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

Matteo Iaiani, Valeria Casson Moreno, Alessandro Tugnoli, Valerio Cozzani*

LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, Italy.

**Corresponding author, e-mail: valerio.cozzani@unibo.it*

Process facilities, in particular those where hazardous substances are processed or stored, may be the target of malicious acts aiming at interfering with the normal operations. The security threat to such industrial facilities includes both physical and cyber intrusions and it may arise both from outside the business organization managing the facility (i.e. outsider threat) or from inside (i.e. insider threat). In the present study a database of security-related events that affected the process industry and similar industrial sectors worldwide (Bioprocesses, Chemical&Petroleum, Energy production, Pipelines, Transportation, Water/Wastewater) was investigated. The database collects a total of 369 records. The data were analysed, focusing on time and geographical trends, threat actor, industrial sector affected, and final scenarios triggered by the security attacks. Overall, the results point out the concreteness of security-related events in process industry and frame a clearer picture of the threats and the scenarios triggered by intentional acts, providing useful information in the security risk assessments of process facilities.

Keywords: Past accident analysis, Process industry, Security, Cybersecurity, Incident, Intentional act

1. Introduction

Process facilities, in particular those where hazardous substances are processed or stored (e.g. "Seveso" sites in Europe), may be the target of malicious acts aiming at interfering with the normal operations. Their attractiveness may be due to (Ackerman 2007; Nolan 2008): i) the socio-political location of the target; ii) the potential impacts that can be triggered with consequences similar to those originated by internal causes (i.e. safety-related accidents); iii) the potential of stealing materials that can be used as precursors of explosives ; iv) the potential of obtaining proprietary information important for the business (e.g. through a cyber intrusion).

The threat actor may exploit the vulnerabilities of the Physical Protection System (PPS, e.g. physical security barriers such as the site fences) of the target facility or its IT-OT system (Information Technology - Operational Technology) and start events such as the releases of hazardous substances, fires, explosions and loss of the process control and monitoring (French Ministry of Ecology 2015).

The American and European scenarios are quite different with respect to the security issues in process facilities. In Europe, the Seveso Directives focus on safety-related issues and on accidents triggered by natural events (NaTech), without addressing security issues. A mention to unauthorized accesses may be part of some country-specific transpositions of the Directives: for instance, the Italian transposition of the 2012/18EU Directive (Italian Government and Parliament 2015) suggests to consider malicious acts and unauthorized accesses for the definition of the internal emergency plan. The prevention, preparedness and response to terroristic attacks involving installations of the energy sectors (electricity and Oil&Gas) is promoted by the EPCIP (European Programme for Critical Infrastructure Protection), but no extension is made to the process industry (Commission of the European Communities 2006).

In the U.S., policies and legislation aimed at enhancing the preparedness against terroristic attacks were developed after the terroristic attack of "9/11". In particular, in 2007 (and re-codified in 2014) the US Department of Homeland Security, issued the CFATS (Chemical Facility Anti-Terrorism Standards) (Department of Homeland Security 2017) that require a Security Vulnerability Assessment (SVA) or Security Risk Assessment (SRA) for those process facilities that are in possession of specific quantities of Chemicals of Interest (COI), aiming at protecting their assets and employees, maintaining the integrity of the operations and preserving the value of investments.

The CCPS methodology (CCPS 2003), the VAM-CF methodology (U.S. Department of Justice 2002), the API RP 780 methodology (API 2013), and the RAMCAP methodology (Moore et al. 2007), are some of the SVA or SRA techniques suitable for the process facilities. These methodologies typically rely on past event analysis with respect to the phases of

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0_5761-cd

identification of vulnerabilities, threat scenarios, final outcomes, and security countermeasures.
In a previous study by Casson Moreno et al. (2018), a database collecting physical security-related events (i.e. events that do not involve the cyberspace in the attacks, but only physical actions performed by the attackers) and cybersecurity-related events (i.e. events that involve the cyberspace in the attacks, but that can also involve physical actions by the attackers) was built. In the present study, the database was revised, extended and updated until December 2019. The data collected were analysed in order to frame a clearer picture of the threats and the related scenarios that affect process facilities.

