, L., Jayne, A., Kosal, M., Lucas, S., Moran, K., Seroki, L., Vadlamudi, S., 2007. Assessing Terrorist Motivations for Attacking Critical Infrastructure.

American Petroleum Institute (API), 2016. API standard 581: Risk-Based Inspection Technology.

American Petroleum Institute (API), 2013. API RP 780 - Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries.

Argenti, F., Landucci, G., Reniers, G., Cozzani, V., 2018. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. Reliab. Eng. Syst. Saf. 169, 515–530. https://doi.org/10.1016/j.ress.2017.09.023

Badr, A., Yosri, A., Hassini, S., El-Dakhakhni, W., 2021. Coupled Continuous-Time Markov Chain–Bayesian Network Model for Dam Failure Risk Prediction. J. Infrastruct. Syst. 27, 04021041. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000649

Bagster, D., Pitablado, R., 1989. Thermal hazards in the process industry. Chem. Eng. Prog. 85, 69–75.

Bajpai, S., Gupta, J.P., 2007. Terror-proofing chemical process industries. Process Saf. Environ. Prot. 85, 559–565. https://doi.org/10.1205/psep06046

Bajpai, S., Gupta, J.P., 2005. Site security for chemical process industries. J. Loss Prev. Process Ind. 18, 301–309. https://doi.org/10.1016/j.jlp.2005.06.011

Baybutt, P., 2018. On the completeness of scenario identification in process hazard analysis (PHA). J. Loss Prev. Process Ind. 55, 492–499. https://doi.org/10.1016/J.JLP.2018.05.010

Baybutt, P., 2017. Issues for security risk assessment in the process industries. J. Loss Prev. Process Ind. 49, 509–518. https://doi.org/10.1016/J.JLP.2017.05.023

bbc.com, 2019. Drone strikes set Saudi oil facilities ablaze [WWW Document]. URL https://www.bbc.com/news/world-middle-east-49699429 (accessed 11.6.20).

Bostick, T.P., Connelly, E.B., Lambert, J.H., Linkov, I., 2018. Resilience science, policy and investment for civil infrastructure. Reliab. Eng. Syst. Saf. 175, 19–23. https://doi.org/10.1016/j.ress.2018.02.025

Brewer, D., 1993. Applying security techniques to achieving safety. Springer, London.

Carreras Guzman, N.H., Kozine, I., Lundteigen, M.A., 2021. An integrated safety and security analysis for cyber-physical harm scenarios. Saf. Sci. 144, 105458. https://doi.org/10.1016/J.SSCI.2021.105458

Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631. https://doi.org/10.1016/j.psep.2018.03.026

Center for Chemical Process Safety (CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites.

Chen, C., Reniers, G., Khakzad, N., 2019. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach. Reliab. Eng. Syst. Saf. 191, 106470. https://doi.org/10.1016/j.ress.2019.04.023

Chen, C., Yang, M., Reniers, G., 2021. A dynamic stochastic methodology for quantifying HAZMAT storage resilience. Reliab. Eng. Syst. Saf. 215, 107909. https://doi.org/10.1016/J.RESS.2021.107909

cnbc.com, 2019. Satellite photos show extent of damage to Saudi Aramco plants [WWW Document]. URL https://www.cnbc.com/2019/09/17/satellite-photos-show-extent-of-damage-to-saudi-aramco-plants.html (accessed 11.6.20).

Commission of the European Communities, 2006. Communication from the Commission on a European Programme for Critical Infrastructure Protection.

Cozzani, V., Gubinelli, G., Salzano, E., 2006. Escalation thresholds in the assessment of domino accidental events. J. Hazard. Mater. 129, 1–21. https://doi.org/10.1016/j.jhazmat.2005.08.012

Cozzani, V., Tugnoli, A., Bonvicini, S., Salzano, E., 2013. Threshold-Based Approach, in: Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier B.V., pp. 189–207. https://doi.org/10.1016/B978-0-444-54323-3.00009-9

Cusimano, J., Rostick, P., 2018. If It Isn't Secure, It Isn't Safe: Incorporating Cybersecurity into Process Safety. AIChE Spring Meet. Glob. Congr. Process Saf.

