Physical security in the process industry

Theory with applications

Landucci, Gabriele; Reniers, Genserik; Khakzad, Nima

Publication date
2020

Document Version
Final published version

Citation (APA)
Landucci, G., Reniers, G., & Khakzad, N. (2020). *Physical security in the process industry: Theory with applications*. Elsevier. https://www.elsevier.com/books/physical-security-in-the-process-industry/landucci/978-0-444-64054-3

Physical Security in the Process Industry

Theory with Applications

Gabriele Landucci

Department of Civil and Industrial Engineering
University of Pisa, Pisa, Italy

Nima Khakzad

School of Occupational and Public Health
Ryerson University, Toronto, Canada

Genserik Reniers

Safety & Security Science Group (S3G)
Delft University of Technology, Delft, the Netherlands

ELSEVIER

Index

Note: 'Page numbers followed by "f" indicate figures, "t" indicates tables'.

Elsevier
Radarweg 29, PO Box 211, 1000 AE Amsterdam, Netherlands
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-444-64054-3

Publisher: Susan Dennis
Acquisitions Editor: Kostas Marinakis
Editorial Project Manager: Michelle W. Fisher
Production Project Manager: Sojan P. Pazhayattil
Cover Designer: Miles Hitchen

Typeset by TNQ Technologies

1 An introduction to physical security

1.1 Security as a part of safety

If one thinks about it, security has a very long and rich history. In Ancient Egypt or old Persia for instance, there were already soldiers and personal guards. But also even earlier, in the ancient China, security was very important. As an example of the importance of security in those ancient times, the terracotta army depicting the armies of Qin Shi Huang, the first Emperor of China, can be mentioned, found in the city of Xi'an in the province Shaanxi in China. Actually, it is possible to go as far back in time as desired: while humans were settling in communities for agricultural reasons, there were undoubtedly security issues and problems such as theft, manslaughter, and murder. In fact, where humans are, or have ever been, there was or is need for security. In that sense, the "security officer" is arguably the oldest profession in the world.

We now can ask about the definition of security and what it in fact contains and entails. What is it that makes a certain topic, situation, or issue belong to the *security* field, or to another domain, for example, *safety*? The answer is surprisingly simple, and at the same time somewhat complex, and may be traced back to the understanding of one concept: human intention. However, the clear distinction between safety and security in terms of intention only *seems* easy, but in fact it is not.

Let us first discuss the concept of "safety" more in depth before defining, describing, and discussing the concept of security. What is *safety*? Here the difficulty starts: there is no single and widely accepted definition of "safety" by safety scientists. Definitions such as "freedom from danger," "a dynamic non-event," or "the result of conditions for which the likelihood of non-intentional negative consequences is low," all try to be as clear or as general as possible, but none of them represents a generally accepted definition. These varying definitions indicate that it is difficult to find an acceptable, useable, and understandable definition for safety. The main problem consists of the fact that the meaning of safety varies according to the perspective of the person looking at the concept. A specific situation might seem safe for one person, while the same situation may seem very unsafe for another person.

Safety can actually be seen as a state (perception or real) of a person, a machine, etc., at a certain moment in time. Many possible safety substates can be conceived at one certain moment in time, but individually these substates do not reveal anything on the potential consequences of unsafety, about the likelihood that a certain state (aggregated from the substates) turns out bad or good, about what kind of safety

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00001-9

measures can be taken for each substate, etc. Moreover, the substates change continuously and thus the aggregated safety state in reality is extremely dynamic and changes all the time (Fig. 1.1.1).

In brief, safety can be defined as "the avoidance and/or decrease of losses due to all types of causes (related to safety sub-states), and taking into account all possible sub-states at a certain moment in time."

The concept of "safety sub-state" is usually characterized by being nonintentional or nondeliberate. This is not necessarily the case: looking at safety from a broad perspective, it is clear that the concept is actually linked to avoiding losses of all kind, hence also intentional, that is, deliberately human-caused, losses. If we consider security into the "Safety" definition, we can describe safety as "the avoidance and/or decrease of losses due to all types of causes (related to safety sub-states), and taking into account all possible (non-intentional as well as deliberate) sub-states at a certain moment in time."

One important problem arises: the description of the substates or the aggregated safety state does not allow us to quantify. The substates are rather theoretical and hypothetical by nature, and in principle, an infinite number of substates exists. Hence, at this moment for us the "safety state" is an abstract concept. Based on an abstract concept, it is impossible to rationally take safety measures to lower unsafety and to increase safety. For this exact reason, the concept of "risk" is introduced.

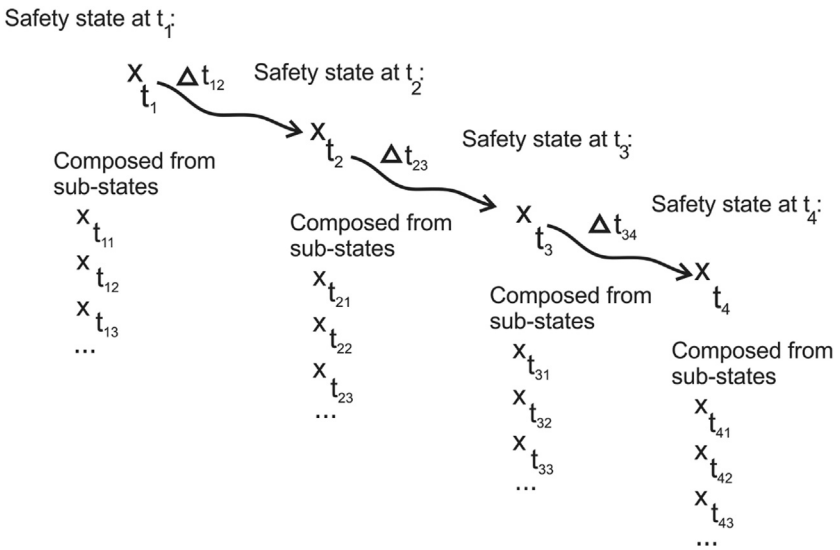


FIGURE 1.1.1 Structure and evolution of safety states: substates, aggregated state, and timeline.

1.2 Risk sandglass and security risk trias

Dealing with security risks is actually a part of managing operational risks, and thus, security management can be situated within the field of "engineering risk management."

Obviously, other risks such as financial risks, quality risks, environmental risks, ethical risks, and health risks are all risks that need to be controlled and managed within this field. Before diving into the similarities and differences between managing safety risks and managing security risks, the concept of "risk" should be defined. International guidelines can be employed to obtain a better understanding of the concept of risk. According to ISO 31000 (ISO-International Standardization Organization, 2009), the umbrella "Risk Management" Guideline by the International Standardization Organization, "risk" can be defined as "the effect of uncertainty on objectives." This is a very broad definition of risk, indicating that without objectives (or aims) or without uncertainties, risk does not exist and that both making profits and suffering losses are intrinsically linked to the risk concept. To "take risks," in order to make profits by carrying out certain activities, goes hand in hand with "risking," in which losses can be suffered due to carrying out of these activities. "Risk appetite," a term often used in the financial sector, is thus intrinsically linked with the risk to lose a lot of money (and not only with the uncertainty of gaining a lot of money).

If only looking at the negative side of risk, a number of different definitions of the risk concept exists and some examples (out of a large list) are: "risk is the likelihood that a loss will occur," "risk is the probability that a hazard will be transformed into damage or loss," or "risk is the possibility that positive expectations will not be realized." These are all definitions describing risk in a negative way. However, as mentioned earlier, the most recent scientific insights indicate that risk should be viewed as a coin with two sides, and one side does not exist without the other side. It depends on the observer, which side he/she wants to tackle (or both sides, preferably). The two sides can be represented by using the risk sandglass. The risk sandglass is a metaphor making the two sides of risk obvious. On the positive side, there are the opportunities (positive uncertainties), which may lead to profits if you are exposed to them, while on the negative side, dangers exist (negative uncertainties) possibly (if there is exposure) leading to losses.

The negative triangle, at the bottom of Fig. 1.2.1, is the so-called "risk trias" composed of dangers, exposure, and losses. If the dangers are called "hazards," we talk about the "safety risk trias." This terminology is used by safety management; however, the term "hazard" does not hold in the case of security risk management. For the latter field, specific terminology is needed, which will form the "security risk trias," explained in the next paragraph.

From the aforementioned, it has become crystal clear that safety and security are entangled, the only difference being the human intention of causing the losses. This difference translates into the conceptual description of the two concepts and the resulting approach, and hence, the way the risk is managed and treated. For non-intentional risks (safety), three issues need to be determined and dealt with: hazards, exposures to hazards, and possible losses. In case of intentional risks (security), an analogy can be made: (intentional) threats, vulnerabilities toward the threats, and

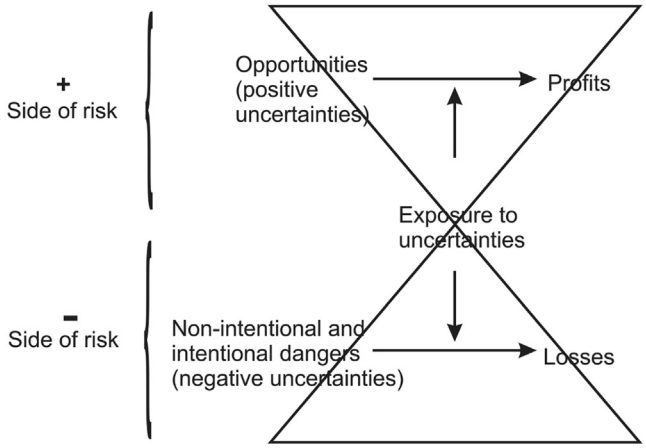


FIGURE 1.2.1 Risk sandglass. *Source: Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed. De Gruyter, Berlin.*

potential (intentionally caused) losses. Together, the three latter terms form the so-called "security risk trias" (see Fig. 1.2.2).

The existing risk assessment techniques for nonintentional risks (for instance, Hazop, What-if analysis, Fault Tree Analysis, the bow-tie method, and many others (CCPS—Center of Chemical Process Safety, 2000)) are designed to identify as many hazards as possible, all thinkable exposures to these hazards, and considering as many loss scenarios as realistically feasible due to the combinations of hazards and exposures. Afterward, safety investment decisions can be made based on the known safety risks.

For the case of intentional risks, there is an analogy: security risk assessments should determine as many threats as possible, identify the vulnerabilities through which the threats may be exploited, and take into account as many potential consequence scenarios as deemed realistic. When the threats, vulnerabilities, and possible intentional losses are known, adequate security control and management measures can be taken.

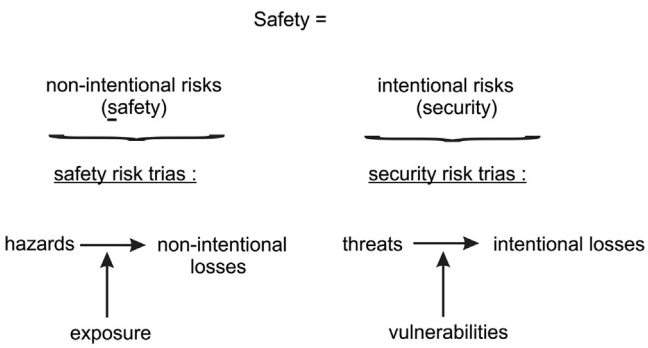


FIGURE 1.2.2 Analogy between safety risk and security risk.

In this book, we do not go into detail about the positive risks of the risk sandglass, but we elaborate in the further chapters how the intentional negative risks can be dealt with. As explained earlier, the threats, vulnerabilities, and possible intentional losses need to be known, based on security risk assessment techniques. If these are known, measures can be thought of to decrease or eliminate these factors, since:

- no/decreased threats = no/decreased security risks,
- no/decreased vulnerabilities = no/decreased security risks,
- no/decreased intentional losses = no/decreased security risks.

If we would know *all* threats, *all* vulnerabilities, and *all* possible intentionally caused losses (which in reality is evidently not possible), we could really make optimal decisions with respect to decreasing or eliminating security risks. This is actually not as straightforward as it seems at first sight.

1.3 Quantification of security risk

Quantifying security risks is one of the requirements to make good Safety decisions, to make trade-offs based on prioritizations, and to take adequate security measures. Besides the threats, vulnerabilities, and potential intentional losses as described in the previous section, one more important factor needs to be considered: the security risk scenario. It is obvious that many security risk scenarios at any certain point in time (we can call them the potential "sub-states" from a security viewpoint) are possible, actually an infinite number, and they can all be described in some way. But they can also be quantified. Based on the concrete information available about the threat, vulnerability, and intentional loss of one risk scenario (one substate) at any certain point in time, it is possible to quantify the abstract, theoretical concept of the security risk linked to this scenario. In theory, all the substates at any certain point in time can thus be calculated, and based on this information, choices can be made.

Reality as it occurs can be regarded as a continuous expected value of summed risk scenarios that are all characterized by a likelihood of certain consequences happening. A much used formula for calculating a risk R_i linked to risk scenario i is "the scenario likelihood multiplied by the scenario consequences." Hence:

$$R_i = L_i \times C_i \tag{1.3.1}$$

where R_i is the calculated risk linked to a scenario i, L_i is the likelihood of scenario i occurring, and C_i are the consequences when scenario i occurs.

If the perception of people with respect to the risk needs to be considered in the risk quantification, a so-called "risk aversion factor a" can be used:

$$R_i = L_i \times C_i^a \tag{1.3.2}$$

where, if $a = 1$, a risk-neutral attitude is considered (consequences and likelihood are considered equally); $a > 1$ indicates a risk-averse attitude (the consequences are stressed

and made more important compared with the likelihood in the risk calculation, using the risk aversion factor); and if $a < 1$, a risk-seeking attitude is implied.

Assume that $a = 1$, then it is possible to define for a situation at a certain point in time (a "state"), a number of scenarios (the "sub-states" of this "state"). Assume further that a situation can be characterized by three scenarios or substates (which obviously is an extremely rough estimation, since in reality there are an infinite number of substates or scenarios with most of them having an extremely low likelihood).

The three scenarios in our example are:

- *Scenario 1:* nothing happens: $L_1 = 0.90$; $C_1 = 0€$
- *Scenario 2:* small intentional incident (e.g., theft): $L_2 = 0.099$; $C_2 = -1000€$
- *Scenario 3:* serious intentional incident (e.g., terrorist attack): $L_3 = 0.001$; $C_3 = -900{,}000€$

The expected value of the security risk of this state of aggregated substates (as already mentioned, an extremely simplified situation) can then be calculated, for instance, for a risk-neutral attitude, summing up the risk contribution associated with the three scenarios:

$$R = 0.9 \times 0€ + 0.099 \times (-1000€) + 0.001 \times (-900{,}000€) = -990€ \tag{1.3.3}$$

When taking decisions on what level of security investments needs to be carried out as regards this situation, it can be recommended, based on a risk-neutral attitude and assuming that these are the only three possible intentional scenarios related to a certain state, not to invest more than 990€.

In current industrial practice, a choice is usually made of one particular scenario, for instance, the worst possible scenario in terms of consequences ("worst-case scenario") or the scenario with the highest possibility ("most probable scenario"), or a combination of these two, that is, the worst scenario that is deemed possible in reality ("worst credible scenario"). Based on the scenario that one has chosen, the risk calculations are carried out. Currently no expected values of aggregated substates are used to determine the security risk, but rather single scenario-based risks.

The risk formula mentioned earlier can be used (multiplying likelihood and consequences of certain scenarios at a certain time) to calculate the security risk level at a certain time. More generally, an expected security risk for every time slice can be quantified such as indicated in Fig. 1.3.1.

Hence, Fig. 1.3.1 shows that at every time t, a number of substates x (scenarios) are possible, all having a likelihood p and some consequences c. The aggregation of these substates via an expected value, toward an overall aggregated security state, leads to the quantified notion of a security situation (the "security risk") at a certain time.

The obtained value can be expressed in expected euros lost, as displayed earlier, but also, for instance, in expected numbers of fatalities, in expected lost time, or in any other unit. At first sight, security seems to be an absolute concept, but it is certainly not. Security risks should be seen and considered relative to each other. A security risk needs

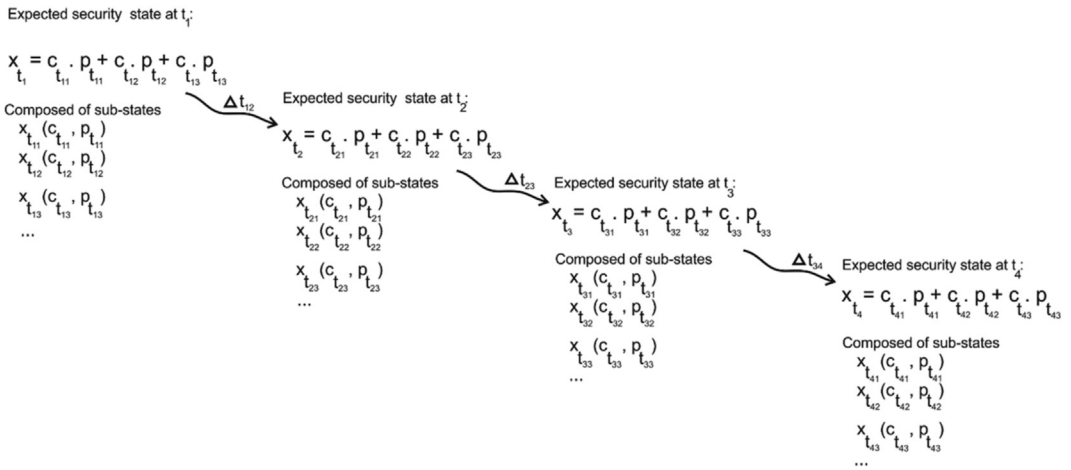


FIGURE 1.3.1 Calculating the expected security risk based on state and substates (*x*) over time (*t*), using probability (*p*) and consequence (*c*).

to be compared with all other security risks being determined, and based on this relative evaluation, it is possible to prioritize all security risks and in an optimal way take the needed actions or make the necessary countermeasure decisions.

One difficulty for operationalizing the aforementioned approach is that the determination of the likelihood in case of security risks is not at all straightforward. In case of safety, for the quantification of the likelihood of an incident scenario, for instance, a frequency or a probability is employed. If no data at all is available, usually also a fairly good qualitative assessment can be made by expert judgment, ranging from "very low" to "very high", for example. In case of security risks, this is much more difficult, especially in case of extremely low likelihood security events. The quantification of security risks needs to be based on criteria such as "success likelihood of attack" and "attractiveness of target." How these parameters can be assessed and quantified will, among others, be discussed in this book.

Hence, the formula for calculating the expected security risk as explained earlier, only works if the security risk scenarios are known (or agreed upon), together with the consequences and probabilities of these scenarios. This is very hard, if not impossible, in reality, and therefore, we elaborate and provide an approach to calculate the security risk based on quantifiable parameters. The following formula for calculating the rational security risk based on the parameters of vulnerability and potential consequences can be suggested:

$$\begin{aligned} &\text{Risk formula } SR_i \\ &SR_i = (Vulnerability)_i \times (Potential\ Consequences)_i^a \end{aligned} \tag{1.3.4}$$

Using the risk formula expressed in Eq. (1.3.4), it is also possible to calculate the expected security risk at certain moments in time and aggregate over time. This is illustrated in Fig. 1.3.2.

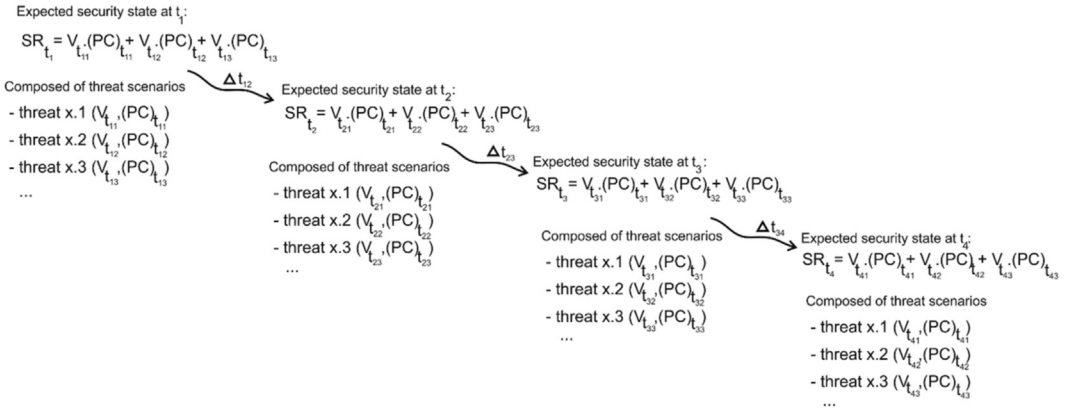


FIGURE 1.3.2 Calculating the expected security risk (*SR*) over time (*t*), taking into account the vulnerability (V) and the potential consequences (PC), and based on threat scenarios (x).

The parameters of Vulnerability and Potential Consequences can then be further elaborated into more quantifiable parameters. Vulnerability can be seen as the combination of several aspects: the likelihood of attack success (if higher, vulnerability increases), the (subjective) consequences as perceived by the adversary (if higher, vulnerability increases), and the security measures taken (if higher, vulnerability decreases). The Potential Consequences (PC) can be regarded to depend on the (objective) quantifiable worst-case consequences (hence, the consequences linked to the worst-case scenario) (if higher, PC increase) and the (safety-related) mitigation measures taken (if better or higher, PC decrease).

This way, the Security Risk formula becomes:

$$SR_i = \frac{(likelihood\ of\ attack\ success)_i \times (perceived\ consequences)_i}{(\text{sec}urity\ barriers)_i} \times \frac{(worst-case\ consequences)_i}{(safety\ (=mitigation)barriers)_i} \tag{1.3.5}$$

If we further only look at the "naked" security risk, we need to take abstraction of the safety and security barriers present. Furthermore, the Security Risk formula as suggested earlier and without the security barriers and mitigation measures included can be reformulated into a very well-known (naked) security risk formula. It is possible to consider the "likelihood of attack success" to represent the vulnerability (*V*). Also, the perceived consequences can be seen as the combination of "attractiveness of the asset to the threat" (*A*) and the parameter "threat" (*T*), since the higher the perceived consequences, the more attractive an asset is to an adversary and the more it may become a threat of a certain category. Further, the "worst-case consequences" obviously represent the consequence (*C*) or impact value of the security risk. This way, the security risk formula becomes:

$$R = V \times (A \times T) \times C = (A \times T) \times V \times C \tag{1.3.6}$$

This is the well-known security risk formulation by API Recommended Practice 780 (American Petroleum Institute (API), 2013), and the different parameters of the formula will be thoroughly explained and elaborated in the next chapters. How the parameters should be defined, and how they can be quantified, also will be expounded in the following.

1.4 Extended security risk formula

For completeness, it should also be indicated that the formula for calculating risk may be extended toward emotional feeling. Especially for security, this can be a very important part of the risk level for decision-making. More concretely, in case of security-related risks, people may feel very strong (and risk-averse) about, for instance, murder or terrorist suicide attacks. Although the likelihood of dying due to such event is extremely low (since the likelihood of being murdered or the possibility of a suicide attack is very low), many people believe it is very important to invest in security measures to prevent and/or mitigate the consequences of such events.

Reniers and Van Erp (2016) therefore suggest to extend the well-known risk calculation formula where only rational parameters (consequences and probability of a scenario in case of safety, or vulnerability and potential consequence of a threat scenario in case of security) are taken into account, toward a risk index wherein both rational and emotional parameters are considered:

Risk formula SR_i^*

$$SR_i^* = \frac{V_i \times (PC)_i^a}{\beta_i \times \left(E_i \times F_i^b\right)} = \frac{SR_i}{\beta_i \times \alpha_i} \tag{1.4.1}$$

where:

- SR_i^* = Risk index of event/scenario i
- V_i = Vulnerability of event related to scenario i
- $(PC)_i$ = Potential magnitude of the consequences of scenario i
- a = aversion factor toward consequences
- $ß_i$ = the policy factor that varies according to the degree which participation in the risk due to event/scenario i is voluntary
- E_i = Acceptability of the principle used to apportion liabilities for undesired consequences for event/scenario i (Equity principle)
- F_i = Acceptability of the procedure by which collective consent is obtained to those who must bear the consequences of event/scenario i (Fairness principle)
- b = factor expressing the availability of alternatives in combination with the anti-recklessness of management
- SR_i = risk of event/scenario i, calculated using a rational approach (with consequence and likelihood estimation)
- α_i = Acceptability of event/scenario i following an emotional approach

By using this extended formula in case of security risk, the emotions that people experience in case of, for instance, terrorist attacks can be incorporated in the security risk calculation. Factors such as the equity principle, the fairness principle, and the antirecklessness of management decisions can make a difference in the prioritization of physical security risks.

1.5 Types of risk

For the calculation and the treatment of security risks, a distinction should be made between two types of security risks:

- Type I: small/regular security risks
- Type II: disaster security risks

Remark that black swan security risks (Paté-Cornell, 2012) can be seen to be an extremum of type II risks. Some illustrative examples may be seen in Fig. 1.5.1.

Type I security risks do regularly occur on a daily basis and are characterized with a high likelihood and a small impact. These risks concern typically well-known and (relatively) low-level security matters such as theft, murder, and manslaughter. Type II risks are rare but occur regularly on a global scale and usually have a rather high to a very high impact (even on a societal level). A typical example of a type II security risk is a terrorist attack. Black swan risks are those that have never occurred before (unprecedented) and can only be imagined with the fantasy of the mind. For instance, the 9/11 attacks to WTC towers in New York City was a black swan before it occurred (pre 2001), but is now a type II security risk as it has already occurred (post 2001). Actually, such events should be seen as extrema of type II risks.

No widely accepted definitions exist for the different types of risk, making it very hard to make a distinction between them in a way that is accepted and understood by everyone. An organization thus needs to decide itself about the concrete difference between type I and type II risks. Both types of risks demand their own security risk assessment and management approaches. An organization needs to identify them

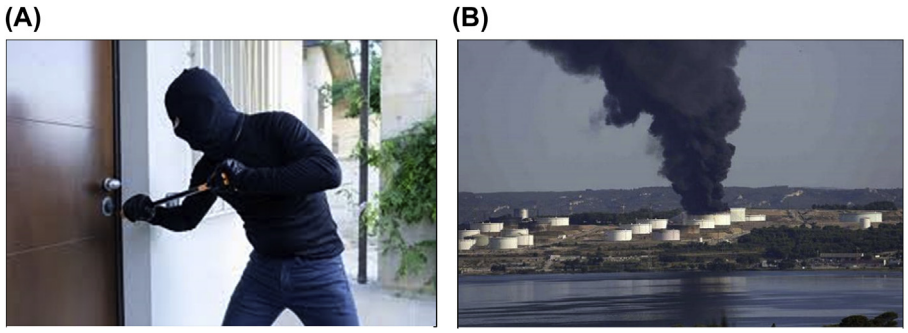


FIGURE 1.5.1 Examples of types of risk: (A) type I security risk; (B) type II security risk.

separately, analyze them with different security risk analysis methods, evaluate and prioritize them separately, and make decisions about their treatment separately, and deal with them with different security countermeasures.

In case of security, the lack of casuistic and information regarding likelihood assessment is thus a true challenge. It is extremely difficult to assess the probability of type II security events, and even of type I security events. Statistics are unreliable and usually highly uncertain. Besides the difficulties to use the expected value formulas for security, it is very important to adequately manage security risks. Hence, the importance of security risk management.

1.6 Security risk management

Risk management can be defined as the systematic and regular study of (negative) risks threatening people, tangible and intangible assets, and activities and formulating and implementing an integrated policy with respect to risk reduction, risk transfer, and risk financing. According to the most widely accepted definition of the ISO31000 Guide 73 (ISO-International Standardization Organization, 2009), risk management comprises the coordinated activities to steer and control an organization when risks are concerned. These are very complex definitions, but to put it in simple terms, risk management can be considered everything that is needed to manage and control risks. To this end, risk management uses a set of approaches, concepts, models, theories, and disciplines, especially developed to manage risks and to make sure that they are adequately controlled.

Risk management is therefore much more than merely looking after the legislative aspect of compliance, or dealing with the technical aspects of risk identification, risk analysis, and risk evaluation. Risk management also includes risk communication, human and organizational aspects, economic aspects, business continuity planning, learning from accidents, risk governance, etc.

Fig. 1.6.1 provides a nonexhaustive overview of the various domains that (operational) security risk managers should be concerned with. Physical security risk management is a term used for managing and controlling all physical security risks.

All the domains mentioned in the physical security risk management set can be applied to the field of physical security. Physical security denotes all security matters besides cyber security. Security managers obviously need to comply with legislation, and organizations often also set their own security objectives and targets. Physical security risks need to be assessed (threats and vulnerabilities, as well as potential intentionally caused losses require identification, quantification, and analysis) and prioritized. Furthermore, economic aspects of security investments need to be considered: insurance premium costs, security countermeasures costs, hypothetical benefits due to security investments, etc., see also Chapter 7 in this book. Emergency planning and crisis management need to take security matters into account, for instance, by involving law

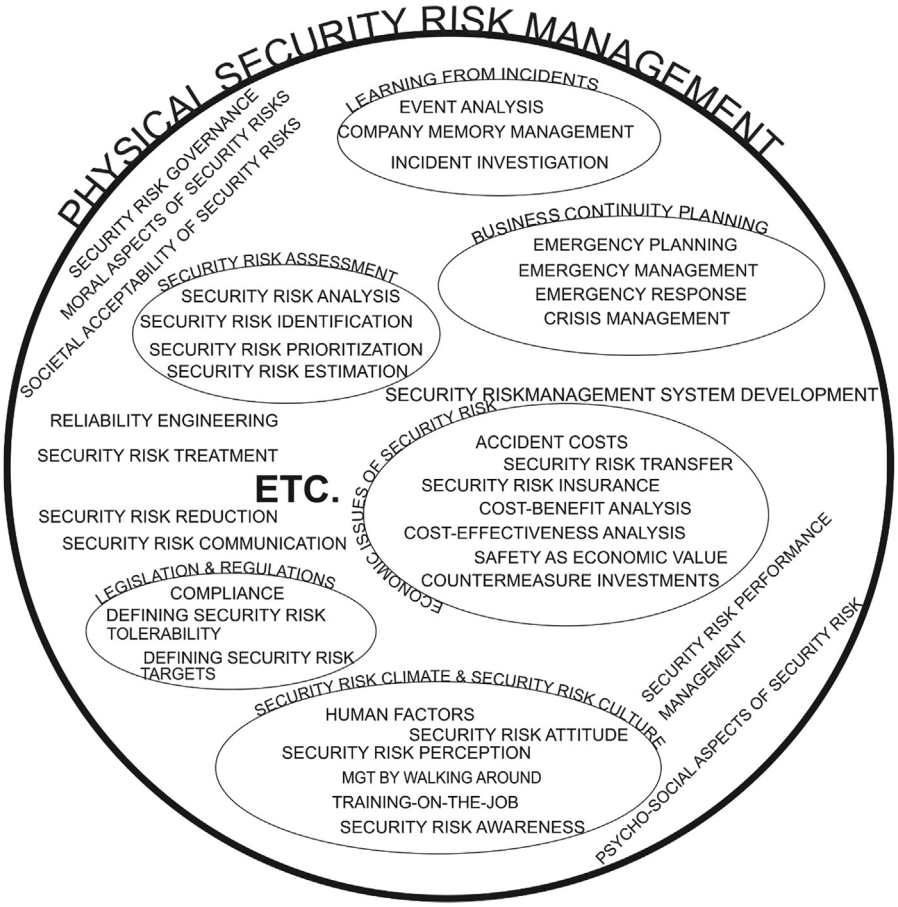


FIGURE 1.6.1 Physical security risk management set. *Source: adapted from Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed. De Gruyter, Berlin.*

enforcement into contingency planning or by developing a bomb incident plan. Security awareness needs to be created in the organization, requiring an adequate security climate and culture. All security incidents, small and large, need to be reported and investigated thoroughly, and a company memory needs to be built up regarding physical security, using security performance indicators. A security management system is developed to streamline all security efforts and to treat security risks. A security risk communication plan is drafted to make sure that in case of a major security incident, good communication is guaranteed.

The basics of security risk management, similar to all other management domains, can be summarized as a "Plan-Do-Check-Act" cycle. This management cycle was originally developed in quality management science and is used to continuously improve not only product or service quality, or safety for that matter, but also security. In the first phase (Plan), a plan for making changes (improvements) is conceptualized. The next

phase (Do) is the step of the implementation of the envisioned plan. In the third phase (Check), results of the implementation are obtained (e.g., using security performance indicators) giving input for the last phase (Act) where the evaluation of the results leads to further improvement strategies and measures. These improvement actions are put into a new plan, and the cycle starts again.

1.7 Safety and security science in a historical perspective

Compared with safety, physical security is a relatively new field of science. Several revolutions have taken place in the field of safety science, as depicted in Fig. 1.7.1.

The first revolution, conveniently called the "Safety First Movement," was initiated by the American railway company. During the period of this revolution (1900–60), research was almost solely carried out by private companies and insurance companies. The main goal was to protect workers and employees within the private industry since too many accidents happened that could have been prevented, and too many costs could have been avoided. This was the main reason for safety research and theorization.

The second revolution (roughly in the period 1960–2020), called the "Loss Prevention" revolution, was characterized by the involvement of research institutes

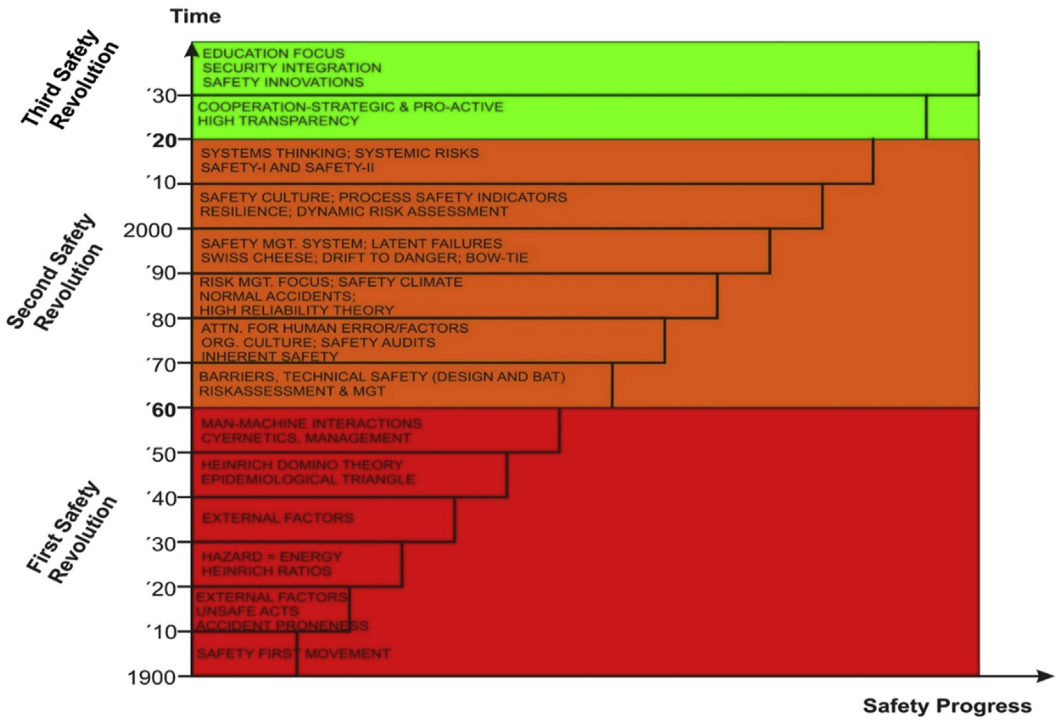


FIGURE 1.7.1 Safety science progress from 1900, in three Safety revolutions. *Source: Reniers, G., Khakzad, N., van Gelder, P. (Eds.), 2018. Security Risk Assessment in the Chemical and Process Industry. De Gruyter, Berlin.*

(universities and governmental research organizations) and authorities to do safety research for improving the safety of communities living nearby industrial sites, and for bettering citizen safety on top of employee safety. Some high hazard industries such as the nuclear industry and the chemical and process industries, and the accidents happening especially in the latter industrial sector, also led to the understanding and realization that research on safety was needed to deal with disaster prevention and loss prevention in such industries.

The third safety revolution (from 2010 onward), the-so called CHESS revolution (Reniers and Khakzad, 2017), results from the fact that due to the digitalization of society, the social media, and interconnectedness of people, a new societal reality can be observed since a decade: new societal expectations with more emphasis on ethical issues, transparency, and collaboration, as well as focus on security. Hence the "CHESS" revolution, an acronym for focus on Collaboration, High Transparency, Education, Security, and Safety innovations. In this revolution, the so-called "Triple Helix Plus" is engaged in Safety research: people from industry, research institutes, and authorities carry out studies and collaborate intensively to improve safety. The "plus" indicates that these three stakeholders are pushed to do more and better research by citizens, who actively mingle in the risk and safety debate.

It has taken a long time for security science to take its place in science, but finally in this third Safety revolution, and due to the growing interconnectedness of citizens and their growing interest in ethical values (and safety, security, environment, etc.), it has taken its place in academia. The maturity of security research is still at a low level, but is climbing steadily. Since both safety and security are about avoiding or decreasing losses, many analogies exist. Therefore, the security research field is able to learn from safety research and to use developed theories, models, and approaches of safety, when these are adapted to the security needs and situations (see also Chapter 5).

1.8 Conclusions

Engineering risk management is comprised of managing operational safety risks on the one hand and managing physical security risks on the other. Nothing more, nothing less. Although some basic management principles are obviously the same for both safety and security, some important differences for the calculation of safety risks and security risks exist, as is explained in this introductory chapter. Safety risk is usually calculated based on the parameters of scenario consequences and likelihood, while security risk needs to be determined by the assessment of vulnerability (including threats, the likelihood of attack, and eventually existing or available security barriers) and potential consequences (eventually including mitigation measures). The formula to calculate security risks thus differs from that for calculating safety risks. Hence, in this book: we explain how physical security should be seen, how risks related to physical security can be determined and calculated, and what ways there are to manage them.

References

American Petroleum Institute (API), 2013. ANSI/API Standard 780 — Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry. American Petroleum Institute, Washington DC.

CCPS — Center of Chemical Process Safety, 2000. Guideline for Chemical Process Quantitative Risk Analysis. American Institute of Chemical Engineers — Center of Chemical Process Safety, New York, NY.

ISO-International Standardization Organization, 2009. ISO/FDIS 31000:2009: Risk Management — Principles and Guidelines. International Standardization Organization, Geneva, Switzerland.

Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed. De Gruyter, Berlin.

Paté-Cornell, E., 2012. On "black swans" and "perfect storms": risk analysis and management when statistics are not enough. Risk Anal. 32, 1823—1833. https://doi.org/10.1111/j.1539-6924.2011.01787.x.

Reniers, G., Khakzad, N., 2017. Revolutionizing safety and security in the chemical and process industry: applying the CHESS concept. J. Integr. Secur. Sci. 1 (1), 2—15.

Reniers, G., Khakzad, N., van Gelder, P. (Eds.), 2018. Security Risk Assessment in the Chemical and Process Industry. De Gruyter, Berlin.

Reniers, G., Van Erp, N., 2016. Operational Safety Economics. Wiley, Chichester, UK.

2

History of terrorist attacks to critical infrastructures involving hazardous materials

2.1 Introduction

Chemical and process facilities are potentially attractive targets due to the storage of hazardous materials in relevant quantities and the presence of chemicals that may be used to manufacture explosive devices.

The French Ministère de l'Ecologie du Développement durable et de l'Energie has published a review of "Accident study findings on malicious acts perpetrated in industrial facilities" (Ministère de l'Ecologie du Développement durable et de l'Energie, 2015) based on a comprehensive sample of 850 accidents that have occurred in France in the period 1992−2014 at classified facilities potentially hazardous to the environment and caused by malicious acts of interference. The results of the analysis evidenced that fire was the prevailing event occurring as a consequence of the malicious acts (77% of occurrences), often combined with a release of hazardous materials (18% of occurrences). Among the relevant events that occurred in chemical facilities, two recent security-related incidents occurred in France in 2015, regarding an attack to a gas production facility located in Saint-Quentin-Fallavier (ARIA database record #46767) and a sabotage of two oil-derivatives storage tanks located near Marseille (Le Guernigou and Revilla, 2015). Furthermore, as reported by the OPCW (Organization for the Prohibition of Chemical Weapons, 2008), many chemicals of industrial application can be employed as precursors for making weapons of mass destruction or can be involved in potential deliberate toxic releases and environmental contaminations (Lou et al., 2003).

Aside from physical attacks, chemical facilities are vulnerable to cyber intrusions due to the increasing use of automated controls and safety instrumented systems. According to the 2016 Internet Security Threat Report, the largest number of cyberattacks was recorded in 2015, reaching a total of 430 million incidents throughout the world (Joyce et al., 2017). In this prospect, cybersecurity can no longer be disregarded in the chemical and process facilities (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).

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00002-0

This chapter discusses the outcomes of recent past accident data analysis studies focused on security-related events that affected chemical and process facilities, caused by either physical actions or cyberattacks. For this purpose, the dataset created by Casson Moreno et al. (2018) was adopted and eventually integrated and discussed, focusing mostly on causes and consequences of the events and on lessons learnt.

2.2 Data collection

2.2.1 Retrieval of data from databases

Past accident data information was derived from (Casson Moreno et al., 2018), in which a dataset was created based on scientific literature, the web, and industrial accident databases. Two criteria were used to include the events in the database: (i) the event should be originated by an intentional malicious act aimed at interfering with normal operations (including theft and cyber intrusion), and (ii) the event involved a hazardous facility.

To this end, the following industrial accidents databases were investigated:

- ARIA Database: managed by the French Ministry of Ecology, it collects more than 40,000 accidents that harmed or showed a potential damage for public health or safety and the environment.
- JRC eMARS: managed by the Major Accidents Hazards Bureau at the European Joint Research Center, it aims to facilitate the exchange of lessons learned from accidents and near misses involving dangerous substances in order to improve chemical accident prevention and mitigation efforts.
- U.S. DoT PHMSA: managed by the U. S. Department of Transportation (DoT), the Pipeline and Hazardous Materials Safety Administration (PHMSA) was built up to support the safe transportation of energy and hazardous materials.
- E.U. Concawe: established in 1963 and managed by the European Petroleum Refiners Association, this database aims to improve scientific understanding of the environmental health, safety, and economic performance of petroleum refining and distribution.
- Dechema ProcessNet: created and handled by the German association of chemical industrial activities (Dechema), this database 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: 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: the European Gas Pipeline Incident data Group (EGIG) is devoted to the collection of incidents involving gas transmission systems.

In order to expand the research, two other databases not specifically dedicated to chemical and process accidents were investigated as well:

- 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. 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), covering terroristic events worldwide 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.

When consulting the latter two databases, only events that affected industrial sectors related to chemical and process facilities were considered, namely:

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

2.2.2 Sorting the collected data

The data collected was sorted with regard to the type of events, geographical information (i.e., continent, country, and city), number of people injured, number of fatalities, substances involved in the event, causes that led to the undesired event, and the dynamics of such events (Casson Moreno and Cozzani, 2015; Casson Moreno et al., 2016, 2018; Marmo et al., 2017).

A total of 304 events were collected, considering both physical security and cyber-security events. The time span covered is 45 years (from 1970 to 2015). A total of 96% of the events were retrieved from the aforementioned open-source databases. The remaining 4% were found in other online editions of newspapers and scientific publications. Among open-source databases, GTD included the highest number of accidents (112 events), followed by ARIA (60 events), Concawe (46 events), RISI and PHMSA (34 events each), and eMARS (7 events). No event was found in ProcessNet, ZEMA, and EGIG. Table 2.2.1 reports the detailed description of the eight macro-sectors of industrial activities defined in order to classify the collected data.

2.3 Results and discussion

2.3.1 Overview

Fig. 2.3.1A 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 since the

Table 2.2.1 Macro-sectors of industrial activities used in the database.

Macro-sector	Description
Chemical and petrochemical (C&P)	Chemical activities, including pesticides production, pharmaceutical industry, production of basic chemicals; petrochemical activities, including refineries.
Power production	Power production plants, including hydroelectric power plants.
Bioprocesses	Treatment of organic waste and waste fermentation juices; food industry; biogas production.
Manufacturing	Metalworking, textile industry, activities related to automotive sector.
Water treatment	Treatment of water for industrial and domestic purposes (excluding bioprocesses-related waters and slurries).
Pipelines (oil and gas)	Oil and gas transportation via pipelines.
HazMat transportation	Transportation of hazardous materials via road, rail, water.
Not specified	Security-related events for which specific industrial sector was not defined by the source.

Adapted from Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.

year 2000. This tendency is also due to a significant growth in cyberattacks as is evident in Fig. 2.3.1B, which may be due to the considerable spread of external connectivity of the software and hardware used in the chemical and process facilities' process control and automation. Nevertheless, an increase in physical attacks was also recorded in the same period.

The distribution of the events with respect to the different threat categories is reported in Fig. 2.3.2. The available data shows that terrorism is the most important threat category, followed by vandalism and theft.

Most of the reported events took place in Europe (44%) and America (26%), Asia (20%), and Africa (10%). Only one event was registered in Oceania. With regard to cyberattacks, however, the number of cyberattacks is the highest in America (50%), followed by Europe (29%), Asia (15%), and Africa (6%). Differences appear also when considering the distribution of the type of threat in the different geographic areas, as shown in Fig. 2.3.3. In Europe, the main security issue is posed by theft, vandalism, and terrorism, whereas in Asia and Africa, it is terrorism and sabotage. As previously mentioned, in the United States, cyberattacks as well as vandalism are the main security threats.

Events included in the database were sorted accordingly to the industrial sector, applying the definitions provided in Table 2.2.1. Fig. 2.3.4 depicts the number of events in the different industrial micro-sectors. In case of fixed installations, chemical and petrochemical facilities have been more frequently affected by security threats. The attractiveness of such facilities could be related to several aspects, the most important of which are: (i) the presence of large amounts of hazardous materials, capable of leading 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 (OPCW, 2008); (iii) often chemical plants are owned by multinational companies that may be in specific contexts attractive sociopolitical targets (Ackerman et al., 2004). Furthermore, cyberattacks to such companies, which represent a 7% of the total, can be

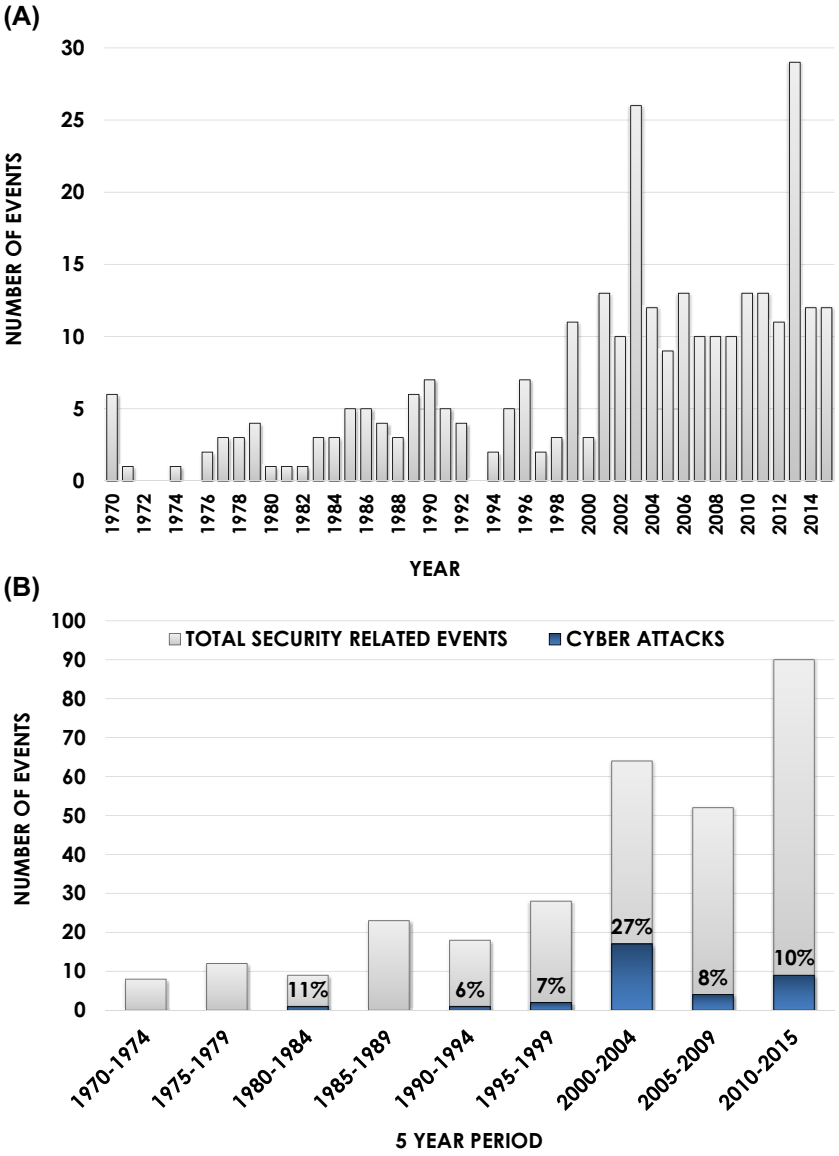


FIGURE 2.3.1 (A) Trend of security events. (B) The share of cyberattacks. *Adapted from Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.*

motivated by the possibility of obtaining proprietary information important for the business (e.g., patents of specific processes) (North America Oli and Gas Pipelines, 2013).

Among the transportation and distribution systems, oil and gas pipelines were the main target of malicious actions. The reason is that the protection of pipelines is very

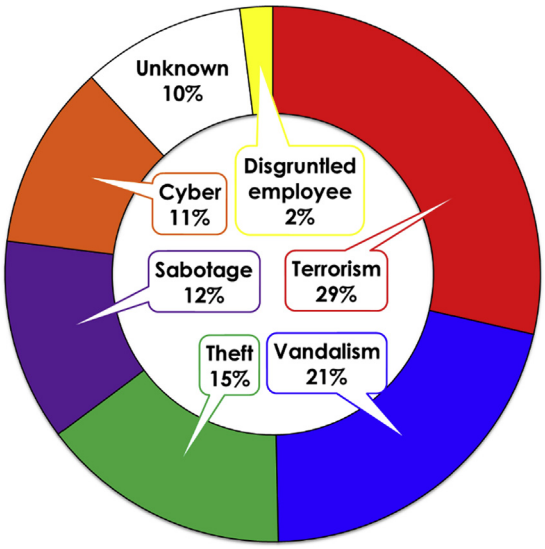


FIGURE 2.3.2 Threat categories identified as the causes of the 304 security-related events (Casson Moreno et al., 2018).

