Analysis of physical and cyber security-related events in the chemical and process industry

Casson Moreno, Valeria; Reniers, Genserik; Salzano, Ernesto; Cozzani, Valerio

DOI
10.1016/j.psep.2018.03.026

Publication date
2018

Document Version
Accepted author manuscript

Published in
Process Safety and Environmental Protection

ANALYSIS OF PHYSICAL AND CYBER SECURITY-RELATED EVENTS IN THE CHEMICAL AND PROCESS INDUSTRY

REVISED VERSION link to formal publ. https://doi.org/10.1016/j.psep.2018.03.026

Valeria CASSON MORENO[1], Genserik RENIERS[2], Ernesto SALZANO[1], Valerio COZZANI[1,*]

[1] LISES - Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum - Università di Bologna, via Terracini 28, 40131 Bologna (Italy)
[2] Safety and Security Science Group, Department of Values, Technology and Innovation, Delft University of Technology, Jaffalaan 5, 2628 BX Delft (Netherlands)

(*) Author to whom correspondence should be addressed.

tel. (+39)-051-2090240; fax (+39)-051-2090247

e-mail: valerio.cozzani@unibo.it

Submitted for publication in: ***Process Safety and Environmental Protection***

HIGHLIGHTS

- a database of 300 security-related accidents in the chemical industry was populated
- threats were analyzed with respect to geographical area and industrial sector
- cyber-attacks were found to play a significant role in recent years
- critical infrastructures are those where hazardous materials are stored
- lessons learnt revealed the need for a robust security management system

ABSTRACT

Security threats are becoming an increasing concern for chemical sites and related infrastructures where relevant quantities of hazardous materials are processed, stored or transported. In the present study, security related events that affected chemical and process sites, and related infrastructures, were investigated. The aim of the study is to frame a clear picture of the threats affecting the chemical and process industry, and to issue lessons learnt from past events. A database of 300 security-related accidents was developed and populated, starting from European and American sources. Threat categories that caused such events were identified and analyzed. The attack modes were investigated. Important differences were found with respect to geographical areas and industrial sectors affected. The use of explosives (both military and improvised explosive devices) is by far the more frequent attack mode, although armed attacks and arson are also frequent events and may result in an in-depth penetration of the attackers. In recent years, cyber-attacks are also posing important threats. Lessons learnt call for the implementation of a specific security management system in the chemical and process industry, aiming at the physical and cyber protection of industrial sites.

KEYWORDS
Security; cyber; attacks; threat; incidents; accidents; chemical and process industry.

1. INTRODUCTION

All over the world, strict regulations are usually applied to the chemical and process Industry (CPI) in order to minimize as much as possible the risk related to industrial activities and to prevent major accidents by implementing high safety standards (e.g. the Seveso Directives in the European Union (European Council, 2012), COMAH Regulations in the UK (Health and Safety Executive, 2015), the OSHA, EPA, and CBS Regulations in the US (Center for Chemical Process Safety - CCPS), The Factories Act in India (Parliament of India, 1948), the NORMA Official Mexicana in Mexico (Dirección General de Normas, 2011), etc..

The requirements are more jeopardized when security is considered. After the well-known terrorist attack of “9/11”, the security of sites where relevant quantities of hazardous chemicals are stored or processed became a concern in the U.S., where security risks are included in formal risk assessments (Argenti et al., 2017). The U.S. Department of Homeland Security (DHS) is required to analyze vulnerabilities and establish risk-based security performance standards for critical infrastructures, which include chemical facilities as one of the highest priority sectors (US Department for Homeland Security, 2008a), and facility operators are required to prepare a security vulnerability assessment and a facility security plan. A number of methods were proposed by several US bodies to apply such requirements to industrial facilities (e.g. see AIChE-CCPS, 2003; API, 2013; US Department of Justice, 2002).

In Europe, security falls outside the scope of the Seveso Directive. The “European Programme for Critical Infrastructure Protection (EPCIP)” (Commission of the European Communities, 2006) promotes the prevention, preparedness and response to terrorist attacks involving installations of the energy sectors (electricity, oil and gas), but does not extend to all the other CPI and depends on its implementation on the Member State.

In any case, the security of industrial sites, and in particular of the chemical and process industry (CPI), has become a matter of increasing concern in recent years (Argenti et al., 2015). Actually CPI sites are potentially attractive targets due to the storage of hazardous materials in relevant quantities, to the possible presence of chemicals that may be used to manufacture improvised explosive devices (IEDs), and to the increasing use of automated controls and safety instrumented systems that may allow cyber intrusions. Terrorist groups could exploit such features and cause major accidents involving fires and explosions (ARIA, 2015), as in the events which happened in France, or involving toxic releases and environmental contaminations (Lou et al., 2003). Furthermore, chemicals could be stolen with the intent of creating explosive devices or weapons (Landucci et al., 2015). As reported by the Organization for the Prohibition of Chemical Weapons (Organization for the prohibition of chemical weapons, 2008), many chemicals of industrial application can be employed as weapons of mass destruction or their precursors.

Further concern is posed nowadays towards the possibility of intrusion via cyber space. According to the 2016 Internet Security Threat Report, the largest number of cyber-attacks, until 2016, was recorded in 2015, reaching a total of 430 million incidents throughout the world (Joyce et al., 2017). In this prospect, cybersecurity is becoming something that the CPI can no longer disregard (Thomas and Day, 2015). In 2008, an analysis of 75 control-system security incidents between 2002 and 2007 revealed that more than 50% of the attacks came through secondary pathways such as dial-up connections, wireless systems and mobile devices (Byres, 2008).

Hacking practice is based on a continuous challenge targeted to overcome increasing levels of cyber security barriers, and hence intended to a recurrent overtaking of the attacker on the defender, and vice versa (Pescatore, 2017). Furthermore, security systems, such as antiviruses and firewalls, have a limited effectiveness towards internal threatening agents.

Indeed, insiders establish the most arduous type of threat, since often internal perpetrators have inside knowledge as well as access to the internal infrastructure and system, or they can more easily obtain credentials with respect to externals.

In addition to this, Nicholson et al. (Nicholson et al., 2012) highlighted that human aspects play a significant role in process control system (PCS) security, since there is a history of success in compromising SCADA systems by exploiting humans (Greene, 2008). Moreover, process control system governs all the operative and safety functions in medium-large scale facilities, and hence it has the potential to create outcomes even more catastrophic if compared to the one that could be set up by means of physical actions on the plant (French Ministry for an ecological and solidary transition, 2016).

In the US, cybersecurity is included in the Chemical Facility Anti-Terrorism Standards (CFATS) (Department of Homeland Security, 2017), and increasingly attention is being payed to it, e.g. with the implementation of the IEC 61508 standard (International Electrotechnical Commission, 2010) (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems).

In this panorama, the present study aims at retrieving and analyzing security-related accidents that affected CPI facilities, caused either by physical actions or cyber-attacks. A database of accidents triggered by intentional acts was created, collecting data from a various set of literature sources. The available data on past accidents were then analyzed, focusing mostly on causes and consequences of the events, and on lessons learnt.

2. METHODOLOGY

Some definition of key terms which are used in the present work are presented in Table 1. The following definitions are taken from the CCPS Guidelines glossary (CCPS - Center for Chemical Process Safety, 2003), and are intended as security-specific concepts.

The next section explains more in depth the approach that was used to investigate security-related events from the process industry and build a database.

2.1 Retrieval of data on past accidents

A database was built retrieving data on past security-related accidents that affected the chemical and process industry. Data were obtained searching the scientific literature, the web, and accessing specific open-source databases reporting data on industrial accidents. Two criteria were used to include events in the database: i) the event should originate from an intentional malicious act aimed at interfering with normal operations; and ii) the event involves an industrial facility or a related infrastructure for the transportation of chemicals (e.g. a pipeline) where relevant quantities of hazardous substances are processed or stored.
The benchmark is not associated with the intentionality of triggering a major accident, but solely with the intention to gain or share a benefit interfering with the normal operation of the facility. An industrial target is affected, actually or potentially leading to an event involving the hazardous substances present on the site. Therefore, theft (or attempted theft) as well as cyber intrusion were also considered.
The starting point of the study was the access to open-source databases dedicated to industrial accidental events:

- ARIA Database (French Ministry of Ecology Sustainable Development and Energy, 2017): managed by the French Ministry of Ecology, it collects more than 40000 accidents that harmed, or showed a potential damage for public health or safety and the environment.
- JRC eMARS (Major Accident Hazards Bureau (MAHB), 2002): the Major Accident Reporting System of the European Commission is managed by the Major Accidents Hazards Bureau at the European Joint Research Centre, and is aimed to facilitate the exchange of lessons learned from accidents and near misses involving dangerous substances in order to improve chemical accident prevention and mitigation of potential consequences.
- U.S. DoT PHMSA (United States Department of Transportation, 2017): the Pipeline and Hazardous Materials Safety Administration (PHMSA) was built up to support the safe transportation of energy and hazardous materials. It is managed by the U. S. Department of Transportation (DoT).
- E.U. Concawe (European Petroleum Refiners Association, 2017): established in 1963 and managed by the European Petroleum Refiners Association, has the goal to improve

scientific understanding of the environmental health, safety and economic performance of petroleum refining and distribution.

- Dechema ProcessNet (Dechema, 2017): created and handled by the German professional association Dechema, represents the national platform for process engineering, chemical engineering and technical chemistry, with the aim of exchanging experiences, discuss current issues and identify new scientific trends, including safety and lessons learnt on accidents and near misses.
- Infosis ZEMA (Deutsch Umwelt Bundesamt, 2017): the "Central reporting and evaluation center for incidents and faults for process industry" is devoted to the collection of accidents and disturbances in the process industry, according to the German "Ordinance on Hazardous Substances". It is developed by the German Federal Environmental Agency.
- E.U. EGIG (European Gas pipeline Incident Data Group, 2017): the European Gas Pipeline Incident data Group (EGIG) is devoted to the collection of incidents involving gas transmission systems.