Cutter, S.L., Ahearn, J.A., Amadei, B., Crawford, P., Eide, E.A., Galloway, G.E., Goodchild, M.F., Kunreuther, H.C., Li-Vollmer, M., Schoch-Spana, M., Scrimshaw, S.C., Stanley, E.M., Whitney, G., Zoback, M. Lou, 2013. Disaster Resilience: A National Imperative. Environ. Sci. Policy Sustain. Dev. 55, 25–29. https://doi.org/10.1080/00139157.2013.768076

Delvosalle, C., Fievez, C., Pipart, A., Debray, B., 2006. ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. J. Hazard. Mater. 130, 200–219. https://doi.org/10.1016/J.JHAZMAT.2005.07.005

Dow Chemical Company, 1994. Fire & explosion index hazard classification guide, 7th ed. New York:: American Insitute of Chemical Engineers (AIChE).

Eames, D., Moffett, J., 1999. The integration of safety and security requirements. Proc. 18th Int. Conf. Comput. safety, Reliab. Secur.

eMARS database [WWW Document], 2021. URL https://emars.jrc.ec.europa.eu/en/emars/content (accessed 12.23.20).

Engelhard, W.F.J.M., 2005. Heat flux from fires – Chapter 6 of the "Yellow Book." Committee for the Prevention of Disasters, The Hague (NL).

European Committee for Standardization (CEN), 2019. EN 1063: Glass in building - Security glazing - Testing and classification od resistance against bullet attack.

European Committee for Standardization (CEN), 1999. BS EN 1522: Windows, doors, shutters and blinds - Bullet resistance - Requirements and classification.

European Parliament and Council, 2012. 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 L197, 1–37.

Feng, Q., Cai, H., Chen, Z., 2019. 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. 191, 105900. https://doi.org/10.1016/J.RESS.2017.07.003

Firesmith, D., 2003. Common concepts underlying safety security and survivability engineering.

Garcia, M.L., 2007. The Design and Evaluation of Physical Protection systems, 2nd ed, Design and Evaluation of Physical Protection Systems: Second Edition. Butterworth–Heinemann. https://doi.org/10.1016/C2009-0-25612-1

Gilligan, J.M., 2021. Expertise Across Disciplines: Establishing Common Ground in Interdisciplinary Disaster Research Teams. Risk Anal. 41, 1171–1177. https://doi.org/10.1111/RISA.13407

Global Terrorism Database (GTD) [WWW Document], 2021. URL https://start.umd.edu/data-tools/global-

terrorism-database-gtd (accessed 12.8.20).

Gupta, N.K., Madhu, V., 1997. An experimental study of normal and oblique impact of hard-core projectile on single and layered plates. Int. J. Impact Eng. 19, 395–414. https://doi.org/10.1016/s0734-743x(97)00001-8

Gyenes, Z., Wood, M.H., Struckl, M., 2017. Handbook of Scenarios for Assessing Major Chemical Accident Risks, EUR 28518. https://doi.org/10.2760/884152

Hashimoto, Y., Toyoshima, T., Yogo, S., Koike, M., Hamaguchi, T., Jing, S., Koshijima, I., 2013. Safety securing approach against cyber-attacks for process control system. Comput. Chem. Eng. 57, 181–186. https://doi.org/10.1016/j.compchemeng.2013.04.019

Hausken, K., 2020. Cyber resilience in firms, organizations and societies. Internet of Things 11, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hausken, K., 2017. Security Investment, Hacking, and Information Sharing between Firms and between Hackers. Games 8, 23. https://doi.org/10.3390/g8020023

Iaiani, M., Casson Moreno, V., Reniers, G., Tugnoli, A., Cozzani, V., 2021a. Analysis of events involving the intentional release of hazardous substances from industrial facilities. Reliab. Eng. Syst. Saf. 212, 107593. https://doi.org/10.1016/J.RESS.2021.107593

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

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021c. Major accidents triggered by malicious manipulations of the control system in process facilities. Saf. Sci. 134, 105043. https://doi.org/10.1016/j.ssci.2020.105043

Iaiani, M., Tugnoli, A., Macini, P., Cozzani, V., 2021d. Outage and asset damage triggered by malicious manipulation of the control system in process plants. Reliab. Eng. Syst. Saf. 213, 107685. https://doi.org/10.1016/j.ress.2021.107685

International Electrotechnical Commission (IEC), 2021. IEC 61025: Fault Tree Analysis (FTA).

International Electrotechnical Commission (IEC), 2018. IEC 60812 standard: Failure modes and effects analysis (FMEA and FMECA).

International Electrotechnical Commission (IEC), 2016. IEC 61882 standard: Hazard and operability studies (HAZOP studies) - Application guide.

Italian Government and Parliament, 2015. Legislative Decree 105/2015: Attuazione della direttiva 2012/18/UE relativa al controllo del pericolo di incidenti rilevanti connessi con sostanze pericolose. Gazz. Uff.