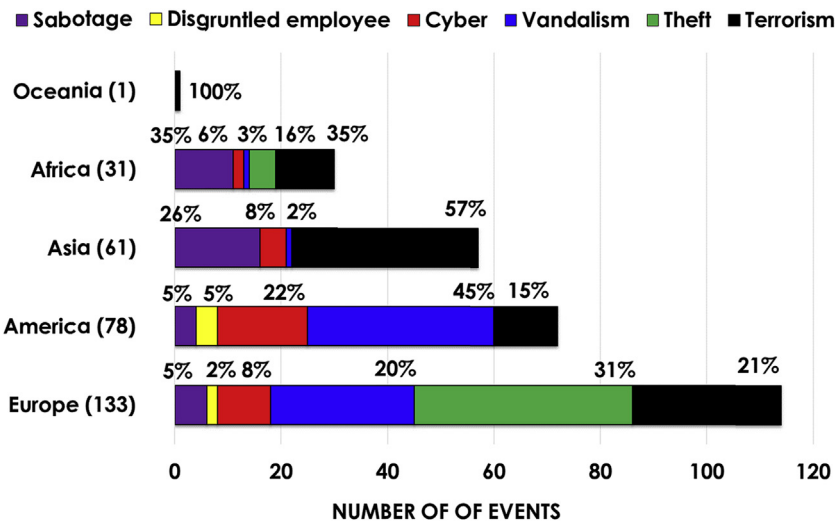


FIGURE 2.3.3 Distribution of the type of threat in the different geographic areas. *Adapted from Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.*

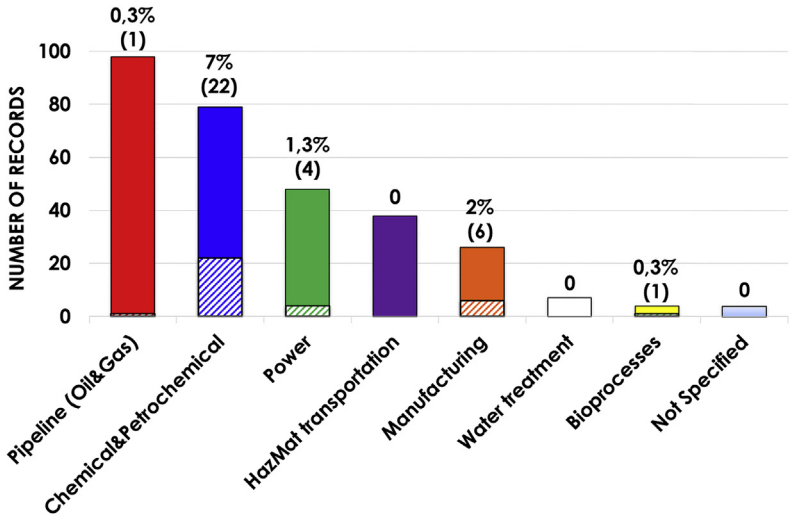


FIGURE 2.3.4 Number of events in the different industrial micro-sectors. The contribution of cyberattacks is shown with striped colors. *Adapted from Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.*

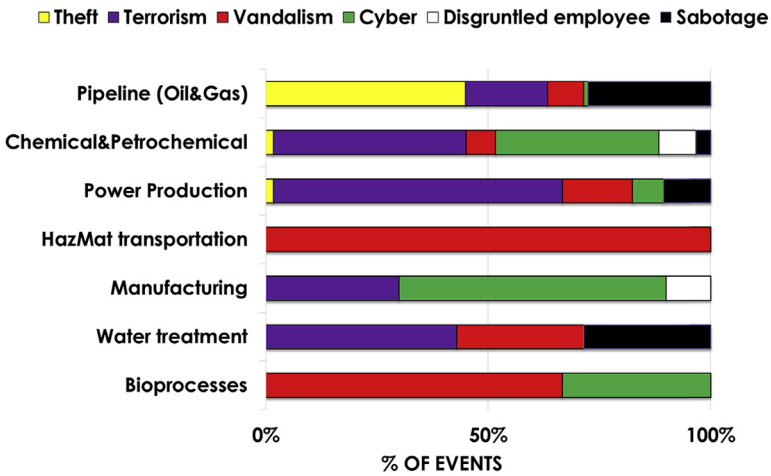


FIGURE 2.3.5 Share of threats with respect to industrial micro-sectors. *Adapted from Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.*

difficult and costly due to their extension over hundreds of kilometers (US Department for Homeland Security, 2008).

Fig. 2.3.5 shows the type of attack scenarios for each micro-sector, pointing out to theft and terrorist attacks as the most frequent type of scenarios for pipelines and chemical facilities, respectively.

2.3.2 Impact of the events

Having a closer look at each industrial micro-sector (Table 2.2.1), the highest number of events causing at least a casualty is reported for the power production industry (12 events). This is also the sector in which cyberattacks caused a significant percentage of human losses. A total of 7 security-related accidents with fatalities took place in the (petro)chemical sector, a total of 6 events are related to oil and gas pipelines, and 1 event is related to activities involving transportation of hazardous materials (Fig. 2.3.6).

Events involving oil and gas pipelines are indeed responsible for 85% of the fatalities. In general, attacks toward distributed systems resulted in a higher severity. In particular, events involving oil and gas pipelines were often originated by thefts of fuel, giving rise to major fire or explosion involving multiple fatalities (e.g., in Nigeria in 2006, where more than 500 people were killed in an attempt to illegally tap oil from a high-pressure oil pipeline).

Compared to oil and gas pipelines, chemical and petrochemical installations are spatially limited and thus generally better protected from external physical threats. Furthermore, in such facilities a more intense surveillance is possible, leading to a more timely activation of safety systems that may contribute to the mitigation of the consequences.

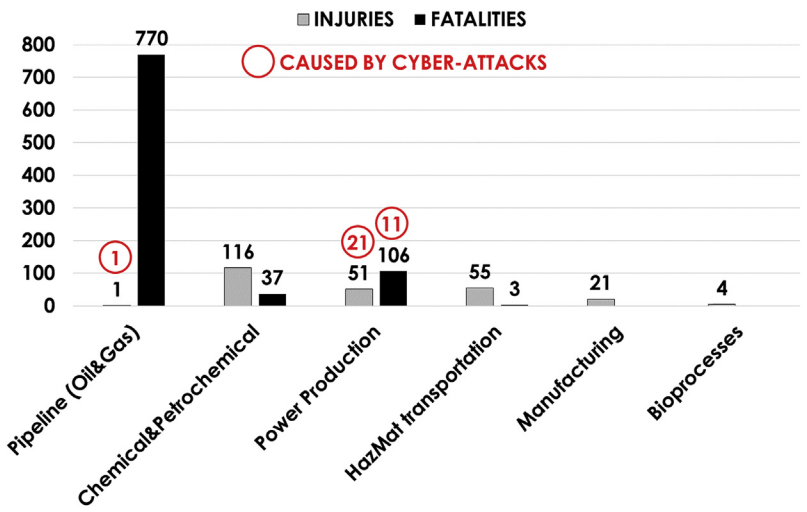


FIGURE 2.3.6 Number of security-related events involving at least one fatality or injury. The circled numbers refer to the fatalities/injuries related to cyberattacks (Casson Moreno et al., 2018).

2.3.3 Final events and attack modes

A total of 110 events (36%) had the release of hazardous chemicals in air, water, or soil as the final event. In 104 events (34%), the final scenario was an explosion, and in 29 (10%), a fire. In 19 events (6%), there was a loss of system control due to cyberattack. No significant consequence was registered in 13 cases (4%). Fig. 2.3.7 displays the share of each micro-sector from the different attack scenarios. While terrorism mainly causes

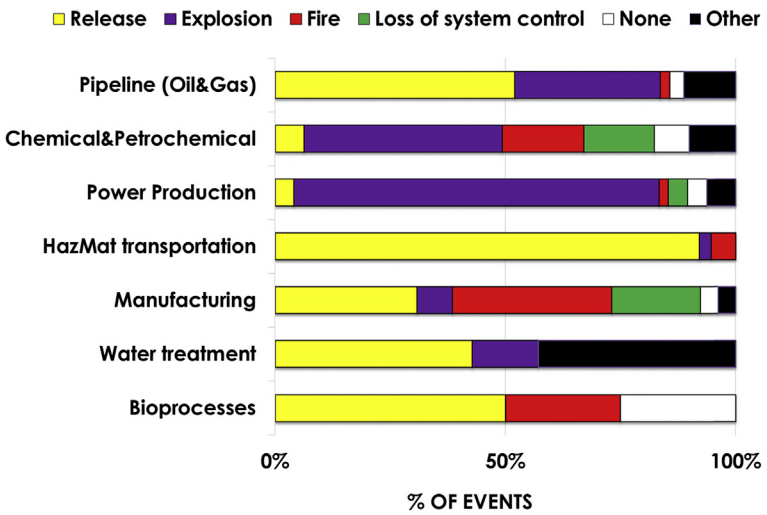


FIGURE 2.3.7 Share of each micro-sector from the attack scenarios. *Adapted from Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.*

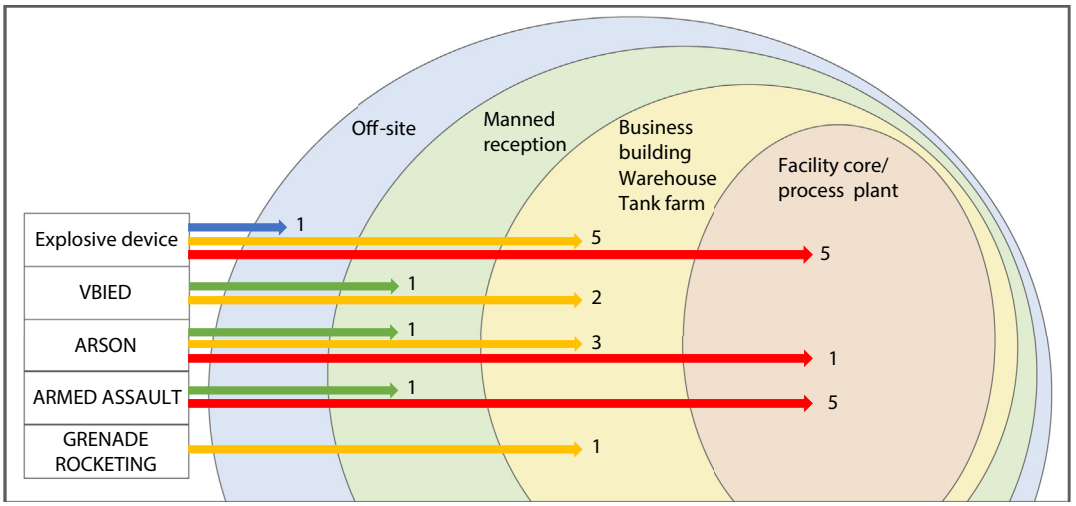


FIGURE 2.3.8 Paths and related penetration depth for different attack modes. Per each attack mode, the number of successful records is reported. *VBIED*, Vehicle-borne improvised explosive device. *Adapted from Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.*

explosions as final scenarios, thefts and vandalisms are more likely to result in the release of hazardous chemicals. Cyberattacks mainly result in the loss of control of the system or in no relevant consequences.

Fig. 2.3.8 represents a schematic overview of the layout of a process plant, including the facility core/the process plant, storage section, business buildings and warehouse and tank areas, and manned reception. The manned reception consists of the access

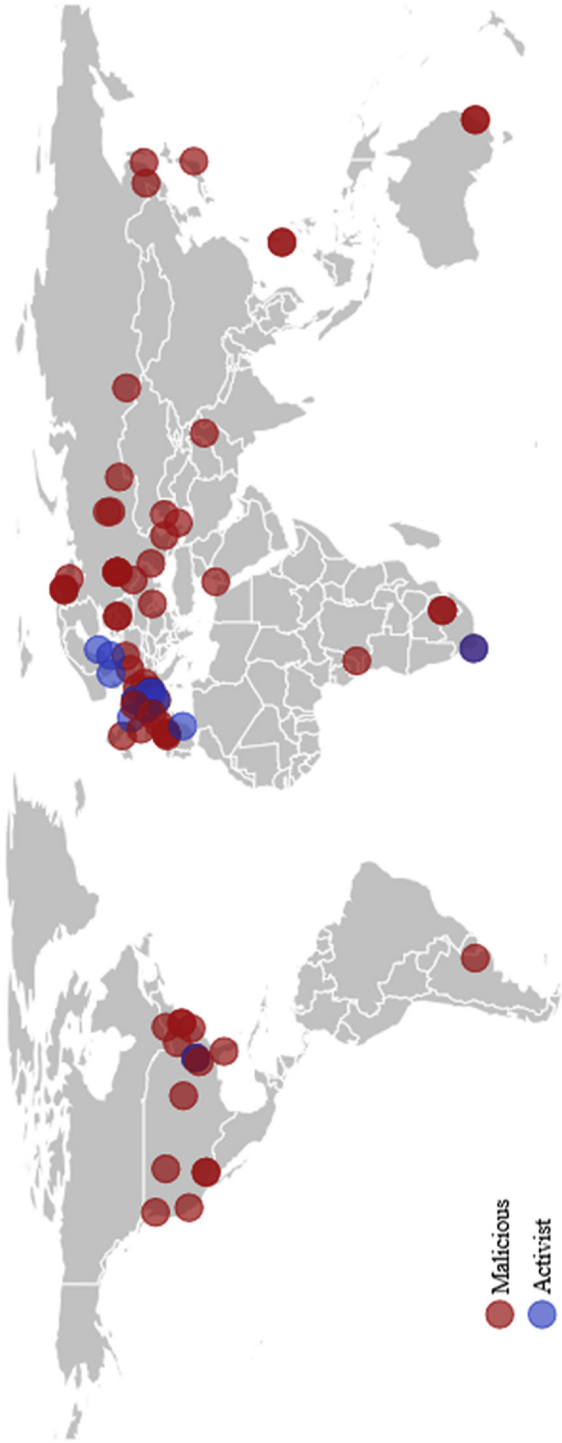


FIGURE 2.4.1 Spatial distribution of terrorist attacks to nuclear plants (1963–2014) (NuFAD).

controls for vehicles and pedestrians. A parking area is usually located outside the premises. Employees and visitors are usually allowed in the parking area with no security control. Fig. 2.3.8 also reports the attack modes and the penetration depth experienced in the facility along with the number of successful attempts attached to each penetration arrow, based on 12 events of the dataset.

2.4 Further remarks

Compared to historical data and available databases for safety-related accidents, the available data for security-related accidents, especially with regard to terrorist attacks, are very scarce. The issue of data scarcity arising from the rarity of terrorist attacks to chemical facilities has further limited the application of conventional frequentist approaches to likelihood estimation. A simplified methodology is proposed by Landucci et al. (2017), but the assumptions made are based on semiquantitative estimations.

In recent years, a number of techniques have been developed to make use of precursor data (indirectly relevant data) in reasoning and risk assessment of rare events where the amount of directly relevant data is not worthwhile (e.g., see Khakzad et al., 2015); application of precursor-based methodologies to, for instance, nuclear plants' security data (Fig. 2.4.1) may be employed to infer chemical plants' security risks.

Besides the application of precursor data to estimate attack likelihood, data mining techniques can effectively be applied to analyze seemingly irrelevant security databases such as terrorist attacks on the public (e.g., in restaurants and movie theaters) (Fig. 2.4.2) (Global Terrorism Database, 2019) so as to figure the trends in the activity, priorities, capabilities, and action plans of terrorist groups; such data bases due to data abundance can be used as a valuable source of information for (approximate) reasoning of attack

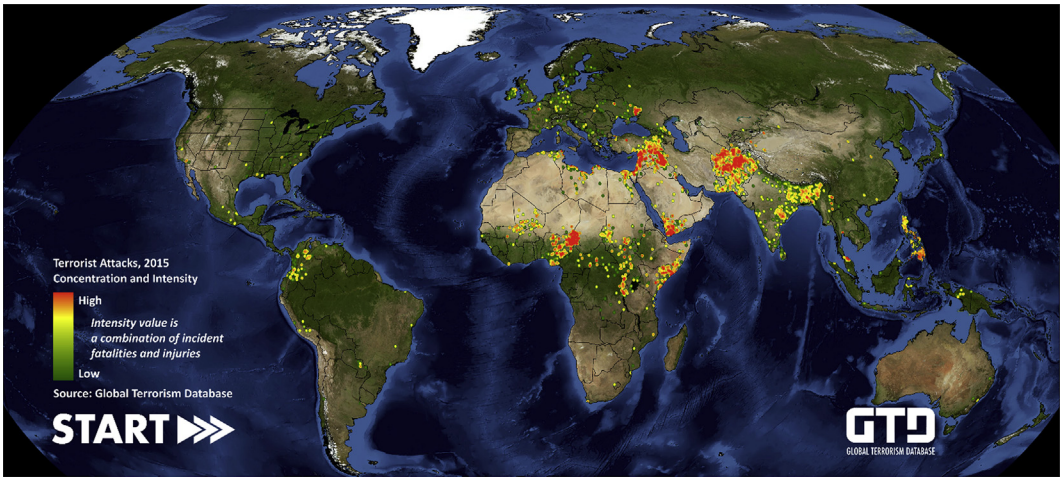


FIGURE 2.4.2 Geographical distribution of public terrorist attacks in 2015 (Global Terrorism Database).

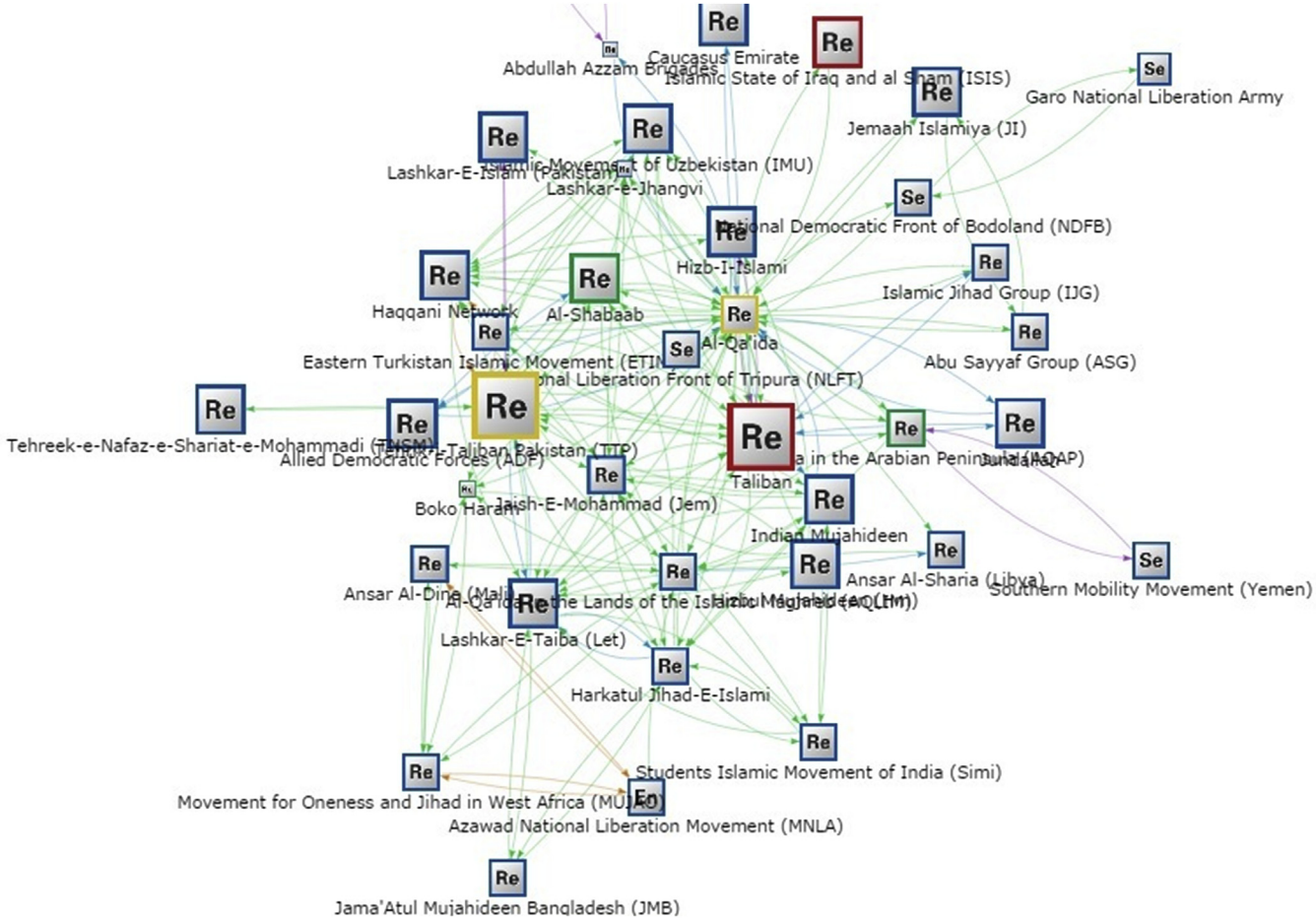


FIGURE 2.4.3 Correlation among terrorist organizations worldwide (Global Terrorism Database, 2019). Re: Religious terrorist groups; Se: Separatist terrorist groups; En: Ethnic terrorist groups.

likelihood (Khakzad et al., 2018). For instance, the attack to a chemical plant in France in June 2015 (see Section 2.1) happened on the same day as foreign tourists were murdered at a beach resort in Tunisia, and a suicide bomber attacked a mosque in Kuwait. It is yet unclear whether these events were correlated, although Islamic extremist groups were linked to all three (Trager, 2015).

In addition to the terrorist databases, the study and analysis of the correlation among the terrorist groups and organizations worldwide may provide useful information about possible activity of specific terrorist groups near a chemical facility of interest and the likelihood of an imminent attack. According to Fig. 2.4.3 (Global Terrorism Database, 2019), for instance, the two terrorist organizations Al-Qaida and Pakistani Taliban, both denoted as yellow squares, are being considered as allied; as a result, the changes in the policies or intent of one can be taken as an implication of the other's. Likewise, The Islamic State of Iraq and Sham (ISIS) and The Afghan Taliban, both denoted as red squares, have been recognized as conflicting groups, in that, the presence of one in a region implies the absence or low activity of the other in the same region (Khakzad et al., 2018).

2.5 Conclusions

According to past accident data analysis, among 304 security-related hazardous industrial accidents, Europe has the highest number of events reported, while most of cyberattacks scenarios took place in the United States. Pipelines, due to their higher vulnerability (extension over hundreds of kilometers, no specific security barrier, etc.), were the most frequently attacked industrial target, with theft as the dominant threat. In the case of fixed installations, however, terrorist attacks are the prevailing threat mode. 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 notable and may result in deep penetration of the targets.

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.

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.

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.

Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.

Department of Homeland Security, 2017. Repository of Industrial Security Incidents. http://www.risidata.com/.

Global Terrorism Database, 2019. http://www.start.umd.edu/gtd.

Joyce, A.L., Evans, N., Tanzman, E.A., Israeli, D., 2017. International cyber incident repository system: information sharing on a global scale. In: 2016 IEEE Int. Conf. Cyber Conflict, CyCon U.S. https://doi.org/10.1109/CYCONUS.2016.7836618, 2016 2017.

Khakzad, N., Khan, F., Amyotte, P., 2015. Major accidents (Grey Swans) likelihood modeling using accident precursors and approximate reasoning. Risk Anal. 35 (7), 1336−1347.

Khakzad, N., Martinez, I.M., Kwon, H.M., Stewart, C., Perera, R., Reniers, G., 2018. Security risk assessment and management in chemical plants: challenges and new trends. Process Saf. Prog. 37 (2), 211−220.

Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Prot. 110, 102−114.

Le Guernigou, Y., Revilla, F., 2015. C [WWW Document]. URL. https://af.reuters.com/article/worldNews/idAFKCN0PO0S420150714.

Lou, H.H., Muthusamy, R., Huang, Y., 2003. Process security assessment : operational space. Process Saf. Environ. Prot. 81, 418−429.

Marmo, L., Danzi, E., Tognotti, L., Cozzani, V., Ernesto, S., Casson Moreno, V., Riccio, D., 2017. Fire and explosion risk in biodiesel production plants: a case study. In: Hazards, vol. 27, pp. 1−10.

Ministère de l'Ecologie du Développement durable et de l'Energie, 2015. Accident Study Findings on Malicious Acts Perpetrated in Industrial Facilities [WWW Document]. URL. https://www.aria.developpement-durable.gouv.fr/synthese/analyses-and-feedback/accident-study-findings-on-malicious-acts-perpetrated-in-industrial-facilities/?lang=en.

National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2017. Global Terrorism Database. URL. https://www.start.umd.edu/gtd/.

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.

Reniers, G., Cozzani, V., 2013. Domino Effects in the Process Industries. Elsevier.

Thomas, H.W., Day, J., 2015. Integrating cybersecurity risk assessments into the process safety management work process. In: 49th Annu. Loss Prev. Symp. 2015, LPS 2015 − Top. Conf. 2015 AIChE Spring Meet. 11th Glob. Congr. Process Saf, pp. 360−378.

Trager, R., July 2015. Failed terror attack raises alarms about chemical plant security. Chem. World. From: https://www.chemistryworld.com/news/failed-terror-attack-raises-alarms-about-chemical-plant-security/8708.article.

US Department for Homeland Security, 2008. Pipeline Threat Assessment.

3

Principles and concepts for security risk assessment

As was made clear in the previous chapter, chemical facilities, where relevant quantities of hazardous chemicals are stored or processed, may be possible targets of malicious acts of interference and terroristic attacks (Casson Moreno et al., 2018; van Staalduinen et al., 2017). Damages induced by external attacks to process and/or auxiliary equipment may indeed cause severe consequences due to the occurrence of severe explosions, fire, toxic dispersion, or environmental contamination scenarios following the release of hazardous materials (Lou et al., 2003).

In the last 15 years, the development of security risk assessment methodologies was promoted to guide and support industrial operators in assessing and managing security risks (Matteini et al., 2018). Among others, it is worth recalling the security risk assessment methodologies proposed by (American Petroleum Institute (API), 2013), American Institute of Chemical Engineering (American Institute of Chemical Engineers - Center for Chemical Process Safety (AIChE-CCPS), 2003), Sandia National Laboratories (Jaeger, 2003), and (U.S. Department of Justice, 2002). These methodologies allow for a qualitative or a semiquantitative (e.g., in the case of API methodology) assessment of security risk, while only general guidance for security risk mitigation and lists of possible solutions in terms of security countermeasures depending on the existing security alert level are provided in the literature (Norman, 2010).

The aforementioned studies allowed deriving the principles and concepts of physical security when dealing with the analysis of chemical and process facilities. In particular, the well-known security risk formulation by API Recommended Practice 780 (American Petroleum Institute (API), 2013) is considered in the following to introduce the key concepts (see also Chapter 1):

$$R = (A \times T) \times V \times C \tag{3.0.1}$$

where R is the security risk, T is the threat, A is the attractiveness of the asset to the threat, V is the vulnerability, expressing the likelihood of success of the physical act of interference, and C is the consequence or impact value.

This chapter deals with the definition and analysis of the physical security concepts and their implementation in security studies dedicated to the chemical and process industry. The chapter is structured as follows:

- Section 3.1 deals with the concept and application of the threat and threat assessment;

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00003-2

- Section 3.2 deals with the attractiveness conceptualization and assessment, both mentioning standard approaches and methods tailored to the chemical and process industry;
- Section 3.3 deals with the concept of vulnerability and shows an example of a particular component of vulnerability assessment, namely the path analysis;
- Section 3.4 deals with consequence assessment, introducing a focus on improvised explosive devices and their impact.

3.1 Threat assessment

3.1.1 The concept of threat in security studies

The aim of threat assessment is to identify and characterize threats against assets and evaluate the assets in terms of attractiveness (see extensive description in Section 3.2) of the targets to each adversary and the consequences if they are damaged or stolen.

Relevant studies in the literature addressed the aspect of threat assessment, with particular emphasis on the analysis of psychological aspects, modus operandi, choice of weapon mode, and targeting, in the perspective of obtaining the harmful outcomes for people of property.

Woo (2009) provided indications to support terrorist threat assessment and management, stating that "adaptive learning" is often the key for addressing the evaluation of attack mode and preferences, since attackers often adopt past terrorist networks' experience to determine if a strategy was proven to be successful or gaining the perception that a strategy has the potential to be successful. A comprehensive review of psychological aspects associated with motivations, intentions, and determination of features of threat agents categories is shown by Victoroff (2005), together with a classification of the different variables based on the work of Schultz (Schultz, 1980), needed to characterize the "dimensions of terrorism": perpetrators number, terrorists sponsorship, relation to authority, scale (national or international), military status, spiritual motivation, financial motivation, political ideology, hierarchical role, willingness to die, and target methodology.

In (Victoroff, 2005), a conceptual distinction is made among approaches that involve the analysis of the characteristics of the individuals and groups that turn into terrorist activities ("bottom-up" approaches) or that seek the seeds of terrorism in political, social, economic, even evolutionary circumstances ("top-down" approaches).

A dual perspective in the assessment of the terrorism psychology is also shown in (Kruglanski and Fishman, 2006), in which terrorism is approached as a "syndrome" or as a "tool," being in the former case a psychologically meaningful construct with identifiable features on individuals or groups; in the latter, terrorism represents a strategic instrument involved in a conflict among parties.

More recently, (Schuurman and Eijkman, 2017) proposed a framework to conceptualize the preattack process through the use of possible indicators of terrorist intent or capability, thus supporting the estimation of the credibility of a terrorist plot materialization, despite the authors stating that the progression to the final attack is "multipronged and chaotic" rather than a "linear" progression among subsequent preparatory stages.

3.1.2 Simplified threat assessment for chemical and process facilities

As mentioned in Section 3.1.1, a full characterization of threat actors and related psychological aspects is a complex interdisciplinary task, which may be out of the scope of a practical assessment book supporting security analyses for chemical and process facilities. In order to carry out a simplified but effective threat assessment, (Landucci et al., 2017) proposed a schematization of threat agent categories (TAC), which are based on the classification suggested in (SFK, 2002) and were applied in advanced security studies (see Chapter 4 for more details).

Table 3.1.1 summarizes the considered TAC for threat assessment specific for chemical and process facilities. These categories, which also include the analysis of potential acts of interference and means, allow supporting attractiveness, vulnerability, and consequence assessment, as described in the remaining part of the chapter.

Table 3.1.1 Schematization of threat agent categories (TAC).

	Threat agent categories (TAC)		
Features	***TAC1*: Threat agent moved by contingent intent**	***TAC2*: Threat agent moved by direct intent**	***TAC3*: Terrorists and extremists**
Agents	Individuals or small groups	Small network of activists, members of organized crime, individuals, radical political groups	Extremist and terrorist individuals and groups
Aim	Limited damage; possible unawareness of attack escalation into major accident	Major damage; escalation into a major accident may be a possible objective	Massive terrorist attack, armed action, causing the maximum possible damage, without regard to people's life (own or others)
Motivation	Revenge, frustration, prove existence of deficits, achieve social effects	Revenge, political radicalism, gaining financial/competitive advantages	Religion-related motives, anarchy, "punishing companies"
Potentiality	Limited potentiality, dependent on the motive	Above-average criminal energy, average communication capability, medium level of organizational support, poor financial backing	Extremely great criminal energy, highly developed communication capability, high level of organizational support, high financial backing
Tools and means	Simple or major tools, possibly simple incendiary devices	Simple and specialized tools, incendiary devices, home-made explosives	Simple and heavy tools, weapons, explosives, incendiary devices

Based on Störfall Kommission (SFK), 2002. SFK-GS-38 Report and adapted from Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Prot. 110, 102–114.

3.2 Attractiveness assessment

3.2.1 The concept of attractiveness in security studies

The attractiveness evaluation in security studies is aimed at supporting the preliminary identification of the most vulnerable and critical targets object of a potential attack. Attractiveness may be analyzed in cyber and/or physical environments.

In cyber or cyber–physical security studies, attractiveness is aimed at supporting the development and improvement of countermeasures, for example, proving metrics to evaluate the most vulnerable targets based on the consequence of foreseen attack scenarios (Orojloo and Azgomi, 2017). Hence, sensor measurements and controller signals, which may have a direct or indirect impact on a given physical–cyber system, are analyzed to rank the key assets of the system based on their sensitivity to a given attack.

In the framework of cyber frauds, the attractiveness may result less critical to identify and protect possible critical targets. One of the key characteristics of cyber fraud is that it can be globalized, so national differences in targets or in the organization of control tend to be less relevant except in some specific cases (Levi et al., 2017). Moreover, technologies become cheaper and more widely available, and the increase in global internet penetration (such as social media) makes the pool of both potential victims and criminal actors grow.

This chapter mainly deals with cyber–physical and physical systems. In this framework, the principles of "situational crime prevention" (Clarke and Newman, 2006) are widely applied to the evaluation of risks to potential targets of external acts of interference (in particular, terrorist attacks). The principles are based on the application of eight criteria that assess the attractiveness. The conceptual framework is known by the acronym "EVIL DONE," since attractiveness of a target is related to the following attributes of a target (Clarke and Newman, 2006):

- **E**xposure: it is related to the easiness of access of the target (e.g., public access without permission, special requirements to enter, etc.) and how often the target is frequented;
- **V**italness: it is related to the role targets play in a community or to the broader society; in particular, electricity grids, water supplies, computer networks are critical to the daily functioning of most communities and feature this attribute (Clarke and Newman, 2006);
- **I**conicity: iconic targets have been conceptualized in terms of symbolism, and this attribute strongly depends on the kind of terrorist group considered in the threat assessment; for example, the Statue of Liberty in New York City or The Pentagon building in Virginia may have a strong iconic value for Al Qaeda terrorist (Boba, 2009), while for ecoterrorists, iconicity captures the extent to which targets are recognizable as harmful to animals and environmental interests (Gruenewald et al., 2015);

- **L**egitimacy: it is the extent to which terrorist sympathizers view targets as legitimate; in other words, legitimate targets are those that are most directly responsible for the ideologically based grievances maintained by terrorists;
- **D**estructibility: based on the fact that terrorists aim at producing the maximum level of damage to a target, this attribute is related to the easiness to achieve the maximum damage in terms of weaponry requirements; in turn, this attribute simultaneously accounts for the structural makeup of targets and the extent to which materials contained within targets serve to possibly escalate accidents (e.g., fuels or chemicals contained in the target installation that may induce secondary events (Landucci et al., 2015));
- **O**ccupied status: as per the case of iconicity, this attribute depends on the terrorist group features and modus operandi. In fact, if the aim of the attack is to result in multiple fatalities (such as is often the case of Islamic terrorists), targets featuring the presence of high population density may be more attractive;
- **N**earness: this attribute may increase attractiveness since the proximity of the target reduces the likelihood of being interdicted by police or other public guardians.
- **E**asiness: this attribute is associated with the ease at which targets can be penetrated without detection, hence is a function of directed systems of human surveillance, screening procedures, and physical barriers. This attribute is expanded when dealing with the vulnerability assessment (see Section 3.3).

The "EVIL DONE" framework was applied to ecoterrorism (Gruenewald et al., 2015), bioterrorism (Clark, 2009), hostage taking and kidnapping (Yun, 2009), Islamic terrorism (Freilich and Chermak, 2009), and other target types (Weenink, 2012). However, for the purpose of supporting security risk assessment procedures, specific attractiveness assessment approaches were specifically developed for chemical and process facilities. In this chapter, the fundamental approaches available in the technical and scientific literature are presented. Moreover, alternative approaches based on recent literature outcomes are introduced.

3.2.2 Attractiveness assessment for chemical and process facilities

In the past, chemical and process facilities were believed to be extremely unlikely targets of terroristic acts when compared to public malls, railway stations, and other crowded locations. After the New York City attacks of "9/11," the security of sites where relevant quantities of hazardous chemicals are stored or processed became a concern (Baybutt and Ready, 2003). In fact, the hazards posed by security threats to this type of facilities, in terms of disruption of operations, destruction of property, injury, or loss of life are somehow comparable to those coming from major accidents due to internal causes (Landucci et al., 2015). To give an example, major accidents may be triggered by external attacks carried out using military explosives or improvised explosive devices. Therefore, security risks started to be included in formal risk assessments (Bajpai and Gupta, 2005).

The attacks perpetrated in France in 2015 against the production site of a chemical company (Ministère de l'Ecologie du Développement durable et de l'Energie, 2016) confirmed the credibility of terroristic threat to industrial facilities located in Western countries. Hence, chemical and process facilities became a possible attractive target for security decision-makers and researchers.

For this reason, methods were developed for the attractiveness assessment in security studies dedicated to chemical and process facilities. In this framework, "attractiveness" is considered as "an estimate of the value of a target to a threat" according to (American Petroleum Institute (API), 2013) and the following factors are suggested to define the threat and to determine the need for any enhanced countermeasures:

- Potential for mass casualties/fatalities
- Extensive property damage
- Proximity to national assets or landmarks
- Possible disruption or damage to critical infrastructure
- Disruption of the national, regional, or local economy
- Ease of access to target
- Media attention or possible interest of the media
- Company reputation and brand exposure

The factors that affect the attractiveness are related to either the consequences/impact or social-economic factors. Attractiveness may be considered as a proxy for attack credibility to a given installation and may be adopted to prioritize resource allocation.

It is worth mentioning that chemical and process facilities feature relevant inventories of hazardous materials, which may be adopted to produce an escalation of events, thus may result attractive also in the light of the "destructibility" attribute, described in Section 3.2.1.

3.2.3 Standard approaches for attractiveness evaluation

In the following, the approach proposed by ANSI/API Standard 780 (American Petroleum Institute (API), 2013) is summarized in order to provide an example of standard approach for attractiveness assessment for process and chemical facilities. According to ANSI/API Standard 780, attractiveness can be evaluated as a composite estimate based on such factors as:

- The perceived value of a target to the threat[1]
- The threat's choice of targets to avoid discovery and to maximize the probability of success

[1]The "Threat" is hereby considered as the individual or group that may potentially carry out an external act of interference or terrorist attack for the facility under consideration.

In the ANSI/API Standard 780, the attractiveness evaluation is based on the assignment of qualitative factors ranging from 1 through 5 ("1" being very low/very unattractive and "5" being very high/very attractive). The assignment is based on brainstorming among different experts involved in the team carrying out the security risk evaluation of the facility under analysis. This suggested scheme gives the team a framework for risk decision-making either on a relative or on an absolute scale. Then attractiveness can be used as a factor to lower the expectation that the threat would attack the particular asset if the attractiveness is considered or to provide an estimate of the real or perceived value of a target to a threat.

As also pointed out in Section 3.2.1, a key factor affecting the attractiveness, also for chemical and process facilities, is related to the features of the threat and its motivation, intent, and capabilities. For example, the threat posed by an international terrorist group and the assets in which it might be interested may be quite different from the assets of interest to an individual activist or criminal with limited weaponry availability.

The attractiveness and the foreseen attack consequences and impact support the definition of the more critical facilities to be then analyzed in details, either for what concerns the definition of site-specific scenarios or for the design of security countermeasures.

A schematic of the approach proposed by ANSI/API Standard 780 is shown in Fig. 3.2.1.

3.2.4 Alternative approaches for the evaluation of attractiveness

An alternative approach for the assessment of attractiveness dedicated to chemical and process facilities was developed by Landucci and coworkers (Argenti et al., 2015; Argenti and Landucci, 2016). The method was developed in order to have input data easy to gather, which could be derived from documents available to plant operators, in order to facilitate method application and to obtain a quick but exhaustive screening tool.

The proposed methodology requires the calculation, for the industrial facility of interest, of an overall attractiveness index (I_A), defined as the product of a hazard-based index (I_H) and of a location-specific "induction index" (φ), as follows:

$$I_A = I_H \times \varphi \tag{3.2.1}$$

The evaluation of the indexes adopted in Eq. (3.2.1) is shown in the following; a tutorial application of the procedure is shown in Chapter 4.

3.2.4.1 Hazard-based attractiveness index

The I_H index describes in a sound way the value of the installation in terms of major accidents and severe damages potential. The quantitative evaluation of I_H is performed accounting for both the process facility inherent hazard, based on the analysis of the hazardous material inventories, and the vulnerability of the area surrounding the facility under analysis that might be impacted by an accident triggered by an external attack. More details are reported elsewhere (Argenti et al., 2015).

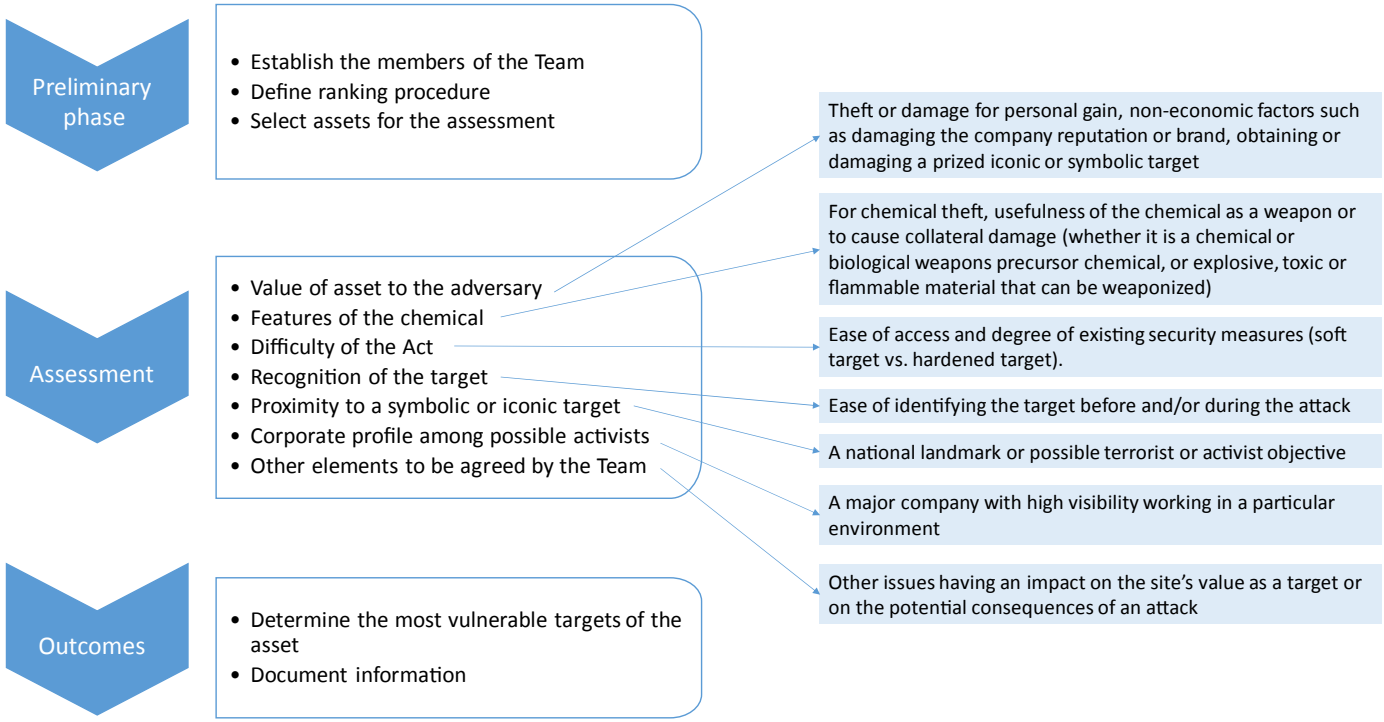


FIGURE 3.2.1 Schematic approach for the assessment of attractiveness of process facilities according to ANSI/API Standard 780 (American Petroleum Institute (API), 2013).

The quantitative evaluation of I_H is performed according to the scheme presented in Table 3.2.1. I_H provides an assessment of both the site inherent hazard, through the index I_{SH}, and the vulnerability of territory surrounding the site, through the index I_{TV}. Table 3.2.2 provides the values that should be assigned to other auxiliary indexes (I_{sub}, I_p and I_{vc}) on the basis of the input parameters.

The site inherent hazard index (I_{SH}) is based on the analysis of the hazardous material inventories of the facility under examination. Such inventories allow a preliminary estimation of the damage potential connected with the facility. Quite obviously, "dangerous" quantities vary from substance to substance: a normalized substance (or substance category) hazard index is hence employed to characterize the inherent damage level of a facility due to the stored and processed quantities of hazardous materials, either flammable or toxic.

The Territorial Vulnerability Index (I_{TV}) is related to the vulnerability of the area surrounding the facility under analysis that might be impacted by an accident triggered by an external attack. For a preliminary assessment, the impact area can be approximated on the basis of the plant substance inventory, as summarized in Table 3.2.1 (see Eq. D). The vulnerability of the area around the plant increases if a higher number of persons is present in the surroundings. The number of persons in a given area is related not only to the population density but also to the possible presence of vulnerability centers (such as hospitals, malls, schools, etc).

Table 3.2.1 Steps to the evaluation of index I_H.

Index	Definition	Description and evaluation	Eq.
I_H	"Hazard-based" attractiveness index	$I_H = I_{SH} + I_{TV}$	(A)
I_{TV}	Territorial vulnerability index	$I_{TV} = I_p + I_{vc}$	(B)
I_{SH}	Site hazard index	To be derived from Table 3.2.2, function of index I_{sub}	(C)
I_p	Population index	To be derived from Table 3.2.2; impact area radius is 1 km in case only flammable substances are present on the site, while 7 km in case also toxic and volatile substances are present	(D)
I_{vc}	Vulnerability Center index	To be derived from Table 3.2.2, relevant only for population density < 2000 inhabitants/km^2	(E)
I_{sub}	Hazardous substance overall index	$I_{sub} = I_{fl} + I_{tox}$	(F)
I_{fl}	Flammable substance overall index	$I_{fl} = \sum_i J_i^{fl}$	(G)
I_{tox}	Toxic substance overall index	$I_{tox} = \sum_i J_i^{tox}$	(H)
J_i	Hazardous substance index	$J_i = W_i/T_i$; wi = total inventory of i-th hazardous material or substance category[a], T_i = threshold value[b]	(I)

[a]Categories of substances are defined by Annex 1 of the "Seveso" Directive (European Commission, 2012).

[b]Thresholds may be provided for categories of substances or for named substances in the Annex 1 of the "Seveso" Directive (European Commission, 2012).

Adapted from 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.

Table 3.2.2 Evaluation of the auxiliary indexes I_{sub}, I_p, and I_{vc}.

Overall index	Value	Parameter	Range
I_{SH}	1	I_{sub}	<10
Site hazard index	2	Overall hazardous substances index	11–50
	3		51–150
	4		151–300
	5		301–650
	6		>651
I_p	1	Population in the potential impact area (inhabitants)	<1,000
Population index	2		1,000–10,000
	3		10,000–500,000
	4		>500,000
I_{vc}	1	Number of vulnerability centers	<2
Vulnerability centers index	2		2–10
	3		11–50
	4		>50

3.2.4.2 Induction index and overall attractiveness increase index

The induction index φ is obtained summing 1 to the F index that represents the contribution of geopolitical, social, and strategic factors in increasing the attractiveness of an industrial facility:

$$\phi = 1 + F \tag{3.2.2}$$

The F index is named "overall attractiveness increase index." Table 3.2.3 reports the different criteria considered for the evaluation of F. The selection of the most relevant criteria was made through a screening of relevant literature (see references in Table 3.2.3). The scores (σ_i, being $i = 1,2, \ldots m$, where m is the number of aspects) to be attributed for the assumed states are given in Table 3.2.4. It is worth to remark that the problem complexity may not exclude a cross-influence among aspects considered in the present study, which was, however, neglected for the sake of method simplicity.

Table 3.2.3 Definition of nontechnical aspects that increase attractiveness.

ID	Definition	Reference
S_1	Company ownership	Bajpai and Gupta (2005)
S_2	Presence of third-party highly attractive targets	Ackermann et al. (2007)
S_3	Presence of chemicals that can be used as WMD	Bajpai and Gupta (2005)
S_4	Past threat history	Bajpai and Gupta (2005)
S_5	Terrorists/activists activity in the area	Bajpai and Gupta (2005)
S_6	Political instability	Kis-Katos et al. (2011)
S_7	Ease in weapons gathering	Kis-Katos et al. (2011)
S_8	Local aversion due to company image and reputation	Pape (2003)
S_9	Aversion due to local stakeholders engagement and awareness of technology	Pape (2003)
S_{10}	Aversion due to economic/environmental reason and/or interactions with cultural/religious heritage	Pape (2003)

Adapted from Argenti, F., Landucci, G., 2016. Advanced attractiveness assessment of process facilities with respect to malevolent external attacks. Chem. Eng. Trans. 53, 133–138.

Table 3.2.4 Scoring of nontechnical aspects that increase attractiveness (see Table 3.2.3 for ID definition).

Aspect ID	State	Description	Score (σ_i)
S_1	Presence	Public ownership/state participation in company management. Company may be seen as a symbol of state authority	1
	Absence	Private ownership	0
S_2	Presence	Presence of military targets, institution buildings, embassies, monuments of high symbolic value, critical infrastructure in the site proximity.	1
	Absence	Absence of military targets, institution buildings, embassies, monuments of high symbolic value, critical infrastructure in the site proximity.	0
S_3	Presence	Chemicals that can be used as WMD are stored, handled, processed, produced in significant quantities in the site.	1
	Absence	Chemicals that can be used as WMD are NOT stored, handled, processed, produced in significant quantities in the site.	0
S_4	Presence	Similar facilities or facilities owned by the same company object of past attacks	1
	Absence	Similar facilities or facilities owned by the same company never object of attacks	0
S_5	Presence	Terrorist/activist groups are active in the area	1
	Absence	No terrorist/activist groups are active in the area	0
S_6	low	A context of political stability and democracy exists. Governing authorities are legitimated and supported by populace.	0
	Medium	Few opposition groups willing to mine government authority exist and may be blamed for violent actions. Existence of political factions.	0.5
	High	Political instability and internal conflicts exist. Social order control and maintenance are periodically disrupted.	1
S_7	low	Strict legislation concerning the transport, selling, and detention of weapons of any nature. Effective and diffuse implementation of controls by police forces.	0
	Medium	Legislation concerning the transport, selling, and detention of weapons is present but control is not a priority.	0.5
	High	The transport, selling, and detention of weapons is poorly ruled and uncontrolled. Third-party interests in favoring the weapons market.	1
S_8	low	Extremely positive reputation; local community judges company beneficial	0
	Medium	Company activities accepted by local community. Few/minor aversion motives	0.5
	High	Company reputation extremely negative. Existence of organized aversion groups.	1
S_9	low	High level of engagement of local stakeholders. Transparency and continuous information sharing to enhance community awareness of company activities.	0
	Medium	Medium level of engagement of local stakeholders. Company activities are accepted by local community. Few aversion motives of minor importance.	0.5
	High	No engagement of local stakeholders, climate of suspicion and mistrust.	1
S_{10}	low	No interactions with cultural/historical, archeological, religious heritage. Absence of activist groups on the area/no evidence of aversion by activist groups.	0
	Medium	No significant negative interactions with cultural/historical, archeological, religious heritage. Sporadic demonstrations of aversion by local activist groups.	0.5
	High	Negative interactions with cultural/historical, archeological, religious heritage.	1

WMD, weapon of mass destruction

Adapted from Argenti, F., Landucci, G., 2016. Advanced attractiveness assessment of process facilities with respect to malevolent external attacks. Chem. Eng. Trans. 53, 133–138.

Table 3.2.5 Criteria weights applied in the calculation of index F (Argenti and Landucci, 2016).

Weight	Related aspect	Value
w_1	Company ownership	0.0324
w_2	Presence of third-party highly attractive targets	0.1445
w_3	Presence of chemicals that can be used as WMD	0.1445
w_4	Past threat history	0.1692
w_5	Terrorist/activist activity in the area	0.1445
w_6	Political instability	0.0819
w_7	Ease in weapons gathering	0.0653
w_8	Local aversion due to company image and reputation	0.0726
w_9	Aversion due to local stakeholders engagement and awareness of technology	0.0726
w_{10}	Aversion due to economic/environmental reason and/or interactions with cultural/religious heritage	0.0726

The overall attractiveness increase index F is calculated as a weighted sum of the scores as follows:

$$F = \sum_{i=1}^{m} w_i \times \sigma_i; \quad \sum_{i=1}^{m} w_i = 1 \tag{3.2.3}$$

Weights (w_i) are adopted in order to account for the different degree of influence that incentives may have on adversaries' targeting logic and may be attributed based on experts' judgment elicitation. An example of weighting for Eq.(3.2.3) was shown by (Argenti and Landucci, 2016), who adopted the analytic hierarchy process through the pairwise comparisons method (Saaty, 1990). The proposed weighting system is summarized in Table 3.2.5.

The calculated overall attractiveness index, I_A, calculated by Eq. (3.2.1), is finally ranked according to a qualitative three-level scale (high, medium, and low). Table 3.2.6 reports the guidelines for assigning the qualitative ranking levels. In order to

Table 3.2.6 Qualitative ranking associated with the indexes defined in the method for attractiveness assessment of chemical and process facilities adopted in the present work.

Index	Score range	Qualitative ranking
I_H	2–5	Low
	5–8	Medium
	>8	High
F	0–0.2	Low
	0.2–0.5	Medium
	>0.5	High
I_A	2–5	Low
	5–8	Medium
	>8	High

demonstrate the potentiality of the method, an industrial case study is proposed as benchmark in Chapter 4.

3.3 Vulnerability assessment

3.3.1 The concept of vulnerability in security studies

Vulnerability is often considered as a global system property that expresses the extent of adverse effects caused by the occurrence of a specific hazardous event (Reniers and Audenaert, 2014; Yazdani et al., 2011). This interpretation of vulnerability is thus closely related to the definition of risk. However, the identification and characterization of scenarios in vulnerability analyses are conditioned upon the occurrence of a specific hazardous event or strain. This concept of vulnerability inspired early developed security vulnerability assessment methodologies (American Petroleum Institute and National Petrochemical and Refinery Association, 2003; CCPS - Center for Chemical Process Safety, 2008; Jaeger, 2003), that, although referring to "vulnerability", were meant to evaluate risks associated to security events.