Queries were carried out defining a set of specific keywords: "terrorist", "vandalism", "theft", "sabotage", "malicious act", "intentional act" and "criminal". Since not always events' summaries were translated in English, the analysis was performed considering both the English version of keywords and their translation in the language of origin of each database. A specific search for cyber-attacks was also carried out, but no related events were found in the aforementioned databases.

In order to expand the research two other databases not specifically dedicated to accidents involving the CPI were interrogated:

- the Global Terrorism Database (GTD) (National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2017): focused on intentional acts of terrorism and sabotage worldwide, is not tailored on industrial activities. The database is managed by the U.S. National Consortium for the Study of Terrorism and Responses to Terrorism (START) in collaboration with the Center for Terrorism and Intelligence Studies (CETIS) and is partially funded by the U.S. Department of Homeland Security (DHS). GTD is an open-source database including information on terroristic events worldwide covering a time span of 45 years (from 1970 to 2015).

- the Repository of Industrial Security Incidents (RISI) (Department of Homeland Security, 2017): an online database reporting cyber-security related events that have or (could have) affected process control, industrial automation or SCADA (Supervisory Control and Data Acquisition) systems.

To be noted that all the sources of information originate from Europe and US, where the accident the reporting systems are more consolidated. However, such sources collect events that may take place in any part of the world.

When consulting the latter two databases, only events that affected industrial sectors related to CPI were considered, namely:

1. Chemical and Petrochemical industry;
2. Transportation via road, rail, water of hazardous materials (HazMat);
3. Pipeline transportation;
4. Manufacturing facilities;
5. Other related sectors (power generation, water treatment).

Specific criteria were defined to search accidental records in open literature. In particular, the keywords “terrorist”, “vandalism”, “theft”, “sabotage”, “malicious act”, “intentional act” and “criminal” were associated (logical “AND”) to one of the following keywords: “industry”, “industrial”, “process”, and “plant”. The search was carried out translating the terms in several European languages (i.e. English, Italian, French, German, and Spanish). Due to the high number of sources exploited, particular attention was posed in avoiding double counting of events. Specific checks were carried out considering the date, country and type of facility involved in the event.

2.2 Accident Database

The data collected were organized in a database, whose structure was adapted from that developed in previous studies (Casson Moreno et al., 2016; Casson Moreno and Cozzani, 2015). Figure 1 shows how the database is structured, evidencing free text fields (in white boxes), and itemized fields (in coloured boxes). Free text fields allow importing details concerning the accidents, such as the original data source, geographical information (i.e. continent, country and city), number of people injured, number of fatalities, substances

involved in the accidental event, causes that led to the undesired event and the dynamics of such events, etc.
Itemized fields are used to introduce an unambiguous classification of scenarios, type of events (according to the definition given by Rathnayaka and coworkers (Rathnayaka et al., 2011) and reported in Table S1 of the Supplementary Material), industrial sector involved, and threat.

A total of 300 events were included in the database, considering both physical security (i.e. physical actions) and cyber security (i.e. cyber attacks) events. The time span covered is 47 years (from 1970 to 2017). The complete list of the events included in the database is reported in Table S3 of the Supplementary Material.
A total of 96% of the events were retrieved from the above mentioned open source databases. The remaining 4% were found in other online editions of newspapers and scientific publications, applying the search criteria discussed above. Among open source databases, GTD included the highest number of accidents (109 events, 36% of the total), followed by ARIA (61, 20%), Concawe (46, 15%), RISI (31, 10%), PHMSA (34 each, 11%), and eMARS (7, 2%). None of the events found in ProcessNet, ZEMA and EGIG fulfilled the inclusion criteria.
Table 2 reports the detailed description of the eight macro-sectors of industrial activities defined in order to classify the collected records in Figure 1 (adapted from the International Standard Industrial Classification of All Economic Activities, published by the United Nations in 2008).

A major issue has been the availability of relevant details on the events collected, mostly due to the lack of specific security-dedicated fields or details in the databases which were developed solely for industrial safety purposes. Thus, in the analysis of the recorded entries, relevant sub-sets were extracted to assess specific aspects, depending on the quality and detail of available information.

3. RESULTS AND DISCUSSION

3.1 Overview

Figure 2-a shows the trend of security-related events included in the database in the time span considered. An increasing trend is shown in the recent years, especially from 1998: this can be ascribed to the implementation of Seveso II Directive (1996), requiring the reporting of major accidents in sites falling under the obligations of the Directive. Moreover, after year 2000, the overall increase in the number of events recorded is also due to a significant growth in cyber attacks (11% of the total records present in the database), evidenced in Figure 2-b. This can be justified by the considerable spread of external connectivity of the software and hardware used in the CPI for process control and automation. Nevertheless, an increase in physical attacks was also recorded in the same period. Table 3 reports some examples of the events included in the database, selected considering the different threat categories identified as causes of the events. A detailed definition of the threat categories identified is given in the Supplementary Material (Table S2).

The distribution of the events with respect to the different threat categories is reported in Figure 3. In general, the distribution of events found, might be influenced by under-reporting of thefts, which are very common events. The available data show that terrorism is the more important threat category that caused the reported security accidents, followed by vandalism and theft. About 10% of the accident files did not report enough data to allow the unambiguous identification of the threat, due to the scarce details available in the original source.

Most of the reported events took place in Europe and America (44% and 26% respectively), 20% in Asia and 10% in Africa. Only one event was registered in Oceania (actually taking place in Australia). This result could be in part ascribed to the different reporting disciplines of each geographic area: for example, in the U.S., incident reporting is included in the National Incident Management System (Department of Homeland Security, 2008), which provides a comprehensive and systematic approach to incident management for all departments and agencies (governmental and non) as well as for the private sector, regardless of cause, size or complexity of the incident. Differently, in Australia, incidents have to be reported only when entailing a "*serious risk*", defined as the death of a person, a serious incident or illness, or an

incident that exposes any person to a serious risk (even if no one is injured) (Safe Work Australia, 2008). This is very similar to the legislation in the U.K. (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations, HSE, 2013).
Figure 4 reports some details in the geographical distribution of the events. It is important to remark that relevant differences appear when comparing the overall distribution of events to that of events caused by cyber-attacks. Actually, the importance of cyber-attacks in the US is far higher than in other parts of the world. Differences appear also when considering the distribution of the type of threat in the different geographic areas, as shown in Figure 5. In Europe, the main security issue is posed by theft, vandalism, and terrorism, whereas terrorism and sabotage in Asia and Africa. As mentioned before, in the US cyber-attacks as well as vandalism are the main security threats that were found. For the sake of clarity, events for which the type of threat is unknown (30 events out of 300, see Figure 3) have not been displayed in Figure 5.

Events included in the database were sorted according to the industrial sector, applying the definitions provided in Table 2. Figure 6 reports the number of events recorded in the different industrial sectors, also showing the specific contribution of cyber-attacks. When fixed installations are considered, chemical and petrochemical facilities seem to be more frequently affected by security threats. The attractiveness of fixed installations where chemicals and chemical products (including petroleum products) are manufactured (Chemical and Petrochemical sector at Table 2) is related to several aspects, the most important being: i) the presence of large amounts of hazardous materials, capable to rise to severe outcomes when release scenarios are triggered by external threats (Reniers and Cozzani, 2013); ii) the materials stored or produced may potentially be sold on the black market, e.g.to build improvised explosive devices, precursors or actual weapons (Organization for the prohibition of chemical weapons, 2008); iii) often chemical plants are owned by multinational companies, that may be in specific contexts attractive socio-political targets (Ackerman et al., 2004). Furthermore, cyber-attacks to such companies, which represent some 7% of the total, can be motivated by the possibility of obtaining proprietary information important for the business (e.g. patents of specific processes) (North America Oli&Gas Pipelines, 2013).

If transportation and distribution systems are considered, pipelines for oil&gas transportation were the main target of malicious actions. Actually, the protection of such devices results in inherent difficulties and high costs due to their extension that may be in the range of hundreds of kilometers (US Department for Homeland Security, 2008b). Also in this case, cyber-attacks might be driven by business reasons, as they can be finalized to obtain information on production statistics, market strategies, drilling plans and pricing sheets (North America Oli&Gas Pipelines, 2013).

Figure 6 shows that cyber-attacks, in particular on facilities and infrastructures related to energy (oil&gas) have an increasing trend, due to the appealing nature of the target in terms of potential impact of direct consequences and of cascading events. Furthermore, obtaining business possibilities (intended as the possibility of gathering financially valuable data) and causing potential damage to the reputation of companies may also contribute to the attractiveness. Moreover, for some black hats, attacking energy firms is a way to gain notoriety (North America Oli&Gas Pipelines, 2013).

Figure 7 shows important differences in the different industrial sectors with respect to the threat categories that caused the events. As shown in the figure, thefts play a relevant role for pipelines, while thermal power stations and chemicals and chemical products (including petroleum products) manufacturing facilities were mainly affected by terrorism.

3.2 Impact of the events

A quite impressive number of casualties is associated to the security attacks analysed: a total of 247 injuries and 913 fatalities were recorded in the accidents included in the database. Cyber-attacks contribute to 1% of fatalities and to 9% of injuries, and mostly occurred in the power production sector.

In order to better understand the severity of the identified security-related events, the number of records where at least one fatality or one injury took place is reported in Figure 8, where the distribution with respect to industrial sectors is also reported.

Focusing on fatalities, the number of events involving at least one fatality is less than 10% of events included in the database. Having a closer look at each industrial sector, the highest number of events causing at least one fatality is reported for the power production industry (11 events, representing the 25% of the events recorded for the sector). This is also the sector in which cyber-attacks caused a significant percentage of the final outcomes in terms of human losses. A total of 7 security related accidents with fatalities took place in the Chemical and Petrochemical sector (9% of the total events for the sector), a total of 6 are related to oil&gas pipelines (6% of the total events for the sector), and 1 is related to activities involving transportation of hazardous materials.

Events involving pipelines for oil&gas transportation are indeed responsible for 85% of the fatalities registered in the developed database. In general, attacks toward distributed systems also had a higher severity. In particular, events involving oil&gas pipelines, often originated by attempted thefts of fuel, gave rise to major accidents involving multiple life loss (two events having a huge impact took place in Nigeria in 2006, where more than 500 persons were killed in the attempt to tap oil illegally from high pressure oil-pipelines).