Jaeger, C.D., 2002. Vulnerability assessment methodology for chemical facilities (VAM-CF). Chem. Heal. Saf. 9, 15–19. https://doi.org/10.1016/S1074-9098(02)00389-1

Ji, Z., Yang, S.H., Cao, Y., Wang, Y., Zhou, C., Yue, L., Zhang, Y., 2021. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Saf. Environ. Prot. 148, 1279–1291. https://doi.org/10.1016/j.psep.2021.03.004

Jon, M.H., Kim, Y.P., Choe, U., 2021. 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. 236, 109000. https://doi.org/10.1016/J.OCEANENG.2021.109000

Khakzad, N., Khakzad, S., Khan, F., 2014a. Probabilistic risk assessment of major accidents: application to offshore blowouts in the Gulf of Mexico. Nat. Hazards 74, 1759–1771. https://doi.org/10.1007/s11069-014-1271-8

Khakzad, N., Khan, F., Amyotte, P., 2013. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Saf. Environ. Prot. 91, 46–53. https://doi.org/10.1016/J.PSEP.2012.01.005

Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliab. Eng. Syst. Saf. 96, 925–932.

https://doi.org/10.1016/J.RESS.2011.03.012

Khakzad, N., Khan, F., Paltrinieri, N., 2014b. On the application of near accident data to risk analysis of major accidents. Reliab. Eng. Syst. Saf. 126, 116–125. https://doi.org/10.1016/J.RESS.2014.01.015

Khakzad, N., Reniers, G., 2019. Low-capacity utilization of process plants: A cost-robust approach to tackle man-made domino effects. Reliab. Eng. Syst. Saf. 191, 106114. https://doi.org/10.1016/J.RESS.2018.03.030

Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Prot. 110, 102–114. https://doi.org/10.1016/j.psep.2017.06.019

Landucci, G., Reniers, G., 2019. Preface to special issue on quantitative security analysis of industrial facilities. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2019.106611

Landucci, G., Reniers, G., Cozzani, V., Salzano, E., 2015. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliab. Eng. Syst. Saf. 143, 53–62. https://doi.org/10.1016/j.ress.2015.03.004

Leoni, L., BahooToroody, A., Abaei, M.M., De Carlo, F., Paltrinieri, N., Sgarbossa, F., 2021. On hierarchical bayesian based predictive maintenance of autonomous natural gas regulating operations. Process Saf. Environ. Prot. 147, 115–124. https://doi.org/10.1016/J.PSEP.2020.08.047

Leveson, N., 1995. SafeWare: System safety and computers. Addison-Wesley, Reading (USA).

Li, Z., Hu, S., Gao, G., Yao, C., Fu, S., Xi, Y., 2021. Decision-making on process risk of Arctic route for LNG carrier via dynamic Bayesian network modeling. J. Loss Prev. Process Ind. 71, 104473. https://doi.org/10.1016/J.JLP.2021.104473

Lou, H.H., Muthusamy, R., Huang, Y., 2003. Process security assessment: Operational space classification and process security index. Process Saf. Environ. Prot. Trans. Inst. Chem. Eng. Part B 81, 418–429. https://doi.org/10.1205/095758203770866593

Mannan, S., 2012. Lees' Loss Prevention in the Process Industries, 4th ed. Elsevier. https://doi.org/10.1016/C2009-0-24104-3

Matteini, A., Argenti, F., Salzano, E., Cozzani, V., 2019. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab. Eng. Syst. Saf. 191, 106083. https://doi.org/10.1016/j.ress.2018.03.001

Moore, D.A., Fuller, B., Hazzan, M., Jones, J.W., 2007. Development of a security vulnerability assessment process for the RAMCAP chemical sector. J Hazard Mater 142, 689–694.

Mudan, K.S., 1984. Thermal radiation hazards from hydrocarbon pool fires. Prog. Energy Combust. Sci. 10, 59–80. https://doi.org/10.1016/0360-1285(84)90119-9

Nammo, 2022. Nammo AS - 5.56mm (.22 Cal) [WWW Document]. URL https://web.archive.org/web/20071111054712/http://www.nammo.com/templates/Product.aspx?id=206 (last accessed 11.03.2022).

National Fire Protection Association (NFPA), 2007. NFPA 555 - Methods for Evaluating Potential for Room Flashover.

nytimes.com, 2019. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran [WWW Document]. URL https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html (accessed 11.24.20).