Johansson et al. (2013) define vulnerability "as the inability of a system to withstand strains and the effects of failures." Haimes (2006) has a similar view as he defines vulnerability as the manifestation of any possible technical, organizational, cultural state that a system may feature and may lead to harm or damage to the system itself. Several literature studies concerning infrastructure safety and security were developed starting from this statement. Setola et al. (2009) investigated the interdependencies among critical infrastructure sectors based on the occurrence of several outage periods; they applied a modified version of the input−output inoperability model to support the development and refining of contingency plans and backup strategies. Levitin et al. (2011) related the vulnerability of a network to the disintegration of the network itself into disconnected subnetworks or clusters and provided a tool for the estimation of the associated damage. Marrone et al. (2013) developed a methodological tool for the railway infrastructure protection based on the concept of vulnerability; the tool is aimed at developing a decision-making system for the evaluation of the effectiveness of security countermeasures against an attack, suggesting the types and dispositions of devices that maximize protection effectiveness.

Haimes (2006) pointed out that, in the perspective of infrastructure and industrial facilities protection, two major considerations need to be taken into account:

i. The ability to recover the desired values of the states of a system that has been attacked, within an acceptable time period and at an acceptable cost;
ii. The ability to reduce the effectiveness of the attack (and thus its probability of success) by other actions that may or may not necessarily change the state variables of the system. Such actions may include detection, prevention,

protection, interdiction, and containment, which also represent the design functions of security protection systems.

The first consideration is associated with the resilience of the system; a classic definition of resilience is given by Woods (2006), which describes resilience as "the capability of recognizing, adapting to, and coping with the unexpected." Resilience may be enhanced, for example, by adding redundancy and robustness. In a specific review, Kriaa et al. (2015) provide several examples of the resilience enhancement of control systems, with particular reference to aerospace and power generation sector.

The second consideration is of particular importance for the chemical sector and is discussed in the following. In particular, vulnerability has been intended as the proxy for the likelihood of external attack success. This is in agreement with the risk formulation proposed in the ANSI/API Standard 780 (American Petroleum Institute (API), 2013). In particular, as discussed in details in Chapter 4, the security risk is intended as a combination of the likelihood that a defined threat will find an asset attractive and successfully commit an act against it, taking advantage of vulnerability to cause a given set of security consequences. In particular, considering this risk formulation, the vulnerability may be considered as the likelihood that the attack will circumvent or exceed the existing security measures or physical protection system (PPS). In other words, vulnerability may be specifically considered the likelihood of attack success. In this case, the likelihood of attack success may be derived from a performance-based assessment of the PPS, as recommended for facilities with high-consequence loss physical assets (Garcia, 2006) and described in Section 3.3.2.

Finally, it is important to distinguish two main approaches supporting the analysis of security vulnerability. According to (Vellani, 2006), vulnerability assessment is commonly based on either an asset-based or a scenario-based approach. In the case of asset-based vulnerability assessment, a broad evaluation of assets and the threats that impact on those assets is carried out without considering and analyzing the attack scenario(s). On the contrary, the scenario-based approach focuses on the attack in order to foresee how targets may be affected, through which means, methods, and tools, thus identifying possible countermeasures. Moreover, the scenario-based assessment directly supports the managerial decision process and provides recommendations on the implementation and/or improvement of security countermeasures.

3.3.2 Security vulnerability assessment (SVA) of chemical and process facilities

Among the commonly adopted approaches to perform the vulnerability assessment of chemical and process facilities, the SANDIA SVA approach (Garcia, 2006) is presented in the following as reference framework method. Vulnerability is associated with the performance effectiveness of the security countermeasures; thus, SVA consists of a systematic evaluation, in which several kinds of techniques are used to predict the PPS

components' effectiveness, with the aim to provide the evaluation of the overall security system. In this way, the critical assets to protect are identified for defined threats and, at the same time, PPS upgrades are evaluated. SVA may be considered a useful managerial tool to support informed decision-making to enhance security of an installation/establishment.

Depending on the type of establishment to be protected, the estimate of the overall effectiveness of the physical protection system and therefore of the vulnerability of this system may be achieved by following a qualitative or quantitative approach. Garcia (2006) points out that the security consequences of the potential acts of interference drive the selection among the different kinds of approaches. Thus, the qualitative approach, usually based on the adoption of tools such as simplified risk matrix, applies to installations with limited extent of the consequences in case of loss or damage (shops, residential complexes, etc.). A quantitative analysis is instead essential for those infrastructures for which the degree of severity of consequences is unacceptable even if the probability of attack is low. This is the case of chemical and process facilities, where relevant inventories of hazardous materials are stored and potential acts of interference may escalate in major accidents affecting the operators and eventually the population in residential areas. Thus, a specific focus on quantitative vulnerability estimation is given.

The quantitative estimate of the vulnerability (V) of a physical protection system is expressed in (Garcia, 2006) in terms of probabilistic estimates as follows:

$$V = 1 - P_E = 1 - (P_I \times P_N) \tag{3.3.1}$$

in which:

P_E is the effectiveness of the PPS system, P_I the probability of interruption (for a given type of interference/opponent), and P_N is the probability of neutralization (for a given type of interference/opponent). Thus, both P_I and P_N strongly depend on the type of opponent or agent. Clearly enough, relevant technical−organizational skills, such as in the case of terrorist groups, may have a greater impact on the PPS effectiveness rather than in the case of isolated criminal acts from individuals or small groups. In the case of chemical facilities protection, the response force action against an adversary is normally immediate and is performed according to the general strategies of denial. A denial strategy can be seen as the best response when protecting critical assets where release of hazardous materials would cause many injuries, deaths, or contamination, particularly for capable and determined adversaries. It may consist simply in adversary interruption or in adversary neutralization by means of a force-to-force engagement after interruption. Therefore, according to the analysis carried out by Landucci and coworkers (Argenti et al., 2017; Landucci et al., 2017), the term P_N may be set as unitary, and the overall effectiveness of the PPS system is identified with the probability of interruption. Eq. (3.3.1) is thus rewritten as follows:

$$V = 1 - P_I \tag{3.3.2}$$

The starting point for the probabilistic evaluation of the PPS performance and, thus, of the P_I term, is to refer to the so-called "adversary path analysis"; this term indicates the evaluation of the paths and the sequence of the opposing actions, which, if completed, result in the success of the attack. The protection elements present along a certain path perform the functions of identification and delay; the effectiveness of every single "barrier" encountered by the adversary in approaching the established target determines the overall performance of the system.

Regardless of the type of attack strategy adopted, the best way to estimate the overall effectiveness of the system is to refer to the concept of "timely detection," which is based on the combination of the following factors (Garcia, 2006):

$$P_I = f(P_{\min}, T_{\min}, T_G) \tag{3.3.3}$$

in which, $P_{\min}$ is the cumulative probability of detection along a certain path, $T_{\min}$ is the minimum cumulative delay time along a certain path, and T_G is the security personnel intervention time. The SANDIA SVA guide offers a flowchart for the evaluation of the term P_I, as shown in Fig. 3.3.1.

The key point of this approach is to evaluate the system's response capability by measuring the cumulative probability of detection at the point (along a certain path) where sufficient time remains for the guard staff to stop the adversary's action. The delay time of the various elements along that path determines the point where the opponent must be identified; at this point, the minimum delay time ($T_{\min}$) along the remaining portion of the opponents' route coincides with the intervention time T_G and is identified by the term "critical detection point."

The probability of interruption, P_I, is therefore the cumulative probability of detection from the beginning of the path up to the critical detection point identified by the analysis of T_R and T_G. Within a chemical facility, there is a number of possible paths that can be adopted to perform an act of interference. Hence, the procedure in Fig. 3.2.1 needs to be applied to each possible path; the "critical path" is the path for which the minimum P_I value is obtained. Thus, the critical path represents the most vulnerable path and immediately identifies the overall effectiveness of the physical protection system. In this perspective, resources may be redistributed in order to improve the PPS performance, thus achieving an increment of P_I for the most critical paths.

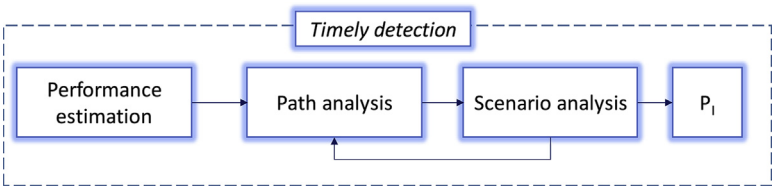


FIGURE 3.3.1 Schematic approach for the evaluation of the probability of interruption. *Adapted from Garcia, M., 2008. The Design and Evaluation of Physical Protection Systems, second ed. Butterworth - Heinemann, Burlington, MA, USA, Garcia, M., 2006. Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann, Newtown, MA.*

3.3.2.1 Path analysis

As previously pointed out, each process facility is characterized by the existence of several points of access that an adversary may use to perform an attack attempt, trying to access the site to reach the target; therefore multiple paths are present. In order to apply any quantitative analysis method (see Section 3.3.2.3), a systematic identification of all the possible paths needs to be firstly carried out. For this purpose, the most commonly applied tool is the construction of the "adversary sequence diagrams" (ASDs) (Garcia, 2008). ASDs are graphical representations of the protection elements present in the installation under examination and illustrate the paths that the adversaries can undertake to complete their intent (sabotage, theft, or attack to a piece of equipment). For a specific PPS and a specific threat, the most vulnerable path (or the path with least PPS effectiveness) can be determined. This path establishes the effectiveness of the total PPS. Moreover, it is likely that for each potential target there are at least two ASDs, for example, one relating to the daytime conditions of the installation, the other valid for the night hours. Other possible site conditions likely to be analyzed in a specific way include the change of workers and security personnel, fires or other emergency situations, blackouts of electricity, bad weather conditions, etc.

The evaluation of the sequences of the opposing actions continues with the determination of the performance of the elements constituting the various levels of protection through the estimation of the probabilities of detection and the delay times; a preliminary estimate of the probability P_I is then provided and the position of the critical detection point determined for all the possible identified paths.

3.3.2.2 Scenario analysis

Among all the possible paths identified through ASD, those considered to be not credible are rejected by applying cut-off criteria based on tactical considerations. For example, some paths will be eliminated because the agent performing the attack does not have the ability to pass the protections in place. The scenario analysis focuses only on the critical paths. For each critical path (see Section 3.3.2.1) and given a type of attacker, the possible aggression tactic is evaluated based on the current weaknesses identified for the particular path in different conditions of the considered installation (day, night, weekdays, holidays, etc.). The scenario analysis is carried out to verify if the previously evaluated aggression or attack modes result in a lowering of the preliminary effectiveness estimate of the PPS, thus affecting the P_I value.

3.3.2.3 Quantitative analysis tools

There are several analytical models that can support the security manager to evaluate the PPS effectiveness; some of these methods used by Sandia Laboratories are listed below:

- Analytic System and Software for Evaluating Safeguards and Security (ASSESS): advance and complex model currently used by the US government in the Department of Energy. It also allows for the analysis of insider threats and also

assesses the force-on-force encounters between adversaries and security, predicting the probability of defeat. The output of ASSESS consists of the ranking of PPS vulnerabilities for all the considered attack paths.

- Estimate Adversary Sequence Interruption (EASI): easy-to-use method aimed at the evaluation of the PPS performance along a given path for a given system/adversary combination. This model computes a probability of interruption from the analysis of interaction of the security functions (detection, delay, response, and communication, more details on the functions are discussed in Chapter 5).
- Safeguards Automated Facility Evaluation (SAFE): starting from the input data (characteristics of the PPS, potential paths, intervention times of the onsite personnel), SAFE identifies the most vulnerable paths to reach the critical assets. The EASI algorithm is then applied to the most vulnerable path and the probability of neutralization is estimated using the Brief Adversary Threat Loss Estimator (BATLE) model.
- System Analysis of Vulnerability to Intrusion (SAVI); this model provides a complete analysis of all the routes within an installation. Based on the input data consisting of the type of opponent, site characteristics, protection elements, and intervention times, the SAVI code lists the 10 most vulnerable routes. The calculation of the performance of each individual route is entrusted to the EASI algorithm.
- Safeguards Network Analysis Procedures (SNAP); this method uses a Network-Modeling approach for the schematization of the structure, of the guard staff, and of the adversary. This method is strongly conditioned by the scenario in question, so when the modeling of a direct comparison between security personnel and assailants is not envisaged, SANDIA suggests to use the EASI code.

The reader is referred to (Garcia, 2008) for more details. In Section 3.3.3 a qualitative method to support the SVA based on path analysis is explained. Section 4.2 provides an example of advanced tool based on the application of Bayesian Networks for the security vulnerability assessment.

3.3.3 Simplified approach for the selection of the intrusion scenarios and evaluation of the PPS system

In the following, a simplified approach for the identification of the most critical paths and qualitative analysis of the security countermeasures in place is presented. The approach is based on the qualitative methods extensively described in the technical literature (American Petroleum Institute (API), 2013; Garcia, 2008, 2006).

Firstly, based on the identification of all the possible intrusion points (namely, α), the intrusion scenarios are defined based on the path between each intrusion point and each sensible target (namely, β). Therefore, for each intrusion scenario, there are three relevant elements to be considered for the path characterization:

1. the distance (D) between the *j*-th combination intrusion point α_j and the target β_j ($j = 1, \ldots m$);

2. the number (n) of security countermeasures against a possible adversary along the j-th path;
3. the probability of failure (P_F) of each i-th security countermeasure of the total n protections present along the path.

An example of path characterization is shown in Section 3.3.4. Based on the three considered elements, the probability of attack success P_σ may be estimated with the following simplified expression for each path:

$$P_{\sigma_j} = \frac{(1 - D_{N,j})}{\sum_{i=1}^{n}(1 - P_{F,i})} \quad j \neq i \tag{3.3.4}$$

where $D_{N,j}$ is the normalized distance obtained as follows:

$$D_{N,j} = D_j / \max_k(D_k) \quad k = 1, .m \tag{3.3.5}$$

A simplified estimate of the terms P_f for some selected PPS elements is given in Table 3.3.1 based on expert judgment; this estimate is reported for exemplification purposes and is adopted in Section 3.3.4 in a tutorial application. Section 5.2 provides extensive details about quantitative performance characterization of an extended set of PPS elements.

Then, a screening criterion is introduced in order to reduce the number of attack scenarios and identify the critical paths Eq. (3.3.5). The screening criterion is based on the estimation of P_σ by using Eq. (3.3.4). The critical paths further considered in the analysis are those for which the following expression is satisfied:

$$P_{\sigma j} > I_{90} = \frac{(m+1) \times 90}{100} \tag{3.3.6}$$

where I_{90} is the 90 percentile of the P_σ values estimated for all the m possible attack scenarios identified for the facility under analysis. In other words, the 90% of cases featuring the lower values of attack success probability (thus, limited vulnerability) are not further considered, focusing the attention to the critical scenarios with the highest vulnerability. Once the critical paths are identified, the review of the existing security countermeasure in place may be carried out in order to strengthen the weak points that emerged from the analysis.

Table 3.3.1 Simplified evaluation of probability of failure P_F of given security protection elements based on expert judgment.

PPS element	P_F	Notes
CCTV (close circuit television)	1×10^{-1}	Based on efficiency level of the video surveillance system
Gate	2×10^{-2}	Possibility to access during opening/closing, once every 50 times
Fence	1×10^{-2}	Doubled efficiency with respect to the gate, being the fence fixed

3.3.4 Example of path analysis for a real case

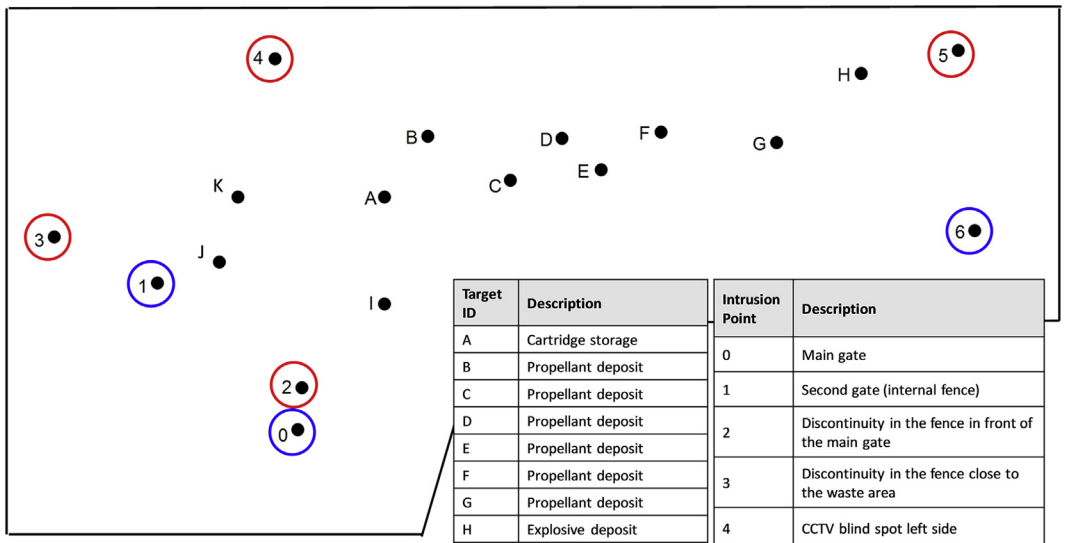
In order to exemplify the path analysis aimed at supporting the vulnerability assessment, an actual chemical facility is considered. The facility is located in Europe and falls under the obligations of the Seveso directive (European Commission, 2012). The facility includes a storage site for different kinds of explosive materials (both propellants and military explosives), but also ammunitions for civil, hunting and military use, and related components. A summary of the substances stored and processed in the site is given in Table 3.3.2.

The overview of the facility is shown in Fig. 3.3.2. For confidentiality reasons, several information and data were omitted or modified without altering the final results of the analysis. The shape of the facility perimeter is schematized; scale and orientation are not given, but the relative distance among the items in each map is based on real observations. The quantities given in Table 3.3.2 are multiplied by random numbers, which, however, do not alter the impact of potential accidents associated with the targets storing hazardous materials in the site. Damage distances with the major accidents potentially affecting the facility are reported in Table 3.3.3.

The site perimeter is surrounded by a path, which might be reached via car or a small truck, but a 3m-high fence securing against external intrusions. The direct access points to the site consist of two main gates (labeled with 0 and 1 in Fig. 3.3.2), which are operated from the personnel in the reception; CCTVs allow for monitoring the access at the gates. Security personnel with specific training is available 24/7 at the reception; however, security surveillance is not the only duty of the personnel (switchboard, suppliers or customer acceptance, etc.), and this might affect the vulnerability of the PPS. The access to the site can be directly carried out by staff members (autonomous gate opening and badge system for registration on the site). The hazardous materials storage and processing areas are secured with a secondary fence; in this area the gate is only operated by the security personnel.

Table 3.3.2 Summary of the hazardous materials stored and processed at the considered facility. All the substances are explosive solids. The quantities are multiplied by an arbitrary factor for confidentiality reasons.

Substance	Maximum quantity (ton)
Black powder (grains) (UN N. 0270 — 1.1D)	108.2
Trinitrotoluene TNT (UN N. 0209 — 1.1D)	28.0
Compound B (UN N. 0118 — 1.1D)	28.0
Smokeless gunpowder (UN N. 0161 — 1.3C)	108.2
Explosives N.A.S. (UN N. 0350 — 1.4B)	0.2
Smokeless gunpowder (UN N. 0509 — 1.4C)	108.2
Cartridges (UN N. 0012 — 1.4S)	54.7
Cartridge primers (UN N. 0044 — 1.4S)	0.5
Triggered bosses (UN N. 0055 — 1.4S)	4.6
Double base gunpowder (UN N. 0161 — 1.3C)	7.0



Target ID	Description
A	Cartridge storage
B	Propellant deposit
C	Propellant deposit
D	Propellant deposit
E	Propellant deposit
F	Propellant deposit
G	Propellant deposit
H	Explosive deposit
I	Cartridge storage
J	Local ammunition loading
K	Cartridge storage

Intrusion Point	Description
0	Main gate
1	Second gate (internal fence)
2	Discontinuity in the fence in front of the main gate
3	Discontinuity in the fence close to the waste area
4	CCTV blind spot left side
5	CCTV blind spot right side
6	Small gate in the secondary fence

FIGURE 3.3.2 Overview of the facility considered for the case study: plot plan with potential targets and intrusion points. Blue circles (dark gray in print version) highlight gates located on the site perimeter, while the red circles (gray in print version) identify discontinuities in the fence/net or blind spots in the CCTV system at the moment of the analysis.

Table 3.3.3 Damage distances (m) associated with the worst-case scenarios for all the possible targets in the facility. Damage distances are referred to selected over-pressure threshold values (Ministero dei lavori Pubblici, 2001).

	Damage distance (m)				
	High lethality	Domino effect	Incipient lethality	Irreversible damage	Weak damage
Target	0.6 bar	0.3 bar	0.14 bar	0.07 bar	0.03 bar
A	–	–	–	–	25
B	56	90	138	237	474
C	58	94	143	246	492
D	60	96	147	252	504
E	60	96	147	252	504
F	60	96	147	252	504
G	71	114	174	299	597
H	71	114	174	299	597
I	–	–	–	–	25
J	19	31	47	81	162
K	–	–	–	–	25

Given consequence assessment of the most relevant accidental scenarios associated with the loss of containment of the hazardous materials present on the site (Table 3.3.3), the most critical targets in case of external attack are represented by the storage area of cartridges (item A in Fig. 3.3.2), propellants (B, C, D and F in Fig. 3.3.2), and explosives (item H in Fig. 3.3.2). Based on the possible access points evaluated for the site (see red circles in Fig. 3.3.2) and the considered critical targets, the possible combinations access point α – target β are identified, as summarized in Table 3.3.4; hence, the relevant elements for the path analysis are evaluated, such as the distance and the number/type of available PPS elements on each path. For each PPS element, the effectiveness is estimated based on the simplified method described in Section 3.3.3, which finally allows for the identification of the most critical paths and scenarios, as summarized in Fig. 3.3.3 and highlighted in Table 3.3.4.

Table 3.3.4 Summary of the potential intrusion scenarios considered in the path analysis. The more critical paths are reported in ***bold*** *and shown in* Fig. 3.3.3*; n is the number of security countermeasures in the path associated with each scenario*.

ID	Intrusion point (α)	Target (β)	Distance (α to β) (m)	n	Type of protections
σ_1	1	A	563	8	5 CCTV + 3 gates
σ_2	1	B	641	10	7 CCTV + 3 gates
σ_3	1	C	632	9	6 CCTV + 3 gates
σ_4	1	D	692	10	7 CCTV + 3 gates
σ_5	1	E	715	10	7 CCTV + 3 gates
σ_6	1	F	778	10	7 CCTV + 3 gates
σ_7	1	G	865	12	9 CCTV + 3 gates
σ_8	1	H	964	11	8 CCTV + 3 gates
σ_9	1	I	540	8	5 CCTV + 3 gates
σ_{10}	1	L	389	5	3 CCTV + 3 gates
σ_{11}	1	M	476	8	5 CCTV + 3 gates
σ_{12}	2	A	291	7	4 CCTV + 2 gates + 1 fence
σ_{13}	2	B	371	8	5 CCTV + 2 gates + 1 fence
σ_{14}	2	C	341	6	3 CCTV + 2 gates + 1 fence
σ_{15}	2	D	417	6	3 CCTV + 2 gates + 1 fence
σ_{16}	2	E	416	5	2 CCTV + 2 gates + 1 fence
σ_{17}	2	F	466	5	2 CCTV + 2 gates + 1 fence
σ_{18}	2	G	562	6	3 CCTV + 2 gates + 1 fence
σ_{19}	2	H	642	6	3 CCTV + 2 gates + 1 fence
σ_{20}	2	I	173	5	2 CCTV + 2 gates + 1 fence
σ_{21}	2	L	208	4	2 CCTV + 1 gate + 1 fence
σ_{22}	2	M	318	6	4 CCTV + 1 gate + 1 fence
σ_{23}	3	A	478	6	4 CCTV + 1 gate + 1 fence
σ_{24}	3	B	524	7	5 CCTV + 1 gate + 1 fence
σ_{25}	3	C	568	7	5 CCTV + 1 gate + 1 fence

Table 3.3.4 Summary of the potential intrusion scenarios considered in the path analysis. The more critical paths are reported in ***bold*** *and shown in* Fig. 3.3.3*; n is the number of security countermeasures in the path associated with each scenario*.—cont'd

ID	Intrusion point (α)	Target (β)	Distance (α to β) (m)	n	Type of protections
σ_{26}	3	D	603	8	6 CCTV + 1 gate + 1 fence
σ_{27}	3	E	662	8	6 CCTV + 1 gate + 1 fence
σ_{28}	3	F	703	9	7 CCTV + 1 gate + 1 fence
σ_{29}	3	G	878	10	8 CCTV + 1 gate + 1 fence
σ_{30}	3	H	878	10	8 CCTV + 1 gate + 1 fence
σ_{31}	3	I	519	7	5 CCTV + 1 gate + 1 fence
σ_{32}	3	L	151	3	1 CCTV + 1 gate + 1 fence
σ_{33}	3	M	330	5	3 CCTV + 1 gate + 1 fence
σ_{34}	**4**	**A**	**251**	**2**	**1 CCTV + 1 fence**
σ_{35}	**4**	**B**	**289**	**2**	**1 CCTV + 1 fence**
σ_{36}	**4**	**C**	**353**	**2**	**1 CCTV + 1 fence**
σ_{37}	**4**	**D**	**382**	**2**	**1 CCTV + 1 fence**
σ_{38}	4	E	436	3	2 CCTV + 1 fence
σ_{39}	4	F	477	3	2 CCTV + 1 fence
σ_{40}	4	G	649	4	3 CCTV + 1 fence
σ_{41}	4	H	640	4	3 CCTV + 1 fence
σ_{42}	4	I	339	4	3 CCTV + 1 fence
σ_{43}	4	L	341	3	1 CCTV + 1 gate + 1 fence
σ_{44}	4	M	240	3	2 CCTV + 1 fence
σ_{45}	5	A	625	4	3 CCTV + 1 fence
σ_{46}	5	B	594	4	3 CCTV + 1 fence
σ_{47}	5	C	504	3	2 CCTV + 1 fence
σ_{48}	5	D	448	3	2 CCTV + 1 fence
σ_{49}	5	E	405	2	1 CCTV + 1 fence
σ_{50}	**5**	**F**	**363**	**2**	**1 CCTV + 1 fence**
σ_{51}	5	G	343	3	2 CCTV + 1 fence
σ_{52}	**5**	**H**	**171**	**2**	**1 CCTV + 1 fence**
σ_{53}	5	I	666	3	2 CCTV + 1 fence
σ_{54}	5	L	818	6	4 CCTV + 1 gate + 1 fence
σ_{55}	5	M	716	6	5 CCTV + 1 fence
σ_{56}	6	A	737	7	5 CCTV + 2 gates
σ_{57}	6	B	700	6	4 CCTV + 2 gates
σ_{58}	6	C	474	4	2 CCTV + 2 gates
σ_{59}	6	D	551	4	2 CCTV + 2 gates
σ_{60}	6	E	411	3	1 CCTV + 2 gates
σ_{61}	6	F	464	3	1 CCTV + 2 gates
σ_{62}	6	G	469	4	2 CCTV + 2 gates
σ_{63}	6	H	302	4	2 CCTV + 2 gates
σ_{64}	6	I	526	4	2 CCTV + 2 gates
σ_{65}	6	L	910	3	1 CCTV + 2 gates
σ_{66}	6	M	826	4	2 CCTV + 2 gates

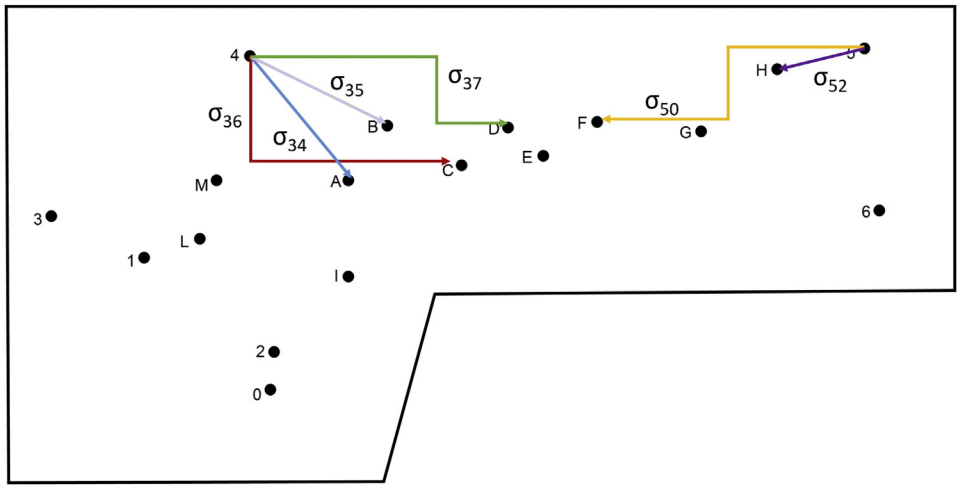


FIGURE 3.3.3 Critical paths identified in the paths analysis. Details on the possible targets and available security countermeasures are reported in Table 3.3.4 at the correspondent ID.

As shown in Fig. 3.3.3, the deposit of the most hazardous substance (TNT) is located close to the access point and features a limited number of PPS elements. More in general, it appears that despite in some paths there are redundant protections (in some cases, eight CCTV + three gates), for some selected paths only a CCTV system and a fence are the security protections available. This is valid for all the critical targets. Thus the present method, despite the relevant simplifications introduced, may help framing an improvement strategy and reallocation of security resources identifying the weak points in the PPS. In particular, after the simplified path analysis, the site manager considered the implementations of the following actions:

- Improvement of CCTV system to revamp currently available equipment and avoid blind spots in the perimeter (thus, increasing the number of protections available in all the possible paths)
- Introduction of security-dedicated personnel, thus without other secondary duties
- Fence material upgrade (more resistant material than the current metal net) — optional.

3.4 Consequence and impact assessment

3.4.1 Cascading events triggered by external acts of interference: an approach to integrate "safety" and "security" scenarios

Industrial facilities where relevant quantities of hazardous chemicals are stored or processed may be possible targets for external acts of interference due to terrorist attacks. The potential severity and credibility of such scenarios were discussed in several

previous studies dealing with the impact evaluation of external attacks on process plants (American Petroleum Institute and National Petrochemical and Refinery Association, 2003; Bajpai and Gupta, 2007; Milazzo et al., 2009; Moore, 2004; Moore et al., 2007, 2006; Nolan, 2008; Pavlova and Reniers, 2011; Störfall Kommission (SFK), 2002). A key aspect that emerges from this analysis is that the events and process upsets triggered by malicious acts of interference may escalate into accident chains affecting several process units or eventually neighboring industrial sites, with an overall increased accident severity, such as in the case of domino effect escalation (Cozzani et al., 2009; Pavlova and Reniers, 2011; Reniers and Soudan, 2010). Hence, external acts of interference to process plants may be seen as both relevant safety and security concerns. In order to highlight the integration among safety and security issues in the impact assessment, Landucci et al. (2015) developed a schematic framework shown in Fig. 3.4.1 and explained in the following.

As shown in Fig. 3.4.1, the attack may take place inside the industrial domain. In this case, the purpose of the attack is to directly damage process equipment through explosives or firearms and to trigger an escalation sequence leading to a domino scenario (also defined as a "cascading event") (Casal and Darbra, 2013; Cozzani et al., 2014; Cozzani and Reniers, 2013; Darbra et al., 2010; Hemmatian et al., 2014; Kadri et al., 2013; Kourniotis et al., 2000; Reniers and Cozzani, 2013). Otherwise, an intentional act of interference may as well be perpetrated from outside the plant boundaries, but still having the plant as the main target (Cozzani et al., 2013; Cozzani and Reniers, 2013;

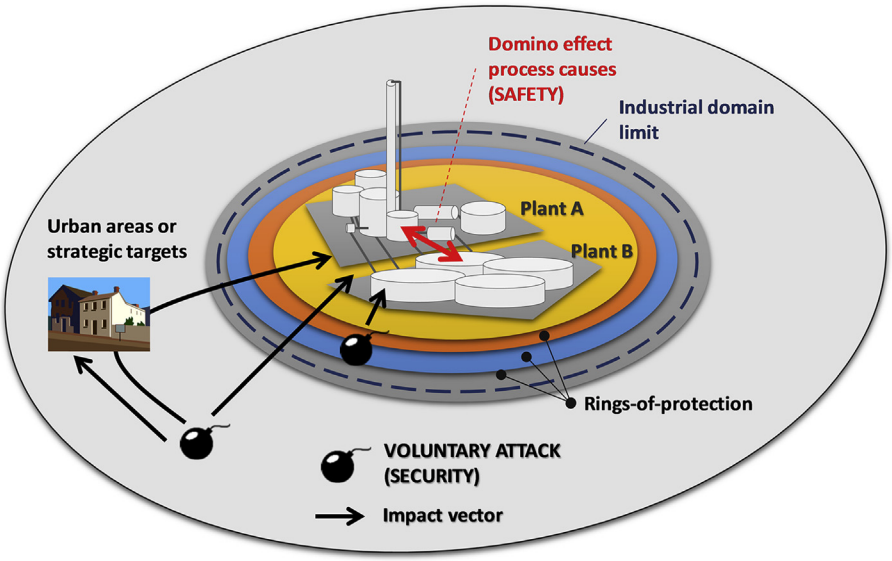


FIGURE 3.4.1 Schematization of possible integrated safety and security events affecting process plants with potential domino effects. *Adapted from Landucci, G., Reniers, G., Cozzani, V., Salzano, E., 2015. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliab. Eng. Syst. Saf. 143, 53–62.*

Reniers, 2010; Reniers and Audenaert, 2014). Moreover, intentional attacks to non-industrial targets (e.g., strategic buildings, urban areas, infrastructures) might produce a large-scale accident, which may in turn trigger indirect external domino effects in an industrial facility. Domino scenarios triggered by such attacks are likely to have an extremely high severity (Casal and Darbra, 2013; Cozzani et al., 2014; Darbra et al., 2010; Hemmatian et al., 2014; Kadri et al., 2013; Reniers and Cozzani, 2013; Scarponi et al., 2018a, 2018b), as remarked in Fig. 3.4.1.

This highlights the importance of an appropriate security management of chemical and process facilities, also integrating the vulnerability analysis of the surrounding area. In this perspective, the impact analysis of the attack scenarios is of utmost importance. On the one hand, assessing the direct impact of the means of interference (explosives, incendiary devices, projectiles, etc.) supports the severity evaluation of possible attacks. Thus, it enables the prediction of potential adverse effects (i) on urban areas (direct impact on population) and (ii) on equipment units, triggering domino events. On the other hand, impact assessment may support the identification of damage modes and release scenarios induced by external attacks on process equipment, thus eventually evaluating the secondary[2] scenarios effects, which feature worsened consequences for the population.

In Section 3.4.2, a methodology for the impact assessment of security-related scenarios is presented, in particular focusing on the consequences of the secondary scenarios induced by different attack modes. A key aspect of the method is the analysis of the direct impact of the external of interference, for which particular detail is given in Section 3.4.3.

3.4.2 Methodology for impact assessment

The impact assessment methodology is shown in the flowchart reported in Fig. 3.4.2. The methodology is primarily aimed at the consequences estimation of the accidents triggered by external acts of interference on process plants. At the same time, it also includes a framework for the analysis of the direct impact of the intentional attack on different kinds of target.

The starting point of the methodology (Step 1 in Fig. 3.4.2) is aimed at the identification of the most attractive equipment items on a given facility, e.g., the equipment that may lead to the most severe consequences in the case of a release caused by the attack. The concept of process plant attractiveness was elaborated in Section 3.2; in the present framework, attractiveness assessment is carried out based on classification of process equipment types, which relies, in turn, on the following input information:

- type of hazard connected with the substance: flammable hazard, toxic hazard, or both;

[2]In this section, the term “secondary” is adopted to identify any accident or accident chain triggered by a loss of containment caused by an intentional act of interference, the primary event.

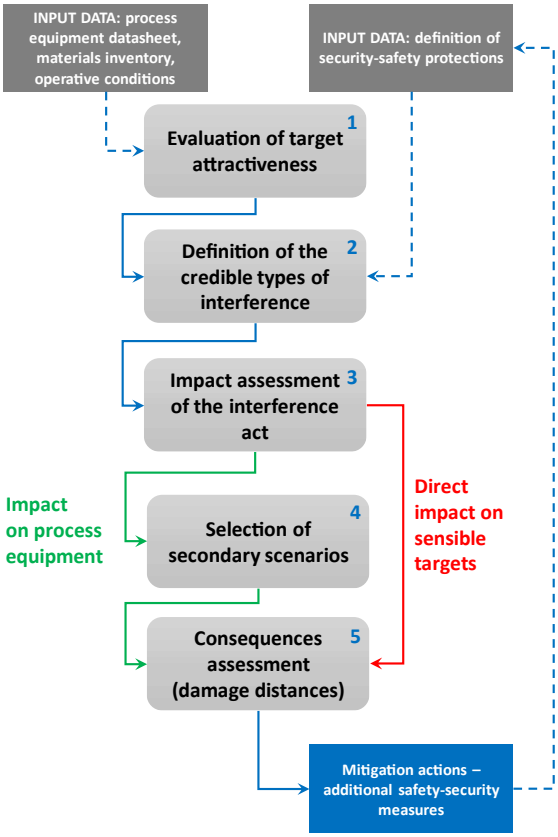


FIGURE 3.4.2 Methodology for the impact assessment of accidents triggered by external acts of interference in process facilities.

- physical conditions of the substance: storage or process conditions of the substance influence postrelease phenomena (Van Den Bosh and Weterings, 2005): formation of a toxic/flammable vapor cloud, boiling liquid pool, liquid spreading, etc.;
- inventory: amount of substance present in the unit (or equipment hold-up).

The unit inventory was directly related to the type of equipment: a storage tank has been considered having a higher hold-up than a column or a shell and tube heat exchanger. Table 3.4.1 reports the values estimated for the attractiveness score of the single equipment items on the basis of the proposed approach. This allows focusing the analysis on the more critical equipment items on the plant.

When the more sensible pieces of equipment are identified, the analysis of the various types of credible interferences is carried out (Step 2 in Fig. 3.4.2). In particular, the attack modes were selected from the set presented in (Störfall Kommission (SFK), 2002), as summarized in Table 3.4.2.

Table 3.4.1 Qualitative equipment attractiveness ranking.

	Equipment type			
Physical conditions of inventory	**Tanks**	**Large diameter pipelines**	**Column-type equipment**	**Reactors/shell and tube equipment**
Liquefied gas stored under pressure	4	4	3	3
Fluids with low vapor pressure stored in liquid phase	3	3	2	2
Gas/liquid stored in gas phase	3	2	2	1
Cryogenic storage	2	2	2	1
Liquid phase	1	1	1	1

Adapted from Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Prot. 110, 102–114.

Table 3.4.2 Characterization of the 10 categories of possible acts of interference for atmospheric (ATM) and pressurized (PRESS) equipment.

Type of interference	**Intrusion required**	**Impact vector**	**Information level**	**Release category (ATM)**	**Release category (PRESS)**
Deliberate misoperation	Yes	n.a.	C	R2	R1
Interference by simple means	Yes	n.a.	C	R2	R1
Interference by major aids	Yes	n.a.	C	R3	R2
Arson by simple means	Yes	Heat radiation	C	R3	R2
Arson by incendiary devices	Yes	Heat radiation	B	R4	R3
Shooting 1 (minor)	No	Mechanical impact	A	R1	R1
Shooting 2 (major)	Yes	Mechanical impact	A	R4	R4
Explosives	No	Overpressure	B	R4	R4
Vehicle/ship impact	Yes	Mechanical impact	B	R3	R3
Plane impact	No	Mechanical impact	A	R4	R4

n.a., not available.

Adapted from Landucci, G., Tugnoli, A., Spadoni, G., Cozzani, V., 2012. LNG regasification terminals: assessment of accidents due to external acts of interference. In: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012, pp. 4373–4382.

In order to carry out the impact analysis, each mode of interference has been characterized by few parameters, such as the potential impact vector (i.e., action or physical effect that may damage process or storage equipment units) and the required level of knowledge needed to perform the attack. In particular, three levels have been identified, ranging from A to C, for an increasing level and detail of information required:

- Level A: no specific knowledge of the plant, apart from its location and basic equipment positioning

- Level B: rough knowledge of the substances stored/processed in the facility and facility plot plan
- Level C: In-depth knowledge of the system inventory and details of the production process, presumably acquired through espionage or internal personnel

It is worth noticing that level B information may be easily acquired, since the plot plan for several industrial facilities can be reconstructed by external observations, guided tours of the plant, or from the web. Moreover, for plants falling under the obligations of Seveso III directive (European Commission, 2012) in the European context, the mandatory public documentation, which the chemical establishment operator needs to release, contains sufficient elements to achieve Level B knowledge and, partially, Level C.

Beside the definition of the possible types of interference, an important issue for the impact assessment is the evaluation of the escalation credibility following the attack. This is related to the safety and security protections present in the plant, whose effectiveness, expressed in terms of success probability of security countermeasures (see Section 3.3), depends on the specific mode of interference, i.e., on the damage vector. A detailed assessment based on probabilistic risk approaches is out of the scope of the present impact assessment. More specific tools are discussed in Section 3.3 dealing with the vulnerability assessment, while advanced tools for probabilistic risk assessment are discussed in Chapter 4.

For the purpose of the present impact assessment, which is aimed at providing a credible worst-case evaluation, a simplified approach is hereby introduced. In particular, a simplified Layer of Protection Analysis (LOPA) is adopted to qualitatively evaluate the credibility of damages following the attack (i.e., attack success), given the features of the equipment and of the attack itself. Fig. 3.4.3 reports a schematic representation of LOPA for given modes of interference; an example of selection of credible attack modes is shown in Section 4.1.

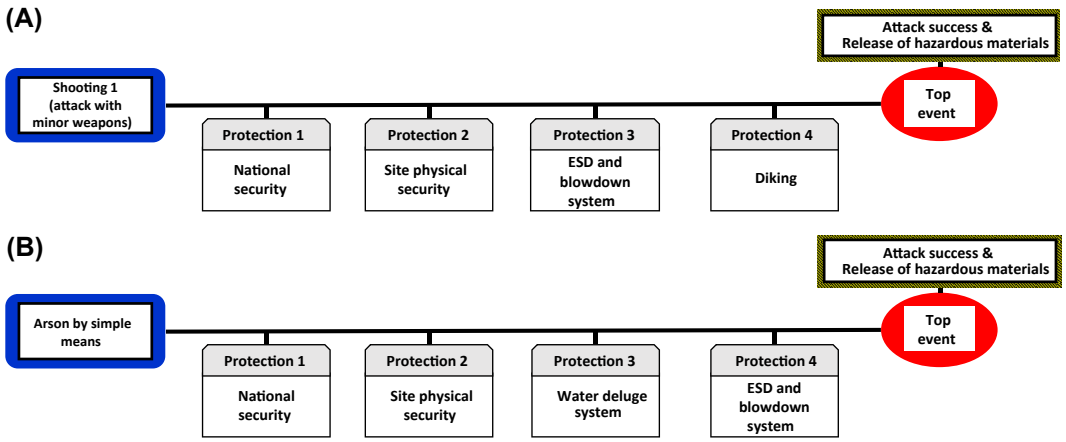


FIGURE 3.4.3 LOPA in case of (A) "shooting 1" and (B) "arson by simple means" interferences. For attack modes features, refer to Table 3.4.2.

As shown in Fig. 3.4.3, an element that has a relevant influence on the credibility of attack mode (and, thus, attack success) is the eventual need of intrusion to perform the act of interference. Thus, Table 3.4.2 specifies which attack modes require the intrusion into the perimeter of the site. For example, in the case of shooting, low potentiality weapons such as those considered in "shooting 1" require the intrusion in the plant and, thus, the security protection of the site may have an influence on the attack success. On the contrary, in case of heavy weapons (e.g., "shooting 2" in Table 3.4.2), the intrusion may not be required, since the attack may be perpetrated at hundreds of meters from the facility, thus with no possible intervention of the security protection on the site.

Once the credible attack modes are selected, the assessment of the impact vector associated with each interference scenario is carried out (Step 3 in Fig. 3.4.2). The first three interference modes shown in Table 3.4.2 do not involve the use of hazardous materials. In particular, "deliberate misoperation" consists of simple acts involving simple operations, such as opening or closing valves when not foreseen, variation of process conditions (temperature, pressure, concentration, etc.), disabling alarms or control systems. "Interference using simple aids" is related to any act of interference carried out with tools and aids that are present on site, while "interference using major aids" involves the use of heavy tools to achieve the destruction of selected parts of the facility. Explosive attacks and incendiary devices involve the use of hazardous materials in order to generate overpressure effects and fire heat radiation, respectively. Explosive devices may be based on military or conventional explosive material, but in the framework of security attacks, the utilization of IED is becoming more diffuse, as demonstrated by several recent terrorist attacks (National Academies and Department of Homeland Security, 2015) (see Section 3.4.3). Finally, the more severe interference scenarios in Table 3.4.2 involve the use of either weapons or vehicles to cause damage through mechanical impact[3] on process units.

If the success of an attack is considered credible based on the previously developed steps, the potential accidental scenarios affecting the personnel, population, and equipment are evaluated. It is worth to mention that in case of attacks with explosive or incendiary devices, the generated impact vector may also be able to directly damage the plant personnel and the population surrounding the facility (regardless of any domino effects). Therefore, as shown in Fig. 3.4.2 ("red" path of the flowchart), in Step 3 of the method, the possible direct effects associated with the attack on the population may be evaluated.

Next, following the "green path" in Fig. 3.4.2, the analysis of the potential domino effects is carried out. In Step 4 (Fig. 3.4.2), the type of expected loss of containment (LOC) event following the attack is assessed. The standard LOC categories derived from "Purple Book" (Uijt de Haag and Ale, 1999) are adopted in this step. Table 3.4.3 describes

[3]in this section, the word "impact" is related to the consequences and effects of accidents triggered by the attacks but, at the same time, it may be used in its specific mechanical meaning. Thus, the wording "mechanical impact" is adopted, indicating a force applied over a short time period by an external body (projectile, vehicle, ship, etc.) on the target equipment shell.

Table 3.4.3 Definition of release types adopted in Table 3.4.2 and considered in the present work. Φ: equivalent release diameter.

Release type	Description	Quantitative features
R1	Continuous release from minor holes/connections	$\Phi < 10$ mm
R2	Continuous release from major connections (process lines or open blowdown lines)	$\Phi =$ *pipe diameter (< 50 mm)*
R3	Major release of limited duration	10 min release of the entire inventory
R4	Catastrophic rupture and major release of limited duration	2 min release of the entire inventory/ instantaneous release

the LOCs considered in the present study, with increasing severity (ranging from R1 to R4). Each interference mode is then associated with a specific LOC in Table 3.4.2. Quite clearly, the inherent fragility of the equipment considered induces a different release scenario, given the same energy involved in the attack. Therefore, a distinction is made between atmospheric (ATM) and pressurized equipment (PRESS) in Table 3.4.2. Next, in order to complete the selection of the accidental scenarios triggered by the attack and associated with each LOC (the secondary scenarios), a conventional event tree analysis is carried out (Lees, 1996). It is worth to notice that some peculiar attacks, as arson or explosive interference, may affect the likelihood of some scenarios, thus increasing in these cases the probability of immediate ignition with respect to "conventional" situations.

Finally, also the consequences associated with each of the identified secondary scenarios are evaluated (Step 5 in Fig. 3.4.2). In the present study, conventional literature models (Van Den Bosh and Weterings, 2005) are used for the calculation of loss intensities and consequence assessment. The threshold values for the effects on humans reported in Table 3.4.4, derived from technical standards, are proposed to calculate a

Table 3.4.4 Threshold values adopted for the estimation of the expected damage distances associated with the accidental scenarios. Threshold values are associated with reversible effects on human according to the Italian legislation for land use planning (Ministero dei lavori Pubblici, 2001).

Secondary scenario and physical effect	Threshold value
Flash fire — transient radiation	$^1/_2$ LFL lower flammability limit, %vol
Fireball — transient radiation	3 kW/m^2
Jet fire — stationary radiation	3 kW/m^2
Pool fire — stationary radiation	3 kW/m^2
Vapor cloud explosion — overpressure	0.03 bar
Physical/mechanical explosion — overpressure	0.03 bar
Toxic exposure	IDLH - immediately dangerous to life and health concentration

conventional damage distance for each scenario. The analysis of the impact area associated with the consequence of the external attack for the considered plant can be also reported on a GIS (geographic information systems) tool, in order to identify the impacted areas and the vulnerability centers that may be affected. Therefore, the analysis of the worst-case scenarios also allows evidencing the eventual additional safety and/or security measures to be installed on the plant to reduce the impact on the population, as remarked in Fig. 3.4.2. In order to show the potentialities of the method, an application example is shown in Section 4.1.

3.4.3 IED (improvised explosive devices) impact analysis

In Section 3.4.2, a critical aspect of the present methodology was related to the characterization of the impact vector associated with the act of interference (Step 3 in Fig. 3.4.2). In the case of arson and incendiary devices, the conventional integral models for fire heat radiation evaluation may be adopted, in order to determine the potential damage effects on personnel, population, or process units (Van Den Bosh and Weterings, 2005). For what concerns the attack modes featuring a mechanical impact on process equipment, relevant works were published to analyze the effects of shooting and vehicle/aircraft impact on process equipment. Either detailed reviews (Corbett et al., 1996; Goldsmith, 1999) or specific studies (Borg et al., 2001; Lecysyn et al., 2008) were devoted to the evaluation of mechanical impact of projectiles on plates and shells, thus representative of chemical process units. For what concerns vehicle or aircraft mechanical impact, specific studies were dedicated to process equipment (Hu et al., 2014; Schneider et al., 1999). Finally, the remaining impact vector considered is the overpressure generated by explosive attacks. In the case of conventional explosives and military devices (such as trinitrotoluene, TNT) (Szala and Sabatini, 2018), detonation energy and explosive characteristics are well known; hence, potential effects for target equipment may be directly estimated using point source explosion models, see (Salzano et al., 2013) for more details.

However, according to the US Government Hazardous Substances Database, several substances and mixtures can be used to prepare home-made explosives (IED), starting from common chemicals sold in markets and pharmacies. Their use in explosive attacks is becoming more diffuse, as demonstrated by several recent terrorist attacks (National Academies and Department of Homeland Security, 2015), while information about their explosive features is not yet consolidated, thus avoiding a sound estimation of potential damages to equipment in case of explosive attack. Among many IED, two are often adopted for terrorist attacks, suicide bombing, and other malicious uses: Ammonium Nitrate (AN)−Fuel Oil (i.e., ANFO) (Fig. 3.4.4A) and Acetone Peroxide or Triacetone Triperoxide Peroxyacetone (TATP) (Fig. 3.4.4B) (Price and Ghee, 2009).

Conventional ANFO explosive is a generally composed by 94% of AN prills and 6% of adsorbed fuel oil. It is extensively used for several authorized purposes, such as in the case of mine blasting. TNT equivalence is typically around 80% and ideal explosion

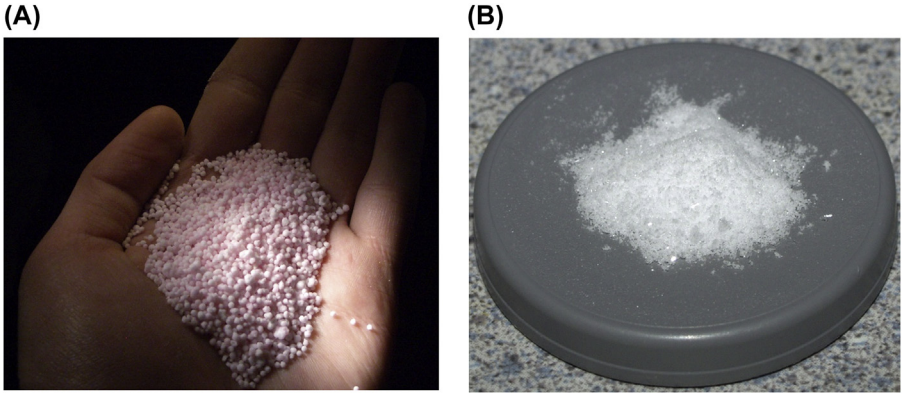


FIGURE 3.4.4 (A) Ammonium Nitrate (AN)—Fuel Oil (i.e., ANFO) prills; (B) Triacetone Triperoxide Peroxyacetone (TATP) powder.