Fixed installations usually have a more limited extension and are generally better protected from external physical threats by security barriers such as fences, which allow an easier protection from intrusion. Furthermore, in facilities where chemical and petrochemical products are manufactured a more intense surveillance is possible, thus a more timely activation of safety systems that may contribute to the mitigation of the consequences of the event can be achieved.

3.3 Final events and attack modes

Figure 9 shows the final events experienced in the scenarios that followed the security attacks. The data in the figure only consider the final scenario directly caused by the attack, without taking into account secondary or cascading events. A total of 110 events (37 %) had the release of hazardous chemicals in air, water or soil as the final event. In 106 events (35 %) the final scenario was an explosion; in 29 cases (10 %) it was a fire. In 19 events (6 % of the total), there was a loss of system control due to cyber-attack. No significant consequence was registered in 11 cases (4%). Most of the latter are events triggered by cyber-attacks. In the other cases (8%), the final scenario was not described or specified in the original source.

Figure 10 shows how the different scenarios are related to the industrial sectors previously defined. Consistently with previous considerations, power production sites, Chemical&Petrochemical industry and manufacturing companies are those mostly affected by Loss of System Control consequent to a cyber-attack.

Figure 11 shows the final scenarios following the different threat categories considered for the events in the database. As shown in the figure, important differences are present. While terrorism mainly causes explosions as final scenarios, thefts and vandalisms are more likely to result in the release of hazardous chemicals. As discussed above, cyber-attacks mainly result in the loss of control of the system or in no relevant consequences.

3.4 Analysis of attack modes and penetration effectiveness

A more detailed analysis was possible for 26 events that affected the chemical and petrochemical industry, for which a higher level of detail was available concerning attack modes, attack paths and penetration. Figure 12 represents a schematic overview of the layout of a process plant. The usual disposition of the macro-areas is highlighted: the facility core – the process plant, storage section, business buildings for employees, and manned reception. The scheme shows that in usual layouts a layered structure is present, in which the process plant is surrounded by warehousing buildings or storages. The manned reception is devoted to the access control, both of vehicles and pedestrians. A parking area is usually located outside of the premises. Employees and visitors are usually allowed in the parking area with no security control.

Figure 12 also reports the attack modes and the extent of penetration experienced in the facility. The figure shows that attacks perpetrated using explosive devices targeted in one case the parking area, in five cases the storage area, while in other five cases the devices exploded inside the process facility. These types of attacks are perpetrated by highly capable and well-motivated adversaries, such as terrorist organizations, perhaps in collusion with insiders. In two cases ammonal was used as explosive. In other three cases the explosive was TNT, and in one case dynamite was used. The explosive composition was not reported for the other five events belonging to this category.

Vehicle-born improvised explosive devices (VBIED) were used in a total of 3 attacks: in one case the VBIED was parked in the parking area, while in the other 2 events the vehicle entered the plant area. It has to be remarked that in one case the vehicle broke through the main portal, but in the second case the attacker was authorized to access the facility, being an employee of a subcontracting company.

Cases of arson took place 5 times, involving mostly (3 out of 5 events) the storage area. The presence of large amounts of chemicals and flammable materials, combined with a relatively low level of security barriers if compared to the core installation, made the target both available and attractive. In one case a malicious fire started off-site, probably lighted by vandals. Nonetheless, in a second case a fire lighted in a bucket of plastic waste located inside the facility core escalated to a vessel and threatened the whole plant. An insider was suspected to have started the event.

Armed assaults to process plants were always executed by highly trained, motivated and equipped attackers. The goal was to reach human targets or take control of the facility. Indeed, 5 out of 6 recorded cases targeted the plant core. In one case, the assault was opposed by armed personnel at the reception, and for this reason it is classified as an off-site attack in Figure 12.

Grenade rocketing consists in the shooting of missiles using a rocket launcher. Also this is an attack mode only available for highly motivated, well trained and well equipped adversaries. Indeed, one attack of this type to the storage area of a facility was recorded, with no intrusion. Such attack may target any part of the plant. However, storage areas are usually more visible from outside the plant and are an attractive target due to the escalation potential and cascading events that may be triggered. In Table 4, the countries were the 26 events analyzed took place are indicated.

3.5 Lessons learnt

In the last years, site security is becoming more and more a hot topic for the chemical industry. The analysis of security related past accidents allows us to draw some lessons and identify early warnings, briefly discussed in the following.

Few events analyzed revealed that some scenarios were not accounted for during the risk assessment of the plant because considered as unlikely to occur when products are compliant with manufacturing standards. The first lesson learnt is about the importance of including security-related events into risk assessment when substances could be improperly used and scenarios could be intentionally forced to happen.

For what concerns physical attacks several lessons can be sketched, in particular related to surveillance that has to be adequately performed even when the installation is not in normal operating conditions. Attention should be paid to closed sites, where hazardous materials and equipment should not be left unattended. Surveillance should include regular inspections of possible openings and breaches in the fences. Automated monitoring systems (e.g. anti-intrusion alarms, video surveillance, systems equipped with motion or heat detection) should be always on to integrate surveillance especially during closing hours. Furthermore site access procedures should be improved and strengthened to prevent those scenarios in which outsiders were authorized (e.g. employee of subcontractors). The role of the insiders cannot be neglected either and restricted access areas should be conceived (Reniers et al., 2015). This consideration on the insider holds for the case of cyber attacks.

To prevent cyber-attacks from outsiders, i.e. hackers, simple rules should assume more importance in industry such as the use of encrypted data and multi-factor authentications, for example using a two-factor authentication. This is a practice used frequently by Payment Card Industry that should be adopted for industrial applications. General good practices to improve the prevention of cyber-attacks are: updating software, in particular when SCADA is a possible target; allowing the access to the company network only to trusted IP; avoiding the use of USB ports and Bluetooth interfaces as much as possible. Also in the case of cyber attacks, the role of the contractors cannot be underestimated: third parties could be used as attack vectors (French Ministry for an ecological and solidary transition, 2016).

Some lessons are not original of the present study, but still important to recall:

- Sharing the information about threats is always a fundamental tile to prevention and management (European Network and Information Security Agency (ENISA), 2010; European Union, 2017). Information about attacks suffered in the proximity of the site or by same industrial group help.
- Vulnerable equipment (e.g. storages) should not be, as much as possible, in a non-isolated zone.
- Improving trainings to prevent physical security threats as well as cyber-security skills and procedures.

4. CONCLUSIONS

A database of 300 security-related accidents that affected industrial facilities and related infrastructures where relevant quantities of hazardous materials were stored or processed was developed and populated. The information collected originated from European and US sources, but events taking place all over the world were reported. Threat categories that caused such events were identified. Important differences are present in the attack mode. Important differences resulted in the distribution of events with respect to threats and geographical areas, with Europe having the highest number of events reported, while most of the scenarios triggered by cyber attacks took place in the US. Pipelines, due to their extension and the difficulties in their protection, resulted in the observation that this is the technical system most frequently targeted. The distribution of threats causing the security accidents shows however relevant differences when looking at the different types of facility, with thefts dominating in the case of pipelines, while terrorist attacks resulted in more frequent threats in the case of fixed installations. The analysis also allowed obtaining some insights on the specific attack mode, in particular for fixed installations. The use of explosives (both military and improvised explosive devices) is by far the more frequent attack mode, although armed attacks and arson are also possible and may result in an in-depth penetration of the attackers. Finally, lessons learnt clearly show the need for the implementation of adequate security assessment as well as of an accurate security management system and of lay-out criteria aimed at the optimization of the available layers of protection of sites.

Overall, the results remark the concreteness of security events involving industrial facilities and critical infrastructures where hazardous substances are transported, suggesting the introduction of a dedicated reporting system allowing the collection of more accurate and detailed data on this category of events.

REFERENCES

Ackerman, G., Abhayaratne, P., Bale, J., Blair, C., Hansell, L., Jayne, A., Kosal, M., Lucas, S., Moran, K., Seroki, L., Vadlamudi, S., 2004. Assessing Terrorist Motivations for Attacking Critical Infrastructure.

American Institute of Chemical Engineers, Center of Chemical Process Safety (AIChE-CCPS), 2003. Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites. New York: American Institute of Chemical Engineers, Center of Chemical Process Safety.

American Petroleum Institute (API), 2013. ANSI/API Standard 780 – Security risk assessment methodology for the petroleum and petrochemical industry. New York: American Petroleum Institute.

Argenti, F., Landucci, G., Cozzani, V., Reniers, G., 2017. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Saf. Sci. 94, 181–196. doi:10.1016/j.ssci.2016.11.022

Argenti, F., Landucci, G., Reniers, G., Cozzani, V., 2018. “Vulnerability Assessment of Chemical Facilities to Intentional Attacks based on Bayesian Network. Reliability Engineering and System Safety 169, 515-530. doi:10.1016/j.ress.2017.09.023

Argenti, F., Landucci, G., Spadoni, G., Cozzani, V., 2015. The assessment of the attractiveness of process facilities to terrorist attacks. Saf. Sci. 77, 169–181. doi:10.1016/j.ssci.2015.02.013

ARIA, 2015. Accident study findings on malicious acts perpetrated in industrial facilities. ARIA database 18.

Byres, E.J., 2008. Protects your plants, 2008. Chem. Process. 71, 20–25.

Casson Moreno, V., Cozzani, V., 2015. Major accident hazard in bioenergy production. J. Loss Prev. Process Ind. 35, 135–144. doi:10.1016/j.jlp.2015.04.004

Casson Moreno, V., Papasidero, S., Scarponi, G.E., Guglielmi, D., Cozzani, V., 2016. Analysis of accidents in biogas production and upgrading. Renew. Energy 96, 1127–1134. doi:10.1016/j.renene.2015.10.017

CCPS - Center for Chemical Process Safety, 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. doi:10.1002/9780470925003

Center for Chemical Process Safety - CCPS, 2017. Global Regulations on Process Safety [WWW Document]. URL https://www.aiche.org/ccps/resources/government-regulations-resources#Regulations (accessed 10.12.17).