2. Methodology

As in the previous study carried out by Casson Moreno et al. (2018), data for the update of the database were gathered from different sources: scientific literature, the web and specific open-source databases reporting data on industrial accidents/incidents and near misses (as defined by Rathnayaka and coworkers (2011)) such as ARIA database (French Ministry of Ecology), Dechema ProcessNet (DECHEMA), E.U. Concawe (European Petroleum Refiners Association), E.U. EGIG (European Gas Pipeline Incident Data Group), eMARS (MAHB), Global Terrorism Database (START), Infosis ZEMA (Deutsch Umwelt Bundesamt), RISI database (Department of Homeland Security), PHMSA database (U.S. DoT).
Two criteria were used to include security-related events in the database: i) the event should originate as a result of a malicious act aimed at interfering with normal operations; and ii) the event involves an industrial facility belonging to one of the following sectors: Chemical&Petroleum, energy production, pipelines, transportation, bioprocesses and water/wastewater treatment as defined at Table 1. Each entry in the database consists in free text fields that retain general details concerning the record (e.g. date, location, data source, etc.) and itemized fields that describe unambiguously

Table 1. Definitions of the itemized fields “Industrial Sector”, “Security Threat” and “Final Scenario”.

Class	Definition
	Industrial Sector
Bioprocesses	Treatment of organic waste and waste fermentation juices. Food industry.
Chemical&Petroleum	Chemical production and storage installations, including pesticides production, pharmaceutical industry, production of basic chemicals. Petrochemical production and storage installations, including refineries.
Energy production	Electric power production plants using hydrocarbons (petroleum and natural gas-based fuels), hydroelectric and nuclear plants.
Pipelines	Oil and Gas transportation via pipelines.
Transportation	Transportation of hazardous materials via road, rail, water.
Water/Wastewater treatment	Water and wastewater treatment for industrial and domestic purposes, including water supply systems (excluding bioprocesses-related waters and slurries).
	Security Threat
Outsider cyber-threat	Events collected in this category are characterized by an attack, via cyberspace, with the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure (IT and/or OT); or destroying the integrity of the data or stealing controlled information.
Insider threat	The attacker is an insider, i.e. an individual who normally has authorized access to the assets of the company, motivated by working dissatisfaction or the possibility of gaining personal advantage.
Sabotage	The attackers aim at disrupting normal operations, but their threatening agent is not defined, as well as their driving motivations.
Terrorism	Terroristic organizations/groups, highly capable, well organized and equipped with the aim of causing a high-impact event, not only in terms of casualties, but also on media.
Theft	Criminal groups or individuals attacking facilities with the intent of stealing material.
Vandalism	Poorly equipped groups or individuals with low level of preparedness and usually no tactic in attack execution.
Unknown	An interference in normal production activities has been achieved via certainly intentional acts, but no more details were given concerning attackers or motivations of the act.

Table 1 (continued). Definitions of the itemized fields "Industrial Sector", "Security Threat" and "Final Scenario".

Class	Definition
	Final Scenario
Release	Event consisting in the discharge of a chemical from its containment, i.e. the process and storage equipment in which it is kept, without any further consequence such as an explosion or a fire.
Explosion	Event consisting in a physical and/or chemical explosion.
Fire	Event consisting in a pool fire, jet fire, fireball, flash fire, or flame.
Loss of process control/monitoring	Event consisting in the physical or cyber interference with the OT (Operational Technology) system, i.e. the Basic Process Control System (BPCS) plus the Safety Instrumented System (SIS), considering both software and hardware, without the occurrence of a release of hazardous substances, a fire, or an explosion.
Other	Event that does not result in a release of substances, a fire, an explosion, or a loss of process control/monitoring (e.g. infection of the IT system of a process facility, use of explosives without involving chemical equipment).
Near miss	An event that does not result in an actual final scenario such those described above, but the attack perpetrated by the attackers has the potential to do so. This can be due to the intervention of the security forces to stop the attack and/or the effectiveness of the physical protection system in place.