(detonation) energy is 3890 kJ/kg[4] AN prills used for mining applications are, however, physically different from fertilizer prills used to prepare IED. Indeed, the commercial ammonium nitrate prills used for blasting have a 20% void space and are coated with #2 fuel oil (mainly C10 to C20 linear hydrocarbons) or kerosene. Hence, ANFO has a bulk density of approximately 840 kg/m^3, starting from AN prills with density of about 1300 kg/m^3 (the density of pure crystalline ammonium nitrate is 1700 kg/m^3). On the other hand, home-made explosives made from AN fertilizer do not have a high void fraction and are less efficient. This is favored also by the new European regulations for fertilizers (European Commission, 2003), which now must contain less than 45% of AN (16% N) for being traded to the general public. Such fertilizers still may be used to obtain explosives, but require an adequate preparation to achieve a detonation. If commercial AN (containing about 50% of inert, as dolomite) and an easily available diesel fuel are used, a detonation energy of about 1071 kJ/kg is obtained, much less than that of pure ANFO. Furthermore, it has been observed that for amounts of dolomite higher than 30% and diesel fuel, no detonation is observed (Buczkowski and Zygmunt, 2011).

TATP, due to the presence of several oxygen—oxygen bonds, features explosive potential without containing nitrogen. Thus, it is used for avoiding conventional chemical bomb detection systems, and it is almost undetectable by sniffer dogs. It can be obtained from common household items such as sulfuric acid, hydrogen peroxide, and acetone. TATP is very unstable: it can be ignited by touch and can explode spontaneously; it is often used for detonators. TATP is actually composed of isomers and conformers, the dimer being more stable but having lower energy. The density of the pure molecule is typically considered to be 1220 kg/m^3. However, home-made TAPT formulations are typically in the range of 450—500 kg/m^3 (Kuzmin et al., 2008), which gives a detonation velocity of about 1400 m/s. Thus, the TNT equivalence, which is 88% in ideal conditions,

[4]Pure ammonium nitrate has an explosion energy of 1592 kJ/kg.

can reach 50% for lower densities. Finally, TATP is often stabilized with carbonaceous liquids and waxes so that the net charge is even lower (Siegel and Saukko, 2012). Nevertheless, previous studies (Lefebvre et al., 2004) demonstrated that home-made TATP is very sensitive to impact or friction, although the strength of explosion may strongly vary according to operative conditions (especially temperature) adopted in the synthesis.

In a recent work, Landucci and coworkers (Landucci et al., 2015; Salzano et al., 2014) investigated the possibility of using home-made ANFO and TATP to damage process equipment, hence triggering a domino chain in chemical facilities by external explosive attack. ANFO and TATP explosive properties were firstly evaluated, based on the currently available data in the scientific literature (see the above discussion) and eventually integrated through the application of the chemical equilibrium model CEA (Basco et al., 2010; Salzano and Basco, 2012). Then, using the classical TNT-energy or mass-scaled analysis (Bounds, 1997), peak overpressures generated by the explosion for given amounts of ANFO or TATP were compared against threshold resistance values (Cozzani et al., 2006) to determine "stand-off distances." Stand-off distance is here defined as the minimum distance between the asset of interest and the area where an explosive device can be placed without causing damages and may be estimated as follows:

$$P = \frac{m_{TNT,eq}^{\frac{1}{3}}}{r} + 4.4\frac{m_{TNT,eq}^{\frac{2}{3}}}{r^2} + 14.0\frac{m_{TNT,eq}}{r^3} \tag{3.4.1}$$

where P is the peak overpressure threshold (bar); r is the stand-off distance (m); and $m_{TNT,eq}$ is the equivalent *TNT* mass (kg) for a specific improvised device.

A summary of the calculated stand-off distances for different types of IDE is reported in Table 3.4.5, together with the evaluated TNT efficiency values (TNT_{eff}) (Landucci et al., 2015; Salzano et al., 2014). In the case of ANFO, commercial AN[5] is considered in combination with diesel fuel. In the table, also the direct effects on human targets due to the explosion overpressure are reported.

Based on the analysis of stand-off distances shown in Table 3.4.5, it appears that relevant quantitates of ANFO need to be adopted in an explosive attack to damage process equipment, due to the limited efficiency of ammonium nitrate in the presence of dolomite as inert material. However, ANFO is sufficiently stable to be accumulated in several tons ($\approx$10–50t), which can be positioned outside the industrial fence loaded in car, van, or even a truck parked in the road adjacent to the industrial installation. If ignited, these quantities may damage equipment units at about 80–100 m distance (see Table 3.4.5). At the same time, the direct impact on population is expected at about 200–400 m, highlighting in this case the relevant severity of the attack itself.

On the other hand, large amounts of TATP are too hazardous to produce, transport, and manipulate (National Academies and Department of Homeland Security, 2015).

[5]About 50% wt. AN and 50% wt. inert dolomite.

Table 3.4.5 Calculated stand-off distance for different equipment categories and associated damage threshold values.

Target category	Overpressure threshold value (bar)	Explosive Mass (kg)	Stand-off distance (m) TATP (TNT_{eff} = 0.61)	Stand-off distance (m) ANFO[4] (TNT_{eff} = 0.23)
Humans	0.03	50	119	68
		100	150	86
		1000	NC	185
		10,000	NC	400
Atmospheric Vessel	0.22	50	25	14
		100	32	18
		1000	NC	39
		10,000	NC	85
Pressurized Horizontal Vessel (toxic)	0.16	50	31	18
		100	39	23
		1000	NC	49
		10,000	NC	105
Pressurized Horizontal Vessel (flammable)	0.31	50	20	12
		100	26	15
		1000	NC	32
		10,000	NC	68

NC, the quantity is Not Credible.

Indeed, TATP is typically an explosive adopted for single-man suicide attacks. Hence, a maximum net charge of 50 kg can be transported, e.g., in a backpack. Quite clearly, a TATP attack can be only directed very close to a piece of equipment ($\approx$20–30 m, see Table 3.4.5).

An example of application of stand-off and damage distances to characterize the possible impact associated with direct IDE attack to process plants is shown in Section 4.1 and 4.3.

3.5 Conclusions

This chapter explored the key concepts of physical security assessment and their evaluation to support physical security studies dedicated to the process and chemical industry. Standard tools and methods based on recognized industrial practice, such as (American Institute of Chemical Engineers – Center for Chemical Process Safety (AIChE-CCPS), 2003; American Petroleum Institute (API), 2013; Garcia, 2006) were summarized in order to derive a consolidated conceptual basis. At the same time, examples of specific studies were reported. However, as the credibility of the threat against chemical and process industry facilities increases, the assessment of security-related and terrorism-related risks should be dealt with using approaches that are more systematic at a

quantitative level, in order to provide an objective measure of existing vulnerability, risk, and of the available level of protection with respect to external attack scenarios. Therefore, more advanced physical security assessment approaches, tools, and methods are needed, as discussed in Chapter 4 with examples and applications of recent developments in this field.

References

Ackermann, G., Abhayaratne, P., Bale, J., Bhattacharjee, A., Blair, C., Hansell, L., Al, E., 2007. Assessing Terrorist Motivations for Attacking Critical Infrastructure. Center for Non-Proliferation Studies, Monterey Institute of International Relations, Monterey, CA, USA.

American Institute of Chemical Engineers – Center for Chemical Process Safety (AIChE-CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers – Center of Chemical Process Safety, New York.

American Petroleum Institute (API), 2013. ANSI/API Standard 780 – Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry. American Petroleum Institute, Washington DC.

American Petroleum Institute, National Petrochemical & Refinery Association, 2003. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries.

Argenti, F., Landucci, G., 2016. Advanced attractiveness assessment of process facilities with respect to malevolent external attacks. Chem. Eng. Trans. 53, 133–138.

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.

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.

Bajpai, S., Gupta, J.P., 2007. Terror-proofing chemical process industries. Process Saf. Environ. Prot. 85, 559–565.

Bajpai, S., Gupta, J.P., 2005. Site security for chemical process industries. J. Loss Prev. Process. Ind. 18, 301–309.

Basco, A., Cammarota, F., Salzano, E., 2010. The risk of storage plant of pyrotechnics. Chem. Eng. Trans. 19, 231–236.

Baybutt, P., Ready, V., 2003. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homel. Def. J. 2.

Boba, R., 2009. Evil done. Crime Prev. Stud. 25, 71–92.

Borg, J., Cogar, J., Tredways, S., Yagla, J., Zwiener, M., 2001. Damage resulting from high speed projectile in liquid filled metal tanks. In: Computational Methods and Experimental Measurements. Wassex Institute of Technologies Press, Southampton, UK, pp. 889–902.

Bounds, W.L., 1997. Design of Blast Resistant Buildings in Petrochemical Facilities. ASCE Publications, Reston, VA, USA.

Buczkowski, D., Zygmunt, B., 2011. Detonation properties of mixtures of ammonium nitrate based fertilizers and fuels. Cent. Eur. J. Energ. Mater. 8, 99–106.

Casal, J., Darbra, R.-M., 2013. Analysis of past accidents and relevant case-histories. In: Domino Effects in the Process Industries: Modelling. Prevention and Managing, pp. 12–29.

Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.

CCPS − Center for Chemical Process Safety, 2008. Guidelines for Chemical Transportation Safety, Security, and Risk Management. American Institute of Chemical Engineers - Center of Chemical Process Safety, New York, NY.

Clark, W.R., 2009. Bioterrorism: a situational crime prevention approach. Crime Prev. Stud. 2, 93−109.

Clarke, R.V., Newman, G.R., 2006. Outsmarting the Terrorists. Praeger Security International, Westport, CT.

Corbett, G.G., Reid, S.R., Johnson, W., 1996. Impact loading of plates and shells by free-flying projectiles: a review. Int. J. Impact Eng. 18, 141−230.

Cozzani, V., Antonioni, G., Landucci, G., Tugnoli, A., Bonvicini, S., Spadoni, G., 2014. Quantitative assessment of domino and NaTech scenarios in complex industrial areas. J. Loss Prev. Process. Ind. 28, 10−22.

Cozzani, V., Gubinelli, G., Salzano, E., 2006. Escalation thresholds in the assessment of domino accidental events. J. Hazard Mater. 129, 1−21.

Cozzani, V., Krausmann, E., Reniers, G., 2013. Other causes of escalation. In: Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier B.V., Amsterdam, the Netherlands, pp. 154−174.

Cozzani, V., Reniers, G., 2013. Historical background and state of the art on domino effect assessment. In: Reniers, G.L.L., Valerio, C. (Eds.), Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier, Amsterdam, the Netherlands, pp. 1−10.

Cozzani, V., Tugnoli, A., Salzano, E., 2009. The development of an inherent safety approach to the prevention of domino accidents. Accid. Anal. Prev. 41, 1216−1227.

Darbra, R.M., Palacios, A., Casal, J., 2010. Domino effect in chemical accidents: main features and accident sequences. J. Hazard Mater. 183, 565−573.

European Commission, 2012. European parliament and council directive 2012/18/EU of 4 July 2012 on control of major-accident hazards involving dangerous substances, amending and subsequently repealing council directive 96/82/EC. Off. J. Eur. Communities L197, 1−37.

European Commission, 2003. Directive 2003/105/EC of the European parliament and of the council of 16 December 2003 amending council directive 96/82/EC on the control of major-accident hazards involving dangerous substances. Off. J. Eur. Communities L345, 97−105.

Freilich, J., Chermak, S., 2009. Preventing deadly encounters between law enforcement and American far-rightists. Crime Prev. Stud. 25, 141−172.

Garcia, M., 2008. In: The Design and Evaluation of Physical Protection Systems, second ed. Butterworth - Heinemann, Burlington, MA, USA.

Garcia, M., 2006. Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann, Newtown, MA.

Goldsmith, W., 1999. Non-ideal projectile impact on targets. Int. J. Impact Eng. 22, 95−395.

Gruenewald, J., Allison-Gruenewald, K., Klein, B.R., 2015. Assessing the attractiveness and vulnerability of eco-terrorism targets: a situational crime prevention approach. Stud. Confl. Terror. 38, 433−455. https://doi.org/10.1080/1057610X.2015.1009798.

Haimes, Y.Y., 2006. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Anal. 26, 293−296.

Hemmatian, B., Abdolhamidzadeh, B., Darbra, R.M., Casal, J., 2014. The significance of domino effect in chemical accidents. J. Loss Prev. Process. Ind. 29, 30−38.

Hu, B., Li, G., Sun, J., 2014. Numerical investigation of K4-rating shallow footing fixed anti-ram bollard system subjected to vehicle impact. Int. J. Impact Eng. 63, 72−87.

Jaeger, C.D., 2003. Chemical facility vulnerability assessment project. J. Hazard Mater. 104, 207−213.

Johansson, J., Hassel, H., Zio, E., 2013. Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems. Reliab. Eng. Syst. Saf. 120, 27–38.

Kadri, F., Châtelet, E., Chen, G., 2013. Method for quantitative assessment of the domino effect in industrial sites. Process Saf. Environ. Prot. 91, 452–462.

Kis-Katos, K., Liebert, H., Schulze, G.G., 2011. On the origin of domestic and international terrorism. Eur. J. Polit. Econ. 27.

Kourniotis, S.P., Kiranoudis, C.T., Markatos, N.C., 2000. Statistical analysis of domino chemical accidents. J. Hazard Mater. 71, 239–252.

Kriaa, S., Pietre-cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139, 156–178.

Kruglanski, A.W., Fishman, S., 2006. The psychology of terrorism: "syndrome" versus "tool" perspectives. Terror. Political Violence 18, 193–215.

Kuzmin, V.V., Solov'ev, M.Y., Tuzkov, Y.B., Kozak, G.D., 2008. Forensic Investigation of Some Peroxides Explosives. Cent. Eur. J. Energ. Mater. 5, 77–85.

Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Prot. 110, 102–114.

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.

Landucci, G., Tugnoli, A., Spadoni, G., Cozzani, V., 2012. LNG regasification terminals: assessment of accidents due to external acts of interference. In: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, pp. 4373–4382. PSAM11 ESREL 2012.

Lecysyn, N., Dandrieux, A., Heymes, F., Slangen, P., Munier, L., Lapebie, E., Gallic, C.L., Dusserre, G., 2008. Preliminary study of ballistic impact on an industrial tank: projectile velocity decay. J. Loss Prev. Process. Ind. 21, 627–634.

Lees, F.P., 1996. In: Loss Prevention in the Process Industries, second ed. Butterworth - Heinemann, Oxford.

Lefebvre, M.H., Falmagne, B., Smedts, B., 2004. Sensitivities and performances of non-regular explosives. In: Proc. VII Seminar on New Trends in Research of Energetic Materials. Pardubice, Czech Republic, pp. 164–173.

Levi, M., Doig, A., Gundur, R., Wall, D., Williams, M., 2017. Cyberfraud and the implications for effective risk-based responses: themes from UK research. Crime Law Soc. Change 67, 77–96.

Levitin, G., Gertsbakh, I., Shpungin, Y., 2011. Evaluating the damage associated with intentional network disintegration. Reliab. Eng. Syst. Saf. 96, 433–439.

Lou, H.H., Muthusamy, R., Huang, Y., 2003. Process security assessment: operational space classification and process security index. Process Saf. Environ. Prot. Trans. Inst. Chem. Eng. B 81, 418–429.

Marrone, S., Nardone, R., Tedesco, A., D'Amore, P., Vittorini, V., Setola, R., Cillis, F. De, Mazzocca, N., 2013. Vulnerability modeling and analysis for critical infrastructure protection applications. Int. J. Crit. Infrastruct. Prot. 6, 217–227.

Matteini, A., Argenti, F., Salzano, E., Cozzani, V., 2018. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2018.03.001.

Milazzo, M.F., Ancione, G., Lisi, R., Vianello, C., Maschio, G., 2009. Risk management of terrorist attacks in the transport of hazardous materials using dynamic geoevents. J. Loss Prev. Process. Ind. 22, 625–633.

Ministère de l'Ecologie du Développement durable et de l'Energie, 2016. ARIA (Analysis, Research and Information on Accidents) Database [WWW Document]. URL. http://www.aria.developpement-durable.gouv.fr/?lang=en.

Ministero dei lavori Pubblici, 2001. Decreto Ministeriale 9 Maggio 2001, Suppl. Ord. G. U. n.138 del 10/Giu/01, Requisiti minimi di sicurezza in materia di pianificazione urbanistica e territoriale per zone interessate da stabilimenti a rischio di incidente rilevante.

Moore, D.A., 2004. The new risk paradigm for chemical process security and safety. J. Hazard Mater. 115, 175–180.

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

Moore, D.A., Fuller, B., Jones, D.A., Hazzan, M., 2006. LNG security vulnerability assessment. In: AIChE Annual Meeting, Conference Proceedings.

National Academies, Department of Homeland Security, 2015. IED Attack Fact Sheet: Improvised Explosive Devices [WWW Document]. URL. https://www.dhs.gov/publication/ied-attack-fact-sheet#.

Nolan, D.P., 2008. Safety and Security Review for the Process Industries. Elsevier Inc., Amsterdam, the Netherlands.

Norman, T.L., 2010. Risk Analysis and Security Countermeasure Selection. CRC Press, Boca Raton, FL.

Orojloo, H., Azgomi, M.A., 2017. A method for evaluating the consequence propagation of security attacks in cyber–physical systems. Future Gener. Comput. Syst. 67, 57–71.

Pape, R.A., 2003. The strategic logic of suicide terrorism. Am. Pol. Sci. Rev. 97, 343–361.

Pavlova, Y., Reniers, G., 2011. A sequential-move game for enhancing safety and security cooperation within chemical clusters. J. Hazard Mater. 186, 401–406.

Price, M.A., Ghee, A.H., 2009. Modeling for detonation and energy release from peroxides and non-ideal improvised explosives. Cent. Eur. J. Energ. Mater. 6, 239–254.

Reniers, G., 2010. An external domino effects investment approach to improve cross-plant safety within chemical clusters. J. Hazard Mater. 177, 167–174.

Reniers, G., Cozzani, V., 2013. Features of escalation scenarios. In: Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier B.V., Amsterdam, the Netherlands, pp. 30–42.

Reniers, G., Soudan, K., 2010. A game-theoretical approach for reciprocal security-related prevention investment decisions. Reliab. Eng. Syst. Saf. 95, 1–9.

Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures w.r.t. domino effects. Process Saf. Environ. Prot. 92, 583–589.

Saaty, T.L., 1990. How to make a decision: the analytic hierarchy process. Eur. J. Oper. Res. 48, 9–26.

Salzano, E., Antonioni, G., Landucci, G., Cozzani, V., 2013. Domino effects related to explosions in the framework of land use planning. Chem. Eng. Trans. 31, 787–792. https://doi.org/10.3303/CET1331132.

Salzano, E., Basco, A., 2012. Comparison of the explosion thermodynamics of TNT and black powder using le chatelier diagrams. Propellants Explos. Pyrotech. 37, 724–731.

Salzano, E., Landucci, G., Reniers, G., Cozzani, V., 2014. Domino effects related to home-made explosives. Chem. Eng. Trans. 36, 349–354. https://doi.org/10.3303/CET1436059.

Scarponi, G.E., Landucci, G., Birk, A.M., Cozzani, V., 2018a. LPG vessels exposed to fire: scale effects on pressure build-up. J. Loss Prev. Process. Ind. 56, 342–358. https://doi.org/10.1016/j.jlp.2018.09.015.

Scarponi, G.E., Landucci, G., Heymes, F., Cozzani, V., 2018b. Experimental and numerical study of the behavior of LPG tanks exposed to wildland fires. Process Saf. Environ. Prot. 114, 251–270. https://doi.org/10.1016/j.psep.2017.12.013.

Schneider, P., Buchar, F., Zápeca, F., 1999. Structural response to thin steel shell structures due to aircraft impact. J. Loss Prev. Process. Ind. 12, 325–329.

Schultz, R., 1980. Conceptualizing political terrorism-a typology. In: Buckley, A.D., Olson, D.D. (Eds.), International Terrorism: Current Research and Future Directions. Avery, Wayne, NJ, pp. 9–15.

Schuurman, B., Eijkman, Q., 2017. Indicators of terrorist intent and capability : tools for threat assessment. Dyn. Asymmetric Confl. 8, 215–231.

Setola, R., Porcellinis, S.D., Sforna, M., 2009. Critical infrastructure dependency assessment using the input–output inoperability model. Int. J. Crit. Infrastruct. Prot. 2, 170–178.

Siegel, J.A., Saukko, P., 2012. In: Encyclopedia of Forensic Sciences, second ed. Academic Press, Elsevier, Amsterdam, the Netherlands.

Störfall Kommission (SFK), 2002. SFK-GS-38 Report.

Szala, M., Sabatini, J.J., 2018. 2,4,6-Trinitrotoluene – a useful starting compound in the synthesis of modern energetic compounds. J. Inorg. Gen. Chem. (Zeitschrift für Anorg. und Allg. Chemie) 644, 262–269.

U.S. Department of Justice, 2002. A Method to Assess the Vulnerability of U.S. Chemical Facilities. Office of Justice Programs, Washington DC. Report NCJ 195171.

Uijt de Haag, P.A.M., Ale, B.J.M., 1999. Guidelines for Quantitative Risk Assessment (Purple Book). Committee for the Prevention of Disasters, the Hague (NL).

Van Den Bosh, C.J.H., Weterings, R.A.P.M., 2005. Methods for the calculation of physical effects (Yellow Book). In: Committee for the Prevention of Disasters, third. ed. the Hague (NL).

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

Vellani, K., 2006. Strategic Security Management: A Risk Assessment Guide for Decision Makers. Butterworth-Heinemann, Oxford (UK).

Victoroff, J., 2005. The mind of the terrorist: a review and critique of psychological approaches. J. Confl. Resolut. 49, 3–42.

Weenink, A., 2012. Situational crime prevention and terrorism: remarks from the field of counterterrorism in the Netherlands on Newman and Clarke's policing terrorism. Rends Organ. Crime 15, 2–3.

Woo, G., 2009. Terrorism threat assessment and management. Def. Against Terror. Rev. 2, 101–116.

Woods, D., 2006. Essential characteristics of resilience. In: Leveson, N., Hollnagel, E., Woods, D. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Aldershot, pp. 21–34.

Yazdani, A., Otoo, R.A., Jeffrey, P., 2011. Resilience enhancing expansion strategies for water distribution systems: a network theory approach. Environ. Model. Softw 26, 1574–1582.

Yun, M., 2009. Application of situational crime prevention to terrorist hostage taking and kidnapping: a case study of 23 Korean hostages in Afghanistan. In: Freilich, J., Newman, G. (Eds.), Reducing Terrorism Through Situational Crime Prevention. Criminal Justice Press, Monsey, NY, pp. 111–139.

4 Physical security risk assessment tools and applications

This chapter deals with the implementation of the security concepts explained in Chapter 3 into comprehensive risk assessment methodologies. The theoretical aspects of standard security risk formulation, such as API 780 (American Petroleum Institute (API), 2013), are firstly implemented into standard tools for security risk assessment, as discussed in Section 4.1. Then, advanced tools based on graphical probabilistic models and innovative methods are shown in Section 4.2. Section 4.3 deals with emergency management and intervention. Specific case studies derived from realistic industrial layouts are presented and discussed, in order to support the reader in the application of both conventional and innovative methodologies. Finally, Section 4.4 gives some concluding remarks.

4.1 Existing security risk assessment tools

4.1.1 State of the art on security risk and vulnerability assessment

Systematic methodologies were developed in the last four decades to support the enhancement of industrial safety, which have been translated into consolidate practices as QRA (Quantitative Risk Assessment) and QARA (Quantitative Area Risk Assessment) studies (CCPS – Center of Chemical Process Safety, 2000; Cozzani et al., 2014; Lees, 1996; Matteini et al., 2018; Uijt de Haag and Ale, 1999).

In contrast, the risk of terrorist activity is not yet effectively considered and may vary significantly over time, depending on rather unpredictable social and political phenomena (European Commission, 2008). Assessing the risk of terrorist acts targeting industrial facilities is a challenging task for at least three reasons:

- There are few prior examples of terrorist acts targeting chemical or process facilities (Casson Moreno et al., 2018); nonetheless they exist, see also Chapter 2).
- Numerous external factors may increase or decrease security risks.
- Interactions among factors influencing security risks are dynamic and change over time (European Commission, 2008).

In part, these difficulties stem from the fact that terrorism is a phenomenon of multicausal factors and from the terrorists' deliberate efforts to defy prediction. The complexity of terrorism combined with the unique attributes of individual groups makes it nearly impossible to capture the explanatory characteristics of the phenomenon in a single model (European Commission, 2008).

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00004-4

For the aforementioned reasons, contributions available in the open literature are mostly speculative and qualitative. Early work on the topic started after 9/11, with the development of the so-called Security Vulnerability Assessment (SVA) methods (American Petroleum Institute and National Petrochemical & Refinery Association, 2003; Jochum, 2005; Störfall Kommission (SFK), 2002; Uth, 2005). In parallel, a number of scholars focused on the psychology of individual terrorists or group processes (Post et al., 2002).

Gupta (2004) started addressing terrorism's nature as a collective action and thus presented arguments rooted in economic and sociopsychological dimensions of human motivations. Few semiquantitative methodologies have been proposed or adopted in practice for the Security Risk Assessment (SRA) of different types of facility. Factors typically accounted for include the threat, the attractiveness of the asset to adversaries, the possible consequences and impacts of an incident, and the degree of vulnerability (American Petroleum Institute (API), 2013; Bajpai and Gupta, 2005; FEMA Federal Emergency Management Agency, 2005).

Despite minor differences being present among the different methods, a common stepwise process can be identified, including the main phases described in Table 4.1.1. More details on the required steps and phases may be found in Matteini et al. (2018).

Table 4.1.1 Steps typically adopted in currently available SRA methodologies.

		Method and reference				
		A	**B**	**C**	**D**	**E**
Phase	**Description**	**American Petroleum Institute (API) (2013)**	**FEMA Federal Emergency Management Agency (2005)**	**Bajpai and Gupta (2005)**	**Jochum (2005), Störfall Kommission (SFK) (2002), Uth (2005)**	**Srivastava and Gupta (2010)**
Step 1	Characterization and screening to determine critical assets	X	X	X	X	X
Step 2	Threat identification	X	X	X	X	X
Step 3	Attractiveness/asset value assessment	X	X			
Step 4	Vulnerability assessment	X	X	X		X
Step 5	Risk assessment	X	X	X		X
Step 6	Risk management: selection of required mitigation options and security upgrades	X	X		X	X

The cells marked with an "X" indicate that a step is included in a given method.

Adapted from 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.

The API standard 780 (American Petroleum Institute (API), 2013) suggests to adopt a systematic approach for security risk assessment. It is presented as a general-purpose SRA methodology applicable in compliance with the U.S. Department of Homeland Security (DHS) Chemical Facility Antiterrorism Standards to a broad range of assets and operations of the industry, including assets containing hazardous materials such as chemical, refining and petrochemical manufacturing operations, pipelines, and transportation operations.

According to API SRA methodology, the security risk is defined as an expression of the Likelihood (L) that a defined Threat (T) will find an asset Attractive (A) and successfully commit an act against it, taking advantage of Vulnerability (V) to cause a given set of security Consequences (C) (see also Chapter 1).

The following expression is proposed for risk evaluation:

$$R = (A \times T) \times V \times C = L_1 \times L_2 \times C \tag{4.1.1}$$

where L_1 is the likelihood of an attempted act against an asset, function of the Threat and the Attractiveness of the asset to the threat; L_2 is the likelihood of success of the act; in other words, it is the likelihood that the attack will circumvent or exceed the existing security measures, which is a measure of vulnerability of the asset to the threat.

The analysis can be performed semiquantitatively using a risk matrix and assessed through the use of expert judgment. The final objective is to assess security risks as a mean to support management in making informed decisions on the implementation and/or improvement of countermeasures to address the threats, vulnerabilities, and potential incident consequences.

It should be remarked that the SRA process is conducted as a scenario-specific analysis: one or more security scenarios are evaluated for each target asset−threat pair, resulting in a detailed analysis, quite demanding in terms of required time and resources (American Petroleum Institute (API), 2013). This scenario-specific approach best fits the needs of directly supporting the managerial decision process and of providing recommendations on security enhancement measures. A risk-based screening process is employed as the first step of the process to focus the analysis and resource attention on more critical events. The key variables considered in the risk screening analysis are “consequences” and “attractiveness.”

The phases described in Table 4.1.1 are prescribed also in the FEMA guidelines (FEMA Federal Emergency Management Agency, 2005) for the evaluation of the risk of potential terroristic attacks against buildings. In this case, scores are assigned to rate the Threat, Vulnerability, and Impact and then combined as follows:

$$R = T \times V \times I \tag{4.1.2}$$

In the work by Bajpai and Gupta (2005), a qualitative threat and vulnerability analysis was carried out and the security risk status of a plant was determined by filling in a table where scores ranging from 1 to 5 were assigned to relevant risk factors and then summed to evaluate the overall risk score. The method was recently updated in order to account for security safety barriers (Srivastava and Gupta, 2010).

A quite different perspective was considered in Lou et al. (2003). Assuming the threat of single or multiple disturbances set by technically knowledgeable attackers, the security risk analysis developed requires a high understanding of the process and of associated control systems and a technical expert to be performed. A process operational space classification method and a process operational security index were thus developed to define the degree of change (minor, moderate, several, or fatal) in operational status undergone by a process that experienced a disturbance.

Most of the above-described SRA methodologies (Bajpai and Gupta, 2005; Srivastava and Gupta, 2010; Störfall Kommission (SFK), 2002) are focused on the consequence assessment of possible scenarios triggered by a terrorist attack. In particular, SRA methodologies are aimed at the characterization of target facility, threat agent, threat (or attack mode) to support the impact estimation of potential attacks. However, a direct link between the impact and the attractiveness of process facilities, thus determining whether security triggered scenarios are credible, was not undertaken in the previously developed methods.

In this chapter, a benchmark case study is adopted in order to provide an example of advanced attractiveness assessment for a process facility; moreover an example of impact assessment is shown in order to evaluate the potential impact of accidents triggered by external acts of interference.

4.1.2 Definition of industrial case studies

This section illustrates the case studies defined to test the attractiveness and impact assessment methodologies.

In recent years, several projects of regasification terminals have been proposed and their realization is in progress (Paltrinieri et al., 2015). In a regasification terminal, LNG (Liquid Natural Gas) unloaded from LNG carriers is stored in liquid phase (about −160°C and 1−4 bar depending on the technology used) and is vaporized to reach the suitable conditions for delivery in the distribution network (about 75−80 bar and 10°C).

Due to the high amount of LNG stored during the process, this kind of facility may represent a critical target with respect to external threats. In the first case study (case A), a Floating Storage and Regasification Unit (FSRU) Moss or Membrane type, with regasification on board, is considered. The FSRU holds and processes up to 137,000 m^3 of LNG and is located 20 km off the West coast of Tuscany (Italy).

A second facility type is taken into account in order to provide a comparison among different kinds of industrial installations. In particular, a petroleum products storage and distribution terminal is considered for case B. The terminal is located onshore in the same industrial area of the FSRU and falls under the obligations of the EC “Seveso” Directive (European Commission, 2012). The input data for the application of the methodology are derived from the available plant information obtained by local competent authorities. This kind of facility features different types of stored and processed substances; hence, the potential impact of accidents may be considerably different.

A scheme for both kinds of industrial facilities is shown in Fig. 4.1.1; the LNG terminal is shown in Panel A, while the petroleum products terminal in Panel B. Table 4.1.2 summarizes the relevant information for the two facilities.

In order to test the influence of peculiar sociopolitical context in determining the perceived value of a potential terrorist target, two further case studies are defined: the petroleum products terminal is considered to be also located in Libya (case C) and the LNG terminal is considered to be installed in United Kingdom (case D).

Table 4.1.3 shows the summary of the defined case studies for the sake of clarity. The case studies will be adopted to show a potential application of the attractiveness assessment method described in Section 3.2 (example 1, Section 4.1.3) and the demonstration of security impact assessment studies (example 2, Section 4.1.4).

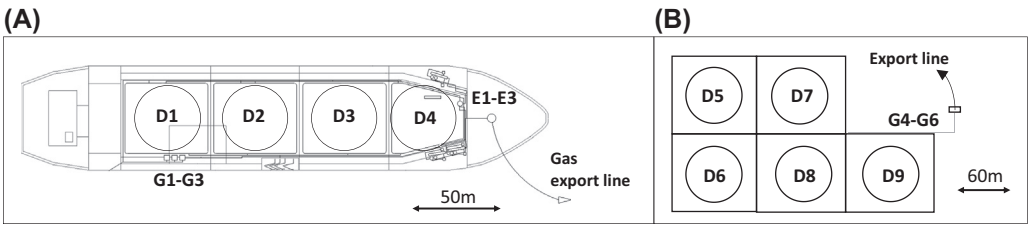


FIGURE 4.1.1 Schematic representation of the plant layout considered for the case studies: (A) LNG storage and regasification terminal (FSRU); (B) petroleum products storage and distribution terminal.

Table 4.1.2 Features of the tanks equipment considered in the case studies.

ID	Facility	Description	Volume (m^3)	Temperature (°C)	Pressure (barg)
D1—D4	LNG FSRU terminal	LNG spherical tanks	33,800 (each)	−161	3.0
G1—G3	LNG FSRU terminal	Booster pumps	—	−148	92.7
E1—E3	LNG FSRU terminal	Vaporizers	—	5	83.5
D5—D9	Petroleum products terminal	Petroleum products storage tanks	15,000 (each)	20	0.2
G4—G6	Petroleum products terminal	Pump system	—	50	10.0

4.1.3 Example 1: the use of attractiveness as proxy for likelihood

As mentioned in Chapter 3, literature methods do not systematically address attractiveness of process facilities to site-specific hazards, related to the inventories of substances and to the vulnerability of the surrounding areas. Moreover, the integration of this type of evaluation with aspects related to the social, economic, and political contest is not available in other methods and would be beneficial for a more structured evaluation of process facilities attractiveness. In this section, the method for

Table 4.1.3 Summary of the case studies considered for the application of the methodologies.

	Features of the case study			
Case ID	**Type of facility**	**Location 1 (Italy)**	**Location 2 (Libya)**	**Location 3 (UK)**
Case A	LNG FSRU terminal — offshore	X		
Case B	Petroleum products terminal, onshore, industrial area	X		
Case C	Petroleum products terminal, close to residential areas		X	
Case D	LNG FSRU terminal, industrial area			X

The cells marked with an "X" indicate that the feature is attributed to the case study.

attractiveness assessment described in Section 3.2.4 is applied to the four case studies summarized in Table 4.1.3, providing the advantage of considering either hazard-based technical factors or geopolitical, ideological, and strategic incentives.

4.1.3.1 Hazard-based attractiveness evaluation

The procedure for hazard-based attractiveness evaluation and related hazard-based attractiveness index (I_H) is discussed in Section 3.2.4.1. Table 4.1.4 summarizes the input data for applying the method and the evaluated indexes are shown in Table 4.1.5.

Table 4.1.4 Summary of input data for the evaluation of hazard-based facility index I_H.

		Input			
Parameter	**Description**	**Case A**	**Case B**	**Case C**	**Case D**
Substance	Reference substance or substance category in the facility	LNG	Petroleum products	Petroleum products	LNG
Substance category	Flammable or toxic	Flammable	Flammable	Flammable	Flammable
W	Total inventory of substance or substance category in the facility (t)	80,000	67,500	67,500	80,000
T	Associated thresholds value (t)	200	2,500	2,500	200
Impact	Impact area radius (km) based on worst case accident	1	1	1	1
Population density	Population density in the potential impact area (inhabitants/km^2)	0	3,150	4,500	2,570
Population	Population in the potential impact area (inhabitants)	0	9,890	14,130	8,070
Vulnerability centers	Number of vulnerability centers	0	Not considered[a]	Not considered[a]	Not considered[a]

[a]Relevant only for population density <2000 inhabitants/km^2.

Data were derived from 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.

Table 4.1.5 Summary of indexes supporting the evaluation of hazard-based facility index based on Argenti et al. (2015).

Index	Description	Equation (see Section 3.2.4.1)	Case A	Case B	Case C	Case D
J^{fl}	Flammable substance index	Eq. I in Table 3.2.1	400	27	27	400
I_{fl}	Flammable substance overall index	Eq. G in Table 3.2.1	400	27	27	400
I_{tox}	Toxic substances index	No toxic substances are present on the considered process facility	0	0	0	0
I_{sub}	Hazardous substances index	Eq. F in Table 3.2.1	400	27	27	400
I_{SH}	Site hazard index	Eq. C in Table 3.2.1	5	2	2	5
I_p	Population index	Eq. D in Table 3.2.1	1	2	3	2
I_{vc}	Vulnerability centers index	Relevant only for population density <2000 inhabitants/km^2	0	0	0	0
I_{TV}	Territorial vulnerability index	Eq. B in Table 3.2.1	1	2	3	2
I_H	Hazard-based attractiveness index	Eq. A in Table 3.2.1	6	4	5	7

The hazard-based evaluation mainly relies on the estimated potential impact distance of accident scenarios involving the hazardous materials present on each site. Hence, the higher flammables inventory of LNG terminals (installation A and D) leads to higher I_{FH} indexes than the other facilities, in which lower quantities of petroleum products are stored (installation B and C).

As far as the vulnerability analysis of the area surrounding the industrial site is concerned, the offshore LNG terminal (installation A) does not affect the population, being about 10 km far from the coast. Hence, the minimum vulnerability I_{TV} index is assigned. Installations B and D are located onshore in industrial areas; hence, the impact on the population is limited. On the contrary, installation C is located close to the population, thus with increment of the I_{TV} score.

4.1.3.2 Evaluation of nontechnical triggers

Besides considering the destructive potential of a successful attack, threat agents may have other incentives to attack a facility. In order to assess the influence of nontechnical triggers to the overall attractiveness of the considered facilities, the effect of locating the different areas is accounted for through the procedure described in Section 3.2.4.2.

The considered locations feature different political and social conditions. For Locations 1 and 3 (i.e., Italy and United Kingdom, respectively), a context of peace time is assumed, yet the absence of dedicated antiterrorism rules and practices is evidenced. However, in the case of the offshore LNG terminal in Italy (case A), many records of protests held by environmental activists and by organized committees of citizens against the project are found in local as well as national newspapers (Allegri, 2010; Cucchi, 2010; Pieraccini, 2012). This supports the evidence of a social context featuring lack of

communication and mistrust between local population, public authorities, and the operating company, which is not featured by the UK installation (case D). In Location 2 (i.e., Libya), the country political instability and the documented presence of terrorist cells moved by political and religious motives are considered, as also confirmed by several news agencies (Al Arabiya News, 2014; IRIN, 2014; Said and Faucon, 2014). Finally, for the sake of simplicity, private ownership of the companies for the four plants and the absence of strategic targets in the proximity of the plants are assumed.

The relevant aspects discussed in Section 3.2.4.2 are reported in Table 4.1.6 together with the correspondent weight and the assigned score. This leads to the evaluation of the attractiveness increase index F, which supports the calculation of the induction index φ for the four cases considered. As shown in Table 4.1.6, the relevant terrorist threat featured by Location 2 (case C) causes a relevant increment of F. In fact, taking into account the documented presence of armed factions and the possible presence of terrorist cells, blamable of violent actions and generally of the unstable political situation in Location 2 (Libya), the obtained F index is higher by almost one order of magnitude than the one calculated for the other locations. However, it is also worth mentioning that relevant increment of attractiveness is due to the local aversion of population for a specific facility or technology. In fact, despite installations for cases A and B being located in the same geographical area (i.e., Italy), the evidence of aversion against LNG-based technologies in case A leads to an F value that is seven times higher than the one for case B.

The combined evaluation of technical and nontechnical triggers allows the assessment of the overall attractiveness index I_A for each plant in the two locations, as summarized in Fig. 4.1.2C, also showing the qualitative attractiveness ranking for the other relevant indexes (I_H and F, respectively in Fig. 4.1.2A and B).

Table 4.1.6 Results of the evaluation of nontechnical triggers: overall attractiveness increase index (F) and induction index (φ).

Aspect ID	Description	Weighed score	Case A	Case B	Case C	Case D
S1	Public company ownership	$\sigma_1 w_1$	0.000	0.000	0.000	0.000
S2	Presence of third-party highly attractive targets	$\sigma_2 w_2$	0.000	0.000	0.145	0.000
S3	Presence of chemicals that can be used as WMD	$\sigma_3 w_3$	0.000	0.000	0.145	0.000
S4	Past threat history	$\sigma_4 w_4$	0.000	0.000	0.169	0.000
S5	Terrorists/activists activity in the area	$\sigma_5 w_5$	0.000	0.000	0.145	0.000
S6	Political instability	$\sigma_6 w_6$	0.041	0.000	0.082	0.000
S7	Ease in weapons gathering	$\sigma_7 w_7$	0.033	0.033	0.065	0.000
S8	Local aversion due to company reputation	$\sigma_8 w_8$	0.036	0.000	0.000	0.000
S9	Aversion due to lack of local stakeholders engagement and awareness of technology	$\sigma_9 w_9$	0.073	0.000	0.000	0.000
S10	Aversion due to economic/environmental reason and/or interactions with cultural heritage	$\sigma_{10} w_{10}$	0.073	0.000	0.036	0.000
F	Overall attractiveness increase index	–	0.255	0.033	0.786	0.000
φ	Induction index	–	1.255	1.033	1.786	1.000

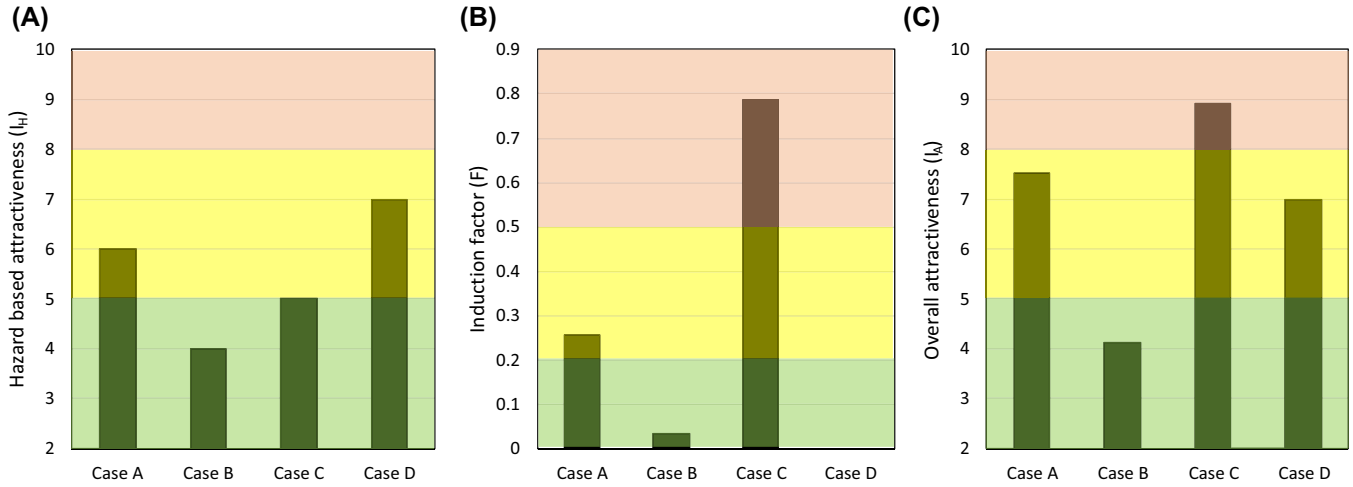


FIGURE 4.1.2 Results of the attractiveness assessment for the four case studies: (A) hazard-based attractiveness index I_H, (B) induction factor F, (C) overall attractiveness index I_A. Qualitative ranking is also reported (green [light gray in print version] = low, yellow [white in print version] = medium, red [gray in print version] = high).

From the present analysis, it may be concluded that hazard-based evaluation of the potential events following a terrorist attack relevantly affects the attractiveness of a given site. However, capturing sociopolitical aspects, as well as ideological and strategic incentives to an attack, is relevant for having a holistic evaluation of attractiveness, which may be strongly increased in a high-risk geopolitical area.

4.1.4 Example 2: the consequences and impact assessment of security-related scenarios

The methodology described in Section 3.4 is applied to the two types of facilities considered in the present study in order to compare the potential outcomes associated with different types of external acts of interference.

Firstly, a preliminary equipment hazard ranking is carried out identifying the most critical items in each plant, as shown in Table 4.1.7. As shown in the table, for both types of facilities, the most critical equipment are the storage tanks and the transfer lines, including pumps. However, due to the inherent physical/chemical properties of LNG (Iannaccone et al., 2019; Ovidi et al., 2019; Scarponi et al., 2016), a higher ranking is associated with the FSRU equipment, thus potentially leading to more severe events.

Once having targeted the most relevant equipment in each facilities, consequence assessment is carried out. Integral models for the estimation of physical effects are adopted to determine the impact of accidents triggered by external acts of interference (Van Den Bosh and Weterings, 2005) according to the procedure described in Section 3.4. Operative conditions of each piece of equipment represented in Fig. 4.1.1 are summarized in Table 4.1.2; LNG composition is schematized as pure methane in the simulations (Ovidi et al., 2019), while pure n-heptane is considered in each tank of the petroleum products terminal. In this latter case, the storage tanks are provided with a containment dike with a total area of 1.2×10^4 m^2.

Table 4.1.7 Preliminary hazard ranking of the equipment considered in the case studies.

Equipment type → / Physical conditions of inventory ↓	Storage tanks	Large diameter pipelines	Column-type equipment	Reactors/shell & tube equipment
Liquefied gas stored under pressure	4	4	3	3
Fluids with low vapor pressure stored in liquid phase	3	3	2	2
Gas/liquid stored in gas phase	3	2	2	1
Cryogenic storage	**2**[a]	**2**[a]	2	1
Liquid phase	**1**[b]	**1**[b]	1	1

Numbers in **bold** character are associated with a relevant piece of equipment analyzed in the impact assessment.
[a]Equipment present in the LNG FSRU terminal.
[b]Equipment present in the petroleum products terminal.

The impact assessment is summarized in Tables 4.1.8 and 4.1.9 for the LNG FSRU and petroleum products terminal, respectively. For the sake of brevity, only the highest damage distance associated with each act of interference is reported, despite the fact that multiple scenarios might be triggered. The tables evidence the equipment that might be potentially affected by the attack, excluding noncredible acts of interference. Then, for each credible target, the resultant loss of containment event is identified according to the procedure described in Section 3.4. Finally, the expected worst-case scenario is reported.

Table 4.1.8 Worst-case consequences for each attack mode for the LNF FSRU terminal.

Act of interference	Equipment and substance	Expected LOC event	Scenario	Damage distance offshore (m)
Deliberate misoperation	D01—D04	R1	FF	70
Interference by simple means	G01—G03	R1	FF	50
Interference by major aids	LNG pipe	R1	FF	30
Arson by simple means	LNG pipe	R5	JF	585
Arson by incendiary devices	LNG pipe	R4	JF	115
Shooting (minor)	LNG pipe	R4	JF	110
Shooting (major)	D01—D04	R3	PF	2000
Explosives	D01—D04	R2	PF	1100
Ship impact	D01—D04	R3	PF	2000
Plane impact	D01—D04	R3	PF	2000

For LOC (loss of containment) events definition, refer to the method described in Section 3.4. *FF*, flash fire; *JF*, jet fire; *PF*, pool fire.

Table 4.1.9 Worst-case consequences for each attack mode for the petroleum products terminal.

Act of interference	Equipment and substance	Expected LOC event	Scenario	Damage distance onshore (m)
Deliberate misoperation	D05—D09	R1	PF	80
Interference by simple means	Transfer pipeline	R1	PF	140
Interference by major aids	Transfer pipeline	R1	PF	140
Arson by simple means	D05—D09	R2	PF	370
Arson by incendiary devices	Transfer pipeline	R5	PF	370
Shooting (minor)	G04—G06	R4	PF	200
Shooting (major)	D05—D09	R3	PF	440
Vehicle or plane impact	D05—D09	R3	PF	440

For LOC (loss of containment) events definition, refer to the method described in Section 3.4. *PF*, pool fire.

For certain acts of interference, such as catastrophic impact, arson, shooting, and explosives, immediate ignition probability is largely higher than in usual situations following "process" failure modes; hence, some of the scenarios due to delayed ignition (e.g., flash fire or vapor cloud explosion) were considered less credible and not simulated.

However, in some of the considered acts of interference, LNG damages may be due to the delayed ignition of the vapor cloud formed after the release, such as in the case of minor misoperations, which, however, lead to limited damage extension. Instead, in the case of the petroleum products terminal, due to the low volatility of n-heptane compared to other lighter hydrocarbons, the most severe scenario is the pool fire in all the simulated cases.

Fig. 4.1.3 reports the worst-case scenario damage circle for each installation, identifying the area affected by the scenario superimposed on the map of each considered location. In the case of the offshore terminal, the impossibility of postrelease containment coupled with the higher damage potential of LNG results in a higher impact compared to the onshore terminal for petroleum products. One order of magnitude difference is obtained in the predicted damage distance. However, due to the geographical position, the impact is with no foreseen consequences on the population in vulnerable areas (see Fig. 4.1.3). At the same time, despite the presence of a dike, which reduces the surface and thus the consequences of the pool fire associated with catastrophic release, it can be seen that the onshore terminal has the potentiality to affect vulnerable residential areas surrounding the plant. Hence, in case of evidence of terrorist activities, the attractiveness of this kind of facility may be considered relevant, to the high damage potential, as determined also in the analysis presented in Section 4.1.4.

It can be concluded that impact assessment of security-related scenarios may provide relevant information for the sound evaluation of the attractiveness of a given site and to support the emergency management in the surrounding areas.

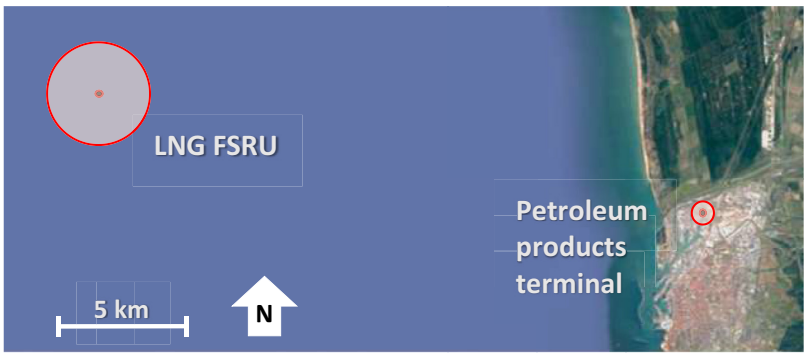


FIGURE 4.1.3 Impact analysis: maximum damage area (*red [black in print version] circles*) associated with the worst-case scenario of each considered facility superimposed on the considered industrial layout and vulnerability centers.

4.2 Advanced tools for security assessment of chemical facilities

4.2.1 Introduction to the advanced tools

Section 4.1 discussed several security risk assessment methodologies, such as those proposed by the American Petroleum Institute (API) (2013) and the American Institute of Chemical Engineering (American Institute of Chemical Engineers – Center for Chemical Process Safety (AIChE-CCPS), 2003). These techniques offer a valid support to operators (site-security managers, safety/security practitioners, etc.) in assessing and managing security risks in chemical facilities. In fact, they provide general guidance for security risk mitigation and lists of possible solutions in terms of security countermeasures depending on the existing security alert level (Norman, 2010).

Nevertheless, the aforementioned techniques only allow for a qualitative or a semi-quantitative (e.g., in the case of API methodology) assessment of security risk. Thus, as the credibility of the threat against chemical and process industry facilities increases, the assessment of security-related and terrorism-related risks should be dealt with using more systematic approaches at a quantitative level, in order to provide an objective measure of existing vulnerability as well as of the available level of protection with respect to external attack scenarios.

This section offers an overview of possible advanced mathematical tools that may be adopted in order to support security risk and vulnerability studies dedicated to process facilities. More specifically, the analysis is focused on outsiders' threat against chemical and process industry facilities and, particularly, high-consequence loss physical assets within the facility (i.e., process equipment, storage tanks, etc.). The focus is further narrowed down to the type of security events that may involve direct damage to process equipment, leading to loss of containment and, thus, to the release of hazardous substances that, in turn, may result in a major accident or extensive environmental contamination.

A probabilistic risk analysis approach, supported by a Bayesian Network, is firstly presented in Section 4.2.2. The model is dedicated to the assessment of industrial facilities vulnerability to the specific type of external attacks. Section 4.2.3 deals with the application of graph theory as a simplified but reliable alternative to complex Bayesian Network to vulnerability assessment of chemical plants. Vulnerability assessment is also discussed in Section 4.2.4, introducing the application of multicriteria decision analysis based on Analytic Network Process (ANP).