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

Dechema ProcessNET, 2017. [WWW Document]. URL http://processnet.org/en/ (accessed 6.28.17).

Department of Homeland Security, 2017. Chemical Facility Anti-Terrorism Standards (CFATS).

Department of Homeland Security, 2008. National Incident Management System. Natl. Incid. Manag. Syst. doi:10.1017/CBO9781107415324.004

Department of Homeland Security, 2017. Repository of Industrial Security Incidents [WWW Document]. URL http://www.risidata.com/ (accessed 6.28.17).

Deutsch Umwelt Bundesamt, 2017. ZEMA [WWW Document]. URL http://www.infosis.uba.de/index.php/de/site/12981/zema/index.html (accessed 1.1.17).

Dirección General de Normas, 2011. NORMA Oficial Mexicana NOM-031-STPS-2011,

Construcción-Condiciones de seguridad y salud en el trabajo.
European Gas pipeline Incident Data Group, n.d. EGIG [WWW Document]. URL https://www.egig.eu/about-egig (accessed 6.28.17).
European Parliament and Council, 2012. Seveso III, Directive 2012/18/UE.
European Petroleum Refiners Association, 2017. Concawe [WWW Document]. URL https://www.concawe.eu/ (accessed 6.28.17).
European Network and Information Security Agency (ENISA), 2010. Good Practice Guide for Incident Management.
European Union, 2017. Security Incident Information Management Handbook, ReliefWeb.
French Ministry of Ecology Sustainable Development and Energy, 2017. The ARIA Database [WWW Document]. URL http://www.aria.developpement-durable.gouv.fr/about-us/the-aria-database/?lang=en (accessed 10.18.17).
Greene, T., 2008. Experts hack power grid in no time. [WWW Document]. URL: https://www.networkworld.com/article/2277908/lan-wan/experts-hack-power-grid-in-no-time.html
Health and Safety Executive, 2015. The Control of Major Accident Hazards Regulations 2015 (COMAH).
HSE, 2013. Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR).
International Electrotechnical Commission, 2010. IEC 61508 Functional Safety.
Joyce, A.L., Evans, N., Tanzman, E.A., Israeli, D., 2017. International cyber incident repository system: Information sharing on a global scale. 2016 IEEE Int. Conf. Cyber Conflict, CyCon U.S. 2016 2017. doi:10.1109/CYCONUS.2016.7836618
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. doi:10.1016/j.ress.2015.03.004
Lou, H.H., Muthusamy, R., Huang, Y., 2003. Process Security Assessment : Operational Space. Process Saf. Environ. Prot. 81, 418–429. doi:10.1205/095758203770866593
Major Accident Hazards Bureau (MAHB), 2002. Major Accident Reporting System (MARS) Data Bank [WWW Document]. URL https://emars.jrc.ec.europa.eu/ (accessed 10.18.17).
National Consortium for the Study of Terrorism and Responses to Terrorism (START), n.d. Global Terrorism Database [WWW Document]. URL https://www.start.umd.edu/gtd/ (accessed 6.28.17).
Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H., 2012. SCADA security in the light of cyber-warfare. Comput. Secur. 31, 418–436. doi:10.1016/j.cose.2012.02.009
North America Oli&Gas Pipelines, 2013. Discussing the role of cyber security in Oil ans Gas Pipelines.
Organization for the prohibition of chemical weapons, 2008. Chemical Weapons Convention.
Parliament of India, 1948. The Factories Act (Act No. 63 of 1948).
Pescatore, J., 2017. Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017.
Rathnayaka, S., Khan, F., Amyotte, P., 2011. SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. Process Saf. Environ. Prot. 89, 151–164. doi:10.1016/j.psep.2011.01.002
Reniers, G., Cozzani, V., 2013. Domino Effects in the Process Industries. Elsevier.
Reniers, G.L.L., Van Lerberghe, P., Van Gulijk, C., 2015. Security risk assessment and protection in the chemical and process industry. Process Saf. Prog. 34, 72–83.

doi:10.1002/prs.11683
Safe Work Australia, 2008. Incident reporting [WWW Document]. URL https://www.safeworkaustralia.gov.au/incident-reporting
Thomas, H.W., Day, J., 2015. Integrating Cybersecurity risk assessments into the process safety management work process. 49th Annu. Loss Prev. Symp. 2015, LPS 2015 - Top. Conf. 2015 AIChE Spring Meet. 11th Glob. Congr. Process Saf. 360–378.
French Ministry for an ecological and solidary transition, 2016. Cybersecurity in industry. doi:10.1002/ejoc.201200111
United Nations, 2008. International Standard Industrial Classification of All Economic Activities, Rev.4. New Jersey.
United States Department of Transportation, n.d. Pipeline and Hazardous Materials Safety Administration [WWW Document]. URL http://www.phmsa.dot.gov/ (accessed 6.28.17).
US Department for Homeland Security, 2008a. A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level.
US Department for Homeland Security, 2008b. Pipeline Threat Assessment.
US Department of Justice, 2002. A Method to Assess the Vulnerability of U.S. Chemical Facilities. Report NCJ 195171. Washington: Office of Justice Programs

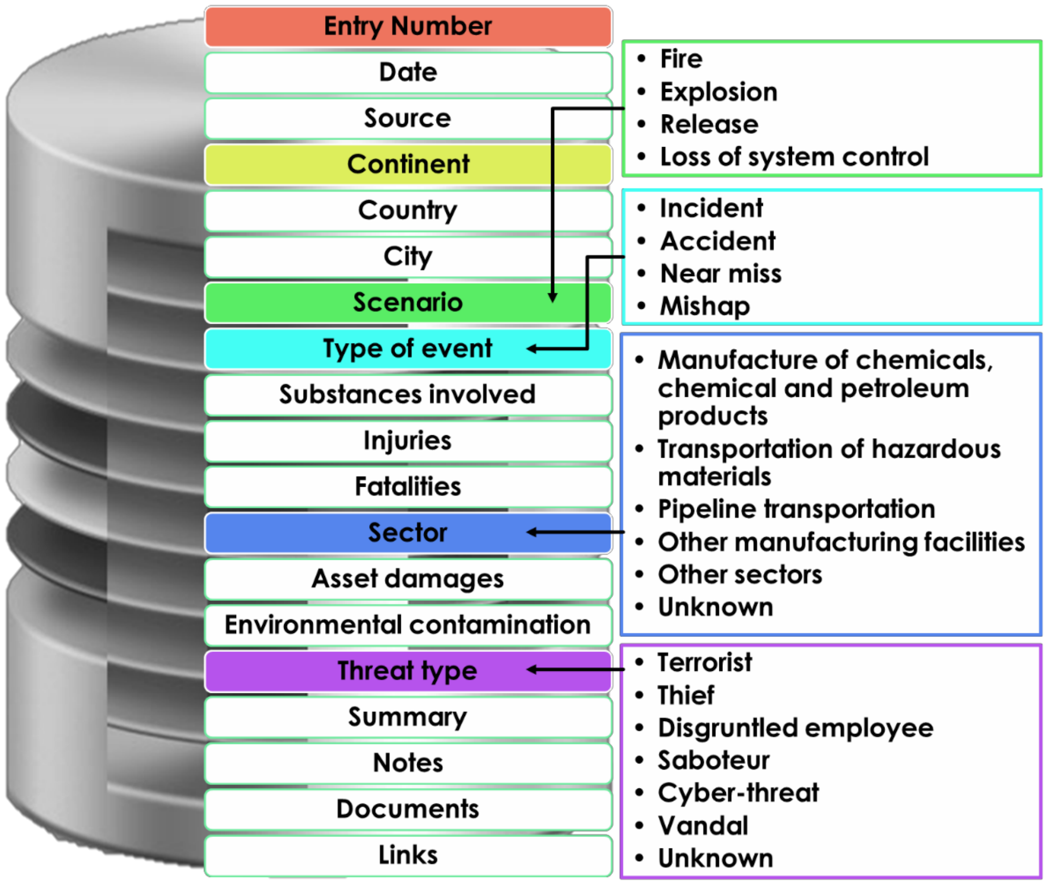

Figure 1: Structure of accident files in the database. White boxes are free text fields, coloured boxes are itemized fields.