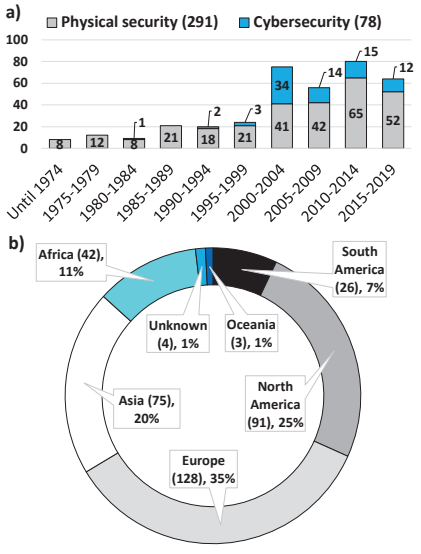

Fig. 1. Time trend (Panel a) and geographical distribution (Panel b) of the total events recorded.

the specific characteristics of the event (i.e. "Industrial Sector", "Security Threat", "Final Scenario"), all defined at Table 1. The data were then analysed, focusing on time and geographical trends, threat actor, industrial sector affected, and final scenarios triggered by the security attacks.

3. Results and Discussion

The updated database contains a total of 369 security-related incidents (both physical security- and cybersecurity-related events), 69 events more than in the previous version, with a time span of 54 years (from 1965 to 2019).

3.1 *The time trend and the location*

Figure 1a shows the quinquennial time trend of the physical security- and cybersecurity-related incidents (respectively 291 and 78 incidents) included in the database. After year 2000, there was a significant increase (almost quadruple) in the number of the incidents recorded, considering both physical and cyber events. In particular, only 5 cybersecurity-related incidents occurred before 1999, which started to be significant in the last 20 years. This can be justified by the fact that cybersecurity was not a significant threat for process facilities at the time (lower attractiveness, lower level of digitalization and network connection). The time trend of the records shows two peaks: one during the five-year period 2000-2004 (75 events), due to a high number of cyber-attacks all over the world, and one during the five-year period 2010-2014 (80 events), due to a high number of physical attacks. The latter peak might be due to the greater attention paid to the topic in the last decades, promoting incident reporting. For instance, for what concerns cyber-security, in the last years, companies have increasingly implemented cyber risk analysis (CRA) in the management of their IT/OT systems. This was supported by the definition of international standards, such as the ISO/IEC 27000 series for IT systems and the ISA/IEC 62443 for the industrial automation and control systems (IACSs). Moreover in Europe, in 2016, the NIS Directive was issued by the European Parliament and Council, setting several goals in the direction of security of IT-OT systems that all EU countries must achieve with specific national regulations. In this context, an increase in cybersecurity awareness by companies and a decrease of cyber-attacks are expected in the coming years.

The geographical distribution of the entries recorded in the database is shown in Figure 1b. Most of the events took place in Europe (128, 35% of the total), followed by America (117, 32%, 91 of which in North America and 26 in South America), Asia (75, 20%), Africa (42, 11%) and Oceania (3, 1%). For 4 records (1% of the total) the location is unknown. This result could be in part ascribed to the different reporting practices of each geographic area. For instance, in Australia, accidental events have to be reported when entailing a "serious risk", defined as “the death of a person, a serious incident or illness, or an incident that exposes any person to a serious risk (even if no one is injured)” (Safe Work Australia 2008). A similar legislation is present in U.K. (HSE 2013). Differently in U.S, reporting is included in the National Incident Management System, which requires reporting “for all the departments and agencies as well as for the private sector, regardless of cause, size or complexity of the incident” (Department of Homeland Security). A probable under-reporting concerns Asia, as the continent has the greatest number of industrial establishments (UNIDO Statistic Data Portal (UNIDO 2019)), but only the 20% of the incidents recorded took place in such continent.

3.2 *The industrial sectors affected*

Figure 2 reports the number of the security-related events recorded in the database with respect to the industrial sectors considered in the present study (defined at Table 1).

Pipelines for crude oil and gas transportation resulted to be the most affected industrial installation by security attacks (132 incidents, 36% of the total). This can be ascribed to the relatively easy accessibility of pipelines and the inherent difficulties and related cost in protecting them (Department of Homeland Security 2008). Moreover, cyber-attacks to the IT-OT systems that manage pipelines can be motivated by the possibility to obtain proprietary information important for the business such as production statistics, market strategies, drilling plans and pricing sheets. However, physical attacks to oil&gas pipelines outnumber by far the cyber-attacks (respectively 125 and 7).