Ovidi, F., van der Vlies, V., Kuipers, S., Landucci, G., 2020. HazMat transportation safety assessment: Analysis of a "Viareggio-like" incident in the Netherlands. J. Loss Prev. Process Ind. 63, 103985. https://doi.org/10.1016/j.jlp.2019.103985

Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., Cozzani, V., 2012. Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. Risk Anal. 32, 1404–1419. https://doi.org/10.1111/j.1539-

6924.2011.01749.x

Paltrinieri, N., Reniers, G., 2017. Dynamic risk analysis for Seveso sites. J. Loss Prev. Process Ind. 49, 111–119. https://doi.org/10.1016/j.jlp.2017.03.023

Pert, A.D., Baron, M.G., Birkett, J.W., 2006. Review of Analytical Techniques for Arson Residues. J. Forensic Sci. 51, 1033–1049. https://doi.org/10.1111/j.1556-4029.2006.00229.x

Pietre-Cambacedes, L., Bouissou, M., 2013. Cross-fertilization between safety and security engineering. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2012.09.011

Planas, E., Pastor, E., Casal, J., Bonilla, J.M., 2015. Analysis of the boiling liquid expanding vapor explosion (BLEVE) of a liquefied natural gas road tanker: The Zarzalico accident. J. Loss Prev. Process Ind. 34, 127–138. https://doi.org/10.1016/j.jlp.2015.01.026

Raj, P.K., 2007. LNG fires: A review of experimental results, models and hazard prediction challenges. J. Hazard. Mater. https://doi.org/10.1016/j.jhazmat.2006.10.029

Rathnayaka, S., Khan, F., Amyotte, P., 2014. Risk-based process plant design considering inherent safety. Saf. Sci. 70, 438–464. https://doi.org/10.1016/J.SSCI.2014.06.004

Rezazadeh, A., Talarico, L., Reniers, G., Cozzani, V., Zhang, L., 2019. Applying game theory for securing oil and gas pipelines against terrorism. Reliab. Eng. Syst. Saf. 191, 106140. https://doi.org/10.1016/J.RESS.2018.04.021

Shariff, A., Leong, C.T., Zaini, D., 2012. Using process stream index (PSI) to assess inherent safety level during preliminary design stage 50, 1098–1103. https://doi.org/10.1016/j.ssci.2011.11.015

Skogdalen, J.E., Vinnem, J.E., 2012. Combining precursor incidents investigations and QRA in oil and gas industry. Reliab. Eng. Syst. Saf. 101, 48–58. https://doi.org/10.1016/j.ress.2011.12.009

Sørby, K., 2003. Relationship between security and safety in a security-safety critical system: Safety consequences of security threats. M.Sc thesis.

Störfall-Kommission (SFK), 2002. SFK–GS–38 - Combating Interference by Unauthorised Persons.

The ARIA Database - La référence du retour d'expérience sur accidents technologiques [WWW Document], 2021. URL https://www.aria.developpement-durable.gouv.fr/the-barpi/the-aria-database/?lang=en (accessed 12.8.20).

Tugnoli, A., Gyenes, Z., Van Wijk, L., Christou, M., Spadoni, G., Cozzani, V., 2013. Reference criteria for the identification of accident scenarios in the framework of land use planning. J. Loss Prev. Process Ind. 26, 614–627. https://doi.org/10.1016/j.jlp.2012.12.004

Tugnoli, A., Landucci, G., Salzano, E., Cozzani, V., 2012. Supporting the selection of process and plant design options by Inherent Safety KPIs. J. Loss Prev. Process Ind. 25, 830–842. https://doi.org/10.1016/j.jlp.2012.03.008

Tyler, B.J., 1985. Using the Mond Index to Measure Inherent Hazards. Plant/Operations Prog. 4, 172–175. https://doi.org/doi:10.1002/prsb.720040313

Uijt de Haag, P., Ale, B., 2005. Guidelines for quantitative risk assessment (TNO Purple Book).

United Nations Statistics Division (UNSD), 1999. Standard statistical classifications: Basic principles.

valkyrie.pro, 2019. VALKYRIE HEAVY PRO New 2019 - datasheet [WWW Document]. URL https://www.valkyrie.pro/ (accessed 7.13.21).

van Staalduinen, M.A., Khan, F., Gadag, V., Reniers, G., 2017. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. Reliab. Eng. Syst. Saf. 157, 23–34. https://doi.org/10.1016/j.ress.2016.08.014

Voorhees, E., 2017. Vehicle Ramming Incidents and Perimeter Protection.

Wiley-VCH (Ed.), 2011. Ullmann's Encyclopedia of Industrial Chemistry, 7th ed, Ullmann's Encyclopedia of Industrial Chemistry.