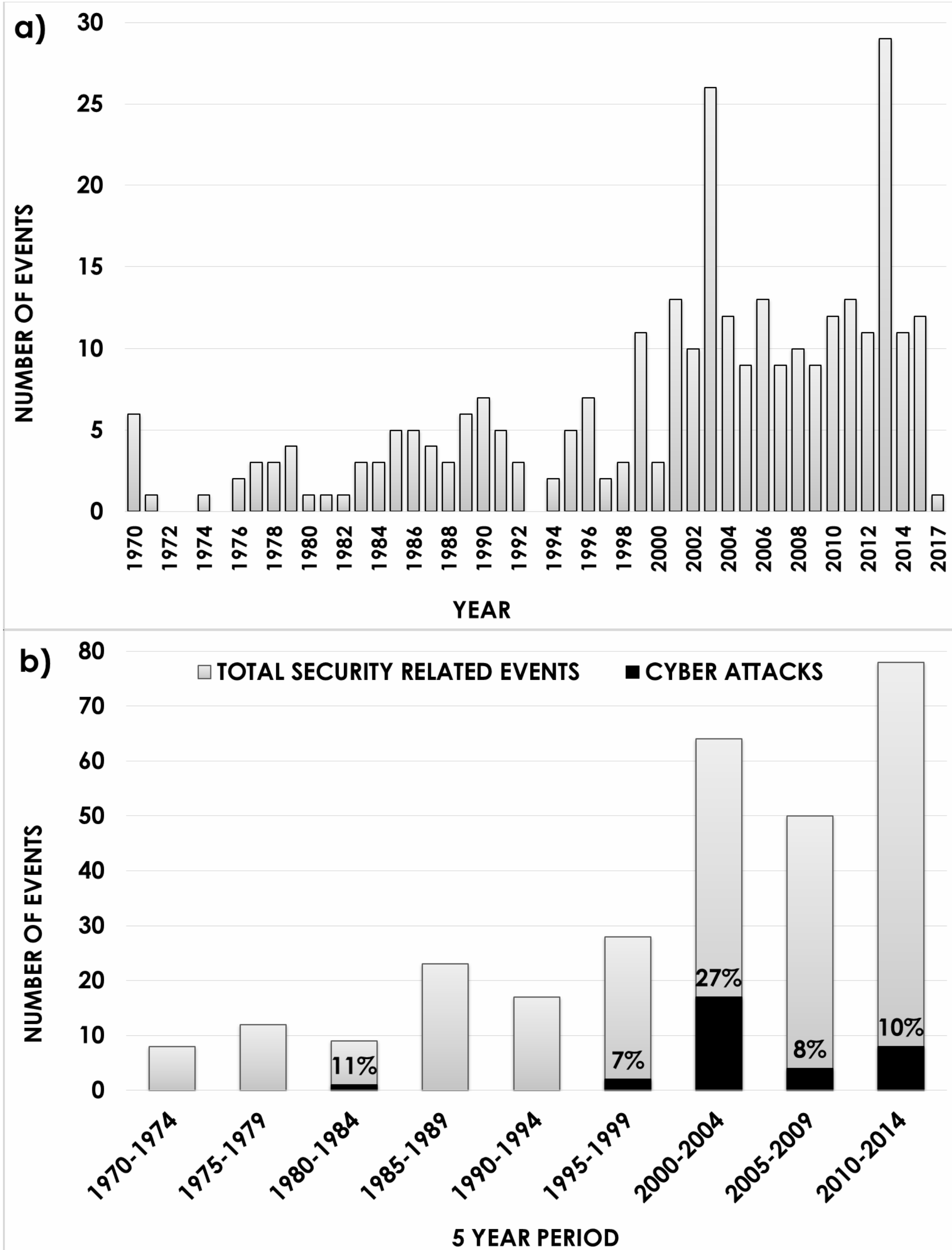

Figure 2: Number of events per year included in the developed database (a), and quinquennial trend of the records also reporting the % of cyber-attacks (b).

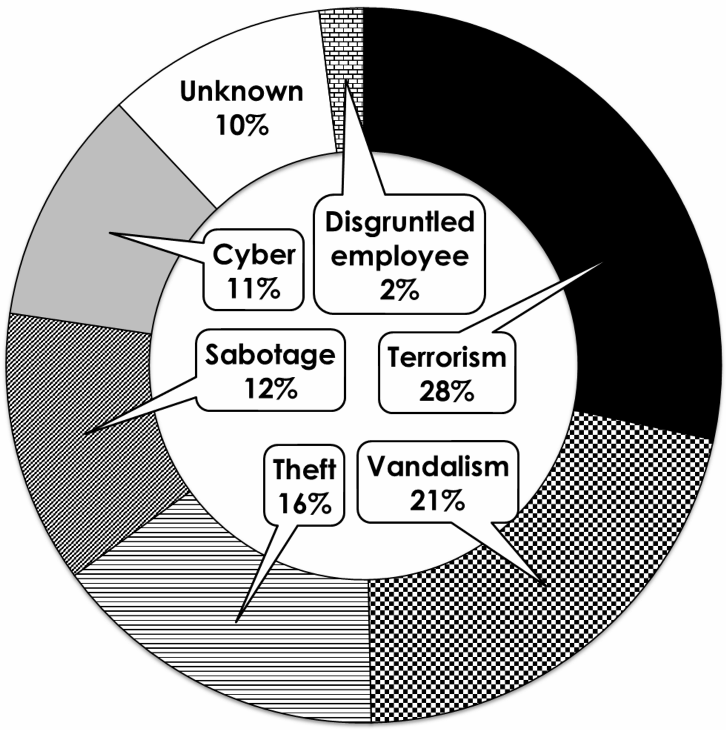

Figure 3: Threat categories identified as the causes of the 300 security-related events considered in the present study.

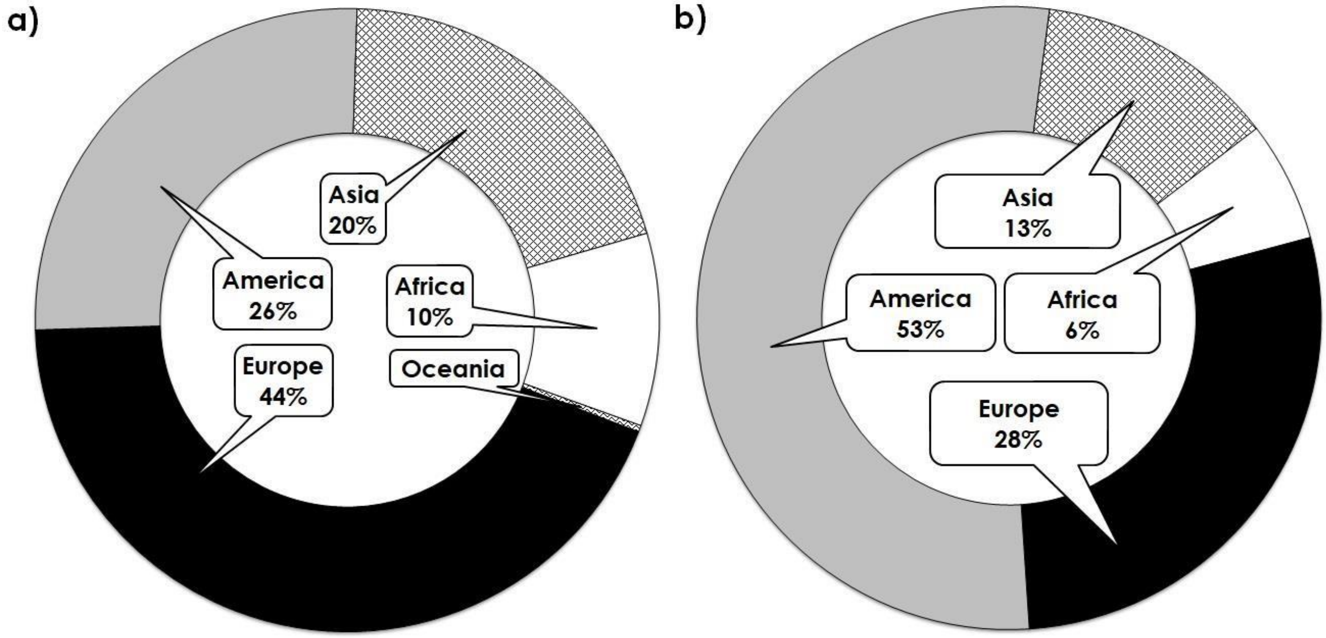

Figure 4: Geographical distribution of the 300 security-related events included in the present study (a) vs. geographical distribution of the cyber-attacks (b).

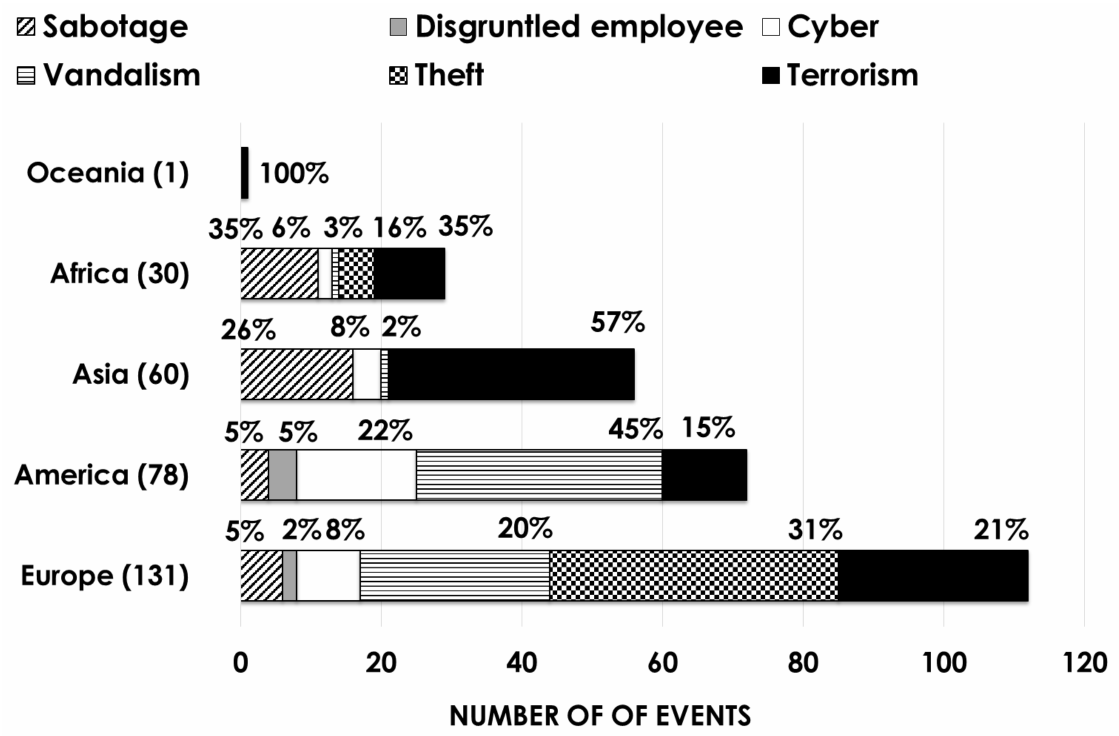

Figure 5: Distribution of the type of threat in the different geographic areas. For the sake of clarity, events for which the type of threat is unknown (see Figure 3) have not been displayed.