The approaches and tools presented in the following are suggested for implementation to the analysis of existing installations by security managers and risk analysts as they provide a quantitative tool to conduct scenario-based security risk and vulnerability assessment.

4.2.2 Application of Bayesian Networks to vulnerability assessment of chemical plants

4.2.2.1 Overview

The first example of advanced security study supported by a graphical mathematical tool is based on the development of a Bayesian Network (BN) model. This was adopted for the assessment of industrial facilities vulnerability to the specific type of external attacks (Argenti et al., 2018, 2016a,b). The approach and BN-based model presented herein are suggested for implementation to the analysis of existing installations by security managers and risk analysts as they provide a simplified but quantitative tool to conduct scenario-based vulnerability assessment.

In this section, vulnerability is intended as the proxy for the likelihood of external attack success. This interpretation of vulnerability is in agreement with the risk formulation proposed in API Recommended Practice 780 (American Petroleum Institute (API), 2013) as described in Section 4.1 (see Eq. 4.1.1). As pointed out by Garcia (2006), performance-based vulnerability assessment is recommended for facilities with high-consequence loss physical assets. Furthermore, vulnerability assessment would benefit from a quantitative analysis of the likelihood of attack scenarios' success, as it would provide a measure of the available level of protection and it would allow obtaining a sufficient analysis resolution to identify weak elements and security functions that need improvement. Hence, vulnerability assessment included in this section is a rather detailed effectiveness assessment of physical security system. This was carried out adopting the metric proposed in Garcia (2006) and making use of the results of a study on the performance assessment of Physical Protection Systems (PPSs) in chemical plants presented in Argenti et al. (2017), which is further discussed in Section 5.3.

Attack success was herein interpreted as the successful accomplishment of the attack scenario by damaging process and storage equipment in a given facility. The attack scenario is characterized in a simplified manner through the identification of attack mode, target and adversary path, and sequence of action toward the target equipment. Starting from this consideration, the vulnerability analysis took into account the uncertainty in adversary's choices in terms of attack mode and path, the presence and effectiveness of PPS elements that may have a preventive function with respect to attack success and the residual resistance of process equipment while exposed to impact vector that may result from an intentional attack. A scenario-based approach was privileged to conduct vulnerability analysis as it best fits the aim of directly supporting the managerial decision process and of providing recommendations on the implementation and/or improvement of security countermeasures (American Petroleum Institute (API), 2013).

4.2.2.2 Description of the probabilistic model supporting the vulnerability assessment

BN is a graphical method of reasoning under uncertainty using probabilities (Jensen and Nielsen, 2007). BNs are direct acyclic graphs, where nodes represent random variables and arcs represent dependencies of different nature between the variables (causal

dependencies, sequential order etc.). In fact, the position and orientation of arcs specify the independence assumptions that hold between the variables. These independence assumptions determine that the probability information required to specify the probability distribution among the variables of the network is limited to the assessment of marginal probability associated to all root nodes and the conditional probabilities of nonroot nodes given their immediate predecessors (Jensen and Nielsen, 2007). In other words, using the chain rule and d-separation rule, BN allows factorizing the joint probability distribution of variables $P(\mathrm{U})$, whose generalized formulation is provided in Eq. (4.2.1), in terms of local dependencies only, as given by Eq. (4.2.2).

$$P(\mathrm{U}) = P(\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3, \ldots \mathrm{v}_\mathrm{n}) = P(\mathrm{v}_1) \cdot P(\mathrm{v}_2|\mathrm{v}_1) \cdot \ldots P(\mathrm{v}_n|\mathrm{v}_1, \mathrm{v}_2, \ldots \mathrm{v}_{\mathrm{n}-1}) \tag{4.2.1}$$

$$P(\mathrm{U}) = \prod_{\mathrm{i}=1}^{\mathrm{n}} P(\mathrm{v}_\mathrm{i}|\mathrm{Pa}(\mathrm{v}_\mathrm{i})) \tag{4.2.2}$$

where $\mathrm{Pa}(\mathrm{v}_\mathrm{i})$ is the parents' set of variable v_i.

BN may be applied to forward as well as backward reasoning through evidence propagation along the network and probability updating. BN takes advantage of Bayes' theorem to update the probability of variables given new information E to yield the updated probability (Jensen and Nielsen, 2007):

$$P(\mathrm{U}|\mathrm{E}) = \frac{P(\mathrm{U}, \mathrm{E})}{P(\mathrm{E})} = \frac{P(\mathrm{U}, \mathrm{E})}{\sum_{\mathrm{U}} P(\mathrm{U}, \mathrm{E})} \tag{4.2.3}$$

BN was selected as modeling tool as it permits to merge knowledge of diverse natures in one model: data from feedback experience, experts' judgment (expressed through logical rules, equations, or subjective probabilities) and observations (Weber et al., 2012).

With respect to possible alternative quantitative methods, such as attack trees shown in (Garrick et al., 2004), the present method takes advantage of BN capability to update marginal probability distributions in real time as new information is revealed and to capture noncausal influences.

Fig. 4.2.1 shows the BN model proposed to support probabilistic vulnerability assessment. HUGIN Researcher Software (http://www.hugin.com/) was used to BN development and applied to BN computation.

The proposed network, once quantified, allowed for the assessment of multiple aspects that determine facility vulnerability throughout the timeline of security events, from emergence of the threat analyzed in terms of foreseen attack scenarios, through its development and the intervention of preventive security measures and systems, to attack effects.

Clearly enough, the structure of the BN has generalized validity; conversely, the quantitative analysis of the network (i.e., the selection of the number nodes states and the quantification of conditional probability tables) has to be carried out considering the specific features of the industrial site under analysis and may involve the choice of including a reduced number of nodes or node states.

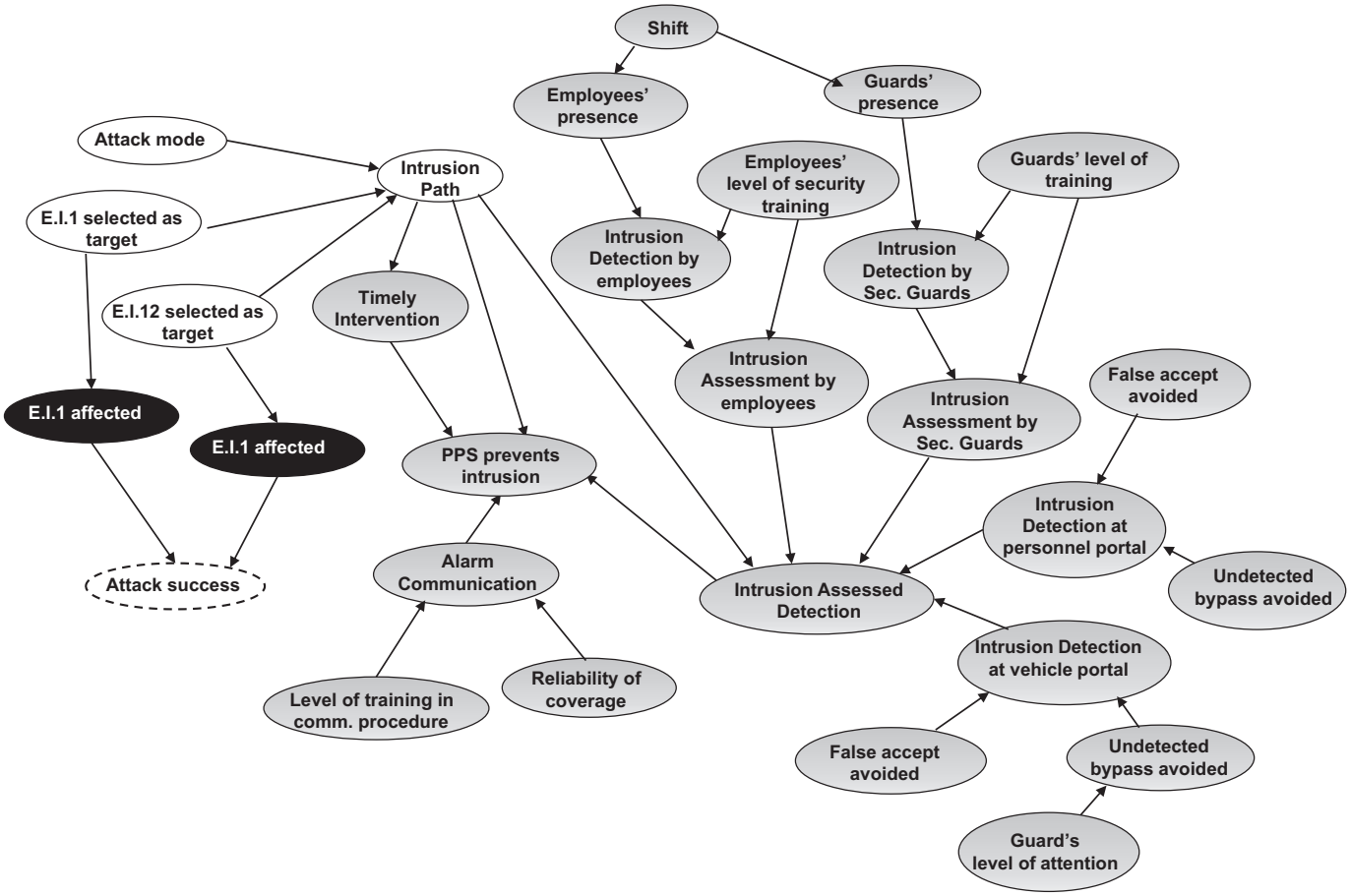


FIGURE 4.2.1 BN model developed for the present analysis. *Adapted from Argenti, F., Cozzani, V., Landucci, G., Reniers, G., 2016a. Probabilistic vulnerability analysis of process facilities to external acts of interference. In: Risk, Reliability and Safety: Innovating Theory and Practice - Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016, p. 344.*

4.2.2.2.1 Attack scenario

In order to conduct a scenario-based analysis, a schematization of the elements that allow for the characterization of an attack scenario was proposed (see nodes in white color in Fig. 4.2.1). The key variables of the model are the equipment selected as target, the attack mode selected by an adversary to cause damage, and the path (in other words, the sequence of actions) needed to damage the selected target through the selected attack mode. In Fig. 4.2.1, two possible targets are consider in order to exemplify the application of the BN model (namely, E.I.1 and E.I.2), but the framework may be easily extended to multiple targets.

A node for each equipment item storing hazardous materials in the facility was introduced to represent the uncertainty associated with the chance of that equipment item being selected as target. The probability of an equipment item being selected as target may be directly set by the user to 1, then evaluating the vulnerability of the protection system for a specific target under evaluation. Otherwise, the simplified attractiveness assessment described in Section 3.2.4.1 may be adopted in order to screen among alternative equipment and derive the probability that a given target is selected for the attack in a simplified manner.

The states of node "attack mode" were determined starting from the classification presented in Störfall Kommission (SFK) (2002) and are described in Table 4.2.1. The assignment of the marginal probabilities of the attack occurring according to a specific attack mode is left to the analyst, based on previous characterization of the adversaries and their presumed capability and weapons.

The node "path" has a number of states equal to m + 1. The number "m" and specific identification of paths to be accounted for are to be selected by the analysis based on site-specific considerations. This process is known among physical security risk analysts as "path analysis" and was exemplified in Section 3.3.4. Clearly enough, only a subset of the m identified paths has a nonnull conditional probability of being selected by the adversary given that a specific target equipment is selected as target (i.e., all paths starting from outside the perimeter whose arrival point is the location of the specific target equipment).

The (m + 1)-th state of node "path" corresponds to "no intrusion." It has a conditional probability of occurrence equal to 1 given all attack modes that represent physical interference at a distance, i.e., interference actions that can be carried out from outside the facility without requiring perimeter trespassing nor intrusion, for instance, shooting 2 or aircraft impact (see Table 4.2.1). As first estimate, the values to populate the CPT (conditional probability tables) of the "path" node can be based on expert judgment (Garcia, 2006).

4.2.2.2.2 Physical protection system effectiveness

The nodes shown in gray color in Fig. 4.2.1 constitute the submodel, i.e., the BN portion, used to analyze the effectiveness of PPS and its contribution in probabilistically determining the outcomes of an attack.

Table 4.2.1 States of the node "attack mode."

State	Description	Success criterion	Intrusion required
Deliberate misoperation	Deliberate acts with simple operations without the use of instruments	Target equipment location is reached	Yes
Interference using simple aids	Deliberate interference using tools and aids that are present on site	Target equipment location is reached	Yes
Interference using major aids	Prepared destruction of installation parts by force	Target equipment location is reached	Yes
Arson using incendiary devices	Incendiary attacks	Target equipment is damaged by fire heat load	Yes
Use of explosives (military or IED[a])	Use explosives to blow up equipment or load-bearing structures to cause their collapse	Target equipment is damaged due to overpressure	Yes/No
Shooting 1	Interference at close distance, using different types of weapons	Target equipment is damaged due to projectile impact	Yes
Shooting 2	Interference at distance, using different types of heavy weapons	Target equipment is damaged due to projectile impact	No
Vehicle accident	Vehicle accident in the establishment aimed to release hazardous substances or damage/destroy important parts of the installation	Target equipment is damaged due to vehicle impact	Yes
Aircraft accident	Aircraft accident aimed to release hazardous substances or damage/destroy important parts of the installation	Target equipment is damaged due to aircraft impact	No

[a]*IED*, improvised explosive devices.

Among the four independent security layers of physical security to manage the risk of a terrorist attack against a given facility (namely, deter, prevent, protect, and contain) identified by Nunes-Vaz et al. (2011), our study focused on the "prevent" layer. In turn, it is based on stopping the attack event sequence and requires the coordination of security functions of "detection," "alarm assessment," "alarm communication," "delay," and "response" to the accomplishment of its protection objectives (Garcia, 2006, 2008; Nunes-Vaz et al., 2011). More details on the security functions of the PPS system are given in Section 5.3.

As it can be noticed from the submodel structure, the effectiveness of PPSs was intended as an overall performance variable measured as the probability of successful PPS intervention, which was derived through a functional analysis of the PPS and modeled as dependent on an adversary's path. The Sandia effectiveness metric (Garcia, 2006) was followed in the modeling of "intrusion assessed detection," "alarm communication," and "timely response force intervention" as parent nodes of "PPS prevents intrusion." A modular structure can be evidenced for the gray nodes in Fig. 4.2.1: the

modules included in the network were selected to mirror the PPS elements, and associated most relevant influencing factors, that are used in a representative set of European industrial sites where relevant quantities of hazardous substances are stored or processed. This information was derived from an expert judgment exercise in which specific data were gathered (Argenti et al., 2017).

In the submodel, the leaf node "PPS prevents intrusion" features a binary state, as it was deemed necessary only to distinguish between successful and unsuccessful denial strategy execution, leading respectively to the attack being stopped by the defenders and to the attack being fully accomplished by the adversaries. The states of the nodes representing overall performance variables (selected according to Sandia method) were kept binary, in order to remark the strong logical relation among all the PPS functions. The states of the nodes representing variables and influencing factors were as well kept binary, distinguishing between a favorable and an unfavorable state with respect to the functional subsystem effectiveness in performing its design function.

The quantitative performance data for the PPS functions and elements were derived from a previous study (Argenti et al., 2017), in which the authors performed the expert elicitation of the following query variables:

- the marginal probability of occurrence of the favorable state of each influencing factor identified as relevant;
- the conditional probability of successfully performing the security function, given that all identified influencing factors are in favorable state (this was considered as "baseline" to represent the best case in which the security function could be performed);
- the measure of impact, to be estimated as a multiplicative factor (<1), that each influencing factor has on the "baseline" conditional probability if it changes from the favorable to the unfavorable state.

Model quantification was carried out using the aggregate performance data derived from expert consultation: more specifically, the median values of probabilistic estimates provided by experts were selected as aggregate performance variables and applied. CPTs' characterization was carried out by calculating probability of success in performing the design security function as follows:

$$P = P_0 \cdot \prod_{h=1}^{Q} (X_h \cdot r_h) \tag{4.2.4}$$

where Q is the number of factors and variables that (independently) affect the performance of the security barrier, P_0 is the baseline conditional probability representing the probability of the security barrier successfully performing its function given that all influencing factors are in the favorable state (most favorable conditions to success are present), r_h is the measure of the unfavorable impact on the baseline conditional probability P_0 from changing the state of the h-th influencing factor from the favorable state to the unfavorable state and assuming that all other influencing factors are still in

the favorable state, and $X_h = 1$ if the h-th influencing factor is in its unfavorable state, while $X_h = 1/r_h$ if the h-th influencing factor is in its favorable state.

A direct dependency on an adversary path has been taken into account for the overall security function of assessed detection of an intrusion attempt and of timely intervention of the response force.

The successful assessed detection at system level is possible if successful assessed detection occurs at least at one of the Rings of Protections (RoP) implementing security barriers suitable to perform the detection function that are crossed by adversary's path. Therefore, the CPT of the node "assessed detection" is populated as if it represents an OR-gate among the nodes representing assessed detection at the different RoP but accounting for path analysis results. In particular, given that the m-th path is considered, the probability of having a successful assessed detection is calculated as follows:

$$P_{\text{success\_m}} = 1 - \prod_{l=1}^{N_l} (1 - \alpha_{l \cdot m} \cdot P_{\text{success,l}}) \tag{4.2.5}$$

where $P_{\text{success,l}}$ is the probability of successful assessed detection at the l-th RoP; $\alpha_{l \cdot m} = 1$ if the l-th RoP is crossed by the m-th path and $\alpha_{l \cdot m} = 0$ otherwise.

The probability of having a timely intervention by the response force depends on the response force intervention time and on the cumulative delay accumulated by the adversary to overcome existing delay barriers, which varies depending on the path. Eq. (4.2.6) was used to calculate the probability of timely intervention along the m-th path, (P_{T_m}) as suggested in (Garcia, 2006):

$$P_{T\_m} = \frac{1}{\sqrt{2\pi(\sigma_{RTF}^2 + \sigma_D^2)}} \int_0^{T_m} \exp\left(- \frac{T_m^2}{\sqrt{2\pi(\sigma_{RTF}^2 + \sigma_D^2)}} \right) dT_m \tag{4.2.6}$$

where $T_m = \sum_{i\_m} T_{D,i} - RFT$; $T_{Di,m}$ is the penetration time for the i-th delay barrier present along the m-th path; RFT is the response force time. A normal distribution was assumed for all parameters related to time. Data on the mean and variance of the normal distribution of delay times associated to barriers can be retrieved from Garcia (2008); while the mean value of response force intervention time is supposed to be known and a variance of 30% can be considered as a first estimate (Garcia, 2008). Clearly enough, if the path node is in the "no intrusion" state, the conditional probability of accomplishing any of the security functions is null.

4.2.2.2.3 Equipment vulnerability and attack success

In the present study, rather than adopting a univocal definition of attack success, different criteria were adopted to define attack success depending on the considered attack mode, as summarized in the third column of Table 4.2.1. However, the BN was quantified in such a way that the successful execution of an attack attempt invariantly corresponds to "true" state of black nodes in Fig. 4.2.1.

The nodes in black color represent the equipment items that may be potentially damaged by an attack and have binary states (namely "true" and "false"). In particular, "true" state of node "E.I.j affected" represents the condition of the j-th equipment item being affected up to a point that a release of hazardous material results, due to the direct

action of misoperation or interference or due to the impact of physical effects generated by the weapons or tools used in the attack.

Clearly enough, the damage condition can only occur if the j-th equipment item has been previously selected as target (i.e., node "E.I.j selected as target" is in "true" state, see Fig. 4.2.1). The conditional probabilities of a generic equipment item being affected given remaining combinations of parent nodes' states are to be calculated based on the following simplified and conservative considerations.

In particular, for attack modes that require intrusion into the site perimeter (misoperation, interference, shooting, etc.), it was assumed that damage condition is certain (probability of damage equal to 1) if PPS intervention is unsuccessful, since the adversary reaches the target location. In other words, the successful preventive action of the PPS is sufficient for the attack attempt to be frustrated. An auxiliary node named "attack success," having a CPT quantified as an OR-gate, was added to the model to represent in an aggregate form all possible variable states that lead to the undesired case, i.e., the successful accomplished attempt of a generic attack.

Is it worth mentioning that the present method is suitable for future upgrade by implementing equipment vulnerability models associated with the possible impact vectors, such as heat radiation, overpressure, or missile projection (Reniers and Cozzani, 2013), thus introducing a damage probability given an attack attempt.

4.2.2.3 Description of the case study

To illustrate BN model application, a simplified case study is analyzed in the following. The layout of the process facility under consideration is shown in Fig. 4.2.2.

The facility features several units storing hazardous materials, in particular E.I.1, E.I.2, E.I.3, and E.I.4. The available PPS elements are summarized in Table 4.2.2.

For the sake of brevity, a single target (E.I.1) and a single attack mode (use of IED) are analyzed; this results in the BN model simplification; the tailored BN is shown in Fig. 4.2.3. It is assumed that the adversary performs the attack after having reached the target through 50 kg of TATP (see Section 3.4 for more details on IDE) loaded in a backpack. Following the indications reported in Section 3.4, this IED amount is sufficient to damage process equipment from a limited distance (<20 m), leading to the release of hazardous material. Two possible adversary's paths, also drawn in Fig. 4.2.2, are considered (path 1 and path 2).

The BN model shown in Fig. 4.2.3 is quantified following the approach described in Section 4.2.2.2, using this information and assuming guess estimate values of the probability of roving guards being present along the two identified paths during night shift and of employees being present along the two identified paths during day shift.

4.2.2.4 Results of the vulnerability assessment based on BN

The numerical results of the probabilistic vulnerability assessment are reported in Table 4.2.3. In particular, the developed BN model allowed quantifying the probability of security functions being successfully performed. Then, the probability of E.I.1 being affected by the attack along the identified paths was evaluated (see Fig. 4.2.4).

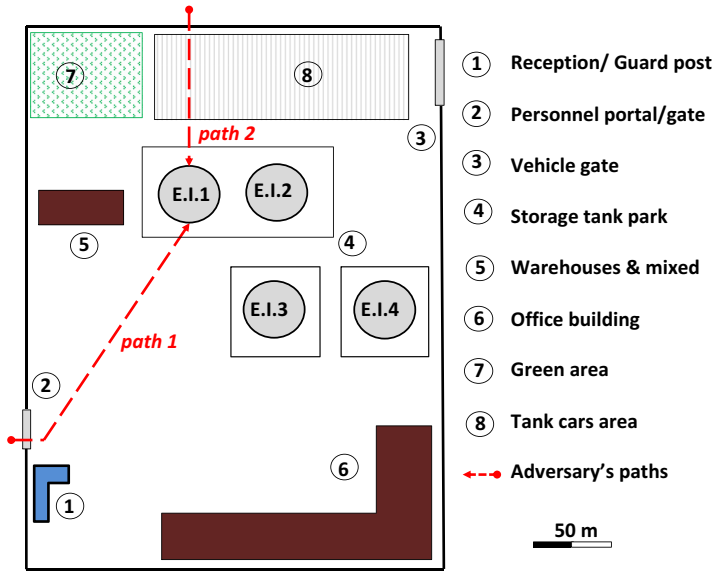


FIGURE 4.2.2 Layout considered in the case study. *Adapted from Argenti, F., Cozzani, V., Landucci, G., Reniers, G., 2016a. Probabilistic vulnerability analysis of process facilities to external acts of interference. In: Risk, Reliability and Safety: Innovating Theory and Practice - Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016, p. 344.*

Table 4.2.2 Summary of available PPS elements in the layout shown in Fig. 4.2.2.

ID	Description	Notes
PPS1	Single line rigid fence with outriggers along the perimeter	—
PPS2	Unsupervised automatic badge check at personnel gate (item 2 in Fig. 4.2.2)	Equipped with cage-like turnstiles and anti-bypass system
PPS3	Supervised automatic credentials check at vehicle gate (item 3 in Fig. 4.2.2)	—
PPS4	Internal guards (internal personnel or dedicated guards)	Roving guards inside the perimeter at night; employees working on site during day shift
PPS5	Radio communication with backup communication means	This enables contact between security guards and local law enforcement agencies
PPS6	Direct intervention of external response force	5 min average intervention time

The third and fourth column of Table 4.2.3 show the probability of successful intervention of each PPS given the evidence that path 1 and path 2 are respectively followed by the adversary. As shown in the table, the security function effectiveness strongly depends on the path, with a drastic decrement in PPS success probability in path 2 with respect to path 1 for the functions "successful intrusion assessed detection" and "timely intervention." Hence, the overall probability of attack success shown in

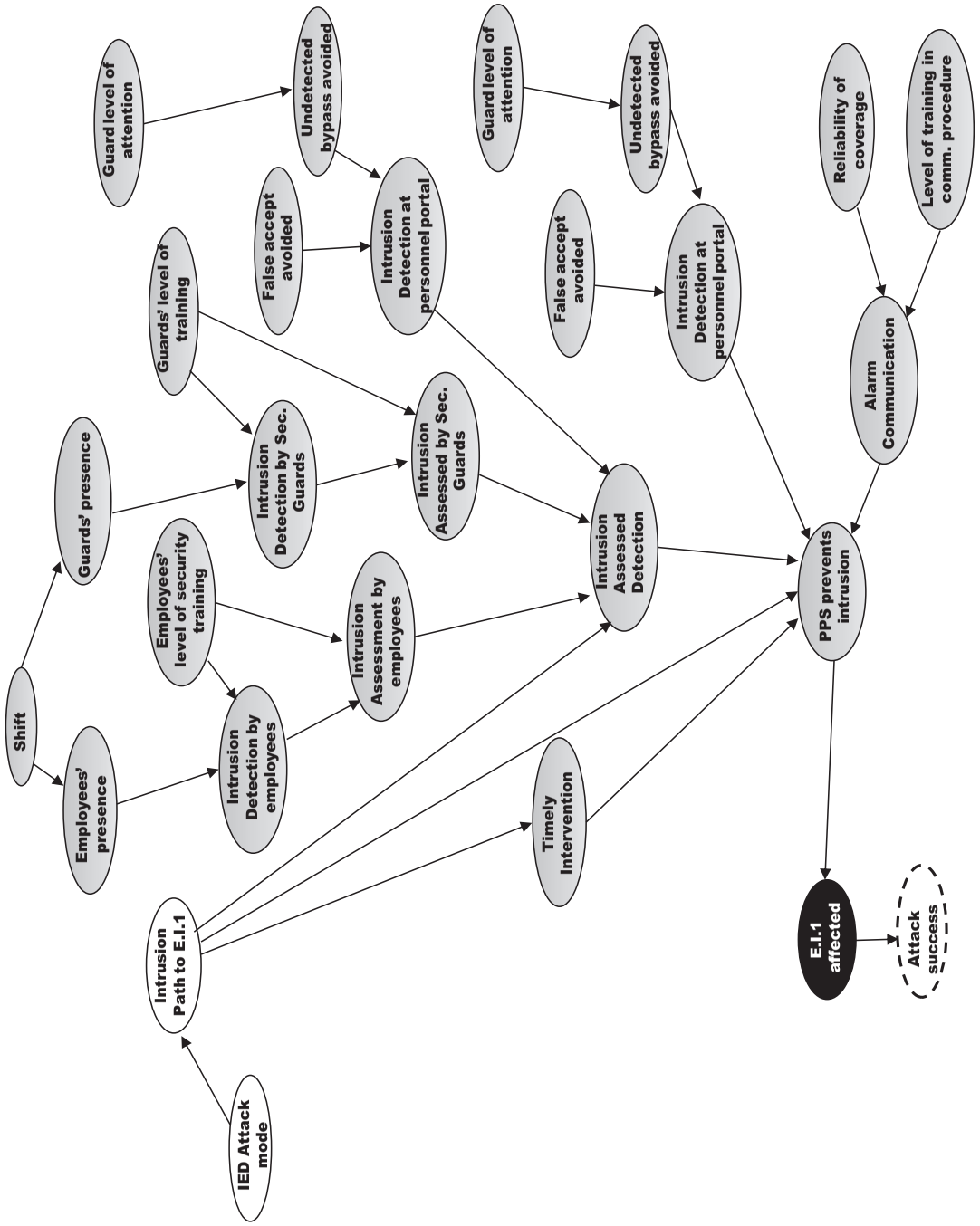


FIGURE 4.2.3 BN model tailored to the analysis of the case study.

Table 4.2.3 Results of the case study: probabilistic assessment carried out through the BN model.

Node state	Priors	Posteriors given path 1	Posteriors given path 2
Successful intrusion assessed detection	0.4807	0.9999	0.2582
Successful alarm communication	0.8602	0.8602	0.8602
Timely intervention	0.1730	0.3200	0.1100
PPS prevents intrusion	0.0997	0.2753	0.0244

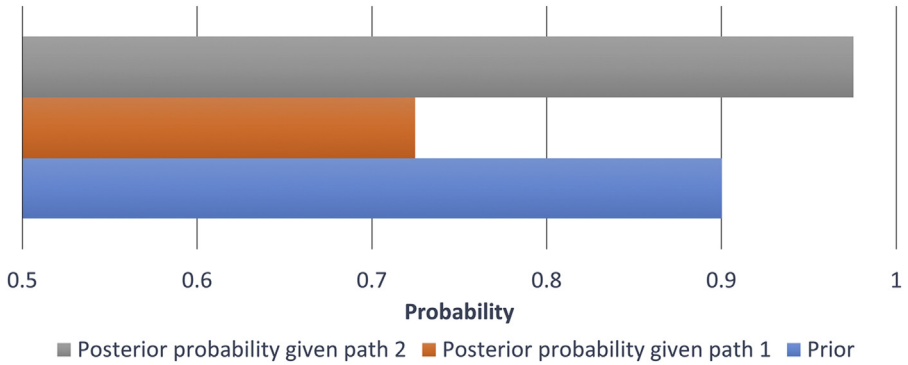


FIGURE 4.2.4 Overall results obtained for the vulnerability assessment: probability of attack success.

Fig. 4.2.4 increases by about 35% in path 2 with respect to the case of path 1. This result is due to two factors. Firstly, path 1 requires the adversary to take more time in reaching the target E.I.1. Secondarily, only two detection actions may occur along path 2 (i.e., by employees and by roving guards inside the facility perimeter) and no detection systems are available at the perimeter along the fence, while path 1 crosses the entry control system at the personnel portal. The same kind of reasoning and BN computations can be applied in the evaluation of the vulnerability of other potential targets (E.I.2, E.I.3, E.I.4) with respect to an extended set of attack scenarios.

The results of the present case study allowed demonstrating the potentialities of the BN model in capturing plant vulnerability with respect to given attack models, following the vulnerability definition reported in Section 3.3. However, the model relies on simplifying assumptions, for instance, the classification of attack modes and the binary nature assumed for the assessment of PPS performance, which, however, needed to be introduced to avoid BN states explosion. Moreover, the extensive use of expert judgment to quantify BN conditional probability tables may affect the quality of the results. However, in light of the complex nonphysically explainable nature of the modeled dependencies and of the lack of reliable quantitative data in the technical literature concerning PPS performance, this was deemed as the best choice in order to feed the BN model with sound quantitative data.

4.2.3 Application of graph theory to vulnerability assessment of chemical plants

4.2.3.1 Overview

This subsection deals with the application of graph theory, as an alternative to BN, to assess potential cascading events triggered by external acts of interference or "intentional domino effects." Presenting the domino effects at a chemical facility as a directed graph, it is shown that graph centrality —metrics — especially the out-closeness — can be used to identify critical units, which under attack can lead to more severe domino effects in the facility. Besides, among two chemical facilities with the same number of units, the one with a higher average out-closeness is shown to be more vulnerable to intentional (and accidental) domino effect scenarios.

4.2.3.2 Graph theory and metrics

A mathematical graph is an ordered pair $G = (V, E)$ comprising a set of vertices $V = \{v_1, v_2, \ldots, v_n\}$ and a set of edges $E = \{e_1, e_2, \ldots, e_m\}$. A vertex is represented by a node, while edges connect the nodes. In a weighted graph, a set of numerical values can be assigned to the vertices or edges of the graph (Freeman, 1978).

In a directed graph, a walk from the vertex v_i to v_j is a sequence of vertices and edges starting from v_i and ending in v_j when each intermediate vertex may be traversed several times. A path, however, is a walk where each intermediate vertex is traversed only once. Similarly, the geodesic distance d_{ij} between v_i and v_j is the length of the shortest path from v_i to v_j. If there is no path between v_i and v_j, then $d_{ij} = \infty$. A path that starts and ends at the same vertex is called a cycle, and a graph that contains at least a cycle is called cyclic. Otherwise, the graph is acyclic, like Bayesian networks.

In a graph, out-closeness of a vertex $C_{out}(v_i)$ measures how many steps are needed to reach to every other vertex of the graph from that vertex (Freeman, 1978):

$$C_{out}(v_i) = \sum_j \frac{1}{d(v_i, v_j)} \tag{4.2.7}$$

Having the out-closeness of the vertices, the graph's average out-closeness can be defined as (Khakzad and Reniers, 2019):

$$C_{out}^{G} = \frac{1}{n} \sum_{i=1}^{n} C_{out}(v_i) \tag{4.2.8}$$

where C_{out}^{G} is the out-closeness of the graph, and n is the number of vertices.

4.2.3.3 Vulnerability assessment

Khakzad and Reniers (2015) demonstrated that if all possible fire escalation scenarios in a chemical facility can be modeled as a directed graph, among the units, the one with the highest out-closeness may lead to the most severe domino effect if selected as the primary unit; the same method was applied for the analysis of protection add-on safety measures (Khakzad et al., 2017a). Following their work, Khakzad and Reniers (2019)

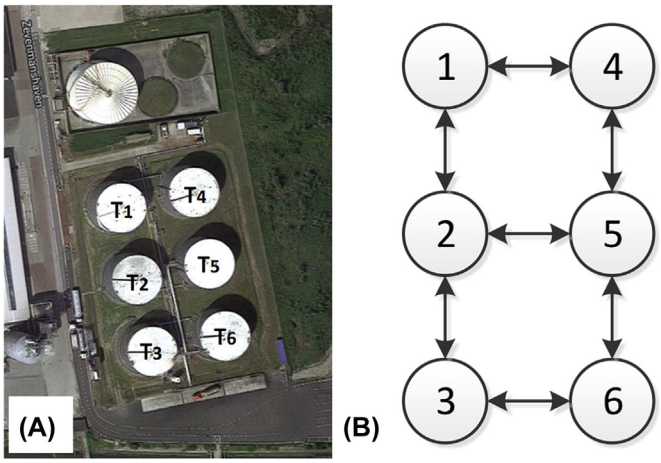


FIGURE 4.2.5 (A) A fuel storage plant consisting of six gasoline storage tanks. (B) Representation of possible domino scenarios as a directed graph.

Table 4.2.4 Heat radiation intensity (kW/m^2) T_j receives from a tank fire at T_i.

$T_i\downarrow$ $T_j\rightarrow$	T_1	T_2	T_3	T_4	T_5	T_6
T_1	–	38	–	22	–	–
T_2	38	–	38	–	22	–
T_3	–	38	–	–	–	22
T_4	22	–	–	–	38	–
T_5	–	22	–	38	–	38
T_6	–	–	22	–	38	–

Values less than 15 kW/m^2 are not presented.

showed that attack to multiple units with higher out-closeness scores would result in a more severe domino effect than attack to the same number of units with lower out-closeness scores.

For the sake of clarity, consider the fuel storage plant in Fig. 4.2.5. The tanks are identical and of a diameter of 30.5 m, height of 9.1 m, and capacity of 8000 m^3. Tank fires are considered the more likely scenarios anticipated from an attack with IEDs, according to the case histories description discussed in Chapter 2. The amounts of heat radiation that each Tank T_j receives from a Tank T_i are calculated using ALOHA software package (http://www.epa.gov/OEM/cameo/aloha.htm) as reported in Table 4.2.4, assuming a wind speed of 2 m/s from NW, 25% relative humidity, and air temperature of 18°C. Since the tanks are atmospheric, the heat radiation threshold capable of causing damage and thus triggering domino effects is considered as 15 kW/m^2 (Landucci et al., 2013, 2009). As such, heat radiation intensity values less than this threshold are not presented in Table 4.2.4.

Table 4.2.5 Out-closeness score of the storage tanks shown in Fig. 4.2.6.

Storage tank	T_1	T_2	T_3	T_4	T_5	T_6
C_{out} of tanks	0.56	0.71	0.56	0.56	0.71	0.56

Having the heat radiation values in Table 4.2.4, possible fire escalation scenarios in the fuel storage plant can be presented as the directed graph in Fig. 4.2.5B. Modeling the graph in igraph (Csardi and Nepusz, 2006), the tanks' out-closeness scores have been calculated as in Table 4.2.5, indicating T_2 and T_5 as the tanks with the ones with the highest out-closeness. As such, a single attack to T_2 or T_5 would trigger a more severe domino effect than a single attack to any other storage tank (Khakzad and Reniers, 2015). Likewise, a simultaneous double-attack to T_2 and T_5 is expected to result in a more severe domino effect than any other double-attacks (Khakzad and Reniers, 2019).

For this purpose, consider a number of single attacks as shown in Fig. 4.2.6A–C and double-attacks as shown in Fig. 4.2.6D–F, where the attacked units have been highlighted with color yellow. Modeling these graphs in igraph (Csardi and Nepusz, 2006), the average out-closeness scores of the graphs as an indication of the storage plant's vulnerability to domino effects (Khakzad and Reniers, 2015) are presented in Table 4.2.6.

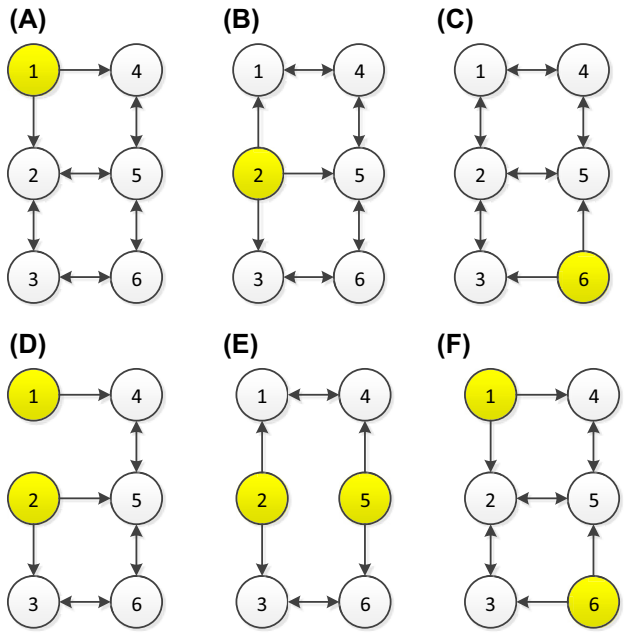


FIGURE 4.2.6 Domino scenarios triggered by attack to (A) T_1, (B) T_2, (C) T_6, (D) T_1 and T_2, (E) T_2 and T_5, and (F) T_1 and T_6.

Table 4.2.6 Average out-closeness and utility values for single-attack and double-attack scenarios depicted in Fig. 4.2.6.

	Single-attack in Fig. 4.2.6			Double-attack in Fig. 4.2.6		
Graph	**(a)**	**(b)**	**(c)**	**(d)**	**(e)**	**(f)**
C_{out} of plant	0.18	**0.42**[1]	0.18	0.14	**0.21**	0.12
Utility	−42.9	**−49.5**	−42.9	−52.8	**−58.7**	−56.8

Utility values have been calculated using the Dynamic Bayesian Network in Fig. 4.2.7.

[1]Numbers in bold identify the most severe domino effect scenarios for each attack mode (single or double attack).

As can be seen, among single-attack scenarios, the graph presented in Fig. 4.2.6B has the highest average out-closeness, indicating that a single attack to T_2 (or T_5) would lead to the most severe domino effect compared to a single attack to other tanks. Likewise, among double-attack scenarios, the graph presented in Fig. 4.2.6E has the highest average out-closeness score, indicating that a double-attack to both T_2 and T_5 would result in the most severe domino effect compared to a simultaneous attack to any other two tanks.

To check the accuracy of the results obtained from the graph theory, the methodology developed by Khakzad (2015) based on dynamic Bayesian network (DBN) for modeling domino effects can be employed. Fig. 4.2.7 displays the DBN to model all possible domino effect scenarios in the storage plant. The DBN has been extended to an influence diagram by adding the node "Utility" to account for the damage inflicted due to domino effects.

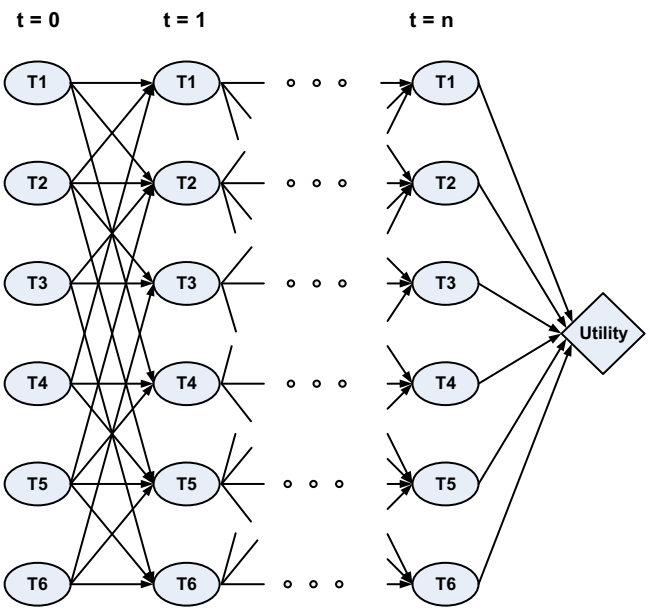


FIGURE 4.2.7 DBN to model possible domino effect scenarios.

Table 4.2.7 Conditional probability table of node T_4 at t = 1 in Fig. 4.2.7.

$T_4^{t=0}$	$T_1^{t=0}$	$T_5^{t=0}$	$T_4^{t=1}$ Tank fire	$T_4^{t=1}$ No fire
Tank fire	Tank fire	Tank fire	1	0
Tank fire	Tank fire	No fire	1	0
Tank fire	No fire	Tank fire	1	0
Tank fire	No fire	No fire	1	0
No fire	Tank fire	Tank fire	P_{15}	$1 - P_{15}$
No fire	Tank fire	No fire	P_1	$1 - P_1$
No fire	No fire	Tank fire	P_5	$1 - P_5$
No fire	No fire	No fire	0	1

To model the domino effect triggered by a single attack to T_1, for example, the state of node T_1 at the first time slice can be instantiated to "T_1 = Tank fire" while the states of the other nodes at t = 0 are instantiated to "No fire." Based on the assigned marginal and conditional probabilities, the developed DBN computes unconditional probabilities of the storage tanks at sequential time slices. For the sake of clarity, the conditional probabilities assigned to node T_4 at t = 1 are listed in Table 4.2.7.

In Table 4.2.7, the probabilities P_1, P_5, and P_{15} are escalation probabilities and can be calculated using a variety of techniques such as probit models (Landucci et al., 2013) based on the intensity of received heat radiation and type and size of target vessels. In addition, for illustrative purposes, we assume that a damaged storage tank − either due to attack with IEDs or due to escalation of domino effects − would be associated with a cost of 10 units. This cost can be incorporated in "Utility" node as a value of −10; likewise, the utility of a safe tank would be 0. For instance, if the attack to T_1 triggers a tank fire escalating to the neighboring storage tanks T_2 and T_4, the respective utility value incorporated in "Utility" in Fig. 4.2.7 would be U(T_1 = Tank fire, T_2 = Tank fire, T_3 = No fire, T_4 = Tank fire, T_5 = No fire, T_6 = No fire) = −30.

Implementing the DBN of Fig. 4.2.7 in GeNie (2019), the expected utilities of single- and double-attack scenarios are calculated as listed in Table 4.2.6 (second row). As can be seen, among the single-attack scenarios, the attack to T_2 would result in the largest disutility (−49.5), whereas among the double-attack scenarios, the attack to both T_2 and T_5 would result in the largest disutility (−58.7). As can be seen, the results of the DBN are in agreement with the results obtained from the graph theoretic approach.

4.2.3.4 Results of the vulnerability assessment based on graph theory

The comparison between the results of graph theory and dynamic Bayesian network in the previous section showed that average out-closeness score of a chemical facility can be used as an indication of the facility's vulnerability to intentional (and also accidental) domino effects. This also implies that in a chemical facility, the units with higher out-closeness scores contribute more to the average out-closeness of the facility and are thus more critical in the context of intentional attacks with the aim of triggering domino effects.

Having this important outcome, Khakzad and Reniers (2019) proposed low-capacity utilization of chemical facilities as a temporary way of reducing their vulnerability to intentional domino effects. Low-capacity utilization can be implemented in a variety of ways, including shutting down the critical units and operations or reducing (or emptying) the chemical inventory of critical units. This strategy could turn out very effective especially in the case of impending terrorist attacks (for example, in the case of elevated or imminent alerts) where time is too short to increase the security level of the facility, for instance, via implementing additional security barriers.

Ranking the critical units in a descending order, by considering the loss of revenue due to different low-capacity utilization strategies and the corresponding reduction in the severity (or risk) of potential domino effects, the optimal low-capacity utilization plan can be identified using multicriteria decision-making techniques. Although the focus of the present study has been on intentional domino effects, the outcomes can also be applied to reduce the vulnerability of chemical facilities to accidental domino effects. The developed methodologies can be used in the design phase of chemical facilities in the context of inherently safer and securer plant layouts.

4.2.4 Application of Analytic Network Process to vulnerability assessment of chemical plants

4.2.4.1 Overview

Mainly influenced by the security assessment guidelines issued by, for example, the American Petroleum Institute (API) (2013), most of the methodologies developed for security vulnerability assessment of hazardous industries have been based on the scoring of security risk parameters sequentially and largely independently of each other. The parameters' scores are then combined usually via linear relationships — additive or multiplicative — to calculate the final security risk score of a facility. As a result of such hierarchical and linear scoring, the interactions among the security risk parameters are likely to be neglected, resulting in an inaccurate rank ordering of security-critical units.

For instance, consider the first three steps of the SRA methodology developed by American Petroleum Institute (API) (2013) in Fig. 4.2.8 where the vulnerability of assets (Step 3) is not taken into account when scoring the likelihood of threats (Step 2). As a result of such top-down scoring approach, the influence of plant vulnerability on its attractiveness and thus on the type of threats attracted to the plant would not fully be taken into account.[1]

To alleviate the limitation of hierarchical SRA methodologies, i.e., only considering the influence of higher-level criteria on lower-level subcriteria and alternatives, (Khakzad et al., 2017b) developed a methodology based on ANP (Saaty, 2008). ANP is a multi-criteria decision analysis technique to rank a set of decision alternatives while considering the mutual importance of the decision criteria, subcriteria, and alternatives

[1]The more vulnerable a facility, the easier it could be attacked and is thus more attractive to the adversaries.

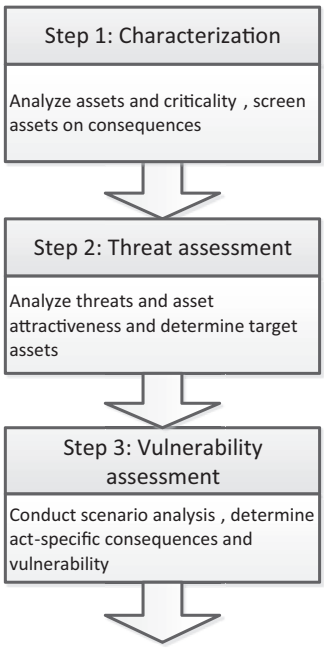


FIGURE 4.2.8 The first three steps of API security risk assessment methodology (American Petroleum Institute (API), 2013).

altogether. By doing so, in the context of SRA, for instance, the potential consequences of an attack can be used to score likely threats interested in such consequences, and also the likely threats can influence the likelihood (score) of potential consequences based on their importance from the threat's viewpoint (the mutual interaction or feedback between threat−consequence).

4.2.4.2 Analytic Network Process

Analytic hierarchy process (AHP) (Saaty, 2008) is a multicriteria decision-making technique consisting of a decision goal, decision criteria, and decision alternatives, in a tree-like structure from top to bottom (Fig. 4.2.9A). In AHP, the decision parameters are scored in a top-down fashion: placing the decision goal at the top of the tree, the decision criteria are compared pairwise and weighted against the decision goal; the decision alternatives are compared pairwise and weighted against each decision criterion (criteria influence alternatives), all based on the fundamental scale as in Table 4.2.8.

The results of the pairwise comparisons are incorporated in comparison matrices. The normalized elements of the principal right eigenvector of each comparison matrix represent the local rank of each criterion and alternative. Final rank of each decision alternative is subsequently calculated as the sum product of the local ranks of the alternative and criteria. As such, the alternative with the highest final rank (score) can be selected as the optimal decision alternative.

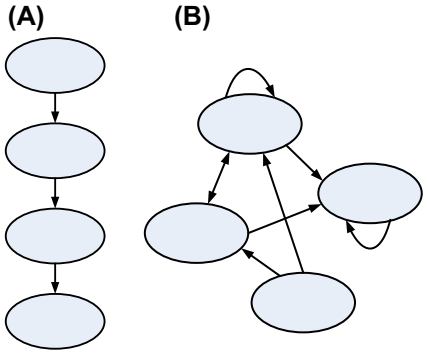


FIGURE 4.2.9 Schematics of (A) AHP and (B) ANP.

Table 4.2.8 Fundamental scale derived from (Saaty, 2008).

Score	Description
1	Equal importance
3	Moderate importance
5	Strong importance
7	Very strong importance
9	Extreme importance
2, 4, 6, 8	Intermediate values
Use reciprocals for inverse comparison	

ANP (Saaty, 2008) has been built on AHP. However, ANP enables the analysts to consider the influences among the decision parameters without forcing a hierarchical scoring unlike AHP (Fig. 4.2.9B). In ANP, the decision parameters are incorporated in clusters C_i (for $i = 1, 2,\ldots, n$) while the parameters within cluster C_i can be labeled as e_{ij} (for $j = 1, 2, \ldots, m$). The elements of clusters can then be compared pairwise and scored in the form of comparison matrices using the fundamental scores in Table 4.2.8. The matrices are then incorporated in an unweighted super matrix as shown in Fig. 4.2.10.

The unweighted super matrix should be normalized columnwise to form a weighted or stochastic super matrix (the sum of elements in each column adds up to unity). Raising the weighted super matrix to a sufficiently large power, the elements of the resultant matrix (also known as the limit matrix) represent the final scores of corresponding decision parameters (Saaty, 2008).

4.2.4.3 Application of ANP to rank ordering of chemical units

Considering the SRA five steps, that is, assets identification, consequence assessment, threat assessment, attractiveness assessment, and vulnerability assessment, the ANP for security vulnerability assessment can be developed as in Fig. 4.2.11.

$$
W = \begin{array}{c|cccc}
 & C_1 & C_2 & \cdots & C_n \\
 & e_{11}\ e_{12}\ldots e_{1k} & e_{21}\ e_{22}\ldots e_{2p} & & e_{n1}\ e_{n2}\ldots e_{nq} \\
\hline
\begin{matrix} e_{11} \\ e_{12} \\ \vdots \\ e_{1k} \end{matrix} C_1 & W_{11} & W_{12} & \cdots & W_{1n} \\
\begin{matrix} e_{21} \\ e_{22} \\ \vdots \\ e_{2p} \end{matrix} C_2 & W_{21} & W_{22} & \cdots & W_{2n} \\
\vdots & \vdots & \vdots & & \vdots \\
\begin{matrix} e_{n1} \\ e_{n2} \\ \vdots \\ e_{nq} \end{matrix} C_n & W_{n1} & W_{n2} & & W_{nn}
\end{array}
$$

FIGURE 4.2.10 ANP's super matrix.