Woodward, R.L., 1978. The penetration of metal targets by conical projectiles. Int. J. Mech. Sci. 20, 349–359. https://doi.org/10.1016/0020-7403(78)90038-3

Ylönen, M., Nissilä, M., Heikkilä, J., Gotcheva, N., Tugnoli, A., Iaiani, M., Cozzani, V., Oliva, G., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Young, H., Roelofs, M., 2021a. Integrated management of safety and security synergies in Seveso plants (SAF€RA 4STER). Final Report.

Ylönen, M., Nissilä, M., Heikkilä, J., Gotcheva, N., Tugnoli, A., Iaiani, M., Cozzani, V., Oliva, G., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Young, H., Roelofs, M., 2021b. Guidelines: Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER).

Zhang, L., Reniers, G., Qiu, X., 2019. Playing chemical plant protection game with distribution-free uncertainties. Reliab. Eng. Syst. Saf. 191, 105899. https://doi.org/10.1016/J.RESS.2017.07.002

Zhu, C., Zhu, J., Wang, L., Mannan, M.S., 2017. Lessons learned from analyzing a VCE accident at a chemical plant. J. Loss Prev. Process Ind. 50, 397–402. https://doi.org/10.1016/j.jlp.2017.11.004

Appendix A: Dataset used for ATs and BTs validation and scenario definitions

Table A1. Details on security-related incidents with some information available on the chain from attack scenarios to physical damage scenarios.

ID	Date	Country	Attack Description	Impact description	Reference
#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.	Ackerman et al., 2007
#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.	(GTD, 2021)
#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.	(GTD, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#22	14/09/1989	Pakistan	Deliberate acts using explosive devices on a chemical store.	The chemical store suffered damages.	(GTD, 2021)

#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.	(eMARS database, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#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.	(ARIA database, 2021)
#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.	(eMARS database, 2021)
#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.	(ARIA database, 2021)

#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.	(ARIA database, 2021)
#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.	(eMARS database, 2021)
#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.	(ARIA database, 2021)
#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 (BBC.com, CNBC.com)

Appendix B: Event Trees

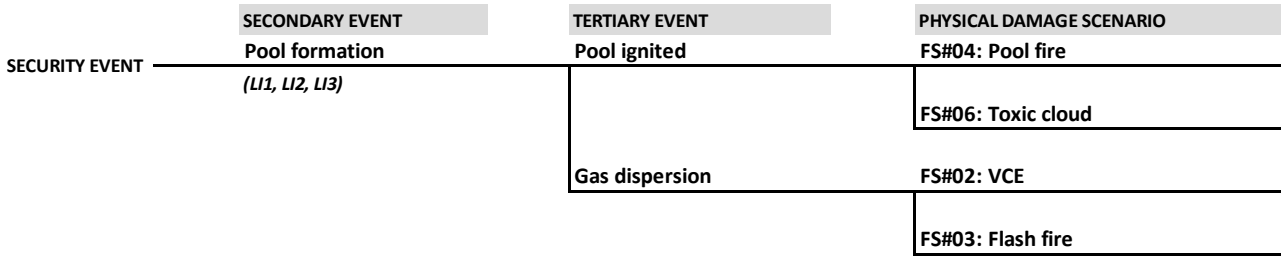

Figure B1. Event Tree for flammable liquids generated with MIMAH methodology (Delvosalle et al., 2006).