The facilities belonging to the Chemical&Petroleum sector turned to be the second most affected by security attacks (100 incidents, 27 % of the total).
This fact is mainly due to the following reasons: i) the high socio-political impact of the events, first of all for those facilities owned by multinational companies and/or located in critical contexts; ii) the potential severity of consequences in facilities processing or storing large amounts of hazardous materials (e.g. Seveso establishments in Europe). Furthermore, as for pipelines, cyber-attacks to such companies, can be motivated by the possibility of obtaining proprietary information, important for business (e.g. patents of specific processes).

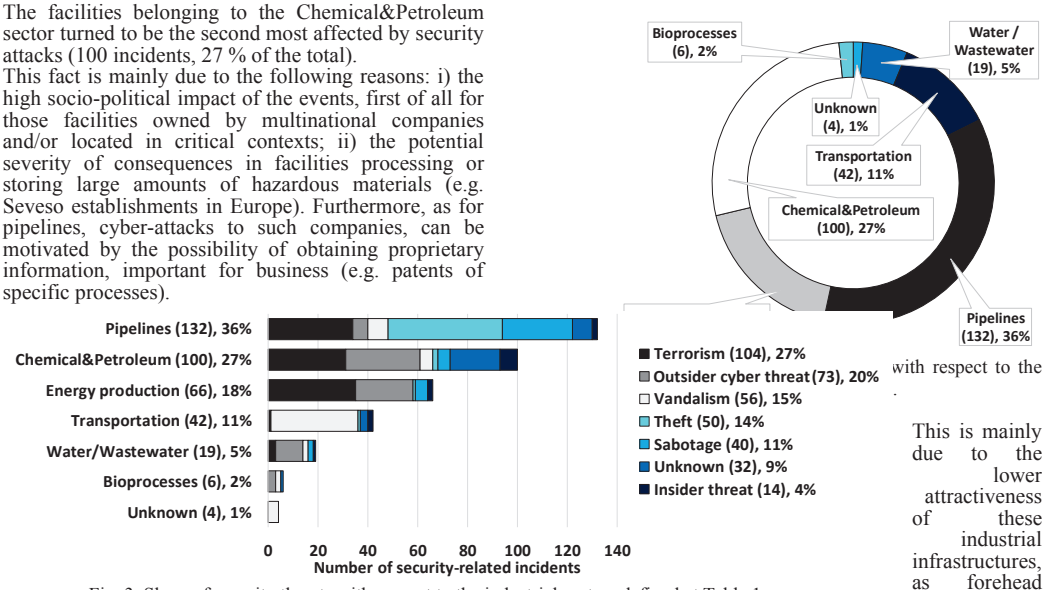

Fig. 3. Share of security threats with respect to the industrial sectors defined at Table 1.

A total of 66 incidents was recorded for the energy production sector (18% of the total) and 42 for transportation via road, rail and water (11%). Only 19 entries involved facilities belonging to the water/wastewater treatment sector (5% of the total) and 6 belonging to the sector of bioprocesses (2%). These are relatively small numbers considering the fact that the worldwide number of water/wastewater and bioprocesses plants is by far higher compared to that of chemical and petrochemical plants as reported by UNIDO Statistical Data Portal (UNIDO 2019). This can be justified considering two factors that stoke each other: firstly, the high security level of water/wastewater treatment plants because of the severe consequences on humans and the environment that can potentially be generated by malicious acts aiming at polluting water (Water Security Agency), and secondly, the low attractiveness of these facility due to the limited amount of hazardous materials processed that makes them target of few threat actors, only those that aim at polluting water and able to perform such attack (e.g. terrorist groups). In 4 incidents (< 1% of the total), the industrial sector was unknown.

3.3 *Security threats and final scenarios*

The share of the 369 security-related events recorded in our database with respect to the security threats defined at Table 1) is reported in Figure 3.
Terrorism resulted to be the most important threat category for the industrial installations with 104 events recorded, the 27% of the total. In particular, it plays an important role for the pipelines for oil and gas transportation, for the chemical and petrochemical facilities and for the energy production sector. Groups of terrorists can be motivated by political and/or monetary gain, revenge or destruction (API 2013) and the attractiveness of such industrial installations has been discussed in the previous section. The figure also reveals that terrorism is not a relevant security threat for transportation via road, rail or water, for water/wastewater plants and bioprocesses companies. with respect to the .