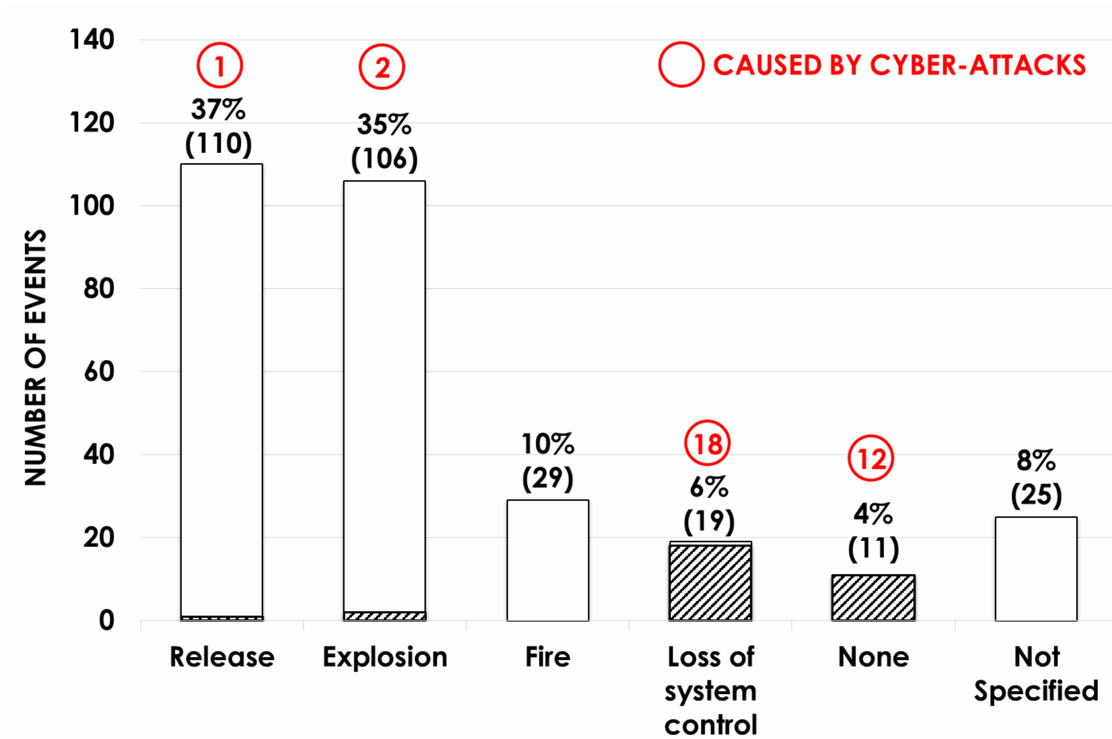

Figure 6: Number of events recorded in the different industrial sectors defined in Table 2. The contribution of cyber-attacks with respect to the total security related events is shown in striped colours. The labels report the % and number of cyber-attacks with respect to the total events recorded.

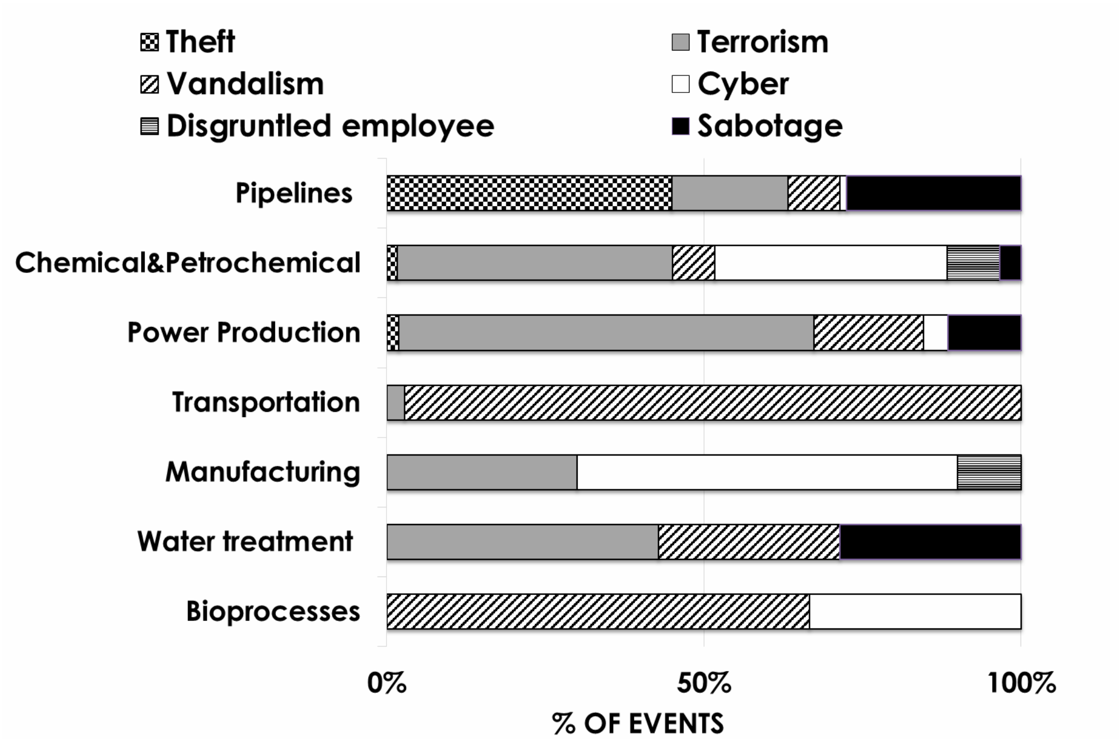

Figure 7: Share of the security threat with respect to industrial sectors defined in Table 2.

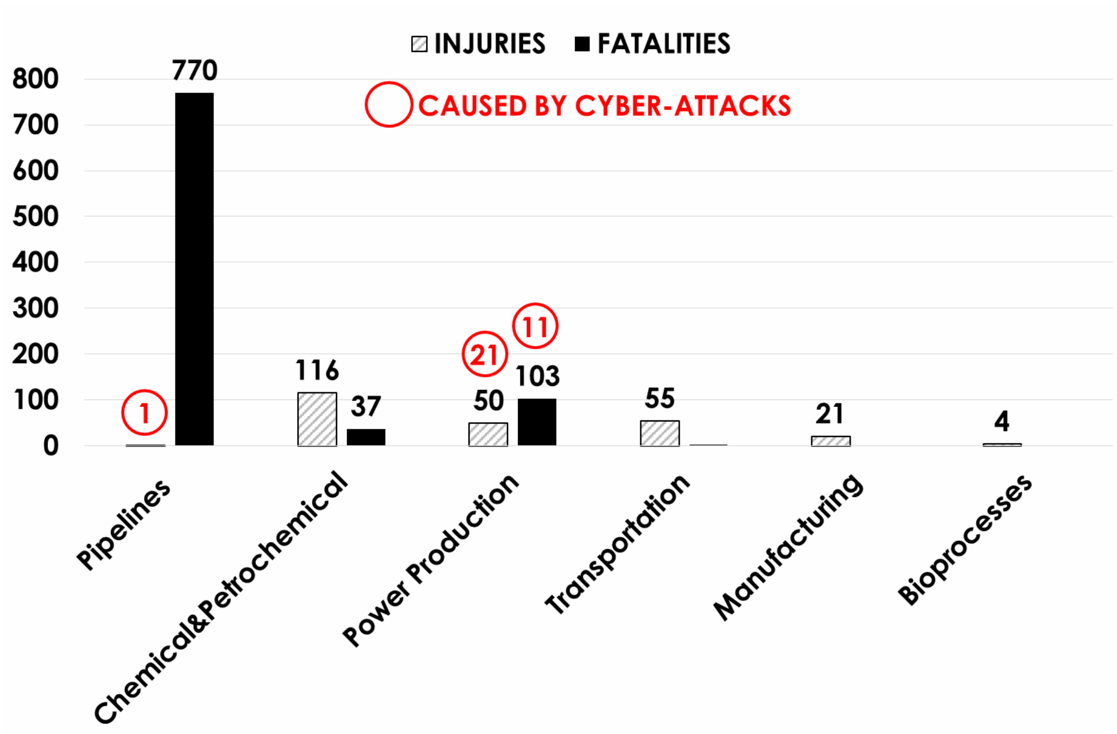

Figure 8: Number of security-related events involving at least one fatality or injury recorded in our database and divided per industrial sector (as defined in Table 1); the numbers inside a circle refer the fatalities/injuries related to cyber-attacks.

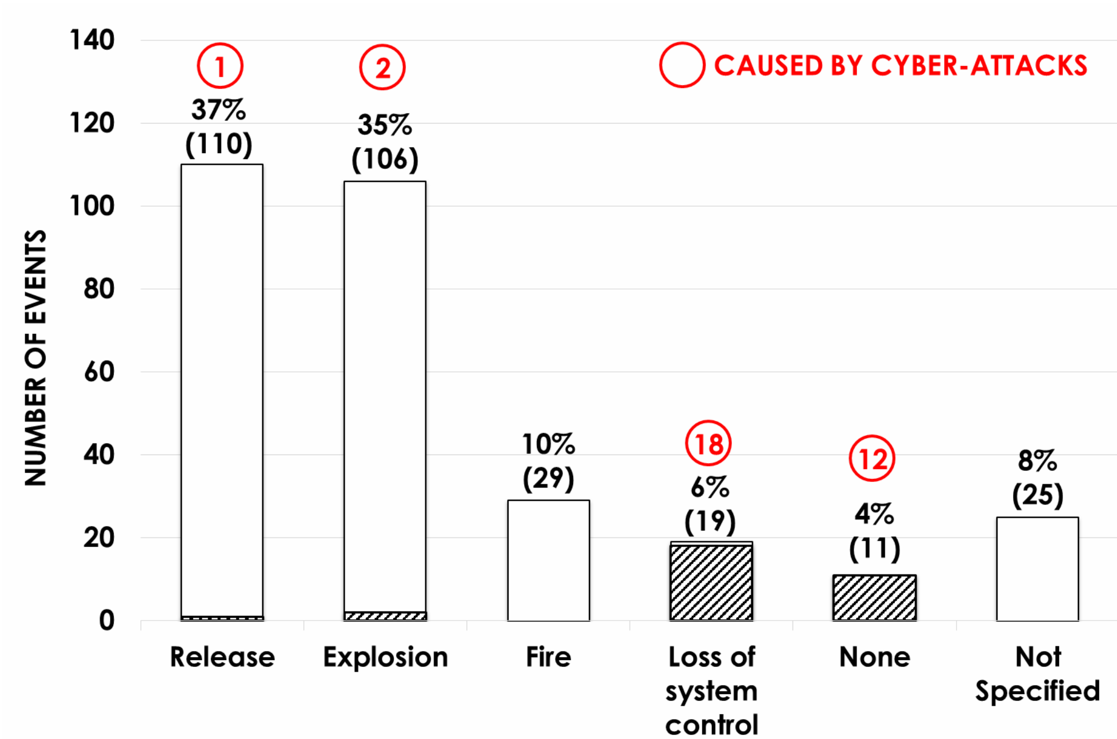

Figure 9: Final events recorded for the accident scenarios considered in the database. The contribution of cyber-attacks with respect to the total security related events is shown in striped colours. The numbers inside a circle refer to the events related to cyber-attacks.