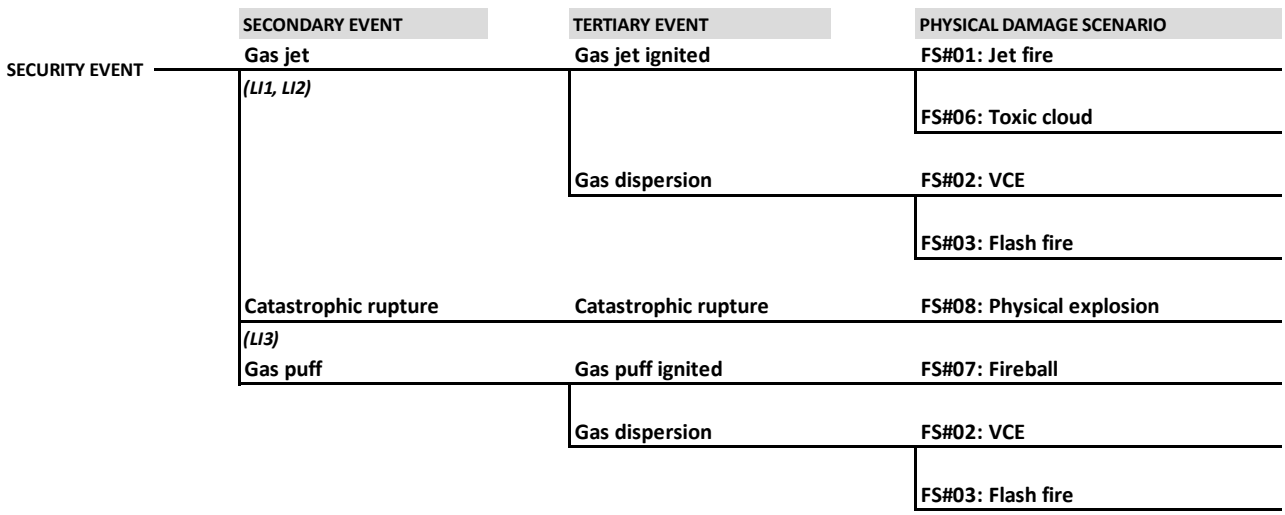

Figure B2. Event Tree for flammable pressurized gasses generated with MIMAH methodology (Delvosalle et al., 2006).

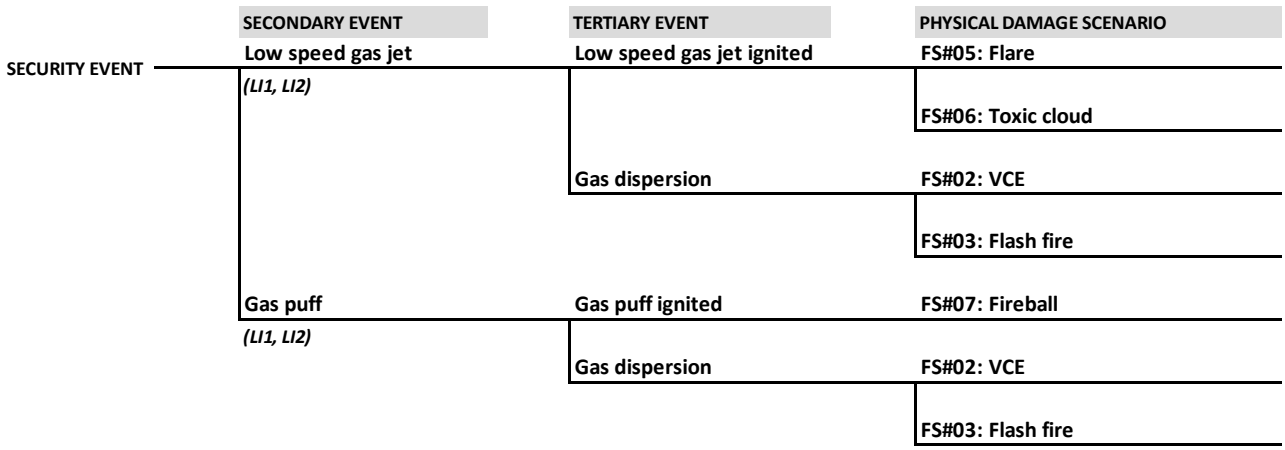

Figure B3. Event Tree for flammable gasses generated with MIMAH methodology (Delvosalle et al., 2006).