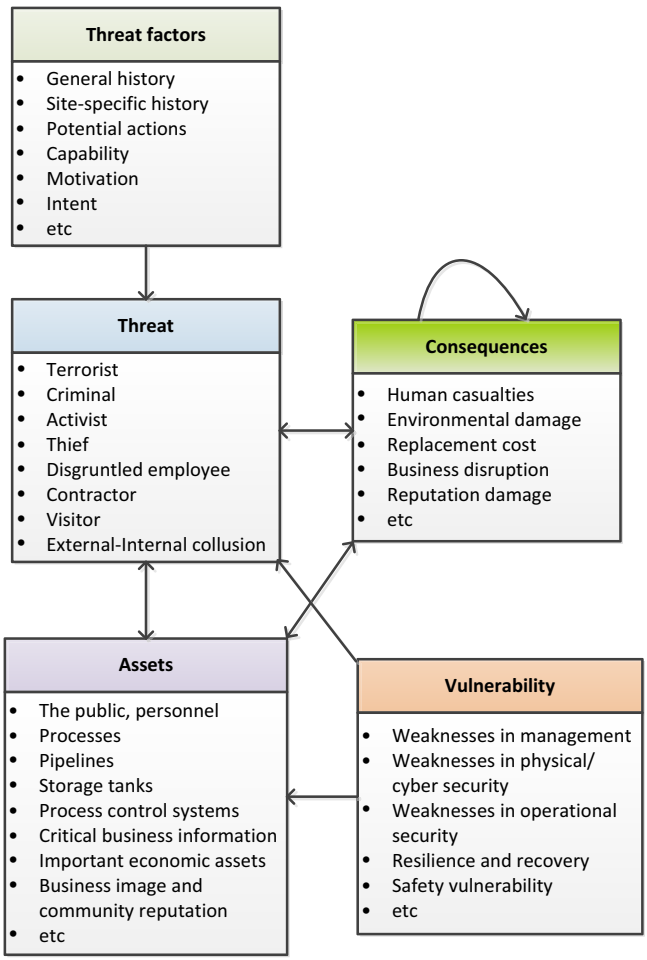


FIGURE 4.2.11 A typical ANP to assess security risk. *Adapted from Khakzad, N., Reniers, G.L.L., van Gelder, P., 2017b. A multi-criteria decision making approach to security assessment of hazardous facilities. Loss Prev. Process Ind. 48, 234–243.*

The single-headed arrow, for example, from "Vulnerability" to "Assets" indicates that the elements of the latter cluster (e.g., pipeline and storage tanks) are compared to each other according to some or all the elements of the former cluster (e.g., weakness in physical security). Likewise, the double-headed arrow between "Threat" and "Assets" implies the mutual interaction between the elements of the two clusters. For example, according to the "public" element in the "Assets" cluster, the weight of a "terrorist" is much higher than that of a "thief" in the "Threat" cluster. This is because a thief is very unlikely to seek public casualty from an attack; on the other hand, according to a "thief" in the "Threat" cluster, the weight of "important economic assets" in the "Assets" cluster is higher than that of "business image and community reputation." An arrow from a cluster to itself, e.g., "Consequences" in Fig. 4.2.11, implies the relative importance of the elements inside the cluster; for instance, regardless of other clusters and embedded factors, facility management may assume a higher weight for "human casualties" than "environmental damage."

When making pairwise comparison, the qualitative weights Very High (VH), High (H), Medium (M), Low (L), and Very Low (VL) defined in API (2012) can be converted to scores via the fundamental scales of AHP listed in Table 4.2.8. To this end, Table 4.2.9 can be used to perform the conversion (Khakzad et al., 2017b). For example, if according to the criterion "Y," the element "X" is weighted as high (H) and element "Z" is weighted as low (L), in pairwise comparison of X and Z according to Y, $X/Z = 5$, whereas $Z/X = 1/5$.

Table 4.2.9 Conversion of qualitative weights to fundamental scales in pairwise comparison.

	VH	H	M	L	VL
VH	1	3	5	7	9
H	1/3	1	3	5	7
M	1/5	1/3	1	3	5
L	1/7	1/5	1/3	1	3
VL	1/9	1/7	1/5	1/3	1

Derived from Khakzad, N., Reniers, G.L.L., van Gelder, P., 2017b. A multi-criteria decision making approach to security assessment of hazardous facilities. Loss Prev. Process Ind. 48, 234–243.

4.2.4.4 An illustrative example

To demonstrate the application of ANP to security vulnerability assessment of chemical facilities, consider a hypothetical refinery as depicted in Fig. 4.2.12 (American Petroleum Institute (API), 2013). Based on a primary assessment of the potential consequences, the central control room (Central Control), the unloading dock (Dock # 1), and the storage tanks (Dock #1 Tank Farm) are identified as the critical assets, which may need additional security countermeasures based on their vulnerability (Table 4.2.10). Further, assume that based on intelligence, terrorists (low), disgruntled employees (medium), and environmental activists (high) have been identified as possible threats to the refinery (Table 4.2.11).

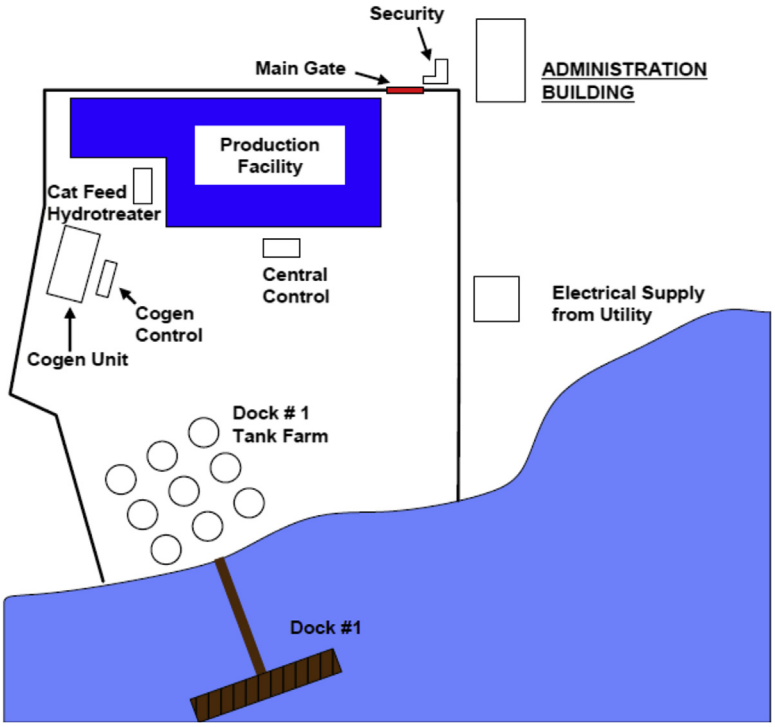


FIGURE 4.2.12 A hypothetical oil refinery. *Derived from American Petroleum Institute (API), 2013. ANSI/API Standard 780 — Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry. American Petroleum Institute, Washington, DC.*

Table 4.2.10 Approximate scoring of potential consequences for critical assets.

Item	Casualties	Environmental damage	Replacement Cost
A1: Central control	H	VL	L
A2: Dock	L	VH	M
A3: Tank farm	L	M	VH

H, high; *L*, low; *M*, moderate; *VH*, very high; *VL*, very low.

Table 4.2.11 Sample threat assessment for the refinery.

Threat agent	General case-specific history	Potential action	Capability	Motivation/intent	Rank
Terrorist	Existence of terrorist groups in the country; no previous attack to the facility or similar facilities	Use of explosives, small arms	Improvised explosives such as car bomb	Causing maximum casualties, damage to critical infrastructures	Low (L)
Disgruntled employee	Reports of sabotage, theft of equipment in the region; reported events in neighboring facilities	Intentional overfill of tanks; tampering of remote control valves	Unrestricted access to all facilities; insider knowledge and training	Causing damage due to disciplinary action and/or staff layoff	Medium (M)
Activist	Existence of environmental activists in the region; demonstrations against the operation of the facility	Temporary shutdown of the facility; damage to critical infrastructures	Improvised explosives in form of duffel bag	The facility poses significant toxic chemicals to the environment	High (H)

Likewise, the assets' vulnerability was investigated by considering the countermeasures in place and their performance for each threat–asset pair. For instance, for the terrorist-dock vulnerability assessment, the items such as lack of access control from water, lack of intrusion detection system, limited CCTV and perimeter surveillance, and long arrival time of coast guard/patrol were identified as inefficiency/lack of physical security; moreover, a recovery time of 3 months was considered given a significant damage to the dock. Following a similar approach, vulnerability of each asset could be identified.

The ANP developed for the chemical plant in Fig. 4.2.12 is displayed in Fig. 4.2.13, assuming that the elements of "Consequences" cluster are of the same importance from the refinery's management perspective (there would otherwise be an arrow from the consequences cluster to itself). Modeling the ANP in decision-making software SuperDecisions 2.8.0 (www.superdecisions.com) would result in the unweighted super matrix in Table 4.2.12.

The elements of the super matrix have been calculated using the same approach as in AHP. For illustrative purposes, the pairwise comparison of the elements of "Assets" (i.e., A1: Control room, A2: Dock, and A3: Tank farm) and the first element of "Consequences" (i.e., C1: Casualties) has been presented in Table 4.2.13. For the sake of clarity, the scores presented in Table 4.2.13 have been presented with bold numbers in Table 4.2.12. (To see the other tables, see the appendix in Khakzad et al., 2017b).

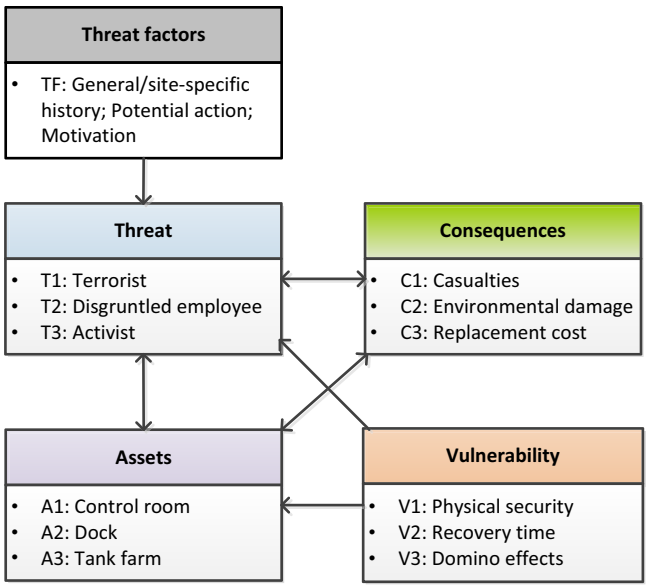


FIGURE 4.2.13 ANP for security risk assessment of the refinery.

Table 4.2.12 Unweighted super matrix of the ANP in Fig. 4.2.13.

	TF	T1	T2	T3	C1	C2	C3	V1	V2	V3	A1	A2	A3
TF	0	0	0	0	0	0	0	0	0	0	0	0	0
T1	0.105	0	0	0	0.792	0.671	0.6	0.111	0.066	0.649	0.081	0.751	0.658
T2	0.258	0	0	0	0.131	0.265	0.2	0.778	0.149	0.072	0.731	0.178	0.156
T3	0.637	0	0	0	0.076	0.063	0.2	0.111	0.785	0.279	0.188	0.07	0.185
C1	0	0.731	0.063	0.091	0	0	0	0	0	0	0.731	0.081	0.081
C2	0	0.081	0.265	0.091	0	0	0	0	0	0	0.081	0.731	0.188
C3	0	0.188	0.672	0.818	0	0	0	0	0	0	0.188	0.188	0.731
V1	0	0	0	0	0	0	0	0	0	0	0	0	0
V2	0	0	0	0	0	0	0	0	0	0	0	0	0
V3	0	0	0	0	0	0	0	0	0	0	0	0	0
A1	0	0.105	0.751	0.649	**0.714**[a]	0.058	0.081	0.072	0.063	0.066	0	0	0
A2	0	0.637	0.07	0.072	**0.143**[a]	0.735	0.188	0.649	0.672	0.149	0	0	0
A3	0	0.258	0.178	0.279	**0.143**[a]	0.207	0.731	0.279	0.265	0.785	0	0	0

[a]See the last column of Table 4.2.12.

Table 4.2.13 Pairwise comparison of assets according to casualties.

C1: Casualties	A1	A2	A3	Local score
A1: Central room	1	5	5	0.714
A2: Dock	1/5	1	1	0.143
A3: Tank farm	1/5	1	1	0.143

The unweighted super matrix in Table 4.2.12 is converted to a weighted (stochastic) super matrix (in which the matrix is normalized columnwise) and raised to a sufficiently large power so as to form a limit matrix. The arrays on each row of the limit matrix are the same though they may differ from one row to another, representing the global score or final priority rank of the element corresponding to the row. Final priority rank of the assets, consequences, and threats, which have been normalized clusterwise, are depicted in Fig. 4.2.14.

As can be seen from Fig. 4.2.14, within the "Assets" cluster, Dock is the most critical target, closely followed by Control room and Tank farm. Within the cluster "Consequences," Casualties is the most important concern of a security event while Terrorist is the most critical type of "Threat," threatening the refinery. The latter observation is surprisingly in contrast to the preliminary ranking of the threats where according to "Threat factors," the refinery management associated the Terrorist with a "low" score (see Table 4.2.11). This score modification highlights the out-performance of ANP in rank ordering of security risk elements where not only the preliminary score of an element but also those of other elements matter in the calculation of the final score of the element.

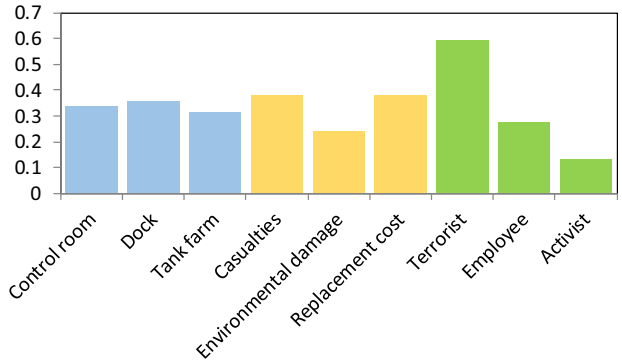


FIGURE 4.2.14 Priority ranks of security risk elements.

4.3 Advanced tools for emergency response planning

A number of guidelines and approaches have been proposed regarding the emergency response and preparedness for security threats and attacks at chemical plants (Bajpai and Gupta, 2007), but there is no specific procedure available for multiplant management of terrorist attacks at chemical clusters. Thus, an efficient clusterwise emergency response seems crucial for prompt and efficient tackling of terrorist attacks.

This section is aimed at developing a decision support tool for multiplant response at chemical clusters. The decision support tool in the form of a decision matrix helps to identify the emergency and alert levels at the single plants within the cluster in order to respond in a pre-agreed procedure to terrorist attacks with IEDs. The emergency levels indicate the potential actions to adopt to prepare for and respond to catastrophic terrorist attacks. The alert levels, on the other hand, help the decision-makers plan for increasing the security of critical assets in the chemical cluster in the prospect of imminent threats or attacks in the future.

4.3.1 Methodology

The approach consists of five main steps: (i) identifying the target assets, (ii) developing and analyzing the most likely attack scenarios, (iii) determining the emergency levels, (iv) developing alert notification system, and (v) establishing a cluster decision matrix. These steps are described in more detail in the following subsections.

4.3.1.1 Identifying the target assets

In security terms, the assets for a chemical facility are defined as people (both on-site and off-site), information (trade secrets, confidential business information, etc.), and property (buildings, process equipment, control systems, etc.). Not all the assets have equal value to adversaries (American Petroleum Institute (API), 2013). In the first step, the assets of each company are identified and prioritized based on their attractiveness as a target for bombing attack scenarios. Some of the relevant attractiveness factors are as follows (American Petroleum Institute (API), 2013; Argenti et al., 2015):

- The potential for causing maximum damage (casualties, economic loss) with a focus on process equipment with significant quantities of flammable or toxic chemicals, the central control room, and utility units
- Being easily accessible to adversaries by considering factors such as the proximity of the assets to the facility boundary, public road, parking lot, or dock area
- The potential for triggering internal and external domino effects with a focus on separation (safety) distance among the critical units
- The potential for causing off-site casualties while considering the land-use developments in the vicinity of the chemical cluster and the vulnerability of the users (residential communities, hospitals, schools, airports, etc.)
- Recognizability of critical targets by outsiders.

4.3.1.2 Developing and analyzing the most likely attack scenarios

IEDs can come in many forms, ranging from small pipe bombs to sophisticated airborne and vehicle-borne IEDs (VBIED) capable of causing massive damage (Kennett et al., 2005). The extent of damage caused by an IED depends on its size, construction, and placement, as described in Section 3.4.

After possible target assets are identified, a number of attack positions can be selected based on the chemical plant layout and the location of the target assets. For instance, a parking lot within a short distance from storage tanks area, or a road between two chemical plants, a road near the control room or dock areas can be considered as potential attack areas. Table 4.3.1 presents a selection of the possible IEDs and their explosive capacity (TNT equivalent mass) based on the maximum amount of material that could reasonably fit into a container or vehicle (Kennett et al., 2005).

In order to evaluate the effects of IEDs on structures and equipment, two parameters are considered: the weapon size, measured in equivalent kilograms of TNT as shown in Table 4.3.1, and whether the generated peak overpressure exceeds the threshold values needed for causing structural damage. In particular, to assess the potential damages, the concept of stand-off distance (i.e., the distance measured from the center of gravity of the explosion to the area that the IED can cause damage) is adopted, following the procedure described in Section 3.4.

The calculated stand-off distances, based on the overpressure damage thresholds presented in Section 3.4, can be used to determine whether the process equipment exposed by the IED's blast overpressure would be impacted or not. The potential

Table 4.3.1 List of possible IEDs and their explosion capacity (Kennett et al., 2005).

Threat description	Explosive mass (TNT equivalent kg)
Pipe bomb	2.3
Suitcase bomb	23
Sedan	454
Moving truck	13,608
Semitrailer	27,216

Table 4.3.2 Damage thresholds due to overpressure and heat radiation for different equipment (Cozzani et al., 2006).

Equipment category	Overpressure (bar)	Heat radiation (kW/m^2)
Atmospheric vessel	0.22	15
Pressurized vessel (toxic material)	0.20	45
Pressurized vessel (flammable material)	0.31	45

damage at process units could result in release of flammable or toxic chemicals, which are likely to cause fire, explosion, and fragment projection that may lead to further damage inside and/or outside the premises of the attacked company. In this study, to determine which units are possibly impacted by such events, the received fire heat radiation or explosion overpressure by a nearby unit is compared with respective threshold values derived from Cozzani et al. (2006) and listed in Table 4.3.2.

Furthermore, to estimate the probability of domino effects, the damage probabilities of target units can be calculated using probit functions (Cozzani et al., 2005). Having the probit value Y calculated from Table 4.3.3, the damage probability D can be calculated as follows:

$$D = \phi(Y - 5) \tag{4.3.1}$$

where ϕ is the cumulative density function of standard normal distribution. Having the damage probabilities of the units, a number of techniques and methodologies can be used to calculate the probability of domino effects inside the plant (or cluster) (Khakzad et al., 2013). Furthermore, based on the calculated D, five cut-off levels for domino effects' probability are defined and categorized in five ranking levels.

Table 4.3.3 Models for domino probability used in this study (Cozzani et al., 2005).

Escalation vector	Target equipment	Vulnerability model for domino probability[a]
Radiation	Atmospheric	$Y = 12.54 - 1.847\ \ln(ttf);\ \ln(ttf) = -1.128\ \ln(I) - 2.667 \times 10^{-5}\ V + 9.877$
	Pressurized	$Y = 12.54 - 1.847\ \ln(ttf);\ \ln(ttf) = -0.947\ \ln(I) + 8.835\ V^{0.032}$
Overpressure	Atmospheric	$Y = -18.96 + 2.44\ \ln(P_s)$
	Pressurized	$Y = -42.44 + 4.33\ \ln(P_s)$

[a] I, radiation intensity on target equipment (kW/m^2); P_s, peak overpressure on target equipment (Pa); *ttf*, time to failure(s); V, equipment volume (m^3).

4.3.1.3 Determining emergency levels

A ranking criterion is provided to classify the different attack scenarios based on the attack severity and its potential impact on the plant, the cluster, and the public. In the criteria table, the attack's consequence is ranked in five levels of severity, similarly to the scale used in API 780 (American Petroleum Institute (API), 2013) from very low to very high. Table 4.3.4 provides the details for consequence ranking.

After the attack consequences are analyzed and ranked, a decision tree is used to determine the emergency levels at the companies within the chemical cluster in case of a terrorist attack. Fig. 4.3.1 shows a part of the developed decision tree if the bombing attack

Table 4.3.4 Attack scenarios' consequence ranking.

Rank	Consequence category	Loss of life	Environmental impact	Property damage impact	Domino effect
1	Very low	No injuries First aid required	None	Limited localized minor damage	Unlikely ($D < 10^{-6}$)
2	Low	Injuries that are not widespread but only in the vicinity of the incident location	Minor environmental impacts only to the incident site area	Significant localized damage of some equipment/buildings, no major repair is required.	Moderate ($10^{-6} \leq D < 10^{-3}$)
⋮		⋮	⋮	⋮	⋮
5	Very high	Possibility of off-site fatalities from large-scale toxic or flammable release; possibility of multiple on-site fatalities.	Major environmental impact on-site and/or off-site (e.g., large-scale toxic contamination of public waterway)	Major on-site structural damage in the cluster; extensive off-site damage	Currently occurring ($0.5 \leq D \leq 1.0$)

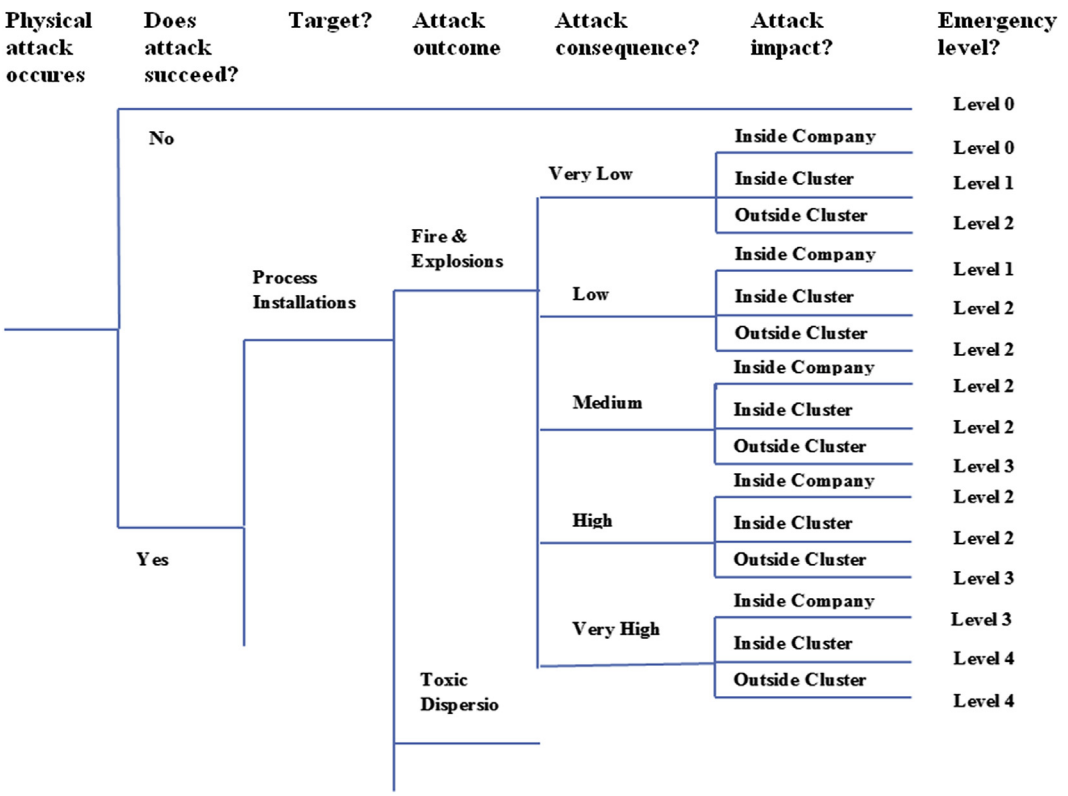


FIGURE 4.3.1 Emergency level decision tree.

causes fire and explosion. Five emergency levels are defined from level 0 (Informative Alarm) to level 4 (High-High Alarm) based on the severity of the attack. Therefore, the attack's consequence is the key element in evaluating the emergency levels.

It is important not to confuse a "security response" intended to engage and hopefully neutralize the adversaries with the broader "emergency response" that follows an attack and attempts to reduce the severity of the event and lessen the consequences in terms of loss of life and destruction of property or production capability. In this study, each emergency level indicates responsible people, response strategies, and resources.

For example, if a terrorist attack impacts a number of companies within the cluster, the emergency level at each company can be at level 0 or 1 (for a company that is not/slightly affected and its impact is within the company's boundary), level 2 (for a company that is moderately affected and may impact outside the company's premises), level 3 (for a company that is highly affected and its impact reaches other companies or outside the cluster), and level 4 (for a company that is severely affected and its impact causes further damage inside/outside the cluster).

4.3.1.4 Alert level notification system for security response

When either there is the possibility of an imminent threat or an attack has happened against a particular asset, it should rapidly be communicated across the industrial area to determine appropriate security responses and to increase the protection of target assets and to make it difficult for an adversary to harm or damage those assets (Sullivant, 2016).

A cluster alert notification system offers help to security decision-makers within the chemical cluster in order to analyze and prioritize the information regarding the potential risks at individual plants. According to API/NPRA Security Vulnerability Assessment (API/NPRA, 2003), each alert level indicates what security measures need to be implemented at the facility based on the level of the threat. For determining the alert levels, two parameters can be considered: the emergency level of the actual attack (evaluated from the previous section) and the likelihood of terrorist attack (L) against other critical asset within the cluster.

As shown in Section 4.1.1, L can be defined as the multiplication of Threat (T) and asset' Attractiveness (A). For illustrative purposes, it is assumed that the likelihood of IED attacks can be considered very high denoted with a probability of 0.8, indicating that there is a credible threat against similar assets.

Furthermore, for evaluating A, the most critical asset − from the terrorists' perspective − at single companies is identified and the respective ranking level is determined from Table 4.3.5. The multiplication of the evaluated ranking probability of A and 0.8 yields L, and its respective ranking level is shown in Table 4.3.6.

A matrix can be developed in order to determine the alert level within the companies of the cluster. The emergency level of an attack (see Section 4.3.1.3) is placed on the vertical axis while the likelihood of the attack on the horizontal axis. The matrix is presented in Fig. 4.3.2 while Table 4.3.7 provides a specific definition of each alert level.

Table 4.3.5 Target asset attractiveness ranking based on American Petroleum Institute (API) (2013).

Ranking	Descriptor	Conditional probability of the act	Threat interest ranking
1	Very low	$0.0 \leq A \leq 0.2$	Threat would have little to no level of interest in the asset.
2	Low	$0.2 < A \leq 0.4$	Threat would have some degree of interest in the asset, but it is not likely to be of interest compared to other assets.
3	Medium	$0.4 < A \leq 0.6$	Threat would have a moderate degree of interest in the asset relative to other assets.
4	High	$0.6 < A \leq 0.8$	Threat would have a high degree of interest in the asset relative to other assets.
5	Very high	$0.8 < A \leq 1.0$	Threat would have a very high degree of interest in the asset, and it is a preferred choice relative to other assets.

Table 4.3.6 Likelihood of attack ranking.

Ranking	Descriptor	Likelihood of attach
1	Very low	$0.0 \leq L \leq 0.2$
2	Low	$0.2 < L \leq 0.4$
3	Medium	$0.4 < L \leq 0.6$
4	High	$0.6 < L \leq 0.8$
5	Very high	$0.8 < L \leq 1.0$

ER level	Likelihood of attack				
	1	2	3	4	5
0	Alert level 0	Alert level 1	Alert level 1	Alert level 2	Alert level 2
1	Alert level 1	Alert level 1	Alert level 2	Alert level 2	Alert level 3
2	Alert level 1	Alert level 2	Alert level 2	Alert level 3	Alert level 3
3	Alert level 2	Alert level 2	Alert level 3	Alert level 3	Alert level 4
4	Alert level 2	Alert level 3	Alert level 3	Alert level 4	Alert level 4

FIGURE 4.3.2 Alert level decision matrix.

Table 4.3.7 Alert level description.

Ranking	Description	Alert level considerations
0	Low	Low risk of terrorist attack, normal security posture and conduct of business operations.
1	Guarded	General risk of terrorist attack, heightened awareness advisory notice by nearby companies or the cluster security.
2	Elevated	Significant risk of terrorist attack, increasing surveillance of critical locations. Coordinating emergency plans as appropriate with nearby companies.
3	High	High risk of terrorist attacks, extend monitoring capability, increase security posture. Preparing to execute contingency procedures (such as evacuation site personnel). Restricting threatened facility access to essential personnel only.
4	Severe	Severe risk of terrorist attacks, increasing or redirecting personnel to address critical emergency needs. Expand surveillance and response capability. Assigning emergency response personnel and prepositioning and mobilizing specially trained teams or resources.

Adapted from DHS Department of Homeland Security, 2019. U.S. National Terrorism Advisory System [WWW Document]. URL: https://www.dhs.gov/national-terrorism-advisory-system.

4.3.1.5 Multiplant decision matrix

The identified attack scenarios are placed on the vertical axis, and all the plants within the cluster are placed on the horizontal axis of the matrix. The emergency levels and the alert levels identified from the decision tree and the decision matrix are shown within each cell of the matrix for the companies being either affected by the attack or a likely target for similar attacks. The established multiplant matrix model is partly depicted in Fig. 4.3.3.

	Company A		Company B		Company C	
	ER level	Alert level	ER level	Alert level	ER level	Alert level
SCEN 01	1	3	2	2	3	4
SCEN 02	3	4	1	2		
...						

FIGURE 4.3.3 Example of a multiplant decision matrix.

4.3.2 Application of the methodology

4.3.2.1 Definition of a case study

In order to demonstrate the developed methodology, a chemical cluster including three plants is taken into account (Fig. 4.3.4).

It is considered that terrorists had managed to access Company 3. They used a truck as a VBIED containing 13,608 kg (TNT equivalent) of explosive mass (Table 4.3.1). They have the truck parked at Attack Position 1 (AP1 in Fig. 4.3.4), near storage tank area 1 and

FIGURE 4.3.4 Chemical cluster comprising three chemical plants adopted in the case study.

Dock 1. The impact of the explosion is large enough to cause damage to nearby process equipment leading to a major fire, following the procedure described in Section 3.4. Features of the equipment affected by the explosion are reported in Table 4.3.8.

For consequence assessment, wind direction of south west (SW), wind speed of 7 m/s, stability class D, and ambient temperature of 20 °C were considered.

Table 4.3.8 Information related to the equipment influenced by VBIED detonation at AP1.

Vessel ID	Type	Diameter (m)	Height (m)	Stored substance	Inventory (m^3)
T1—T4	Atmospheric	60	21.2	Kerosene	54,000
T5—T6	Atmospheric	35	18.0	Kerosene	15,586
T7	Atmospheric	18	15.2	Kerosene	3,481
T8—T11	Atmospheric	60	21.9	Benzene	55,800
T12—T13	Atmospheric	18	15.2	Benzene	1,934
T14	Atmospheric	30	21.2	Ammonia	13,500

4.3.2.2 Results and discussion

The potential impact radius of the explosion against the atmospheric storage tanks in area 1 (at Company 3) is calculated as 192 m, based on the overpressure escalation thresholds of 0.22 bar. The explosion stand-off distance contour is shown in Fig. 4.3.5 while

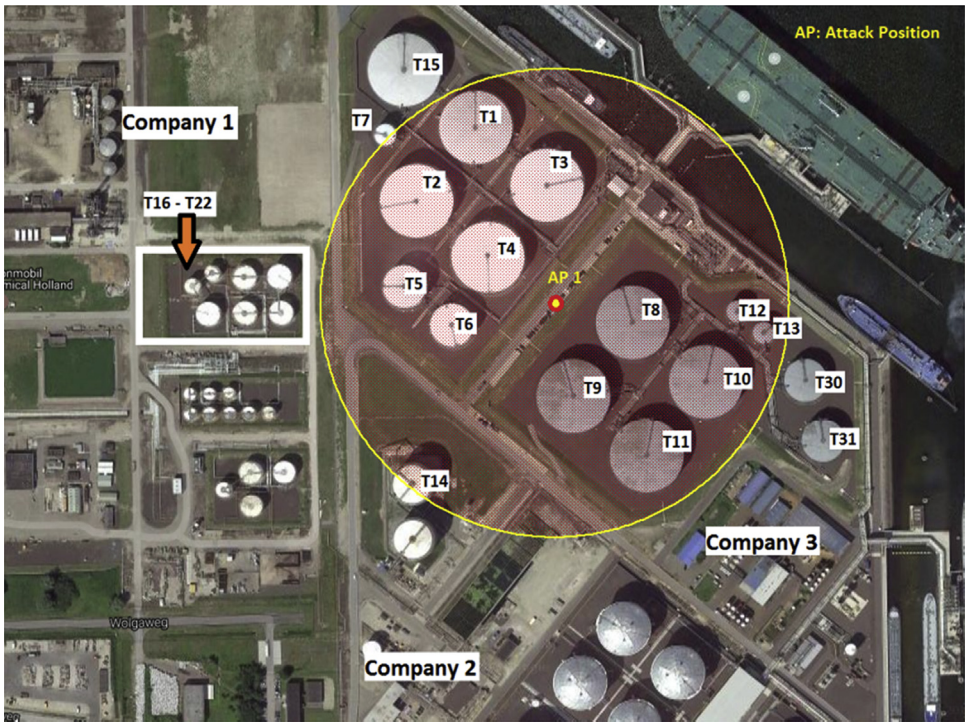


FIGURE 4.3.5 The impact zone (0.22 bar) of a VBIED detonation at AP1.

Table 4.3.9 Primary and secondary scenarios triggered by VBIED detonation at AP1.

Escalation vector	Affected units	Primary scenario	Escalation vector	Secondary units	Damage probability	Possible secondary scenarios
Overpressure	T1—T7	Pool fire	Radiation	T15, T16—T22	0.022 7.35 E7	Pool fire, tank fire,
Overpressure	T8—T13	Pool fire	Radiation	T30, T31	0.005	Pool fire
Overpressure	T14	Leakage/toxic release	—	—		—

Table 4.3.10 Likelihood of attack at the chemical cluster.

Company	Most critical target asset from threat's perspective	Attractiveness score (A)	Threat (T) probability	Likelihood of attack (L = A × T)	Likelihood of attack ranking
1	Chlorine pressurized vessels	1.0	0.8	0.80	5: Very high
2	Ammonia tank	0.8	0.8	0.64	4: High
3	Tank areas 1 and 2	0.9	0.8	0.72	4: High

Table 4.3.9 summarizes the associated equipment items that receive explosion overpressure higher than or equal to the correspondent threshold value.

As indicated in Fig. 4.3.5, the attack not only has severe impact inside Company 3, it also affects the Northern part of Company 2. It is assumed that the damaged units by blast overpressure in Company 3 will initiate pool fires that are able to impact on other companies within the cluster. The consequence of the pool fire scenarios are calculated using the ALOHA software package (http://www.epa.gov/OEM/cameo/aloha.htm) on the nearby units exposed to high heat radiation levels (greater than or equal to the threshold values in Table 4.3.2). The primary pool fire scenarios have the potential to cause further damage and trigger secondary scenarios (such as pool fire, tank fire, explosions, etc.) on target equipment. For example, the pool fire at tank T2 will affect several equipment (T16—T22) in Company 1. The results of the primary pool fire scenarios and the domino probabilities of affected units are reported in Table 4.3.10.

Besides the damage to the properties and equipment, there would be casualties not only at Company 3 but also at the other companies within the cluster. The off-site (outside cluster) casualties may happen due to indirect effects of the attack. For example, the blast overpressure and projections may cause a major leakage at the ammonia storage tank (T14). The personnel of passing ships or boats in the nearby waterway may be exposed to high amounts of the toxic gas (within the AEGL-2) and would experience serious or irreversible adverse health effects. Moreover, the gas cloud (AEGL-1) is likely to reach the residential area outside the cluster (10 km), causing

notable discomfort, irritation, and reversible effects to the public. Using Table 4.3.2 and the decision tree in Fig. 4.3.1, the emergency levels are determined as follow:

- Company 1 is not directly impacted by the attack; however, the results from Table 4.3.9 indicate that several units in this plant are exposed to high levels of heat radiation, and the domino effect is likely. The consequence ranking is medium, and it will not cause further adverse impacts outside the company premises. Therefore, the emergency level can be identified as 2.
- Company 2 is directly impacted by the blast overpressure, and T14 (ammonia storage tank) is damaged and may cause huge impact both inside and outside the cluster. Therefore, the emergency level is 3.
- A large part of Company 3 is damaged by the attack, there is a severe environmental and property damage, and domino effect is almost certain within the company. The consequence is very high, and Dock 1 area and the nearby waterway are impacted accordingly. Therefore, the emergency level is 4.

Since the threat (T) for this security event is considered very high for each chemical plant with a probability 0.8, and the most attractive target assets at the three companies are identified, the likelihood of attack can be calculated as in Table 4.3.10.

After the emergency levels and the likelihood of attack for each company are evaluated, the alert levels can be predicted using the decision matrix in Fig. 4.3.3. The final result is presented in the multiplant decision matrix in Fig. 4.3.6.

The results obtained through the present approach demonstrate the capability of addressing the emergency and alert level in complex chemical clusters populated by several companies. In this way, the response and preparedness account for the individual vulnerabilities of the single plants and units but provide a solution and decision-making support at the level of the entire cluster. Each emergency level identifies the potential actions that each single plant could adopt to prepare for and respond to a terrorist attack scenario. Likewise, each alert level indicates to what extent to increase the security of other critical assets due to either the possibility of an imminent threat or the occurrence of an actual attack against a particular asset.

	Company 1		Company 2		Company 3	
	ER level	Alert level	ER level	Alert level	ER level	Alert level
Attack to the car park area in Company 3	2	3	3	3	4	4

FIGURE 4.3.6 The multiplant decision matrix.

4.4 Conclusions

This chapter demonstrated the capabilities of conventional tools (Section 4.1) and the potentialities of innovative methods, for either provisional assessment (Section 4.2) or emergency response (Section 4.3) in supporting quantitative security risk and vulnerability studies in a dual perspective.

Firstly, the evaluation of vulnerability and, more in general, the likelihood of attack success to the units in a given plant, or even a chemical cluster, may support the identification of the most security-critical equipment items. In the demonstrative case studies presented, the equipment inherent fragility (atmospheric vs. pressurized equipment; storage vs. process units), the location, the different configuration of physical security elements are all elements that are accounted for in both conventional and advanced tools. However, the advantage of quantitative methods is in the possible ranking that may drive a better informed decision-making; moreover, the adoption of specific metrics at unit, plant, and cluster level may lead to an integrated and more effective emergency response (see Section 4.3).

Secondarily, the vulnerability and risk assessment based on quantitative tools allows for the sound identification of the more critical attack scenarios and, eventually, the effectiveness of physical security systems in stopping the execution of an attack. In some cases, it might be also quantitatively demonstrated that security protection is not completely adequate, depending on the type of scenario, such as in the case described in Section 4.2.2.4. Improvements may be obtained if the "Defence in Depth" principle (IAEA, 1996) is applied in the design of physical security elements, by deploying concentric rings of protection to defend critical targets. Each ring represents an independent defense that accomplishes or triggers the success of primary protection functions of assessed detection (which is often critical and not redundant), delay, and response.

Despite the potential value of the results obtained in the perspective of security management in chemical facilities and chemical clusters, it is worth mentioning that the present approaches feature some limitations, mainly due to the simplified assumptions adopted and to the extensive use of expert judgment. The latter is justifiable in light of the complex nonphysically explainable nature of the considered dependencies and of the lack of reliable quantitative data in the technical literature, especially when dealing with security barriers performance. However, the rigorous methods presented surely constitute a step ahead in the concrete determination of the existing level of site protection against external malevolent attacks and in the identification of weak elements. These objectives may not be achieved by the compliance-based assessment of security countermeasures nor by a qualitative assessment of physical security systems seen as a whole, which are still proposed in the majority of security risk assessment methodologies.

References

American Institute of Chemical Engineers - Center for Chemical Process Safety (AIChE-CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers - Center of Chemical Process Safety, New York.

Al Arabiya News, 2014. Second Oil Depot Catches Fire in Lybia's Tripoli [WWW Document]. URL: http://english.alarabiya.net/en/business/energy/2014/07/28/Huge-oil-depot-blaze-puts-Tripoli-under-threat-.html.

Allegri, E., 2010. Offshore: tante scritte sui muri e poco spazio al dibattito e all'informazione, capire il significato e il perché della protesta sul rigassifcatore [WWW Document]. URL: http://www.livornomagazine.it/Inchieste/Allegri_no_offshore.htm.

American Petroleum Institute (API), 2013. ANSI/API Standard 780 — Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry. American Petroleum Institute, Washington, DC.

American Petroleum Institute, National Petrochemical & Refinery Association, 2003. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries.

API/NPRA, 2003. Security Vulnerability Assessment. American Petroleum Institute Publishing Services, Washington, DC.

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.

Argenti, F., Cozzani, V., Landucci, G., Reniers, G., 2016a. Probabilistic vulnerability analysis of process facilities to external acts of interference. In: Risk, Reliability and Safety: Innovating Theory and Practice - Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016, p. 344.

Argenti, F., Landucci, G., Reniers, G., 2016b. Probabilistic vulnerability assessment of chemical clusters subjected to external acts of interference. Chem. Eng. Trans. 48, 691—696.

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.

Argenti, F., Landucci, G., Reniers, G., Cozzani, V., 2018. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. Reliab. Eng. Syst. Saf. 169, 515—530.

Bajpai, S., Gupta, J.P., 2005. Site security for chemical process industries. J. Loss Prev. Process Ind. 18, 301—309.

Bajpai, S., Gupta, J.P., 2007. Terror-proofing chemical process industries. Process Saf. Environ. Prot. 85, 559—565.

Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621—631.

CCPS - Center of Chemical Process Safety, 2000. Guideline for Chemical Process Quantitative Risk Analysis. American Institute of Chemical Engineers - Center of Chemical Process Safety, New York, NY.

Cozzani, V., Gubinelli, G., Antonioni, G., Spadoni, G., Zanelli, S., 2005. The assessment of risk caused by domino effect in quantitative area risk analysis. J. Hazard. Mater. 127, 14—30.

Cozzani, V., Gubinelli, G., Salzano, E., 2006. Escalation thresholds in the assessment of domino accidental events. J. Hazard. Mater. 129, 1—21.

Cozzani, V., Antonioni, G., Landucci, G., Tugnoli, A., Bonvicini, S., Spadoni, G., 2014. Quantitative assessment of domino and NaTech scenarios in complex industrial areas. J. Loss Prev. Process Ind. 28, 10—22.

Csardi, G., Nepusz, T., 2006. The igraph software package for complex network research. Int. J. Complex Syst. 1695.

Cucchi, F., 2010. Rigassificatore di Livorno: proteste e repressione [WWW Document]. URL: http://www.deapress.com/ultime-nove-mainmenu-2/notizie-flash-mainmenu-52/7461-rigassificatore-di-livorno-proteste-e-repressione.html.

DHS Department of Homeland Security, 2019. U.S. National Terrorism Advisory System [WWW Document]. URL: https://www.dhs.gov/national-terrorism-advisory-system.

European Commission, 2008. Council Directive, 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. Off. J. Eur. Communities L345, 75–82.

European Commission, 2012. European Parliament and Council Directive 2012/18/EU of 4 July 2012 on control of major-accident hazards involving dangerous substances, amending and subsequently repealing council directive 96/82/EC. Off. J. Eur. Communities L197, 1–37.

FEMA Federal Emergency Management Agency, 2005. FEMA 452 - A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings. Federal Emergency Management Agency, New York, NY.

Freeman, L.C., 1978. Centrality in social networks conceptual clarification. Soc. Netw. 1, 215–239.

Garcia, M., 2006. Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann, Newtown, MA.

Garcia, M., 2008. The Design and Evaluation of Physical Protection Systems, second ed. Butterworth - Heinemann, Burlington, MA, USA.

Garrick, B.J., Hall, J.E., Kilger, M., McDonald, J.C., O'Toole, T., Probst, P.S., Parker, E.R., Rosenthal, R., Trivelpiece, A.W., Van Arsdale, L.A., Zebroski, E.L., 2004. Confronting the risks of terrorism: making the right decisions. Reliab. Eng. Syst. Saf. 86.

GeNie, 2019. GeNie [WWW Document]. URL: https://support.bayesfusion.com/docs/GeNIe/.

Gupta, D.K., 2004. Exploring roots of terrorism. In: Bjorgo, T. (Ed.), Root Causes of Terrorism. Routledge, London, UK.

IAEA- International Atomic Energy Agency, 1996. Defence in Depth in Nuclear Safety. IAEA-International Atomic Energy Agency, Vienna.

Iannaccone, T., Landucci, G., Scarponi, G.E., Bonvicini, S., Cozzani, V., 2019. Inherent safety assessment of alternative technologies for LNG ships bunkering. Ocean Eng. 100–114.

IRIN, 2014. Fighting, Fuel Fires and Fear in Tripoli [WWW Document]. Rep. 100539. URL: http://www.irinnews.org/report/100539/fighting-fuel-fires-and-fear-in-tripoli.

Jensen, F.V., Nielsen, T., 2007. Bayesian Networks and Decision Graphs, second ed. Springer, New York, NY.

Jochum, C., 2005. Can chemical plants be protected against terrorist attacks? Process Saf. Environ. Prot. 83, 459–462.

Kennett, M., Letvin, E., Chipley, M., Ryan, T., 2005. Federal Emergency Management Agency (FEMA), US Department of Homeland Security, United States of America, US Dept. of Veterans Affairs and United States of America, risk assessment: a how-to guide to mitigate potential terrorist attacks against buildings. FEMA Risk Manag. Ser.

Khakzad, N., 2015. Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. Reliab. Eng. Syst. Saf. 138, 263–272.

Khakzad, N., Reniers, G., 2015. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. Reliab. Eng. Syst. Saf. 143, 63–73.

Khakzad, N., Reniers, G., 2019. Low-capacity utilization of process plants: a cost-robust approach to tackle man-made domino effects. Reliab. Eng. Syst. Saf 191, 106114. https://doi.org/10.1016/j.ress.2018.03.030 (in press).

Khakzad, N., Khan, F., Amyotte, P., Cozzani, V., 2013. Domino effect analysis using Bayesian networks. Risk Anal. 33, 292–306.

Khakzad, N., Landucci, G., Reniers, G.L.L., 2017a. Application of graph theory to cost-effective fire protection of chemical plants during domino effects. Risk Anal. 37, 1652–1667.

Khakzad, N., Reniers, G.L.L., van Gelder, P., 2017b. A multi-criteria decision making approach to security assessment of hazardous facilities. Loss Prev. Process Ind. 48, 234–243.

Landucci, G., Gubinelli, G., Antonioni, G., Cozzani, V., 2009. The assessment of the damage probability of storage tanks in domino events triggered by fire. Accid. Anal. Prev. 41, 1206–1215.

Landucci, G., Cozzani, V., Birk, M., 2013. Heat radiation effects. In: Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier, Amsterdam, The Netherlands, pp. 70–115.

Lees, F.P., 1996. Loss Prevention in the Process Industries, second ed. Butterworth - Heinemann, Oxford.

Lou, H.H., Muthusamy, R., Huang, Y., 2003. Process security assessment: operational space classification and process security index. Process Saf. Environ. Prot. Trans. Inst. Chem. Eng. Part B 81, 418–429.

Matteini, A., Argenti, F., Salzano, E., Cozzani, V., 2018. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2018.03.001.

Norman, T.L., 2010. Risk Analysis and Security Countermeasure Selection. CRC Press, Boca Raton, FL.

Nunes-Vaz, R., Lord, S., Ciuk, J., 2011. A more rigorous framework for security-in-depth. J. Appl. Secur. Res. 6, 372–393.

Ovidi, F., Pagni, E., Landucci, G., Galletti, C., 2019. Numerical study of pressure build-up in vertical tanks for cryogenic flammables storage. Appl. Therm. Eng. 161, 114079.

Paltrinieri, N., Tugnoli, A., Cozzani, V., 2015. Hazard identification for innovative LNG regasification technologies. Reliab. Eng. Syst. Saf. 137, 18–28. https://doi.org/10.1016/j.ress.2014.12.006.

Pieraccini, S., 2012. A Livorno sopravvive solo l'impianto offshore [WWW Document]. URL: http://www.ilsole24ore.com/art/economia/2012-03-07/livorno-sopravvive-solo-impianto-064521.shtml?uuid=Abzc3b3E.

Post, J.M., Ruby, K.G., Shaw, E.D., 2002. The radical group in context: 1. An integrated framework for the analysis of group risk for terrorism. Stud. Confl. Terror. 25, 73–100.

Reniers, G., Cozzani, V., 2013. Domino effects in the process industries: modelling, prevention and managing. In: Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier B.V., Amsterdam, The Netherlands, pp. 1–372.

Saaty, T.L., 2008. Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World. RWS Publications, Pittsburgh, Pennsylvania.

Said, S., Faucon, B., 2014. Fired by Libyan Militia Hit Tripoli Fuel Depot [WWW Document]. He Wall Str. J. URL: http://online.wsj.com/articles/rocket-fired-by-libyan-militia-sets-tripoli-fuel-depot-on-fire-1406989950.

Scarponi, G.E., Landucci, G., Ovidi, F., Cozzani, V., 2016. Lumped model for the assessment of the thermal and mechanical response of LNG tanks exposed to fire. Chem. Eng. Trans. https://doi.org/10.3303/CET1653052.

Srivastava, A., Gupta, J.P., 2010. New methodologies for security risk assessment of oil and gas industry. Process Saf. Environ. Prot. 88, 407–412.

Störfall Kommission (SFK), 2002. SFK-GS-38 Report.

Sullivant, J., 2016. Building a Corporate Culture of Security: Strategies for Strengthening Organizational Resiliency. Butterworth-Heinemann, Oxford (UK).

Uijt de Haag, P.A.M., Ale, B.J.M., 1999. Guidelines for Quantitative Risk Assessment (Purple Book). Committee for the Prevention of Disasters, The Hague, NL.

Uth, H.-J., 2005. Combating interference by unauthorised persons. J. Loss Prev. Process Ind. 18, 293–300.

Van Den Bosh, C.J.H., Weterings, R.A.P.M., 2005. Methods for the calculation of physical effects (Yellow Book). In: Committee for the Prevention of Disasters, the Hague (NL), third ed.

Weber, P., Medina-Oliva, G., Simon, C., Iung, B., 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Eng. Appl. Artif. Intell. 25, 671–682. https://doi.org/10.1016/j.engappai.2010.06.002.

5 Security culture and security management models

5.1 Security culture

Many efforts have been made to better understand the concept and characteristics of organizational safety culture, and it still remains a true challenge to describe it and to try to influence it. Safety culture has been a hot topic not only for academics and researchers since the beginning of the 21st century, but also for practitioners. The topic was studied in the past two decades by a variety of disciplines, for instance, sociologists, psychologists, engineers, safety scientists, and others. Nonetheless, until very recently, no encompassing and widely accepted model has been developed and put forward to capture and understand safety culture. On the contrary, the safety culture concept is a matter of debate and discussion among scientists.

Recently, thorough scientific research has led to the development of a model satisfying the needs of the different scientific disciplines and their separately developed models. This harmonized model for safety culture, the so-called TEAM model (Vierendeels et al., 2018), unifies all aspects of safety science within an organization and explains smoothly and clearly the position of the aspects with respect to one another. We will apply this innovative model to security and expound, from a security perspective, how it can be used in industrial practice. Fig. 5.1.1 illustrates the TEAM model adapted from safety culture to security culture and can be regarded as an encompassing security culture model.

5.1.1 The need for a proactive and integrative approach of security culture

Based on currently available literature, it can be concluded that security research lacks an integrative approach. Mainly the technological security aspects receive attention. It is only in the last decade that the concept of security culture has gained interest from researchers and business leaders, with a dominant position of information/cyber security. There is almost no reference to other types of security issues. However, in analogy with safety culture, a proactive and holistic approach is needed when addressing the security culture of an organization.