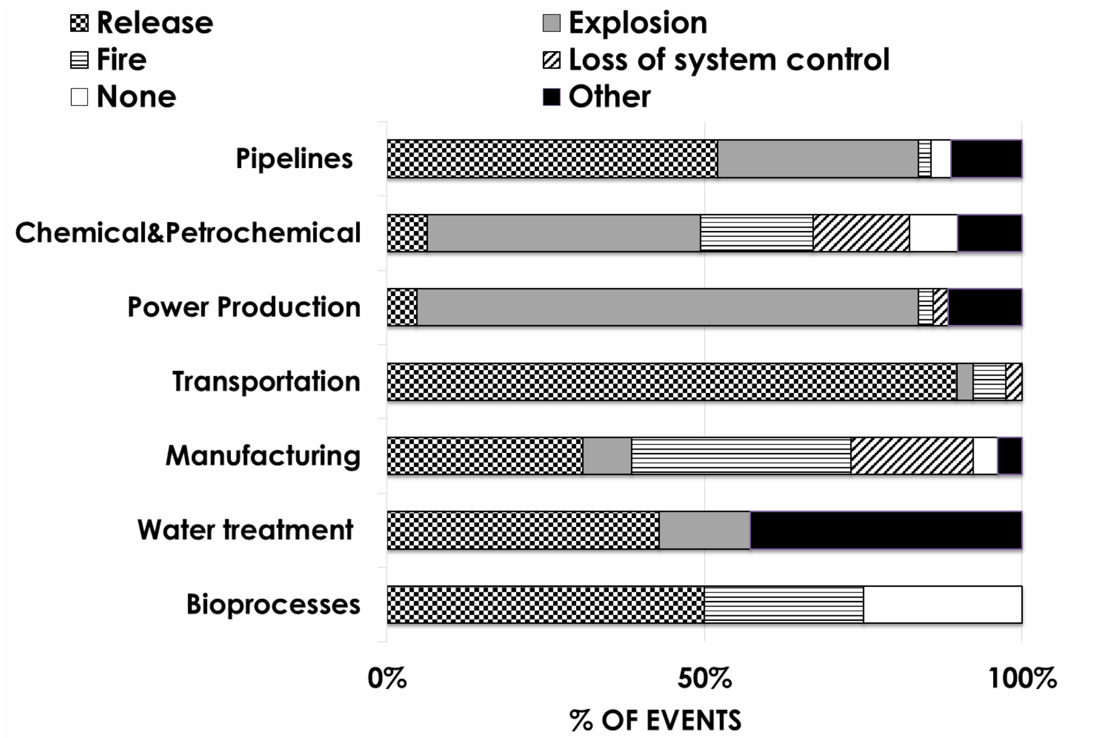

Figure 10: Share of the scenario with respect to industrial sectors defined at Table 2.

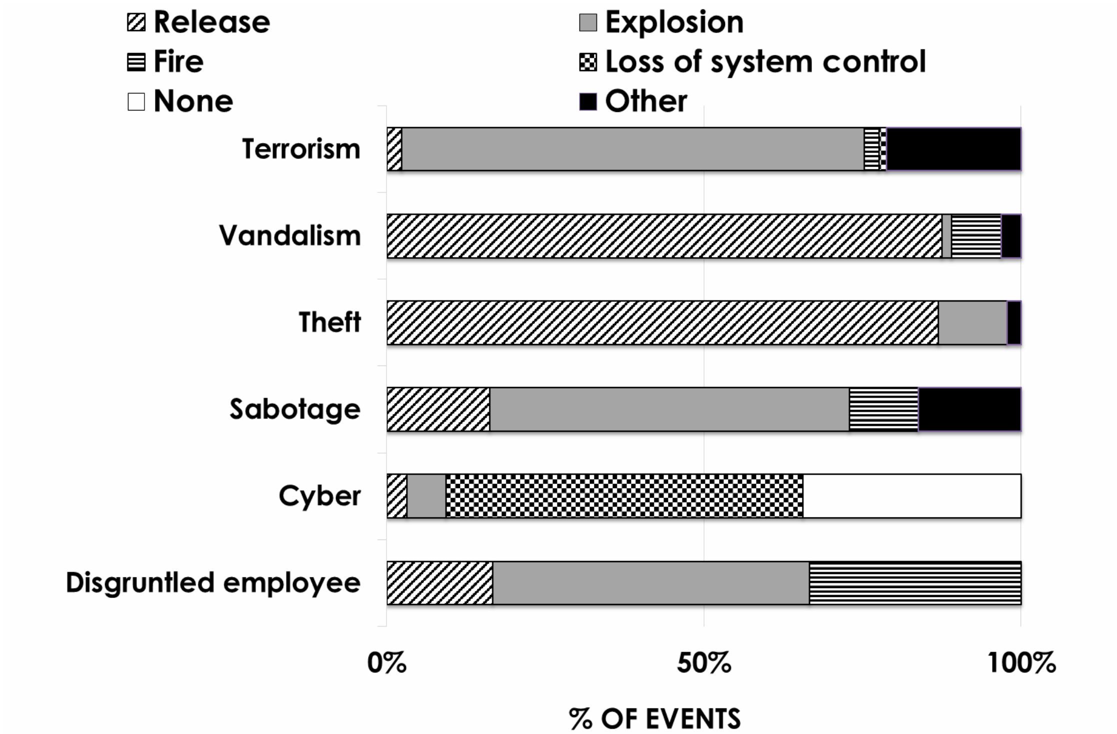

Figure 11: Share of the scenario with respect to the type of security threat.

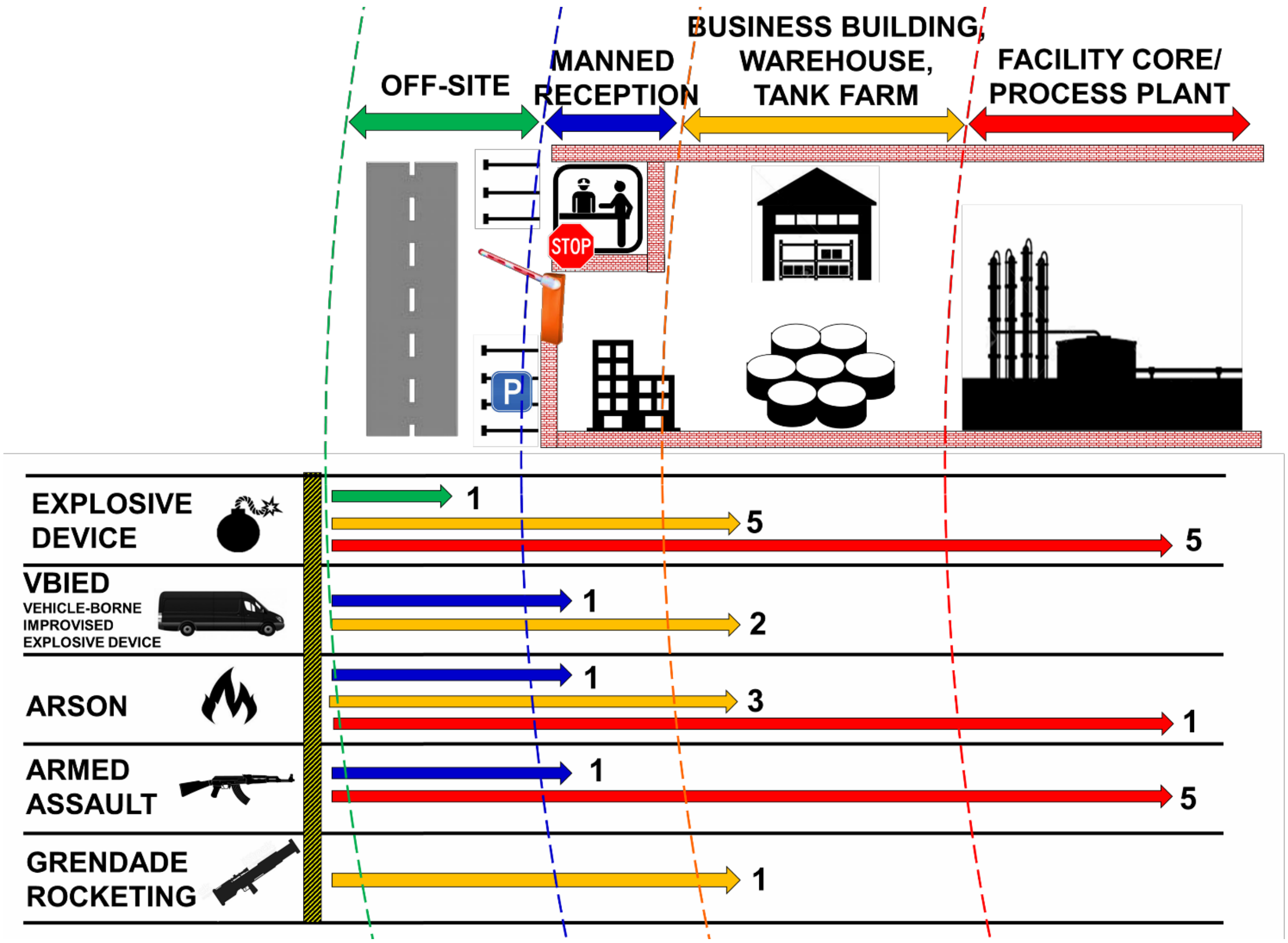

Figure 12: Paths and related penetration effectiveness for different attack modes recorded for Chemical&Petrochemical facilities. The colour of the arrows refer to the area affected by the attack, i.e. off-site/parking (green), manned reception (blue), business building-warehouse-tank farm (yellow), and process plant (red). Per each attack mode, the number of successful records is reported.