This is mainly due to the lower attractiveness of these industrial infrastructures, as forehead mentioned.
Outsider cyber threat, with 73 incidents recorded (20%), is among all, the second most important threat category, which is relevant for all the industrial sectors considered in the present study with the logical exception of the transportation sector: typically there is no possibility to connect remotely to the networks managing the operations of such transportation systems (it may be possible for a train (Kour et al. 2019; Pawlik 2019), but difficultly for a truck. Nevertheless, transportation is an easier target for vandals (35 of the total 56 incidents of vandalism occurred in this sector).
Fifty (50) security-related incidents (14% of the total) were characterized by theft of materials: most of them occurred in the oil and gas pipelines (e.g. theft of crude oil or natural gas). However, this class of security threat is affected by under-reporting, since thefts are very common events (Casson Moreno et al. 2018).
Sabotage (40 incidents, 11% of the total) is common to almost all the industrial sectors, as well as the insider threat, being the latter less common (14, 4%). Insiders are potentially a very critical category of attackers since they usually have extensive knowledge of both the process and the plant, and they usually have physical and/or remote authorized access to the assets of the facility they work for (they do not need to bypass all the security barriers in place as for outsider attackers).
For a high number of incidents (32, 9% of the total) it was not possible to identify the threat category, which fell into the category “unknown”.
Figure 4 shows the final scenarios (defined at Table 2) that occurred as a direct consequence of the security attacks perpetrated by the attackers (secondary or cascading events are not taken into account). A major event, i.e. a physical or chemical explosion, a fire or a release of a hazardous substances, was experienced in 250 incidents (almost the 68% of the total); in the remaining 119 cases a loss of process control or monitoring, an event of minor nature or a near miss, took place. In particular, the explosion resulted to be the most experienced final scenario by industrial facilities since it occurred in 123 events (the 34% of the total), followed

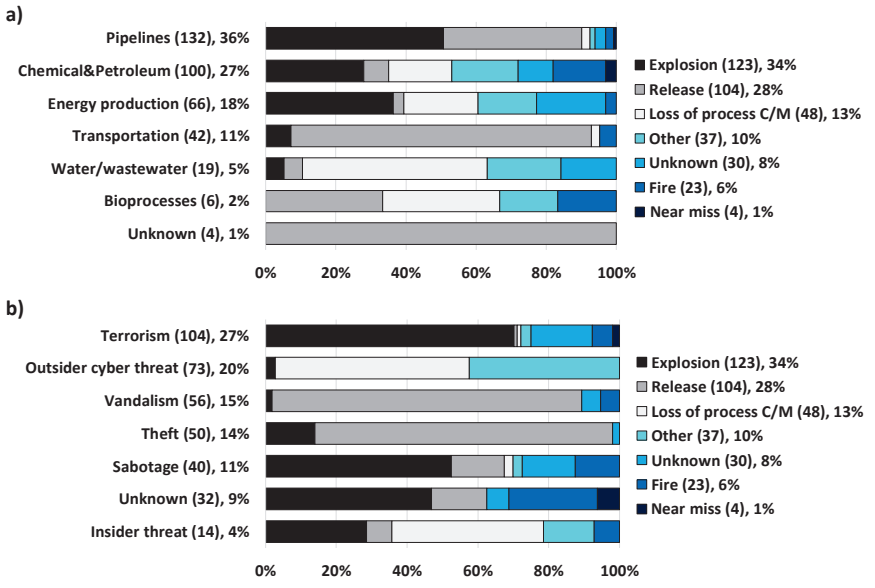

Fig. 4. Share of the final scenarios with respect to the industrial sectors (Panel a) and with respect to the type of security threats (Panel b).

by the release of hazardous substances in air, water or soil (104, 28%). Fire took place for 23 incidents (6%). The loss of process control/monitoring (i.e. the interference with the control and supervision system of a plant without the occurrence of a major scenario as defined above) was found for 48 incidents (13%). In 37 events (10%) the final scenario was labelled as "other", i.e. it is neither a generalized major event nor a loss of process control/monitoring (e.g. as regards cyber intrusions it may consist in the infection of the facility IT system, while as regards physical security it may consist in an event that does not involve a chemical equipment, e.g. the detonation of an explosive device that causes damages on the business buildings of the affected facility). The final scenario is unknown for 30 records of our database (8%) and a near miss was registered in 4 events (1%, labelled with "none"). For instance, among the latter, in 2018 in Pakistan the detonation of explosives planted at a gas pipeline was avoided by the security forces that defused such devices, and similarly in the same year in Saudi Arabia, the air-defence forces intercepted two ballistic missiles targeting an oil facility, avoiding their crash on the plant and buildings and its consequences (START).