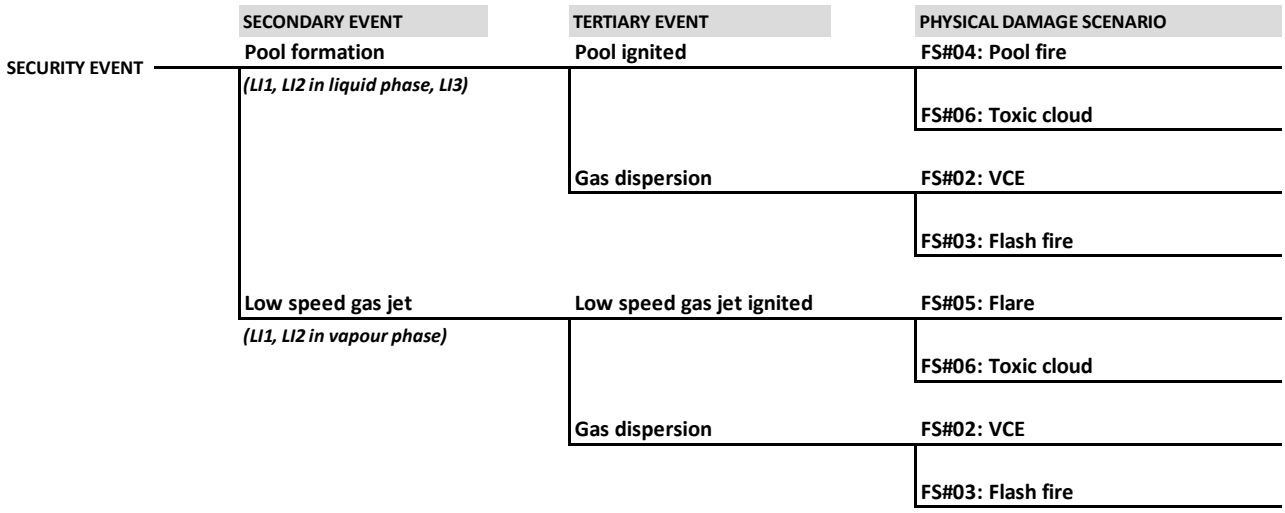

Figure B4. Event Tree for flammable cryogenic liquids generated with MIMAH methodology (Delvosalle et al., 2006).

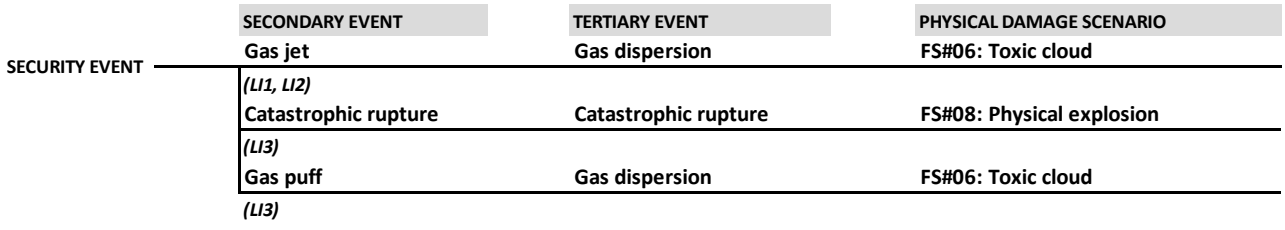

Figure B5. Event Tree for toxic pressurized gasses generated with MIMAH methodology (Delvosalle et al., 2006).

	SECONDARY EVENT	TERTIARY EVENT	PHYSICAL DAMAGE SCENARIO
SECURITY EVENT	Gas jet	Gas dispersion	FS#06: Toxic cloud
	(LI1, LI2 in vapour phase)		
	Pool formation	Gas dispersion	FS#06: Toxic cloud
	(LI1, LI2 in liquid phase, LI3)		
	Two-phase jet	Gas dispersion	FS#06: Toxic cloud
	(LI1, LI2 in liquid phase)		
	Catastrophic rupture	Catastrophic rupture	FS#08: Physical explosion
	(LI3)		
	Areosol puff	Gas dispersion	FS#06: Toxic cloud
	(LI3)		

Figure B6. Event Tree for pressurized liquefied toxic gasses generated with MIMAH methodology (Delvosalle et al., 2006).

	SECONDARY EVENT	TERTIARY EVENT	PHYSICAL DAMAGE SCENARIO
DECOMPOSITION	Decomposition	Decomposition	FS#09: Confined chemical explosion
	Decomposition	Toxic secondary products	FS#06: Toxic cloud

Figure B7. Event Tree for oxidizing solids generated with MIMAH methodology (Delvosalle et al., 2006).

Table B1. Definitions of the physical damage scenarios (FS) considered in the present analysis, adapted from the "Yellow Book" of TNO (Van Den Bosh, C.J.H. Weterings, 2005).

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.

Appendix C: Analysis of the potential damage caused by incendiary attacks (AM#02)

In this section the potential damages caused by incendiary attacks (AM#02) to the three categories of reference target storage installations considered in the present study (RI1: atmospheric storage installation; RI2: pressurized storage installation; RI3: storage warehouse), are analysed.

In particular, the two Reference Act of Interference (RAI) associated to this AM were considered in the characterization of the attacks in the calculations (see also Table 1):

- RAI#02-A: ignition of 50 L of gasoline (unconfined pool)
- RAI#02-B: ignition of 1000 L of gasoline (unconfined pool and confined pools 2x2/3x3/4x4 m^2)

It's important to underline that for RAI#02-B, different pool sizes were considered due to the potential presence of obstacles limiting the pool spreading (e.g. curbs, other units, bunds) in case of a relatively large pool.