Table 1: Definitions of key security terms used in the present work (CCPS - Center for Chemical Process Safety, 2003).

Term	Definition
Security Risk	Risk is an expression of the likelihood that a specific vulnerability of a particular attractive target will be exploited by a defined threat to cause a given consequence.
Threat	Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.
Attractiveness	*("target attractiveness")* An estimate of the value of a target to an adversary based on factors such as: potential for fatalities, economic damage, disruption of economic, access to target, etc.
Vulnerability	Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.
(Security) Event	Possibly referred to as "undesirable event", defined as: An (intentional) event that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment.

Table 2: Macro-sectors of industrial activities used in the database for the classification of the records

Macro-sector	**Description**	**International Standard Industrial Classification of All Economic Activities, United Nations, 2008.**
Chemical and Petrochemical (C&P)	Chemical activities, including pesticides production, pharmaceutical industry, production of basic chemicals; petrochemical activities, including refineries.	- Manufacture of chemicals and chemical products - Manufacture of coke and refined petroleum products - Extraction of crude petroleum and natural gas
Power Production	Power production plants using hydrocarbons (thermal power stations). (Hydroelectric and nuclear power plants are not included).	Production, collection and distribution of electricity
Bioprocesses	Treatment of organic waste and waste fermentation juices; food industry.	- Waste collection, treatment and disposal activities; materials recovery - Manufacture of food products
Manufacturing	Metalworking, textile industry, activities related to automotive sector.	- Manufacture of basic metals - Manufacture of fabricated metal products - Manufacture of textiles - Manufacture of motor vehicles, trailers and semi-trailers
Water treatment	Treatment of water for industrial and domestic purposes (excluding bioprocesses-related waters and slurries).	Water collection, treatment and supply
Pipelines	Oil and gas transportation via pipelines.	Transport via pipelines
Transportation	Transportation of hazardous materials via road, rail, water.	- Land transport - Water transport
Not specified	Security-related events for which specific industrial sector was not defined by the source.	

Table 3: Definition of the type of security attacks used in the present study.

Threat type	Examples of event
Terrorism	Case 1 (Major Accident Hazards Bureau (MAHB), 2002): The accident occurred in an unmanned natural gas storage plant storing low pressure natural gas (mainly methane). A terrorist explosive device was placed on a side of the middle lift of a gas holder, most likely earlier in the night when it was not inflated. When the device blown off, the roof of the gasholder peeled partly off, the upper lifts collapsed and approximately 33 tons of natural gas was released. The gas was immediately ignited resulting in a fireball. The smaller adjacent gasholder experienced a seal fire; whereas the larger gasholder was punctured in its third lift resulting in a jet-fire of approximately 0.5 m^2.Three people were injured. Case 2 (French Ministry of Ecology Sustainable Development and Energy, 2017): A severe explosion, felt several kilometres away, occurred in a fertilizers production plant in Toulouse, France. The substances involved are the manufacturing residues of ammonium nitrate. A quantity of these products (estimated between 15 and 20 tonnes) detonated in a mass explosion leading to a damage corresponding to a TNT equivalent of between 20 and 40 tonnes. The detonation gave rise to an overpressure in the order of 140 mbar at a distance between 280 and 350 m and 50 mbar at a distance between 680 and 860 m. There were victims resulting from indirect effects up to 500 m away and injuries caused by broken glass at distances of a few kilometres away. As a precautionary measure, the local governmental authority requested that the population confine themselves to their homes. Case 3 (French Ministry of Ecology Sustainable Development and Energy, 2017): A certified delivery driver entered a lower-tier Seveso-rated industrial gas plant. He drove the vehicle, containing flammable and combustive gas bottles, to a closed hangar. He opened the bottles and created explosive atmosphere inside the vehicle that combusted when making contact with an unidentified ignition source. Pieces of the vehicle's interior compartment, blasted during the explosion, structural parts of the building roof and siding as well as some of the production machinery. Notified by plant security agents, fire-fighters from a nearby fire station arrived at the scene in less than 10 minutes. While surveying the explosion site, they caught the driver in the process of manually opening the valves on industrial gas bottles stored both inside the building (inert gas) and outside (flammable gas). Two responders chased him down and neutralised him. During the action, one of them sustained slight injuries to the arm. Flames were seen spewing from the valves of two flammable gas bottles, which were immediately closed. Fire-fighters and plant personnel stopped all leaks by closing the valves on other open bottles and locking down the installation.

Threat type	Examples of event
Cyber	Case 1 (Department of Homeland Security, 2017): Multiple hackers gain access to a manufacturing company network and then entered the control system. This resulted in an incident where a furnace could not be shut down in the regular way, resulting in massive damage to the whole system. Case 2 (Department of Homeland Security, 2017): Hackers shut down alarms, cut off communications and super pressurized the crude oil in the line which resulted in an explosion of an oil&gas company pipeline, resulting in the destruction of the pipeline, $5 million a day in transit tariffs during the closure; $1 billion in export revenue while the line was shut down. Case 3 (Department of Homeland Security, 2017): A former IT employee of a pharmaceutical company, gained unauthorized access a user account to access a company server. Once the server was accessed, he took control of a piece of software that he had secretly installed on a server weeks before. He used this program to delete the contents of the company's computer network. The attack froze operations for a number of days. The company suffered at least $800,000 in losses.
Vandalism	Case 1 (Major Accident Hazards Bureau (MAHB), 2002): A pyromaniac set on fire some papers and packing materials in the storage area of an organic chemical industry for seed production and treatment. The area was containing saw dust, starch glue, seed, agrochemicals and seed treatment machinery. Toxic substances (i.e. methiocarb, thiram, carbofuran, ecc.) were stored in the same place, leading to their combustion and release during the accident. Case 2 (United States Department of Transportation, n.d.): A trespasser gained access into a facility where multiple tankers were staged and maliciously opened valves on numerous tanks on site causing the leak of their contents onto the ground. The vandal had broken the seals on valve caps then opened all valves releasing the material. Of all containers affected only one was storing an hazardous material (acetic acid).
Theft	Case 1 (Major Accident Hazards Bureau (MAHB), 2002): The accident occurred in a storage area for flammable gases. The component involved was a hand valve on the loading line of an unattended propane trucks loading facility not in operation. After the normal working time, unauthorized persons attempted to steal LPG in an unattended propane truck loading facility. A blind flange was removed and a hand valve opened on the loading line, resulting in a leakage of several litres of liquid propane. When leak was detected, the whole installation was checked to identify the possible leak sources and the gas concentration was measured within the installation. The gas cloud dispersed safely without igniting. Case 2 (French Ministry of Ecology Sustainable Development and Energy, 2017): An armed band of 1 woman and 2 men stole 1280 kg of aluminum powder from a plant producing metal inks for packaging. They neutralized the security guard and enter the site.
Disgruntled employee	Case 1 (French Ministry of Ecology Sustainable Development and Energy, 2017): Subsequent to a strike against their employer for placing the company under supervised liquidation, 153 staff members poured 5000 litres of sulphuric acid and dyes into a stream that ran through the plant and emptied into a river. Fire fighters were able to contain the pollution before it arrived to the river.

Threat type	Examples of event
	Case 2 (French Ministry of Ecology Sustainable Development and Energy, 2017): In a thermal power station classified Seveso low threshold, the operations of the plant has been severely disrupted by a strike for 10 days. In particular, during the unloading of a ship, the positioning of several valves was modified with respect to normal operations: 2 tanks were put in communication, leading to the gravity filling of the oil. The system was equipped with a high level and a very high level activating visual and audible alarms. Only the visual alarms were activated in the control room, the audible alarms were disabled. The visual alarms were not perceived by the operators in the control room and the tank overflowed. The oil has flowed through the overflow in the retention of the tank which was not equipped with a hydrocarbon detector. The retention isolation valve was open. Hydrocarbons then flowed into the rainwater water system. In normal operation, this network leads to a catch basin. During the event, the basin was under construction. The rainwater system was purged using an immersed pump that was discharged directly into the natural environment.
Sabotage	Case 1 (Major Accident Hazards Bureau (MAHB), 2002): The accident occurred, outside the normal working hours, in a pesticide industry and involved a pallet with 2000 containers of insect disinfectants: the pallet caught fire because of arson (sabotage action). 600 containers were burnt before the fire brigade could extinguish the fire. The population within 55 metres of the establishment was warned. Firefighting water and contaminated soil were collected and disposed. The sabotage was made possible because of the inadequate safeguarding of the installation outside the normal working hours. Case 2 (French Ministry of Ecology Sustainable Development and Energy, 2017): In a sawmill, a supply line from an electric generating set was punctured at the outlet of a fuel oil tank, leading to 3000 litres of fuel oil spreading across the site and into a neighbouring ditch. The site operator sprinkled sawdust to absorb the product. Fire-fighters set up a straw dam in order to prevent the fuel oil from reaching a watercourse. Several other malicious acts had been committed during the previous month because of tense relations with neighbours. The operator wound up moving the activity to another site.

Table 4: Countries were the 26 events that affected the chemical and petrochemical industry analysed took place.

Attack mode		Country			
Explosive Device (total: 11)		US: 3 Spain: 2	Germany:1 Greece: 1	Nigeria: 1 Peru: 1	Russia: 1 Yemen: 1
Armed Assault (total: 6)		France:2 Ukraine: 2	US: 1 Libya: 1		
Arson (total: 5)		France:2 US: 2	Ukraine: 1		
VBIED: Vehicle-Borne Improvised Explosive Device (total: 3)		Colombia: 1 France:1 Kuwait: 1			
Grenade Rocketing (total: 1)		France:1 Libya: 1			