Figure 4a shows the distribution of the final scenarios with respect to the industrial sectors considered in the present study. Explosions took place mainly in the oil and gas transportation via pipelines, in the chemical and petrochemical facilities, and in the energy production plants. For instance, in Nigeria in 2006, after the intentional rupture of a pipeline (from the investigations it seems an act of fuel theft carried out with an earthmover), there was a violent explosion that caused the death of 260 people and other 60 injured (BBC News; REUTERS). Another example is the accident that occurred in 2017 in the Aj Jalisiyah power plant in Samarra (Iraq) where at least three suicide bombers, equipped with grenades and firearms, gave rise to explosions that injured 12 people and killed 10 more (START).

A release of a hazardous substance, as well as a loss of process control/monitoring is a common scenario to all the industrial sectors. In particular, almost all the incidents recorded for transportation sector were characterized by a release. For example, in 1988, unauthorized persons stole LPG from an unattended propane truck by removing a blind flange and opening a hand valve on the loading line, resulting in a leakage of several litres of liquid propane that did not ignited (MAHB). Moreover, a relevant case of loss of process control/monitoring occurred in 2010, where attackers infected the control system of the Natanz nuclear power plant (Iran) and sabotaged more than 1000 centrifuges by fluctuating their spinning speed although the monitors detected any malfunctions (Department of Homeland Security).

The final scenario "fire" was experienced in industrial installations belonging to almost all the industrial sectors even if with different percentages, clearly enough with the exception water/wastewater treatment plants. A relevant case of fire occurred in 2003 in Iraq, where as a consequence of an act of sabotage, a fire broke out in a sulfuric factory and spread to neighbouring reserves, causing the direct death of one person and that of 4 others due to the toxic cloud that had been generated (French Ministry of Ecology).

Similarly, also the final scenario "other" was registered for all the industrial sectors, except for that of transportation. For example, in 2006 in Japan, security data regarding the location of the control room and the instrument panel room, and other confident data on a thermal power plant was leaked onto the Internet from a virus-infected personal computer belonging to an employee (Department of Homeland Security).

The distribution of the final scenarios with respect to the security threats is shown in Figure 4b. Important differences are present. While terrorism mainly causes explosions as final scenarios, thefts and vandalisms are more likely to result in the releases of hazardous substances. Outsider cyber-attacks mainly result in the loss of process control/monitoring and in the infection of the IT network of companies (which is considered

within the final scenario "other"). Only two cases of explosions were found as a consequence of malicious manipulations of the control system. The first occurred in 1982, when the control software of the Trans-Siberian gas pipeline became infected with a malware that caused, by the remote manipulation of devices such as pumps and automatic valves, its over-pressurization and the consequent explosion (Department of Homeland Security). The second event, occurred in 2008, when the attackers remotely shutdown the alarm systems, cut off communications with the control room and pressurized a section of the BTC (Baku-Tbilisi-Ceyhan) crude oil pipeline causing an explosion followed by a fire which lasted for two days (French Ministry of Ecology; Department of Homeland Security).

4. Conclusions

The present study is based on the revision, extension and update of an existing database. The database collects now 369 past physical security- and cybersecurity-related incidents that affected facilities of process industry and similar industrial sectors (Bioprocesses, Chemical&Petroleum, Energy production, Pipelines, Transportation, Water/Wastewater).

The time trend showed an increase in the number of events recorded after year 2000, also due to a significant growth in cyber-attacks. Important differences were found in the geographical distribution, with Europe having the highest number of incidents reported, followed by the Americas. A probable under-reporting affects Asia.

Pipelines for oil and gas transportation resulted to be the most affected industrial installations by security attacks due to the inherent difficulties and high costs in protecting such devices, followed by fixed installations, especially those were large amount of hazardous substances are stored or handled (e.g. Seveso plants in Europe).