As elaborated in the safety culture model of Vierendeels et al. (2018), safety culture consists of three main domains related to technological, organizational, and human

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00005-6

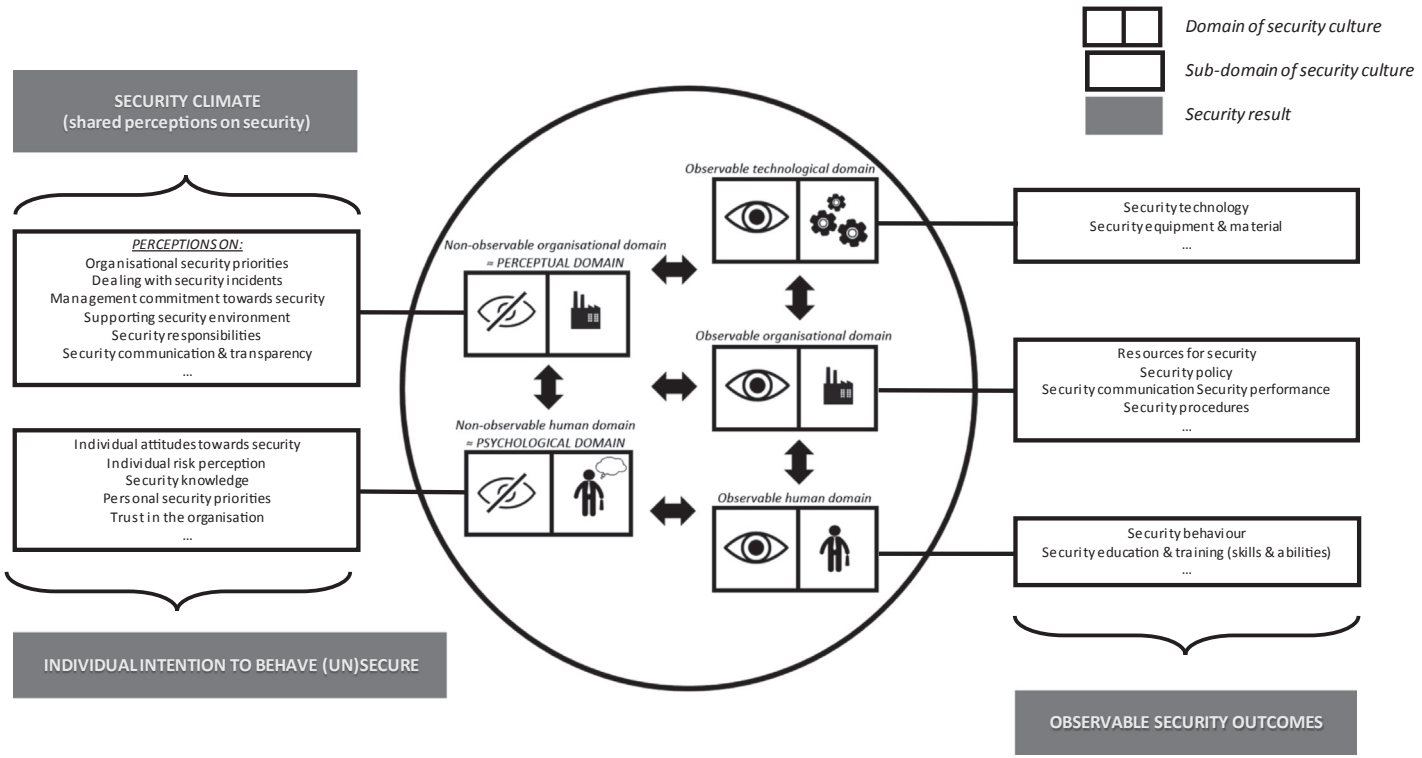


FIGURE 5.1.1 An integrative conceptual framework for physical security culture in organizations. Reproduced from *van Nunen, K., Sas, M., Reniers, G., Vierendeels, G., Ponnet, K., Hardyns, W., 2018. An integrative conceptual framework for physical security culture in organisations. J. Integr. Secur. Sci. 2 (1), 25–32.*

aspects. This approach can be extended to the field of security culture, where security culture also consists of three main domains:

(1) A technological domain, which comprises aspects regarding the present security technology, material, and equipment present in the company.
(2) An organizational domain, which comprises aspects such as the security management system and procedures, the company security policy, and the resources available for security.
(3) A human domain, which comprises aspects such as knowledge, attitudes, assumptions, decisions, and actions of individuals regarding security.

Both the organizational and the human domains are manifested at two levels:

(1) Firstly, there are the tangible, observable aspects regarding security. These are the aspects that are observable when walking around in the company. This concerns, for instance, the security behavior of employees, or the security rules, procedures, instructions, etc., that can be consulted in documents of the company.
(2) Secondly, there are the less tangible, nonobservable aspects. These are the aspects that cannot be observed by walking around in a company. This concerns, for instance, what employees think of the level of security in the company, or the attitude they have toward security.

The technological domain consists only of observable aspects. This structure leads to five domains, as can be seen in Fig. 5.1.1, which together form the physical security culture of an organization. The five domains can be further divided into several subdomains, which are represented as the white boxes in Fig. 5.1.1. Important are the arrows in the model, which symbolize that all the different domains of the physical security culture are related in a cyclic way.

The gray boxes in the conceptual model represent the security results. In case of the three observable domains, the several subdomains result in observable security outcomes. In case of the nonobservable organizational domain or the perceptual domain, the several subdomains result in the security climate of an organization, being the shared perceptions on security. In case of the nonobservable human domain or the psychological domain, the several subdomains result in the individual intention to behave securely or insecurely.

5.1.2 Addressing the security culture of an organization

To address the physical security culture of an organization, several steps should be taken as illustrated in Fig. 5.1.2. Firstly, the security culture should be diagnosed. In order to obtain a clear image of the current physical security culture in the organization, all subdomains constituting physical security culture should be measured.

Subsequently, based on this measurement, recommendations should be formulated and implemented in order to improve the current physical security culture (van Nunen et al., 2018). It is important that continuous attention is being paid to the security of a company. Follow-up is needed in order to meet with possible changes within the

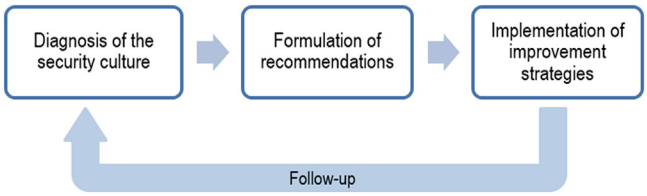


FIGURE 5.1.2 Addressing physical security culture. Reproduced from *van Nunen, Sas, M., Reniers, G., Vierendeels, G., Ponnet, K., Hardyns, W., 2018. An integrative conceptual framework for physical security culture in organisations. J. Integr. Secur. Sci. 2 (1), 25–32.*

company as well as external developments and trends in the field of security. It is an everlasting process, a cycle of evaluation and maintenance or change.

During this continuous process of addressing security culture, some aspects should be taken into account, in analogy with addressing safety culture (van Nunen et al., 2018). It is, for instance, important to use a multimethod approach in order to adequately explore and understand the security culture of an organization. Also, the involvement of the entire organization is important. Employees, supervisors, managers, contractors, clients, suppliers, etc., all should be taken into account when diagnosing the security culture. This comprehensive involvement is crucial not only during the diagnose of the security culture, but also during the phase of formulating improvement strategies and setting priorities. This comprehensive involvement not only leads to a more accurate diagnose of the security culture, it also leads to the creation of a foundation to successfully implement and maintain the improvement strategies.

The proposed conceptual framework for physical security culture in organizations has the advantage of bringing technology, organizational issues, and human aspects together in a coherent, integrative, and related way. The aim of the cultural model is to take all security-related aspects into account, leading to a proactive approach of physical security in the organization, instead of working on an incident-driven base. The framework provides specific points of departure to make the security culture measurable and by extension controllable. The importance of continuous attention for security is being stressed, as well as the importance of the involvement of the entire organization in order to obtain sustainable improvements in the field of security.

In current industrial practice, internal and external audits are a much-used approach to “measure” the security level of a company. Such audits, however, only provide an idea of a part of the observational security domain and fail to give insight into the (much more extensive concept of) security culture or of the “security DNA” of an organization. To be able to “grasp” the security level of an organization, several research methods need to be combined (as already mentioned) and security performance indicators need to be used to ensure continuous improvement. The different methods that need to be employed are (i) document- and observational assessments to capture and evaluate the observable factors, (ii) questionnaires to capture and evaluate the perceptual factors and the security climate, and (iii) in-depth interviews with individual employees and with groups of employees, to capture the personal psychological factors and the intentions to

behave and the motivation of employees. In summary, a multimethod design needs to be developed and used to understand the security culture of a company and to describe it and to accurately know what measures are needed to improve it.

Furthermore, performance management science needs to be used to guarantee that the security culture is continuously monitored and that required improvements are made as promptly as feasible. Concrete and unambiguous indicators should thus be developed and monitored by an organization, linked to objectives, to assess its security culture at regular intervals and take action when deemed necessary.

5.2 Security performance management indicators

Some guidelines exist to define indicators. Indicators, for instance, need to be formulated as "SMART." SMART is an acronym that implies that indicators should be (i) *specific* and well-described (or in other words, unambiguously defined); (ii) *measurable* so that it is possible to verify with a certain frequency what the result of an indicator is; (iii) *achievable* and demonstrable such that every indicator has a purpose that is flexible enough to realize improvement, but not in an extreme way such that the indicator will not lead to discouragement; (iv) *relevant* for the organization and what it tries to accomplish; and finally (v) *time-bound* in terms of realistic deadlines for the realization of the aims of every indicator.

Objectives can be formulated in different ways: as an absolute number (a so-called target value), as a percentage (for example satisfy x% of the criteria, decrease of y%, satisfy z% of a checklist, etc.), or as a relative measurement compared with a certain benchmark (for example, higher than the national average, lower than the average of the industrial sector where the organization belongs to, better than the result of last year or than the average of the three last years, etc.).

Moreover, different kinds of indicators exist, and the different kinds need to be determined for both types of security risks (type I and type II). The different indicator types are:

- management indicators;
- process indicators;
- result indicators.

Management indicators provide an idea to higher management whether the conditions to achieve certain predetermined objectives are present or not. Hence, these are leading, proactive, indicators giving insight into the means (time, money, manpower, etc.) that are needed to achieve objectives.

Leading process indicators proactively answer the question whether a certain goal would be achievable and whether the efforts that are necessary to achieve the goal are carried out in an optimal way. These indicators provide information about the processes present in the organization (primary work processes, administrative processes, supporting processes, etc.) and give insight into how the objectives can be reached in an optimal way. Since these are the indicators leading to continuous improvement in this

case regarding security issues, they are the most needed to improve company security policy and finally achieve an ever-improving organizational security culture.

Result indicators, on the other hand, which are (lagging) reactive indicators, provide an idea of past achievements and thus give an indication whether predetermined goals were achieved or not. They give insight into those objectives being achieved and those not being achieved.

The development and fine-tuning of indicators is a science in itself and requires a variety of knowledge and know-how. Performance management science is far from evident and depending on the organizational context (e.g., a large organization vs. a small company, or a highly hierarchical management approach vs. a very flat management structure, etc.), a trial-and-error approach is needed to come to an adequate package of management-, process-, and result indicators that is able to monitor and steer the security culture of an organization.

The three kinds of indicators (i.e., management, process, and result) can be directly linked to the observational part of the security culture model (see Fig. 5.1.1). These indicators, directly monitoring the observational part of the model and hence optimizing the observational parameters, also will indirectly influence and improve the non-observational dimensions of security culture, that is, the security climate (aggregated perception) and the motivation (intention to behave) of employees.

If the observational dimension of the security culture model is used to optimize security in an organization, indicators need to be elaborated for the three observable domains Technology, Procedures (and organizational aspects), and People (observable behavior). For every domain, the three kinds of indicators need to be worked out. In general, mostly process indicators are needed, since they are focused at continuously improving the (human and nonhuman) processes within the organization, and they are proactively leading to a better situation within the workplace. Since management indicators are key (overall) leading indicators that need to steer company policy on a long term, not many of them are needed. Also in the case of result indicators, providing information on what went wrong in the past (and hence, the measurement is too late — they are reactive/lagging), not many indicators are required. As a rule of thumb, if 100 indicators are employed for performance management of security within an organization, there should be 10 management indicators, 10 result indicators, and 80 process indicators. Table 5.2.1 provides examples of possible indicators, for the different domains, see also Meyer and Reniers (2016).

Furthermore, Mazri et al. (2012) indicated that certain basic information, technical data, organizational information, and IT data are required for every indicator. Table 5.2.2 provides an overview of the information required to ensure adequate use of performance indicators and to install a true company memory management system.

Performance management is a very powerful tool to systematically map the effectiveness with which every aim or goal (short-term or long-term) within the different security dimensions and domains of an organization is reached. It can also be used to prioritize actions, budget allocations, etc.

Table 5.2.1 A nonexhaustive list of security performance management indicator examples.

Management indicators
- 2-Yearly budget available for purchasing and/or upgrading security software.
- 5-Yearly budget available to carry our security risk assessments.
- Time and manpower yearly available to carry out security risk assessments
- 2-Yearly budget available for security training and education of company personnel.
- Overall 2-yearly budget assigned to security activities.
Process indicators
- An external audit of the company's safety and security policy is carried out every 5 years.
- Number of legally prescribed security procedures that are not fulfilled are less than 5% of all legally prescribed security procedures; this is checked every 3 years.
- Every 5 years the entire plant is checked by using security vulnerability assessments (i.e., at least per 5 years, an SVA is carried out for every installation within the plant).
- A 3-yearly internal audit of the security management program is carried out.
- The business continuity plan is tested every 2 years.
- When an internal security audit is performed, long-term recommendations for continuous improvement are given in the audit report.
- A 4-yearly check is carried out by the security department whether all security procedures are written down, understandable, up-to-date and whether they can be easily consulted by its users.
- Every 3 years, a security survey is organized among company personnel
- Every 2 years, contractor security achievements are discussed with the contractors.
- A security awareness learning trajectory for employees exists within the company.
- Percentage of executed improvement propositions within 2 years resulting from emergency plan exercises.
- Security inspections are carried out at least every 6 months in every installation of the plant.
- Access and gate control: The number of daily controlled persons out of total number of persons passing the gate.
- Number of yearly improvement proposals as a result of an internal audit in the company.
- Percentage of standardization of security documentation, checked per 6 months.
- Percentage of procedures, still leading to difficulties and incidents, evaluated per year.
- A frequency of SVAs to be carried out per installation is determined and the circumstantial conditions/approaches are described.
- Degree to which existing security legislation is taken into account by company procedures is checked every 6 months.
- Level of standardization of security documents (procedures, guidelines, working instructions, etc.)
- Number of scenarios (circumstances) for which a frequency of external audits is fixed.
- Degree to which the external emergency plan is elaborated and tested for security situations (e.g., a terrorist attack).
- Percentage of employees within an installation that has security competences.
- Number of weekly visits of management to work floor, to assess security aspects.
- Number of monthly meetings where employees receive information and feedback about the importance of security.
- Levels of satisfaction (questionnaire scores) regarding cooperation with external partners after yearly emergency exercises.
- Daily operational staff meetings are held on security.
- Every 3 months, a drill for security guards and dogs is held.
Result indicators
- Number of security incidents attributed to the same cause in 2 years.
- Score given to "security awareness" in a 2-yearly questionnaire.
- Scores employees receive during security observations using 360 degrees feedback reviews carried out every 3 years.
- Score given to "mutual communication as regards security topics" in a 2-yearly questionnaire.
- Number of recorded security events per year.

Table 5.2.2 Performance indicators – information table. *Reproduced from*

General information	
Short name	Unique codified name of indicator.
Long name	Detailed name of indicator.
Description and purpose	What does and doesn't the indicator measure? (What would there possibly be confusion about?)
Source	Who issued this indicator?
References	Available reference document(s) concerning the indicator.
Nature	Qualitative, semiquantitative, or quantitative.
Risk domains covered	Depending on the needs and the management systems implemented, a myriad of risk domains can be covered. For example, environment risks, health and safety risks, security risks, operational risks, process risks, occupational risks, quality risks, ethical risks, etc., or any combinations thereof. Note that a unique indicator may be more or less relevant for several domains.
Technical information	
Formula and unit	With what formula was the indicator's value calculated (if applicable)?
Target value	Target value (to reach a predefined performance).
Minimal and maximal values	Describe the minimal and maximal limit values within which the indicator value may be considered as "acceptable." If the indicator's value is out of these limit values, actions need to be taken.
Input data required	Information required to implement the formula described above (that led to the calculation of the indicator).
Frequency of measurement	What is the frequency with which this indicator should be measured (the periodicity of monitoring will influence on the level of resources required)?
Related indicators	Indicators are part of a "network of indicators" monitoring different system components. The relationship(s) between the indicators should be mapped and a list of additional indicators providing extra information on the indicator under consideration should be drafted.
Organizational information	
Indicator reference person (or owner)	A reference person in the organization should be affected to each indicator. This person will be responsible for the quality of the whole process from data and information collection to interpretation and communication of the results.
Data provider(s) or registrator(s)	Person(s) need to be appointed to collect and deliver the required data/ information (necessary input data).
Interpretation procedure	Person(s) need to be identified who are capable of, and who have the competence and the authority to, correctly interpret the measured indicator value and to translate this value into knowledge and insights.
Communication procedure	Person(s) within and outside the organization that should be informed about the indicator results are to be identified. The method of communicating the results is to be determined.
Relevance assessment procedure	The relevance of any indicator should be questioned at regular time intervals and according to a predefined procedure.
IT-information	
Software availability	Existing software is listed that improves the use of the indicator or that makes it more easy.
Adequacy with existing/local information system	The configuration of existing software may facilitate the input of collected data, or it may complicate this process. This fact should be taken into account beforehand.

Mazri, C., Jovanovic, A., Balos, D., 2012. Descriptive model of indicators for environment, health and safety management. Chem. Eng. Trans. 26, 465–470.

5.3 Security management models based on safety models

As already mentioned in Chapter 1, security science is a relatively young field of science, and it can learn a lot from the research that has been carried out in safety science. Over the past decades, a lot of safety theories, concepts, metaphors, and management models have been suggested by safety scientists and accident investigators. The models have thus been built after decades of experience and research, within a variety of academic disciplines, and encompassing diverse industrial sectors. Therefore, it is no surprise that the models used to deal with risks are very diverse, and that incidents and accidents were a driver and an inspiration for the builders of the models. Hereafter, a number of these theories and models will be discussed for security.

5.3.1 Physical model of security risk

In Chapter 1, we indicated that security risks are characterized by three factors: threats, vulnerabilities, and intentional losses, which together form the "Security Risk Trias." Nonetheless, risk is obviously a theoretical concept and can be described in another way. To have a profound understanding of risk, we also need to discuss this second − more "physical" approach, which is well-known for safety and based on safety science.

In order to physically describe what a security risk is, some of its key components should be defined. The notion of the "target" needs to be introduced. By definition, the target can be represented by:

- a human;
- the environment;
- a natural monument;
- a process in a company;
- a company;
- the brand image;
- Etc.

A danger is the potential of a hazard or a threat to cause damage to a target. A danger can be intentional − then it is related to the field of security and a threat is involved − or it can be accidental or by coincidence, in which case it is safety-related and a hazard is involved.

Risk exists as soon as a hazard or a threat affects one or many possible targets. An identified hazard that does not affect any target does not represent a risk, and the same goes for an identified threat not affecting any target. For example, life in Iraq or Syria may be full of threats, but as long as these threats do not affect targets in or from Canada, for instance, there are no losses possible in Canada, and hence no security risk from the identified threats in Canada. Risk is found at the interface, or at the cross section, of a hazard/threat and a target, as illustrated in Fig. 5.3.1.

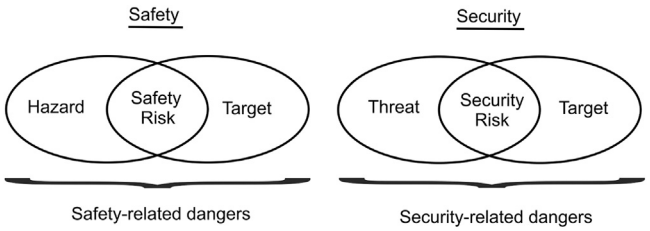


FIGURE 5.3.1 Physical risk model.

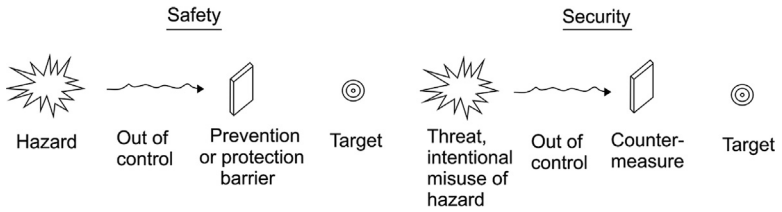


FIGURE 5.3.2 Constitutive elements of safety risk and security risk.

Basically, a risk is physically characterized by four elements:

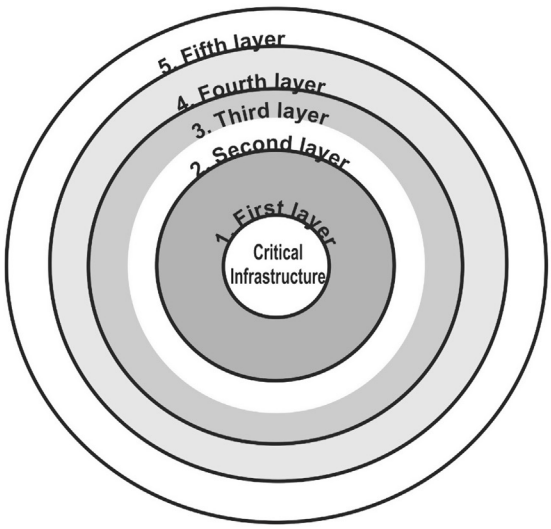
1. A hazard/threat.
2. One or several targets threatened by the hazard.
3. The evaluation of the level of the interface, and hence, danger.
4. The measures taken to reduce the danger.

These elements, depicted in Fig. 5.3.2, show that a protection and/or prevention barrier in case of safety, and a countermeasure in case of security, is required to prevent a hazard or a threat that may be(come) out of control, from reaching the target.

5.3.2 Rings of protection

The fundamental basis of security management can be expressed in a similar way to the layers of protection used in chemical process plants to illustrate safety barriers. In the similar concept of concentric rings of protection (CCPS, 2003), the spatial relationship between the location of the target asset and the location of the physical countermeasures is used as a guiding principle. Fig. 5.3.3 exemplifies the rings of protection in terms of five "layers of security protection" and a nonexhaustive list of possible component countermeasures.

In terms of security, the target is broadly defined as people (employees, visitors, contractors, nearby members of the community, etc.), information (formulae, prices, processes, substances, passwords, etc.), and property (buildings, vehicles, production equipment, storage tanks and process vessels, control systems, raw materials, finished products, hazardous materials, natural gas lines, rail lines, personal possessions, etc.) that are believed to be crucial to preventing major business disruption and substantial economic and/or societal damage.



1. First layer of security protection (Inner ring):
- Alert personnel
- Door and cabinet locks
- Network firewalls and passwords
- Visitor escort policies
- Document shredding
- Emergency communications
- Secure computer rooms
- CCTV
- Intelligence

2. Second layer of security protection (Inner Middle ring) :
- Locked doors
- Receptionist
- Badge checks
- Access control system
- Parcel inspection
- Carry out SVAs

3. Third layer of security protection (Outer middle ring):
- Lighting
- Fences
- Entrance/exit points
- Bollards
- Trenches
- Intrusion detection
- Intrusion sensors
- Guards on patrol at property fenceline

4. Fourth layer of security protection (Outer ring):
- Badge checks
- Access control system
- Turnstiles
- Window bars
- Receptionist

5.Fifth layer of security protection Law enforcement (Outside ring):
- Police
- Fire fighters
- Other law enforcement organisations

FIGURE 5.3.3 Security rings of protection illustrated as "five layers of security protection." *Adapted from Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed., Berlin: De Gruyter.*

By considering the sequence of events that might lead to a potentially successful attack, another representation can be given, illustrating the effectiveness of the rings of protection (see Fig. 5.3.4).

Firstly, companies can clearly protect themselves in a much better way against external attacks than against attacks from within the company itself, because in the latter case there only exists indoor security to avert the threat, and there are only two layers of security protection (first and second layer). Secondly, as the effective prevention,

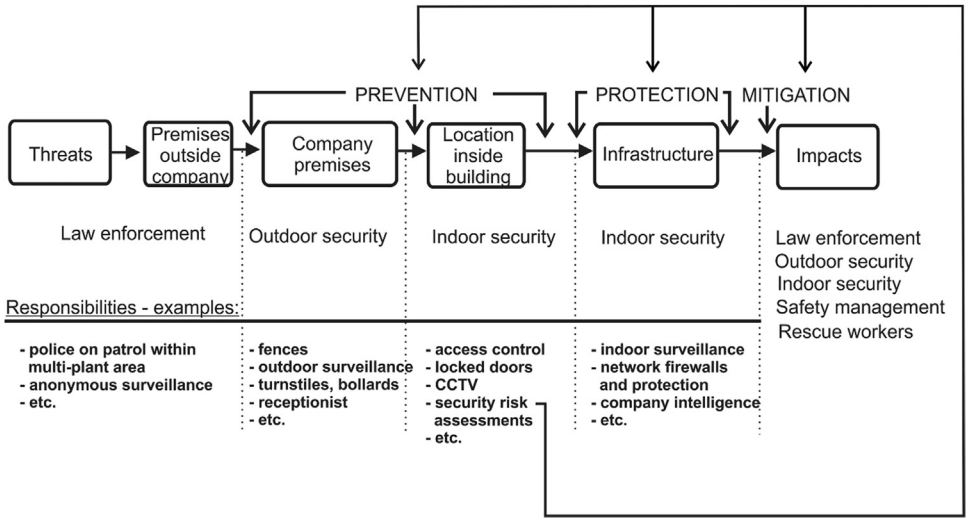


FIGURE 5.3.4 Anatomy of an attack: the role of the rings of protection described in Fig. 5.3.3. *Adapted from Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed., Berlin: De Gruyter.*

protection, and mitigation of attacks depend on meticulously carrying out security risk assessments, the latter is of crucial importance to deter, detect, deny, delay, and defend (also known as security 5 D's, see also Section 5.4.2) against possible threats within a single company as well as within an industrial area of companies.

5.3.3 Swiss cheese model

The "Swiss cheese" model was developed by the British psychologist Reason (1997) to explain the existence of accidents by the presence of "holes" in the risk management system (see Fig. 5.3.5, adapted to security). A solid insight into the working of the organization allows for the possibility to detect such "holes," while risk assessment includes the identification of suitable measures to "close the holes."

It is important to notice that the Swiss cheese is dynamic: holes may increase in number or size (e.g., caused by unawareness of security by some personnel, failing/badly maintained technology, incomplete security procedures, etc.), but they may also decrease (because of solid risk management and adequate countermeasures). This model is very powerful in its use of "barrier" thinking (or "rings of protection" thinking). The holes within the barriers should be made as small as possible through adequate risk management, and this should be done for type I (e.g., thefts, sabotage) as well as type II (e.g., terrorist attacks) security risks (see Section 1.5 for risk types definition).

5.3.4 STOP principle

When looking for appropriate solutions to safety or security problems, we first have to clarify whether the hazardous or threatening phenomenon can be deleted by replacing certain substances and some dangerous processes; this is the so-called inherent safety

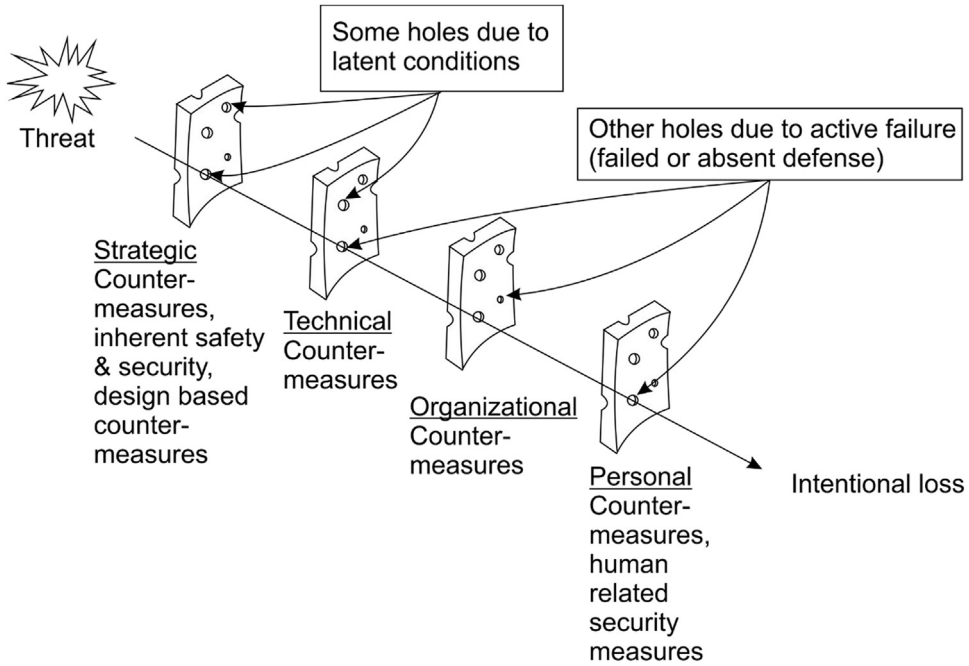


FIGURE 5.3.5 The Swiss cheese model for security.

principle, see Section 5.3.5. If it is not possible to delete the hazard, for instance, by improving the construction work or by using less hazardous substances, we must then proceed with technical and organizational measures and, as a last resort, human measures. This can also already be seen in the Swiss cheese barriers from Section 5.3.3.

The STOP (strategic, technical, organizational, and personal measures) principle (see also Meyer and Reniers, 2016) underlines this approach by giving priority to the measures in the following order:

i. *Strategic* measures: *strategic*, substitution of processes or substances giving a less hazardous/threatening result (e.g., substituting, eliminating, lowering, modifying, abandoning, etc.); abandon process or product, modify final product.
ii. *Technical* measures: *technical* protection against hazardous/threatening phenomena that cannot be eliminated, lowering the likelihood of success of an adversary attack, the attractiveness of a target, decreasing the vulnerability, and reducing the spread of the damage (e.g., replacing, confining, isolating/separating, automating, firewall, EX zones, bodyguards, etc.).
iii. *Organizational* measures: *organizational* modifications of the work, training, security instructions, information concerning residual security risk and how to deal with it (e.g., awareness training schemes, communicating, planning, supervising, warnings signs, etc.)

iv. *Personal* measures: *securing* people by means of personal security equipment, awareness training, security communication, coordinating, planning, etc.

The hierarchy of the priorities should be viewed upon in the following order:

i. Acting at the *source*: the source is in case of security the adversary, the person with malicious intent. He/she should be kept out of the organization as much as possible.
ii. Acting at the *interface* (on the trajectory between the source and the target): limiting the propagation (active barriers/passive barriers), catching/neutralizing (local or general ventilation, air purification, substance neutralization), people control (raising barriers, access restrictions, evacuation signs), and surveillance (cameras and sensors in the field, energy levels in the zone, excursions or deviations (alarms)).
iii. Acting at the *target*: different types of target can be envisioned: (i) *target 1 = infrastructure:* deleting the risk (substituting product or process, in situ neutralization), limiting target risks (re-enforcing the system, lowering the energy levels), predictive measures (rupture disk, valves), and surveillance (cameras and sensors at the installations). Increasing security awareness and social control on site. (ii) *target 2 = human capital*: lowering the vulnerability (personal security and protective equipment selection, special training), reducing exposure (e.g., automation), reducing the time (job rotation), and supervising (individual exposure, biological monitoring, medical survey, correct personnel protection equipment (PPE) use, and following rules).

In general, we must combine measures to obtain the required adequate security level. It is important that the choice of security measures enables the reduction of the likelihood and severity of the threatening events. Once the priorities have been established, it is possible to determine the correct method to master each of the identified security risks.

Table 5.3.1 presents a recap of the ordering of measures and the considered environment, illustrated by few examples for each category. Directions of approach are from top to down and then from left to right.

Eliminating the hazard is the most favorable approach when reducing risks; substitution is interesting as long as it does not generate new hazards or threats. No hazard, no threat, no risk. In the STOP principle, the elimination and substitution phases are included in the strategic measure S. They are, however, rarely possible in practice, thus eliminating and substituting may sometimes not be applicable.

Note that in practice, personal protection measures are usually put into place before the technical and organizational measures. This happens for many different reasons, including costs, delays, implementation simplicity, loss of responsibility, to have no time or take no time to analyze the situation, the complexity, etc. Many organizations have invested heavily in personnel, processes, and technology to better manage their security

Table 5.3.1 The STOP table for security with illustrative examples.

	At the source (Outer ring)	At the interface (Middle ring)	At the target (Inner ring)
Measures S (strategy)	• Substitution • Change process	• Automation, telemanipulation • Land-use planning • Redundancy of critical systems	• Criteria for selection of security-aware operators • Enforced infrastructure
Measures T (technical)	• Cameras/intrusion detection • Fences • Bollards and trenches • Intrusion sensors	• Locked doors • Access control system • Turnstiles	• Doors and cabinet locks • Network firewalls and passwords • CCTV
Measures O (organizational)	• Guards on patrol at property fence-line • Passport controls at entrance	• Visitor escort policies • Receptionists in buildings • Badge checks	• Security instructions • Intelligence • Emergency plans • Document shredding
Measures P (personal)	• Education/training of the entrance guards	• Information/instruction on threats	• Instruction for the use of security equipment

risk. However, these investments often are not optimal. To manage security in a most efficient and effective way, scarce resources need to be managed well, making better decisions and reducing the organization's exposure to negative events by adequately implementing the four-level steps comprising strategic, technical, organizational, and personal aspects.

5.3.5 The inherent safety/security principle

In Section 5.3.4, we indicated that the first and foremost approach to deal with safety and security problems is to cut away the hazardous or threatening phenomenon. If the danger is away, there is no possibility anymore for an undesired event, be it nonintentional or indeed deliberate. Inherent safety also leads to inherent security: if there are no dangerous preconditions that can be exploited by adversaries, there are no threats and no vulnerabilities, and hence, no security risks and no security-related dangers. The principle of inherent safety consists of five concepts, that is, intensification, substitution, attenuation by moderation, attenuation by limitation of effects, and simplification. The concepts are illustrated in Fig. 5.3.6.

The concepts have been developed by Kletz (1998) and further improved by both Kletz and Amyotte (2010). The first concept, intensification, indicates that by intensifying the activities and/or processes, for instance, using less of a hazardous/dangerous material, safety can be bettered. In this concept, it is important to verify whether there is no risk homeostasis, since different operating conditions (higher pressure, higher temperature) may lead to other risks, or the risk may have been partially relocated. In the latter cases, that is, when the risks are relocated, the same total risk still exists. The second concept, substitution, aims at replacing substances and procedures by less

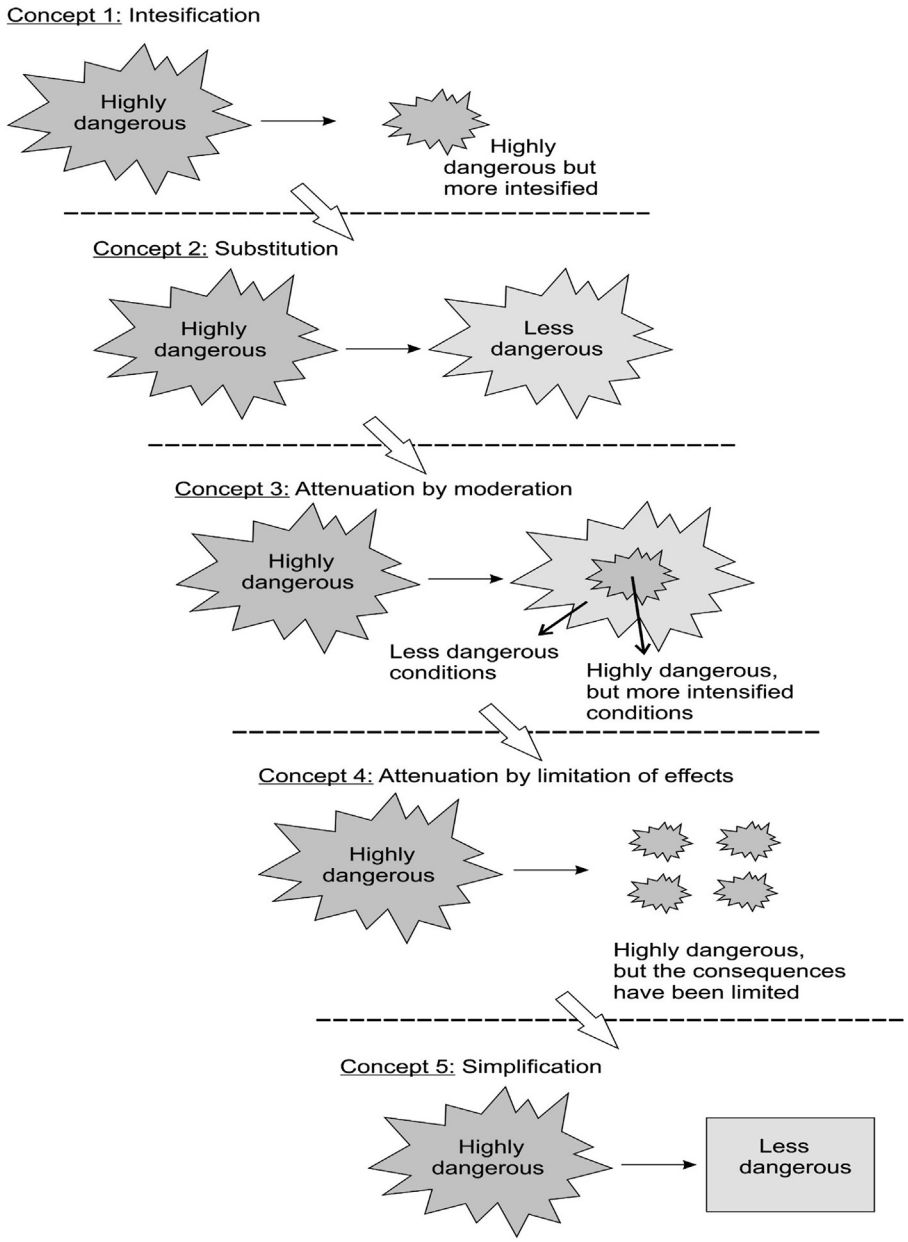


FIGURE 5.3.6 Five concepts of inherent safety/security (for taking strategic measures from STOP principle).

hazardous ones, by improving construction work, etc. Also in this case, care should be taken that there is not simply a replacement of the risk. The third concept, attenuation by moderation, indicates that safety may improve by working under more benign conditions, for instance, less dangerous process conditions or improved/stronger

materials. The fourth concept, attenuation by limitation of effects, notes that it is always better to try to lower the total potential consequences of a single undesired event as much as possible. The idea is that minimizing the overlapping of losses from a single event will lower the severity of any unwanted event. This can, for instance, be done by facility siting (US terminology) or land-use planning (European terminology), which boils down to the segregation by separation of high-risk units. Another way of segregation is by duplicating some essential (not to lose) high-risk units. The fifth concept, simplification, follows the simple observation that complex processes and situations always are more dangerous than simple ones. This is due to the fact that making mistakes is much easier in complex surroundings than in simple surroundings.

5.3.6 Security incident bipyramid

Heinrich (1950), Bird and Germain (1985) and Pearson (James and Fullman, 1994), among other researchers, determined the existence of a ratio relationship between the numbers of (safety-related) incidents with no visible injury or damage, over those with property damage, those with minor injuries, and those with major injuries. This accident ratio relationship is known as "the accident pyramid" (European terminology) or "the safety triangle" (US terminology). Accident pyramids unambiguously indicate that accidents are "announced." Hence, the importance of awareness and "incident" analyses. Different ratios were found in different studies (varying from 1:300 to 1:600) depending on the industrial sector, the area of research, cultural aspects, etc. However, the existence of the "accident pyramid" has obviously been proven from a qualitative point of view. It is thus possible to prevent serious accidents by taking preventive measures aimed at near-misses, minor accidents, etc. These "classic" accident pyramids clearly provide an insight into type I accidents where many data is at hand.

If one looks upon this accident pyramid paradigm with security goggles, and taking type I and type II events into consideration, the following analogy can be made. The accident pyramid possibly and probably also exists for security, forming a "security incident pyramid," with some specific conditions, that is, under the paradigm with the following assumptions:

(i) All minor criminal incidents are not the same in their potential for serious crime. A small subset of low severity crimes come from vulnerabilities that act as a precursor to serious crime.

(ii) Crime and security-related accidents of differing severity have differing underlying causes.

(iii) Reducing serious crime often requires a different strategy than reducing less serious crime or major security-related incidents.

(iv) The strategy for reducing serious crime and major security-related incidents (such as terrorism) should use precursor data derived from minor criminal facts, security incidents of all kind, near misses, and vulnerabilities.

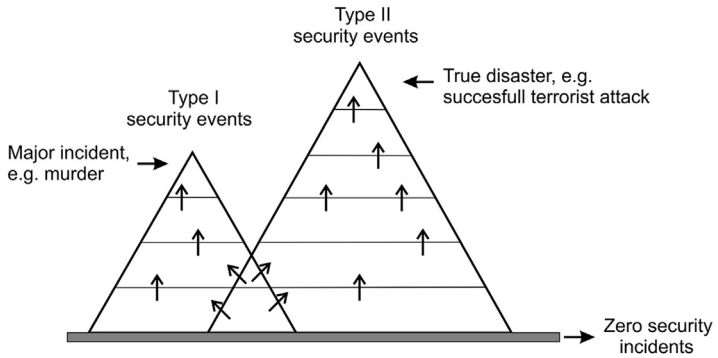


FIGURE 5.3.7 The security incident bipyramid.

Fig. 5.3.7 shows the "security incident bipyramid," which can actually be drawn as two pyramids with a small overlap. One pyramid represents type I risks, leading at most to a serious event (e.g., a murder), but not to a major catastrophe, and the other pyramid represents type II security risks, with the possibility to lead to a true disaster (e.g., a terrorist attack with multiple fatalities).

The bipyramid illustrates that there is a difference between "type I" security risks and "type II" security risks – in other words "regular crime" (and the incidents going hand-in-hand with them) should not be confused with "major crime" such as terrorism. Not all small crime events have the potential to lead to disaster, but only a minority of such events may actually eventually end up in a security-related catastrophe. Obviously, to prevent disasters and catastrophes, security risk management should be aimed at both types of security risks, and certainly not only at the large majority of "regular" security risks. Last but not least important, different performance indicators should be used for the two different types of security.

5.3.7 Security risk management

Security management is one form of risk management and, more specifically, engineering risk management (ERM). Many flowcharts exist in the literature to describe the sequences of ERM; the main steps involved are displayed in Fig. 5.3.8. The process is

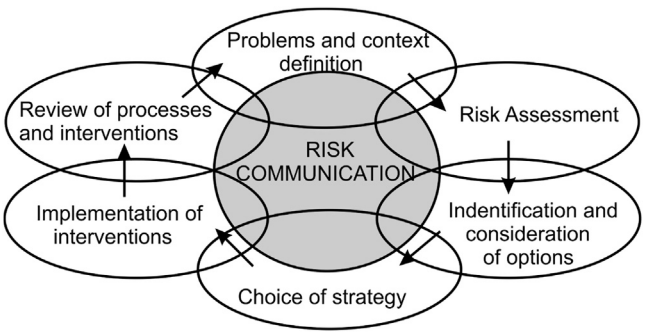


FIGURE 5.3.8 The engineering risk management process. *Based on Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed., Berlin: De Gruyter.*

based on a structured and systematic approach covering all of the following phases: the definition of the problem and its context, risk evaluation, identification and examination of the risk management options, the choice of management strategy, intervention implementations, process evaluation and interventions, as well as risk communication. The phases are represented by circles, and the intersections show their interrelations.

The process normally starts at the problem definition step and proceeds clockwise. The central position of the risk communication phase indicates its integration into the whole process and the particular attention this aspect should receive during the realization of any of these phases.

Although phases must generally be accomplished in a successive way, the circular form of this process indicates that it is iterative. This characteristic enables the revision of phases in light of all new significant information that would emerge during or at the end of the process and would enlighten the deliberations and anterior decisions. The made decisions should be, as often as possible, revisable and the adopted solutions should be reversible. Although the iterative character is an important quality of the process, it should not be an excuse to stop the process before implementing the interventions. Selecting an option and implementing it should be realized even if the information is incomplete.

The flexibility must be maintained all along the process in order to adjust the relative importance given to the execution and the revision of the phases, as well as the depth level of analysis to perform or the elements to take into consideration.

It is also interesting to look at the risk management iterative ring through the questions that must be answered in order to get the process moving forward. A summary of these questions is presented in Fig. 5.3.9.

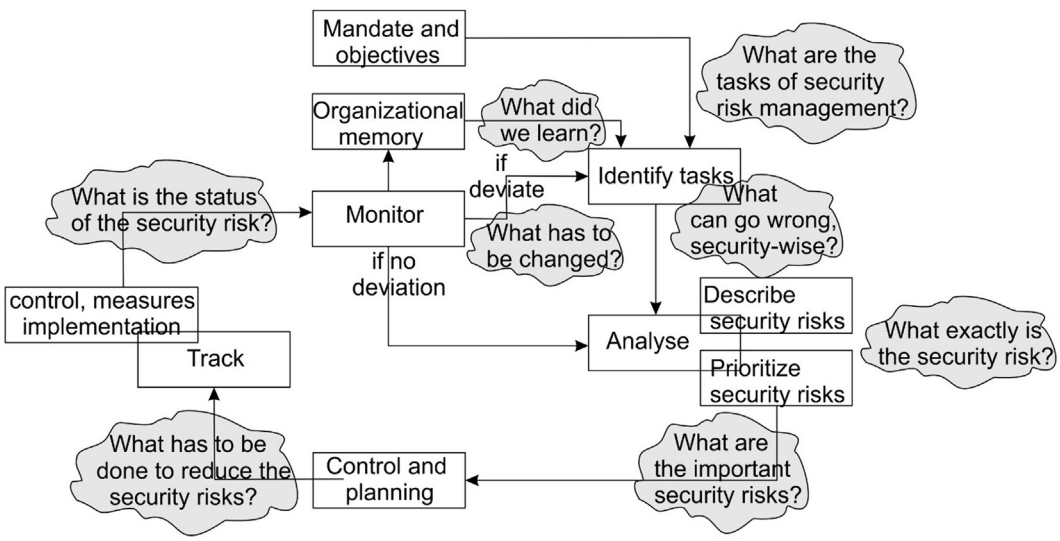


FIGURE 5.3.9 Main questions of the security risk management process. *Based on Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed., Berlin: De Gruyter.*

The starting point is the instruction or mission being the answer of "What are the tasks of security risk management?" Hence, we should identify "What could go wrong, security-wise?" in the identification step. Answering "What exactly is the security risk?" allows for describing, analyzing, and prioritizing risks. Then, in order to control and plan, the question "What are the important security risks?" is raised. To implement the adequate measure for risk reduction, we have to answer "What has to be done to reduce the security risk?" This allows also for controlling and tracking the implementation of security measures. The task is not yet over, as we should not forget to monitor the situation by asking several questions: "What is the security risk status?" allows following the time evolution of the considered security risk. If something begins to deviate, then "What has to be changed?" brings us back to the risk identification step. Another important point, often forgotten in risk management, is the answer to "What did we learn?". In summary, the security risk management process is not only an identification and treatment process, it is a learning process that never ends and must be continuously performed.

Another characteristic of engineers is to simplify complex systems in order to master them more efficiently. From this perspective, a simplification of the risk management process as depicted in Fig. 5.3.10 can be envisioned.

Going back to the principles of risk management, ISO 31000:2009 (International Organization for Standardization, 2009) indicates that for risk management to be effective, an organization should at all levels comply with the following principles:

- Risk management creates and protects value. Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, e.g., human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance, and reputation.
- Risk management is an integral part of all organizational processes. Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

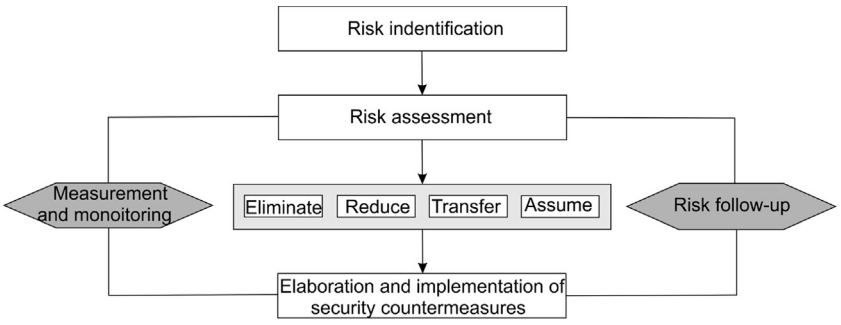


FIGURE 5.3.10 Simplified risk management process. *Adapted from Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed., Berlin: De Gruyter.*

- Risk management is part of decision-making. Risk management helps decision-makers make informed choices, prioritize actions, and distinguish among alternative courses of action.
- Risk management explicitly addresses uncertainty. Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
- Risk management is systematic, structured, and timely. A systematic, timely, and structured approach to risk management contributes to efficiency and to consistent, comparable, and reliable results.
- Risk management is based on the best available information. The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts, and expert judgment. However, decision-makers should inform themselves of, and should take into account, any limitations of the data or modeling used or the possibility of divergence among experts.
- Risk management is tailored. Risk management is aligned with the organization's external and internal context and risk profile.
- Risk management takes human and cultural factors into account. Risk management recognizes the capabilities, perceptions, and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.
- Risk management is transparent and inclusive. Appropriate and timely involvement of stakeholders and, in particular, decision-makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
- Risk management is dynamic, iterative, and responsive to change. Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.
- Risk management facilitates continual improvement of the organization. Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

The success of risk management will depend on the effectiveness of the management framework that provides the foundations and arrangements to embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision-making and accountability at all relevant organizational levels.

It is not really so important what scheme is used, the most important aspect is that with time one remains consistent in the use and in the follow-up. It is better to have a simplified system in adequate use rather than a complex scheme that will be only partially used.

A variety of risk management schemes and frameworks are available to be used in industrial practice. A framework should always have a feedback loop built into it, where one is certain that risk management efforts never stop. Risk policy, assessment, communication, and monitoring should also always be part of the scheme.

5.3.8 Security risk management system

Many organizations already follow the plan-do-check-act loop because of their acquired know-how of internationally accepted standards, e.g., ISO 9001, ISO 14001, ISO45001, or/and ISO 31000, continuously improving performance concerning risks. Hence, some degree of basic standardization for operational risk governance already exists in many organizations and thorough documented and well-implemented risk management systems are available.

A security risk management system (SRMS), as part of the risk management system, aims to ensure that the various security risks posed by operating the facility are always below predefined and generally accepted company security risk levels. Effective management procedures adopt a systematic and proactive approach to the evaluation and management of the security risks of the plant, including its products and its human resources.

To enhance security for type II risks, the SRMS considers security features throughout scenario selection and process selection for vulnerability and threat assessments, inherent safety/security and process design, and cooperation arrangements with law enforcement, among others. To enhance security regarding type I risks, security equipment such as cameras and fences are provided, security awareness training programs are installed, and task capabilities are checked. In brief, arrangements are made to guarantee that the means provided for a secured operation of the industrial activity are properly designed, set up, tested, operated, inspected, and maintained and that persons working on the site (contractors included) are properly instructed on type I and type II security requirements and features/policies.

Four indispensable features for establishing an organizational SRMS are:

- the parties involved;
- the policy − objectives;
- the list of actions to be taken;
- implementation of the system.

The essence of security protection practices consists of security data, threats and vulnerabilities reviews, security procedures, and awareness training. These elements need to be integrated into a security management document that is implemented in the organization on an on-going basis. To enhance implementation efficiency, this can be divided into 10 subjects (after Meyer and Reniers, 2016):

1. Security awareness training − The necessity to periodically organize security awareness training sessions emerges from the continuously changing environment

of plants, installations, and installation equipment, as well as the surrounding of the plant and the local/global political situation. Employees and contractors at all levels should be equipped with the knowledge, skills, and attitudes relating to security-related awareness matters and also what to do in case of suspicious events. Security training sessions should also lead to a more efficient handling of any incident or accident.