The liquid pool fires (FS#04, see definition in Table B1) originated in the two aforementioned RAIs and the heat load generated by flames, were modelled using the correlations derived by Mudan (1984), Raj (2007), Bagster and Pitablado (1989) reported in the "Yellow Book" of TNO (Engelhard, 2005). Gravel was considered as ground material for calculation of diameter in case of unconfined pools originated in the storage area where RI1 and RI2 installations are generally located, while concrete was considered as ground material inside warehouses (RI3 installations).

In case of RI1 and RI2 installations (steel-made equipment), the radiative heat flux was evaluated as function of the distance and of the duration of the fire. These parameters were compared with the damage criteria (damage threshold values) provided in a study by Cozzani et al. (2006), which correlate the heat flux with the time to failure (*ttf*) of atmospheric (RI1) and pressurized (RI2) steel-made equipment, in order to assess the extent of damage with distance. Distances for which the damage threshold value (evaluated considering the fire duration) can not be reached, were considered safe for the target equipment.

The damage threshold values above were not adopted for storage warehouses (RI3 installations) as not applicable to the typical containers used for flammable substances (rigid plastic containers, thin metal sheet containers or bags). Given the lack in literature of damage threshold values for such materials, 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" (NFPA, 2009) was adopted to define the extent of damage with distance in case of incendiary attacks to storage warehouses.

It is important to underline that, as common in the assessment of fire scenarios (Cozzani et al., 2006), it was not possible to discriminate a priori between loss intensities LI1, LI2, and LI3: in fact, the extension of damage depends on specific features of the target installations and of the attack.

The results for atmospheric (RI1) and pressurized (RI2) storage installations are summarized in Table C1. The table shows for both RAI#02-A and RAI#02-B (see definitions above), the duration of each pool fire, the thermal radiation at 0 m, 5 m, 10 m, and 15 m from the flame centre (calculated using the aforementioned correlations), and the damage threshold values (thermal radiation for damage at pool fire duration). It is important to underline that thermal radiation in a point inside the flame has been taken equal to the actual surface emitter power (SEP), which is intended as the heat load per unit area which takes into account the effects of soot and smoke produced by the fire (Engelhard, 2005).

From Table C1 both RI1 and RI2 installations resulted safe from the heat load emitted by the ignition of an unconfined pool on gravel formed by 50 L of gasoline (RAI#02-A): in fact, the damage threshold value (Cozzani et al., 2006) at the pool fire duration (lower than 1 minute) is far greater than the calculated actual SEP (109 kW/m^2), which is the maximum heat flux (it decreases with distance).

On the other hand, as regards the ignition of 1000 L of gasoline contained e.g. inside IBC tanks (RAI#02-B), only atmospheric storage installations (RI1), and in presence of obstacles limiting the pool spreading, can be damaged within a distance of about 5 m from the centre of the flame (a few meters from the surface of the flame). Pressurized installations (RI2) can be damaged in close proximity to the fire or in case

of flame engulfment: these scenarios are not deemed credible since moving IBC tanks to such location would require equipment already considered in AM#01 and AM#06 (see Table 1).

As regards incendiary attacks to storage warehouses (RI3), the NEPA555 (NFPA, 2009) defines conventional separation distances of 1 m beyond which the items are not considered part of the same fuel package. Therefore, given the dimensions of the pool fires reported in Table C1 (diameter greater than 1 m), it is reasonable that arson attacks inside RI3 installations can easily involve multiple fuel packages.

Table C1. Duration and thermal radiation effects 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. (2006). The star (*) marks a value of thermal radiation for a point inside the flame (it is taken equal to SEP).

RAI code	**Pool size [m^2]**	**Pool fire duration [min]**	**Thermal radiation distance from flame centre [kW/m^2]**				**Thermal radiation for damage at pool fire duration [kW/m^2]**	
			0 m	**5 m**	**10 m**	**15 m**	**Atmospheric (RI1)**	**Pressurized (RI1)**
RAI#02-A	5 (unconfined on gravel, D=2.5m)	< 1	109*	14	5	2	140	>140
	5 (unconfined on concrete, D=3.5m)	< 1	99*	18	6	3	140	>140
RAI#02-B	103 (unconfined on gravel, D=11.5m)	< 1	50*	50*	16	9	140	>140
	201 (unconfined on concrete, D=16m)	< 1	38*	38*	18	10	140	>140
	16 (confined, 4x4m)	7	90*	22	9	5	22	74
	9 (confined, 3x3m)	12	100*	18	7	4	15	54
	4 (confined, 2x2m)	27	112*	12	4	2	12	45