Important differences were also found in the distribution of the security threats with respect to the industrial sectors, with thefts dominating in the case of pipelines, and terrorist attacks in the case of fixed installations. Cyber-attacks were experienced by almost all the sectors, even if chemical and petrochemical facilities as well as energy production plants were the most affected.

The final scenarios triggered by the security attacks were investigated, both with respect to the industrial sectors and the security threats. A physical or chemical explosion was by far the most common scenario experienced by the affected facilities, followed by the release of a or hazardous substance. A relevant number of cyber- attacks infecting the control and supervision system of industrial installations was registered, two of which resulted in an explosion.

Overall, the results point out the concreteness of security-related events in process industry and similar sectors and they can be used as useful information in the application of the techniques used to handle security-risks in process facilities where hazardous substances are stored or processed such as the SVA (Security Vulnerability Assessment) or SRA (Security Risk Assessment) techniques.

Acknowledgement

This work was supported by INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) under the SAFERA-4STER project.

References

Ackerman, G., P. Abhayaratne, J. Bale, A. Bhattacharjee, C. Blair, L. Hansell, et al. (2007). Assessing Terrorist Motivations for Attacking Critical Infrastructure, University of California.

API - American Petroleum Institute (2013). ANSI/API standard 780 – Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry.

BBC News. Lagos pipeline blast kills scores. http://news.bbc.co.uk/2/hi/africa/6209845.stm (accessed February 1, 2020).

Casson Moreno, V., G. Reniers, E. Salzano, and V. Cozzani (2018). Analysis of physical and cyber security-related events in the chemical and process industry. Process Safety and Environmental Protection 116, 621–31.

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

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

DECHEMA - Deutsche Gesellschaft für chemisches Apparatewesen. Dechema ProcessNET.

Department of Homeland Security (2008). National Incident Management System.

Department of Homeland Security (2008). Pipeline Threat Assessment.

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

Department of Homeland Security. RISI Database - The Repository of Industrial Security Incidents.

Deutsch Umwelt Bundesamt. Infosis ZEMA.

European Gas Pipeline Incident Data Group. E.U. EGIG.

European Petroleum Refiners Association. Concawe.

French Ministry of Ecology. ARIA database – La Référence Du Retour d'expérience Sur Accidents Technologiques.

French Ministry of the Ecology (2015). Accident Study Findings on Malicious Acts Perpetrated in Industrial Facilities. Aria Database 18.

HSE - Health and Safety Executive (2013). RIDDOR - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013.

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. Gazzetta Ufficiale.

Kour, R., R. Karim, and A. Thaduri (2019). Cybersecurity for railways - A maturity model. Journal of Rail and Rapid Transit 0: 1–20.

MAHB - Major Accidents Hazards Bureau. eMARS Database - Major Accident Reporting System of the European Commission.

Moore, D.A., B. Fuller, M. Hazzan, and J.W. Jones (2007). Development of a security vulnerability assessment process for the RAMCAP chemical sector. Journal of Hazardous Materials 142, 689–94.

Nolan, D.P. (2008). Safety and Security Review for the Process Industries: Application of HAZOP, PHA, What-IF and SVA Reviews (4th ed.). Gulf Professional Publishing.

Pawlik, M. (2019). Railway Safety and Security Versus Growing Cybercrime Challenges. Communications in Computer and Information Science 1049, 57–68.

Rathnayaka, S., F. Khan, and P. Amyotte (2011). SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. Process Safety and Environmental Protection 89, 151–64.

REUTERS. TIMELINE: Deadly Nigerian pipeline disasters. https://www.reuters.com/article/us-nigeria-pipeline-disasters-idUSL1566948020080515 (accessed February 1, 2020).

Safe Work Australia (2008). Incident Reporting 2008.

START - National Consortium for the Study of Terrorism Responses to Terrorism. Global Terrorism Database.

U.S. Department of Justice (2002). A Method to Assess the Vulnerability of U.S. Chemical Facilities.

U.S. DoT - United States Department of Transportation. PHMSA Database - Pipeline and Hazardous Materials Safety Administration.

UNIDO - United Nations Industrial Development Organization (2019). INDSTAD 2 2019, ISIC Revision 3 database 2019.

Water Security Agency. EPB 363- Security at Water Treatment Plant