2. Group meetings – An organization should establish a regular security group meeting for the purpose of improving, promoting, and reviewing of all matters related to security of its assets. This way, communication and cooperation between management, employees, and contractors are promoted, ensuring that security issues are addressed and appropriate actions are taken to achieve and maintain a secured working environment.
3. Pursuing in-house security rules and complying with security guidelines, recommendations, and regulations.
4. A set of basic security rules and regulations should be formulated in the organization to regulate security behaviors. The rules and regulations should be documented and effectively communicated to all employees and contractors through promotion, training, or other means, and should be made readily available to all employees and contractors. They should be effectively implemented and enforced within the organization. The company rules should be in conformance with the legislative requirements and rules that are nonstatutory should conform to international standards and best practices.
5. Security promotion – Promotional programs should be developed and conducted to demonstrate the organization's management commitment and leadership in promoting good security behaviors and practices.
6. Contractor and employee evaluation, selection, and control – The organization should establish and document a system for assessment and evaluation of contractors to guarantee that only trustworthy contractors are selected and permitted to carry out contracted works. This way, personnel under external management, but working within the organization, are treated, evaluated, and rewarded in the same manner (concerning security issues) as internally managed personnel.
7. Security inspection, monitoring, and auditing – The organization needs to develop and implement a written program for formal and planned security inspections to be carried out. The program should include security inspections, plant and equipment inspections, any other inspections (including surprise inspections), and security auditing. This way, a system is established to verify compliance with the relevant regulatory requirements, in-house security rules and regulations, and secure work practices.
8. Security risk assessment and security incident investigation and analysis – All threats and vulnerabilities in the organization need to be methodically identified, evaluated, and controlled. The process of security risk analysis should be thoroughly documented. Written procedures should also be established to ensure that

all security-related incidents and accidents (including those by contractors) are reported and recorded properly. Furthermore, procedures for incident and accident investigation and analysis so as to identify root causes and to implement effective corrective measures or systems to prevent recurrence should be installed.

9. Control of movement and use of dangerous goods − A system should be established to identify and manage all dangerous goods through the provision of material safety data sheets and procedures for the proper use, storage, handling, and movement of hazardous chemicals. To further ensure that all up-to-date information on the storage, use, handling, and movement of dangerous goods in the organization reaches the prevention and risk management department, a continuously adjusted database with information should be established.
10. Documentation control and records − An organization should establish a central security documentation control and record system to integrate all documentation requirements and to ensure that they are complied with.

SRMSs are a must for organizations to handle security risks at an operational level. SRMSs deal with assessing all the security risks (via proxies such as the likelihood of attack − see the introductory Chapter 1) and with treating them, that is, trying to prevent the events associated with them, and, in the case of an unfortunate event happening despite all measures taken, in trying to mitigate the consequences.

5.3.9 The bow-tie model for security

The bow-tie is a very powerful technique developed in the safety community for having an overview of possible scenarios related to a so-called central event in the middle of the bow-tie (loss of energy, leak, etc.) leading to unintentional losses. It can also be seen as a metaphor (such as the Swiss cheese metaphor, see Section 5.3.3) to visualize the scenarios. The approach dates back to the 1990s and is widely used for analyzing (major) occupational and process safety incidents.

If applied to security, a bow-tie is able to present a clear overview of all causes (threats) and all consequences (intentional losses) of one particular undesired security-related event (for instance, an explosion due to a successful terrorist attack on asset x). The method combines a so-called fault tree with an event tree, and, as already mentioned, represents a number of different scenarios in the form of the cause of an event, its consequences, and the barriers that stop the event from happening. In security terms, the bow-tie is a metaphor for an attack (malicious action) process. The bow-tie technique is illustrated in Fig. 5.3.11.

To understand the meaning of the concept of the "central event," it is important to get clear about the concept of process security in relation to this bow-tie figure. As already explained in the introductory chapter, in process security, the threat comes from the adversary misusing or intentionally attacking one or more processes or process installations, for instance, causing a release of a hazardous substance or a release of energy (for instance, in the form of an overpressure wave, that is, due to an explosion). A

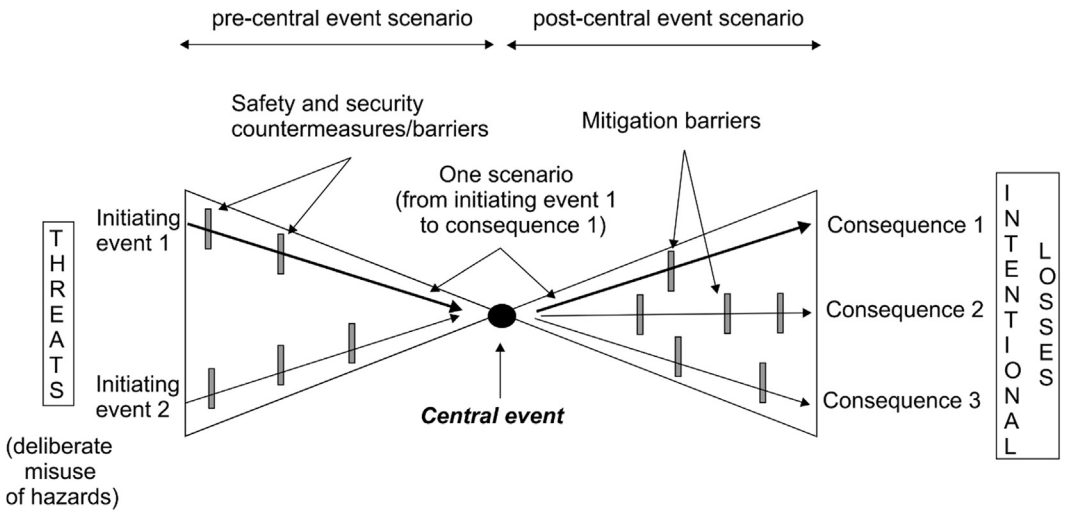


FIGURE 5.3.11 The bow-tie technique/metaphor applied to security scenarios.

"central event" (see Fig. 5.3.11) is a situation in which the threat (the deliberate release of a hazardous substance or energy) has become uncontrollable. As was also made clear in Chapter 1, a hazard is the intrinsic ability to cause any kind of losses (human and nonhuman). Cockshot (2005) describes hazard as "a condition that could lead to injury, damage to property or the environment." He defines a central event as "the initial consequence which involves the release of a hazard." If "initial consequence" here is (freely) translated as an effect, effect is reflected in the central event and can be defined as the direct result of the release of the hazard. In the right part of the bow-tie, the scenario develops further into the final consequences: victims, wounded, damage, production losses, etc.

Table 5.3.2 shows the relationship between the terms threat, effect, and consequence. For example, the intentional release of a flammable gas can lead to a jet fire or fireball with a certain heat radiation, which in turn causes burns and possibly death. As another

Table 5.3.2 The relation between Threat, Effect, and Consequence.

Left bow-tie **Pre-central event scenario**	**Central event**		**Right bow-tie** **Post-central event scenario**	
Threat = deliberate misuse of a hazard	*Effect* (intentional release of a hazard; loss of control of the threat)		*Consequence* (intentional losses)	
Deliberate misuse of energy, flammable and toxic substances	**Loss of containment** →	Heat radiation Overpressure Toxic concentration	Burn Internal injury Poisoning	→ Casualties, wounded, damage, and/or production loss

example, in the context of terrorism, the deliberate release of a toxic gas (*threat*), for instance, chlorine, may lead to a toxic cloud with a certain concentration of the lethal material chlorine (*effect*), leading to the poisoning of a group of people (*consequence*).

5.4 Specific security management models

In the previous section (Section 5.3), the discussed management models and approaches were developed for the "safety world" and for safety professionals, but here we adapted and explained them to the needs of security professionals. This section focuses on management models specifically designed and developed for security.

5.4.1 The 5D principle

The "5D" principle is well known by security professionals and one of the most applied management models in the security management community. The acronym of "5D" stands for Deter, Detect, Deny, Delay, and Defend. The first management strategy, Detect, is a security strategy to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems, such as warning signs, lights, uniformed guards, cameras, etc., are examples of systems that provide deterrence. The second management strategy, Detect, is a security strategy to identify an adversary attempting to commit a malicious act or other criminal activity in order to provide real-time observation, interception, and postincident analysis of the activities and identity of the adversary. Countermeasure examples for this strategy are cameras, VCA (Video Content Analysis) technology, observation technology, and security awareness practices of all kind. The Deny management strategy has the objective to keep unauthorized persons out at the deny perimeter, while allowing authorized persons to enter. To perform this function, the deny perimeter typically has access control technology or a manned security gate at the point of entry. The intention of surveillance at this point is to provide visual verification to the biometric or card access system. Access technology and practices for distributing keys among the personnel are countermeasure examples of the Deny strategy. The fourth management strategy is summarized as "Delay" and serves to provide various barriers to slow the progress of an adversary in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in apprehension and prevention of theft. The last management strategy is "Defend" and is typically a security personnel response that attempts to apprehend the intruder. Surveillance is used at this perimeter to record the apprehension and determine the effectiveness of the response. This final perimeter often includes the involvement of law enforcement and typically overlaps the other perimeters.

5.4.2 The PICER model

Before commencing the design of the protection barriers (that is, the rings-of-protection), the different steps corresponding to an adversary's intrusion should be understood. These steps will help the security manager in generating security specifications.

A description of an intrusion can be presented via the acronym "PICER." The so-called PICER model thus represents the mind-set and approach of the adversary and illustrates the different stages in which an attack can be divided.

The first stage is "Preparation," where the adversary does his/her "homework": looking up all kind of information about the target, searching data and info about the company (and the specific target within the company) on the internet, trying to get connected and asking questions to company personnel, going to the company as a visitor (e.g., on a "visit the Company" day, if it exists), etc. In this phase, mainly the measures for deterring the adversary are important.

The second stage represents the intrusion of the organization. Physically being able to get access to the company and bypassing all measures existing to detect, deny, and delay the intruder are the adversary's goal in this phase.

The third phase, "Collect," concerns the adversary doing what he/she wants to do: for instance, steal chemicals, place an improvised explosive device at a certain location, etc. In this phase, the detection measures are very important to deal with the exact situation at hand.

The fourth stage concerns the "Exit" plan of the adversary to leave the organization after a successful "Collect" stage. In this Exit stage, Detect and Defend measures are most important.

The final stage, "Reward," is determined by the end purpose, the objective, of the adversary. It can be the selling of a stolen good, it can be the use of a chemical for drug manufacturing, it can be the explosion of a bomb and creating chaos and fatalities, and what have you. This phase is usually the domain of law enforcement and judicial police instead of the responsibility of a company.

The principle of "PICER" is mentioned in a handbook that is published by the Belgian Institute of Security (Institute of Security Belgium, 2013). The handbook is used in training sessions as required by Belgian Law (Belgian Official Gazette, 1990) but is regrettably not publicly available. The PICER principle indicates that the design of the protective rings should be focused on the first perimeter, or at least as early as possible in the protection process. The first, second, etc., perimeters should be able to react as soon as possible, even (and preferably, if possible) during the preparation stage. Camera surveillance may, for example, help to identify people loitering around the first perimeter or it might detect people trying to collect information about the strength of the fence. Indeed, when a CCTV system is installed on a large site, then it will not only return information about an intrusion itself, but it can also be used at a preventive stage by guards on patrol (receiving information from a distance), who are able to manually inspect the condition of the fence: intact, broken, cut.

At the moment an attack starts, a detection indicator should be executed. The later the detection takes place, the greater the difficulty of interception becomes. If an intrusion is detected, there must be a way of engaging a matched response in terms of force.

5.4.3 The OPER model

As already noted, physical protection in itself will not prevent an attack. It is typically a combination of different security measures that need to be employed, a principle that is defined as "OPER." Similarly to PICER, the "OPER" principle is mentioned in the training handbook of the Belgian Institute of Security (Institute of security Belgium, 2013). The OPER acronym stands for:

- Organizational – about security awareness, management requirements for security, and other procedures to prevent intrusion
- Physical – security equipment such as barriers, fences, etc.
- Electronics – security equipment such as access controls, burglar alarms, cameras, etc.
- Reporting – transmission of an alert to an internal control room or an external dispatch service

The design process of the rings-of-protection will be based upon this OPER principle. Each perimeter (equal to a certain ring-of-protection) will consist of a fence with gates or barriers. The access to these rings will be equipped with the right access control system and (depending on the organization) often in combination with intrusion detection and CCTV. In the event of an adversary attempting to gain access, the activation of the systems will generate a response.

5.4.4 Perimeter thinking or the sanctuary principle model

In Section 5.3.2, the concept of the rings-of-protection (that is, defenses in depth or plant perimeters of protection) was explained. Since the rings will usually be the basis of the complete security plan of a chemical company, there will be security breaches if they are not well identified and assessed.

Prior to determining the rings-of-protection, an inventory of each part of the plant (building, building level, department, and other "clusters" of the plant) needs to be prepared. The plant's so-called "vital points" deserve special attention (see also Reniers et al., 2015). Vital points (assets) mainly include water inlet, water outlet, storage rooms for waste, electrical generator rooms, and storage locations of highly dangerous goods, but also people and information storage devices/terminals might be included. The inventories of every location situated within the premises of the plant serve to identify the targets.

The subsequent site visit should shed light on the flows of materials (including raw materials, produced materials, and waste), cars, people (own employees, maintenance personnel, contractors, visitors, and others), information, and Information and Communications Technology (ICT). These flows will help determine the most appropriate locations for access points and also for other security measures, taking into account a criticality assessment. Once a complete inventory has been finalized, the protection level of zones and perimeters may be determined. In Fig. 5.4.1, a generic arrangement of a chemical plant, using the rings-of-protection concept, is shown.

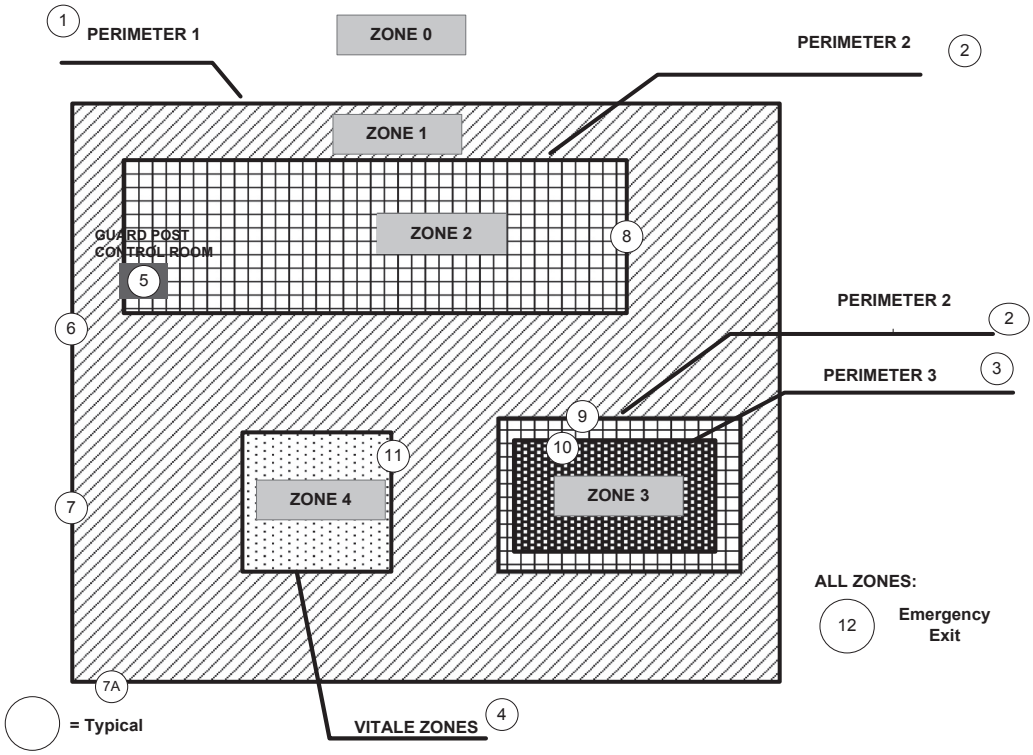


FIGURE 5.4.1 Generic arrangement of a chemical plant explaining the ring of protection concept. Reproduced from *Reniers, G., van Lerberghe, P., van Gulijk, C., 2015. Security risk assessment and protection in the chemica land process industry. Process Saf. Prog. 34 (1), 72–83.*

Fig. 5.4.1 schematically shows zones and perimeters for areas with different risk profiles. So-called "Typicals" are also indicated on this drawing. A Typical is a summation of technological items constituting a security barrier and thus describes the specific detailed technical characteristics of a security measure installed at a plant or at a part thereof. For example, a Typical for car access will indicate all the security elements of which this access point consists: a barrier, a badge reader to enter the site, and a vehicle loop to leave the site. These Typicals will be used to describe physical security needs for the perimeters as well as the requirements for accessing the different zones. The PICER principle (see Section 5.4.3) will be used to determine the needed protection within the perimeters and zones. Note also that the security needs are met by the OPER principle (see Section 5.4.4): the measures are built up from organizational, physical, electronic, and reporting elements.

For example, "(6)" indicated in Fig. 5.4.1 is the Typical that represents access for pedestrians and cars to ZONE 1, whereas "(7)" is an indication of access for trucks, and (7A) indicates access for railway carriages.

During this setup, the zone outside the plant borders, called zone "0," should not be neglected. Although this zone may seem unimportant, it is potentially the starting point

of any intrusion. This zone actually becomes crucial if several chemical installations, not being located at the same premises, form part of one larger chemical plant. If such is the case, there may be public domain between the different installations of the plant, and zone "0" may become an important zone where people and/or materials are transported between the installations. Some secured goods or people will be traveling from one secured plant to another secured plant. Hence, they will be remaining for a defined, or nondefined, time in a "non"secured zone. In such instances, measures need to be set up for securing this zone or for securing the zones where travel and/or transportation is possible in between.

The first protection ring will in most cases be the boundary of the plant site. Other zones will be:

- 2 = administrative offices for exploitation of the site
- 3 = buildings, essential administrative offices as well as storage rooms, and production clusters
- 4 = vital zones (see earlier), the operational center, and the central security room
- 5 = high-security areas

To better identify the security countermeasures required, a specific methodology can be used, according to Reniers et al. (2015). The methodology applies "User Requirements Basic" (URB) and "User Requirements Specific" (URS). This method is based on practitioners' experiences in the security field and is based on a multidisciplinary approach integrating security and safety needs and taking financial considerations into account. This object-oriented approach represents concepts as "objects" that have data fields (attributes that describe the object) and associated procedures known as methods. Gabbar and Suzuki (2004) describe the design of a safety management system using an object-oriented approach. In the application of the approach to the field of security explained by Reniers et al. (2015), the URBs explain the generic needs of a specific part of the perimeter and the throughput in a zone. The URSs define the specific rollout of the physical protection system. The URB and the URS are a combination of all possible security requirements (human, organizational, and technical issues).

The way an URB is written down is given in the procedure displayed in Fig. 5.4.2. This URB reporting structure is actually based on the OPER principle.

The generic procedure in Fig. 5.4.2 gives for the first URB the syntax as displayed in Fig. 5.4.3.

Once the complete set of URBs has been defined, the URSs can be drafted. An URS describes the technical specifications of the URB. It is, however, neither a technical descriptive of the solution, nor is it a set of procedures. In the case of an existing plant, it is often common that several URSs are present but that some of them differ with respect to one or more specific parts. As an example, for the URB 1, six URSs can be identified, namely:

- URS 1 = the fence itself
- URS 2 = the access points for pedestrians and cars

URB – <indicate the name of the URB>

/ <Start of the rules>

#D <Description part>

#O <The organizational measures to be taken into account>

#P <The specific physical security measures, including resistance time and the technical norms>

#E <The specific electronic security measures, with an indication of the probability of detection ($D_{etection}$) expressed in % (value between 0 and 100%) wanted>

#R <Indication of the way this alarm will be transmitted and displayed, with an indication of the Alarm priority (A value between 1 and 5)>

#D <Indication of the approach for threat deflection: evacuation, call police, action by site security, …>

#L <List of applicable regulations like: internal laws, SEVESO, …>

*/ <End of the rules>

FIGURE 5.4.2 Scheme of an URB (user requirements basic).

URB – Perimeter 1

/*

#D <Boundary between Zone 0 and 1>

#O <Indicate the boundary of the chemical plant>

#P <Fence with a resistance time of t seconds according to following technical norms: N1, N2, etc., access for cars and people must be possible>

#E <Electronic Detection for non-authorised access, based upon Nx with $D_{etection}$ = y % >

#R <Alarms connected to the central Security Management Systems $A_{PRIORITY}$ = 1>

#D <Site security personnel sent to the threat in t minutes>

#L <applicable Regulations>

*/

FIGURE 5.4.3 Definition of URB for perimeter 1.

- URS 3 = the access points for the trucks
- URS 4 = the access points for the trains
- URS 5 = the access points for the boats
- URS 6 = the access points to the utilities such as water and electricity

It is worth noting that places where energy is produced or where cooling water or water needed for production is being stored are often forgotten as targets for adversaries. However, these locations should also be protected (Arata, 2006), hence the URS 6 in our aforementioned list.

FIGURE 5.4.4 Chemical plant and its Typicals. *Reproduced from Reniers, G., van Lerberghe, P., van Gulijk, C., 2015. Security risk assessment and protection in the chemica land process industry. Process Saf. Prog. 34 (1), 72–83.*

On the schematic security drawing of the plant, Typicals (that is, as mentioned, the summation of technological items constituting a security barrier) with a number and a letter should be mentioned. An important point, especially in chemical plants, is also to make an inventory of ATEX-zones or other zones with explosion risks, for example, in Fig. 5.4.1, marked as Zone 3. These zones will need specific equipment for every kind of security technology that will be installed.

To explain in detail the concept of Typicals, an example is given here. To enhance the understanding of Typicals, a plan of a chemical plant with the rings-of-protections and the Typicals on that plan are shown in Fig. 5.4.4.

Fig. 5.4.5 gives a schematic drawing of one illustrative Typical, that is, the security equipment needed for a standard emergency exit. The emergency exit may only be used

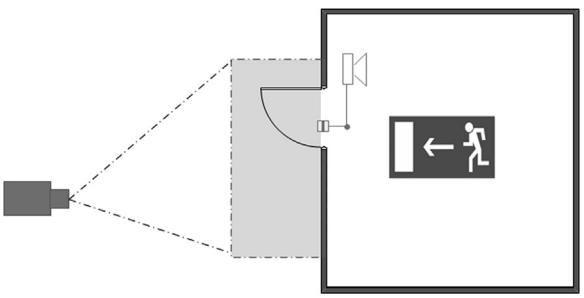


FIGURE 5.4.5 Typical 12: "Emergency exit."

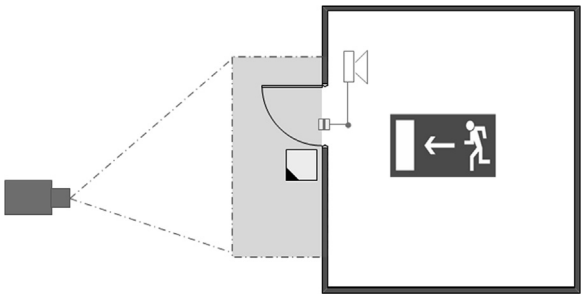


FIGURE 5.4.6 Typical 12A: "Emergency exit with access-IN."

to leave a building in the event of evacuation. As often seen, this door is also used for shortcuts or for smoking outside the building. To prevent the opening of this door by means of the panic bar, a magnetic contact will be added in combination with a loud sounder and a camera. In the event of the door opening, the sounder will indicate the opening of the door, and the camera will start recording the person(s) leaving the building.

Fig. 5.4.6 shows the same Emergency Exit of Fig. 5.4.5, but now this door also needs to be used as an access point to the building. As its main function is to be an Emergency Exit, the number of the Typical is kept but a capital "A" is added. This door has the same functionality as the one in Fig. 5.4.5, but with a specific operating instruction, namely the use of the door as an entrance with a badge reader.

This emergency exit can be described by using the technical sheet as given in Fig. 5.4.7.

Every ring-of-protection is made up of a perimeter and the corresponding zones (enter- and exit zones). The perimeter will have a specific resistance based upon the results of the so-called critical path method (or path analysis). The critical path method is a step-by-step technique for security intrusion that defines the path an intruder could use to reach his or her goal. More details are reported in Section 3.3.

The first perimeter, usually being the property boundary of the plant, is mostly a simple wired fence. The fence is a physical measure. It usually serves to prevent trespassing attempts and for keeping out unwanted visitors. If it is also to act as a perimeter with a certain protection against adversaries (such as burglars, terrorists, etc.), then a more appropriate fence type can be chosen. If it also has to prevent attacks from vehicles, then it may be extended with an antiramming device like a barrier of concrete. However, preventing or mitigating attempted illegal entry should not be regarded as sufficient protection. Evidence of a potential trespasser should be available as promptly as possible. To this end, an appropriate perimeter detection system (see for example Fig. 5.4.8) may be installed, introducing an electronic measure. For chemical plants, the

TECHNICAL SHEET	TYPICAL 12A	Reference	TF.XX.0022
	BPC400	Edition /Date	V008-26/03/2013
PROJECT:	Emergency Exit with access-IN		

Organisational measurements	
Yearly maintenance of all equipments Guards have to execute a guard tour every day to look for open doors.	
Physical measurements	
Access persons	Emergency door must be in accordance with the most restrictive standards of the zone, from whereat the emergency exit takes place.
	Emergency door must be in accordance with the guidelines of the law
Electronic measurements	
CCTV	When using this door there will be a trigger given to the CCTV to start recording all images during the time of the buzzer. (in this way one can find out who has used the emergency exit's)
	At activation of an alarm the cameras will register the alarm so that a verification is possible and the recorded images can be analysed afterwards.
Access control	At unauthorized exit activates an internal buzzer and report it to the person that the use is not allowed. A message is given to the monitoring team.
	When a person wants to enter the building than he has to use a card reader. This reader will overrule the standard alarm functions of this door. The buzzer can be reset only by intervention of the monitoring.
Intrusion detection	Emergency door is connected to the central system which is located in the control room.
	Every move to this door will be reported as an alarm, the alarm message only in the event of evacuation will not come through. (overruling)
	When you open the door to leave the secure zone is activated the siren
	There is a sabotage sensitive magnetic contact present at the door
Reporting measurements	
Monitoring will start the service reset and alarm handling.	

FIGURE 5.4.7 Technical sheet for the Typical 12A from Fig. 5.4.6. *Reproduced from Reniers, G., van Lerberghe, P., van Gulijk, C., 2015. Security risk assessment and protection in the chemica land process industry. Process Saf. Prog. 34 (1), 72–83.*

use of thermal cameras with VCA is suggested. As the premises of chemical plants are usually rather large, often with trees and other vegetation present, tests indicated that thermal camera systems have the lowest rate of false alarms when used as perimeter detection. Even in the event of climbing and cutting the fence, this seems to be a good solution. Tests have revealed that well-organized intruders can overcome some of the other security countermeasures such as leaking coax or seismic pressure systems in several seconds without setting off any alarm (also electronic measures). A schematic drawing of such a perimeter protection is illustrated in Fig. 5.4.8.

It is worth mentioning that the performance, in terms of availability and effectiveness, of each Typical drastically affects the vulnerability of a given installation against an external attack.

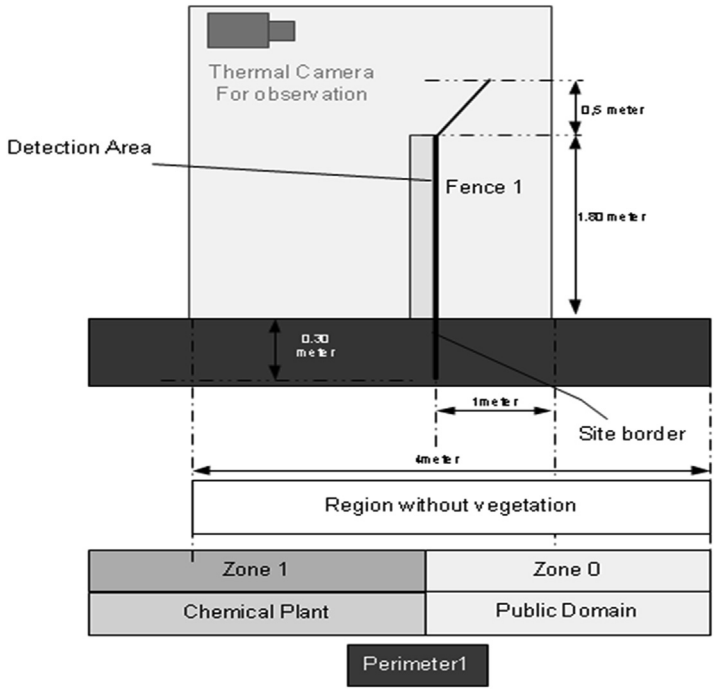


FIGURE 5.4.8 Schematic drawing of Typical perimeter 1 for a chemical plant. *Reproduced from Reniers, G., van Lerberghe, P., van Gulijk, C., 2015. Security risk assessment and protection in the chemica land process industry. Process Saf. Prog. 34 (1), 72–83.*

5.5 Conclusions

The present chapter dealt with security culture and management in organizations, with particular reference to the chemical and process industry. After the presentation of concepts and characteristics of physical security culture, security performance management indicators were discussed with some application examples. Finally, the chapter introduced specific security management models and basic elements for the comprehension of physical security barriers and systems. Chapter 6 will provide an in-depth discussion on the definition of physical protection system effectiveness with quantitative elements to support advanced security risk and vulnerability studies.

References

Arata Jr., M.J., 2006. Perimeter Security. McGrawHill, San Francisco, USA.

Belgian Official Gazette, 1990. Wet tot regeling van de private en bijzondere veiligheid (in Dutch), p. 10963.

Bird, E., Germain, G.L., 1985. Practical Loss Control Leadership, the Conservation of People, Property, Process, and Profits. Institute Publishing, Loganville, GA.

CCPS, Center for Chemical Process Safety, 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers, New York.

Cockshot, J.E., 2005. Probability bow-ties − a transparant risk management tool. Process Saf. Environ. Prot. 83 (B4), 307−316.

Gabbar, H.A., Suzuki, K., 2004. The Design of a Practical Enterprise Safety Management System. Kluwer Academic Publishing, Dordrecht, the Netherlands.

Heinrich, H.W., 1950. Industrial Accident Prevention, third ed. McGrawHill Book Company, New York.

Institute of security Belgium, 2013. Handbook "Basisopleiding Bested Voor Leidend Personeel Van beveiligingsondernemingen." (In Dutch). Ministry of Home Affairs, Brussels, Belgium.

International Organisation of Standardization (ISO), 2009. Risk Management Standard − Principles and Guidelines. ISO, Geneva, Switzerland.

James, B., Fullman, P., 1994. Construction Safety, Security and Loss Prevention. Wiley Interscience, New York.

Kletz, T., 1998. Process Plants. A Handbook for Inherently Safer Design. Braun-Brumfield, Ann Arbor, USA.

Kletz, T., Amyotte, P., 2010. A Handbook for Inherently Safer Design, second ed. CRC Press, Boca Raton, USA.

Mazri, C., Jovanovic, A., Balos, D., 2012. Descriptive model of indicators for environment, health and safety management. Chem. Eng. Trans. 26, 465−470.

Meyer, T., Reniers, G., 2016. Engineering Risk Management, second ed. De Gruyter, Berlin.

Reason, J.T., 1997. Managing the Risks of Organisational Accidents. Ashgate Publishing Limited, Aldershot, UK.

Reniers, G., van Lerberghe, P., van Gulijk, C., 2015. Security risk assessment and protection in the chemical land process industry. Process Saf. Prog. 34 (1), 72−83.

van Nunen, K., Sas, M., Reniers, G., Vierendeels, G., Ponnet, K., Hardyns, W., 2018. An integrative conceptual framework for physical security culture in organisations. J. Integr. Secu. Sci. 2 (1), 25−32.

Vierendeels, G., Genserik, R., van Nunen, K., Koen, P., 2018. An integrative conceptual framework for safety culture : the Egg Aggregated Model (TEAM) of safety culture. Saf. Sci. 103, 323−339.

6

Advanced design of physical security systems

In order to avoid the propagation of a hazard toward a sensible target (operators, residential population, environment, asset, etc.), a specific design activity is dedicated to evaluate and implement effective barriers, defenses or, more in general, layers of protections (Reason, 2000). Chapter 5 explored the concepts related to layered defense, illustrating the different models and methods for identifying and evaluating the necessary security systems aimed at protecting process plants. In this chapter, specific examples of security risk strategies are illustrated with quantified examples.

In general, the strategy for reducing risk, whether directed toward reducing frequency or consequence of potential accidents, can be classified into four categories (CCPS — Center of Chemical Process Safety, 2001a,b). These categories, in decreasing order of reliability/robustness, are

- inherently safer design (ISD);
- passive barriers;
- active barriers;
- procedural/emergency barriers.

ISD as effective and crucial safety measure has widely been employed by safety experts and decision-makers to prevent major accidents and mitigate their consequences. However, the attempts made to use ISD in the context of security risk assessment and management have been very few. In this chapter, we will demonstrate how the security-risk-based design of the layout of a chemical facility can "limit the effects" of intentional attacks by limiting the extent of potential domino effects. In this regard, we show the role of two design alternatives: (i) designing the physical layout of a chemical plant where making changes to the number of hazardous units and the safety distances among which is still possible, and (ii) designing the industrial control system of a chemical facility where making changes to the aforementioned physical characteristics is not possible. Both design alternatives have been applied to tank terminals and respectively discussed in Sections 6.1 and 6.2.

Section 6.3 is dedicated to add-on safety and security measures, namely systems that are implemented in a given facility to reduce and control the risk induced by external acts of interference. Firstly, a methodology for the performance assessment of security Typicals discussed in Chapter 5 is presented; quantitative data supporting advanced studies such as the ones described in Chapter 4 are reported. Next, a detailed focus on "safety" barriers, i.e., hardware barriers designed to reduce the risk of worst-case events

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00006-8

typically associated with unintentional causes, is reported in the perspective of safety–security integration. Active and passive barriers (i.e., systems requiring or not requiring external activation, respectively) are mainly discussed in the section. Finally, some reflections are given in Section 6.4.

6.1 Security-based design of the layout of process plants w.r.t physical attacks

6.1.1 Introduction

Early applications of land use planning (LUP) to major accidents in Europe dates back to the early 1970s when the Flixborough disaster in 1974 in the United Kingdom led to the Act 1974, requiring industries to keep internal risks (on-site risks) as well as external risks (off-site risks) as low as reasonably practicable (HSE, 2014). Accordingly, local planning authorities have been obliged to obtain advice from HSE in the case of land developments around major hazard installations (MHIs) (Franks, 2004; HSE, 1989, 2014).

The majority of relevant work over the past two decades, however, has been inspired by the EU Council Directive 96/82/EC, also known as Seveso Directive II. Articles 8 and 12 of the Seveso II explicitly mandate the EU Member States to consider domino effects and LUP, respectively, for the prevention of major accidents and the limitation of their consequences to humans and the environment. Article 12 is mainly devoted to (i) sitting of new installations, (ii) modification to existing installations, and (iii) land developments in the vicinity of existing installations, particularly those developments that would increase either the population at risk or the severity of the risk. In other words, it does not apply to an existing installation unless there are any internal modifications to the plant or external land developments in the vicinity of the plant.

Provision of domino effect in Seveso II has been made to ensure adequate internal safety distances among the units of an MHI where it is possible that a major accident in a unit propagates to neighboring units, triggering other secondary accidents. Likewise, requirements of LUP have been included in Seveso II to warrant adequate external safety distances between an MHI and residential areas, areas of public use, or areas of particular natural sensitivity and interest (Christou et al., 2006). From 1 June 2015, the new Seveso Directive III has come into force in Europe, containing the same LUP philosophy as its predecessor Seveso II.

LUP has traditionally been considered from two perspectives: (i) land use development in the vicinity of an existing MHI and (ii) design/modification of a new/existing MHI considering nearby land developments. From the first perspective, off-site individual risk or societal risks are calculated for an MHI considering major accident scenarios (Laheij et al., 2000; Taveau, 2010; Hauptmanns, 2005; Cozzani et al., 2014; Kontic and Kontic, 2009). Accordingly, pieces of land in the vicinity of MHI are designated to particular developments based on their vulnerability and the levels of risks they are exposed to. According to the second perspective, however, LUP requirements have

been considered in the development or modification of new/existing MHIs (Papazoglou et al., 2000; Sebosa et al., 2010; Bernechea and Arnaldos, 2014; Khakzad and Reniers, 2015a,b, 2017) such that the modifications would decrease or at least not increase the level of off-site risks.

In the present study, we will demonstrate that a risk-based design of the layout of a chemical facility (a tank terminal) can reduce the severity of both on-site and off-site consequences by "limiting the effects" of potential domino scenarios in case of a physical attack to the facility.

6.1.2 Design of hazardous facilities considering land use planning

Several methods have been adapted around the world to implement LUP such as the method of generic distances, consequence-based method, and risk-based method. These methods are not necessarily contradictory and in most cases a combination of them are employed (hybrid methods). Comprehensive reviews and comparisons of conventional LUP methods adapted within European countries have been discussed by Papazoglou et al. (1998); Christou et al. (1999, 2011); Cozzani et al. (2006a,b); Basta et al. (2007); Demichela et al. (2014); Pasman and Reniers (2014).

The risk-based method includes several steps: (i) to identify and estimate the probability of potential accident scenarios, (ii) to identify and estimate the intensity of physical effects (e.g., heat radiation, overpressure, toxic concentration), (iii) to estimate the adverse effects of the physical effects on exposed population, and (iv) to analyze off-site risks in form of individual risk (IR) contours or societal risk curves (F−N curve) (Christou et al., 2006). Quantitative risk analysis methods are usually applied to estimate the probabilities of potential accidents while dose−effect relationships and probit models are used to estimate the adverse effects of the physical effects on off-site targets (usually human).

Fig. 6.1.1 depicts a buffer distance comprising three zones separated by IR contours, resulting from a risk-based approach adopted in the United Kingdom. Circumventing an

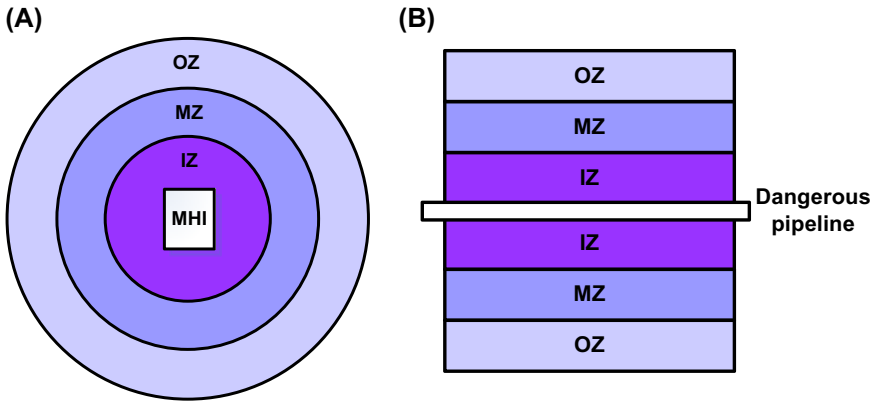


FIGURE 6.1.1 Buffer zone around a major hazard installation (A) and a pipeline (B) (PADHI, 2011).

MHI (Fig. 6.1.1A) or a hazardous pipeline (Fig. 6.1.1B), the boundaries of the inner zone (IZ), the middle zone (MZ), and the outer zone (OZ) are identified by IR contours corresponding to 10^{-5}, 10^{-6}, and 3×10^{-7}, respectively (HSE, 2014; PADHI, 2011). Land developments inside a buffer zone should be limited according to the magnitude of IR and vulnerability and number of population at risk. To this end, for example, the HSE of the United Kingdom has defined four levels of vulnerability for land developments: level 1 including factories with limited number of employees; level 2 including residential houses with limited number of residents; level 3 including primary schools and old people homes; and level 4 including football stadiums and large hospitals.

Based on these vulnerability levels and amount of IRs, the following decision matrix (Table 6.1.1) can be used to Advise Against (AA) or Not to Advise Against (NAA) land developments (PADHI, 2011).

Table 6.1.1 Decision matrix used by HSE for risk-based LUP (PADHI, 2011).

Level	IZ	MZ	OZ
1	NAA	NAA	NAA
2	AA	NAA	NAA
3	AA	AA	NAA
4	AA	AA	AA

AA, Advise Against development; *NAA*, Not Advise Against development.

6.1.3 An illustrative example

Consider a hypothetical fuel storage plant (Fig. 6.1.2), which is planned to sit near a residential area and a hospital. The plant is required to store 24,000 m^3 of crude oil in atmospheric storage tanks. Furthermore, the distances from the center of the plant to the residential area and the hospital are 100 and 150 m, respectively.

The aim is to find an optimal layout for the storage plant of interest so that under attack (e.g., with home-made bombs) the respective on-site risks and off-site risks would be the lowest assuming that the aim of attack would be to cause the maximum property loss and human loss. To this end, six alternatives are considered as potential layouts for the storage plant (see panels *A* to *F* in Fig. 6.1.3). The specifications of the layouts and the storage tanks are listed in Table 6.1.2. Also, the safety distances among the storage tanks in each layout have been determined based on the volume and diameter of storage tanks as suggested by Flammable Liquids Bulk Storage Regulations of Canada (2014).

6.1.4 Results

For illustrative purposes, let us assume that the only constraints the plant owner faces in designing the layout are the required land to sit the storage tanks and the budget required to buy the storage tanks. The land can be estimated for each layout as the area (m^2) occupied by the storage tanks and the safety distances among them. Approximate

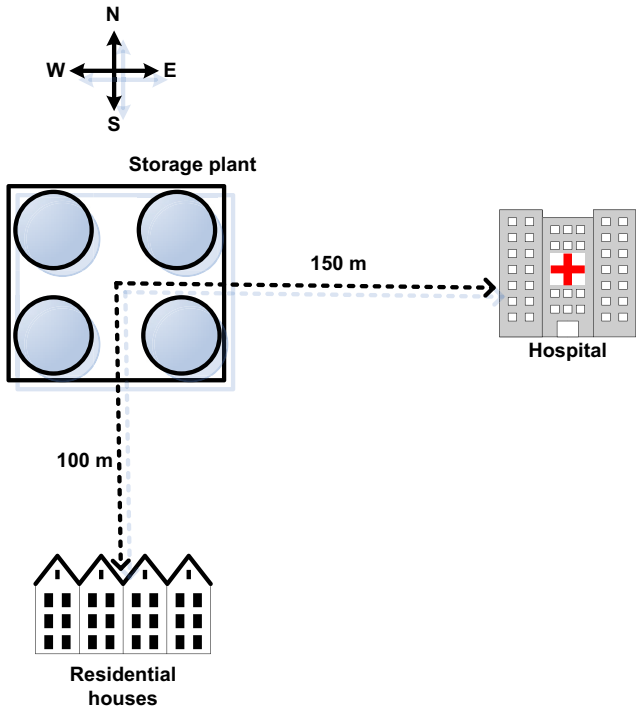


FIGURE 6.1.2 A hypothetical fuel storage plant.

cost of each type of storage tank (USD) can also be obtained from a variety of sources (e.g., www.matche.com). The required land and total cost of each layout have been calculated as listed in the third and fourth columns of Table 6.1.3.

To calculate on-site risks (i.e., risk of damage to storage tanks and the loss of chemical inventory), the plant layouts presented in Fig. 6.1.3 and potential domino effects due to attack to each storage tank were modeled using the BN methodology proposed by Khakzad et al. (2013). It was also assumed that an attack to any of the storage tank would result in a tank fire (due to the flammable content of the tank), which in turn could trigger secondary fires in the adjacent tanks. For instance, given an attack to tank #2 in the design layout presented in Fig. 6.1.3C and subsequent tank fires, the magnitudes of heat radiation the other tanks would receive have been listed in Table 6.1.4.

Considering a threshold value of $Q_{th} = 15\ kW/m^2$ (Cozzani et al., 2009) for heat radiation, only those heat radiations whose magnitude is greater than or equal to 15 kW/m^2 are kept in the analysis (e.g., bold numbers in Table 6.1.4). Fig. 6.1.4A illustrates the plant layout of Fig. 6.1.3C in which only heat radiations that are greater than or equal to Q_{th} have been presented.

Having the probability of fire for each storage tank (directly due to the attack or indirectly via triggered domino effect), the value of risk for a storage tank can be calculated as the product of the damage probability and the monetary value of the

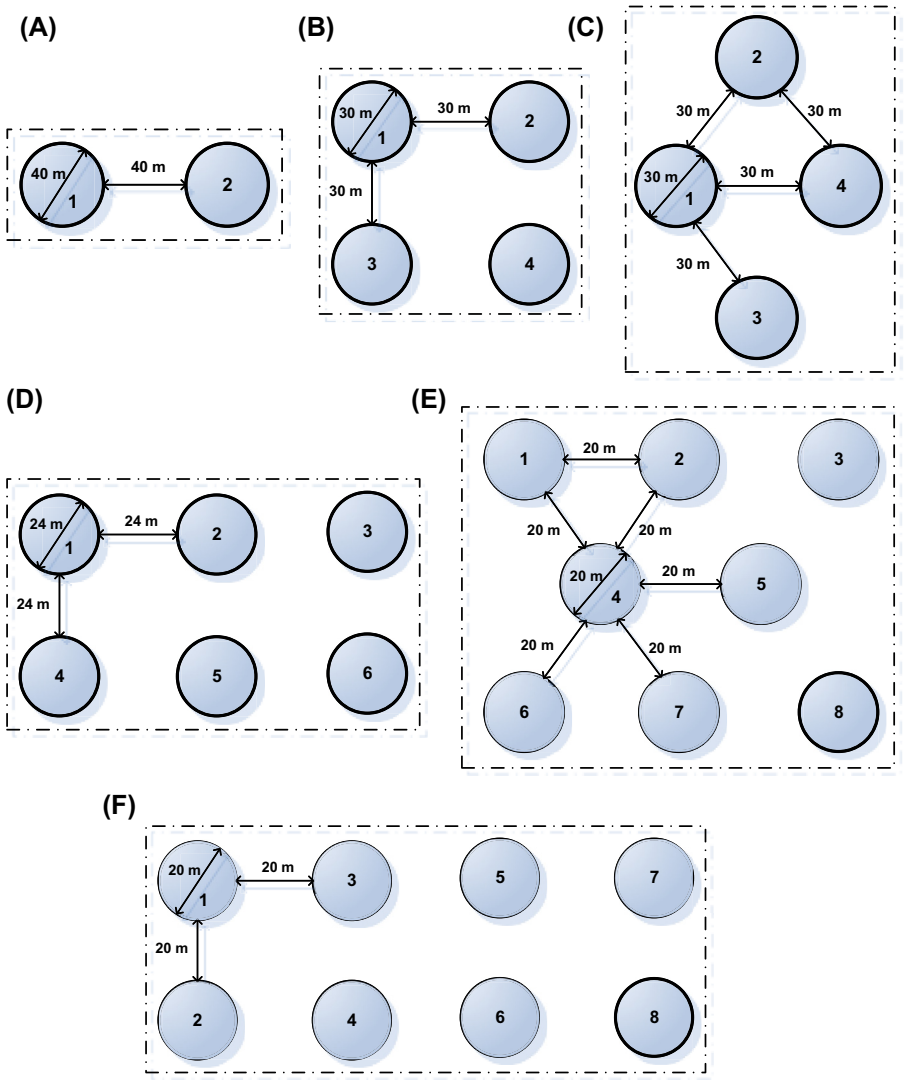


FIGURE 6.1.3 Alternatives for the layout of the fuel storage plant.

Table 6.1.2 Characteristics of plant layouts and storage tanks.

Layout in Fig. 6.1.3	Number of tanks	Diameter (m)	Height (m)	Volume of each tank (m^3)	Safety distance (m)
A	2	40	10	12,000	40
B	4	30	10	6,000	30
C	4	30	10	6,000	30
D	6	24	10	4,000	24
E	8	20	10	3,000	20
F	8	20	10	3,000	20

Table 6.1.3 Characteristics of plant layouts regarding required resources, on-site risk, and off-site risks.

		Required resources			Off-site risk (Individual risk)	
Decision alternative	**Layout design in Fig. 6.1.3**	**Land (m^2)**	**Cost of storage tanks (10^6 USD)**	**On-site risk (USD)**	**Residential**	**Hospital**
1	A	4800	1.65	276.7	2.34E-05	1.02E-05
2	B	8100	2.27	295.4	3.71E-05	9.09E-09
3	C	6000	2.27	300.4	3.18E-05	2.62E-08
4	D	8640	2.35	297.8	2.45E-06	2.26E-09
5	E	8400	2.68	307.6	1.26E-08	5.98E-10
6	F	9000	2.68	311.3	2.04E-06	2.60E-12

Table 6.1.4 Heat radiation (kW/m^2) at different locations resulting from tank fires in storage tanks of plant layout shown in Fig. 6.1.3C.

	1	**2**	**3**	**4**
1	NA	**17.5**	**61**	**35.6**
2	**33.1**	NA	4.21	**61**
3	10.9	2.05	NA	**17.5**
4	10.9	10.9	**33.1**	NA

Heat radiation intensities greater than 15 kW/m2 are presented with bold font.

storage tank, that is, the cost of the tank plus the value of its chemical content. It is assuming that during a tank fire the storage tank and the entire chemical inventory would be lost, considering the price of 1 m^3 of crude oil as 315 USD. The values of on-site risk for the layouts presented in Fig. 6.1.3 are listed in column 5 of Table 6.1.3.

After the probabilities of tank fire for the storage tanks are estimated, the off-site risks can readily be calculated. To this end, first the magnitudes of heat radiation at the residential area and the hospital are determined. Accordingly, the probability of death for a human agent (i.e., the individual risk) is estimated by extending the BN (Fig. 6.1.4B) and using the dose–effect relationship (Yellow Book, 1997). The individual risks of the plant layouts in Fig. 6.1.3 are presented in columns 6 and 7 of Table 6.1.3.

Analytic hierarchical process (AHP) (Saaty, 2008) is a multicriteria decision analysis (MCDA) technique consisting of a set of decision criteria and decision alternatives. Decision criteria are influential decision factors based on which the optimal decision

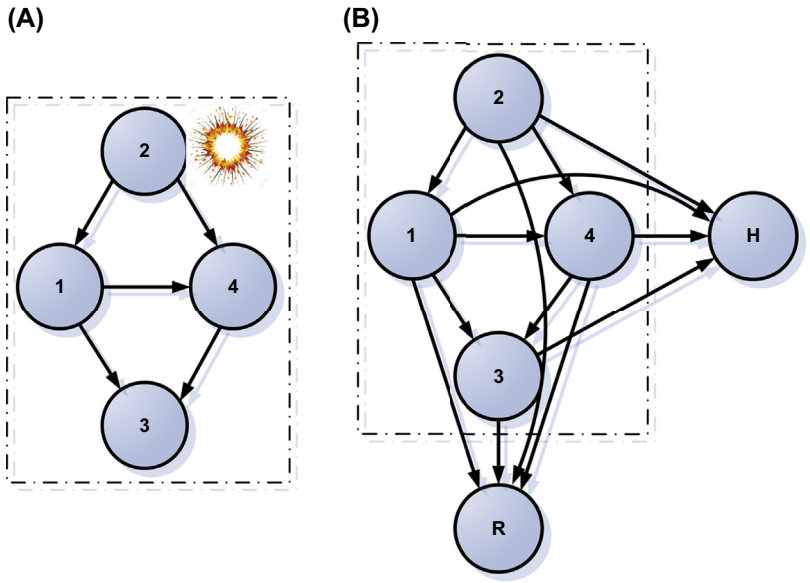


FIGURE 6.1.4 (A) Attack to tank #2 with home-made bomb, which would trigger a tank fire at the attacked tank. Other tanks would receive radiated heat from the attacked tank, which may trigger secondary fires at them; (B) the extended BN to calculate off-site individual risks at hospital (H) and residential house (R).

alternative is to be selected. In AHP, decision criteria are compared pairwise and weighted according to their relative importance to the decision to be made. Similarly, the decision alternatives are compared pairwise and weighted against each decision criterion. Weights are assigned based on a fundamental scale table (Saaty, 2008), ranging from 1 to 9. The results of the pairwise comparisons are populated in respective matrices. The normalized elements of the principal right eigenvector of each matrix represent the local rank of each decision criterion and decision alternative. Final rank of each decision alternative can subsequently be determined using the local ranks of the decision alternative and the local ranks of each decision criterion. Accordingly, the decision alternative with the highest final rank is selected as the optimal decision.

Considering the characteristics of plant layouts listed in Table 6.1.3, the most optimal layout is the one for which the required resources as well as the on-site (asset damages) and off-site risks (IR) are the lowest. However, in the case of having conflicting decision criteria, which is the case in most MCDA applications, an optimal decision is less likely to satisfy all decision criteria. For example, to decrease off-site risks of a fuel storage plant with a predefined inventory of fuel, the fuel content of storage tanks can be reduced. This, however, demands for a larger number of storage tanks, which in turn not only requires more resources (such as land) but also increases the possibility of domino effects and thus increases on-site risks.

To find an optimal plant layout, an AHP can be developed (Fig. 6.1.5) comprising a decision "optimal layout", three decision criteria "resources," "on-site risk," and "off-site risk," and six decision alternatives, i.e., plants depicted in Fig. 6.1.3. The decision criteria

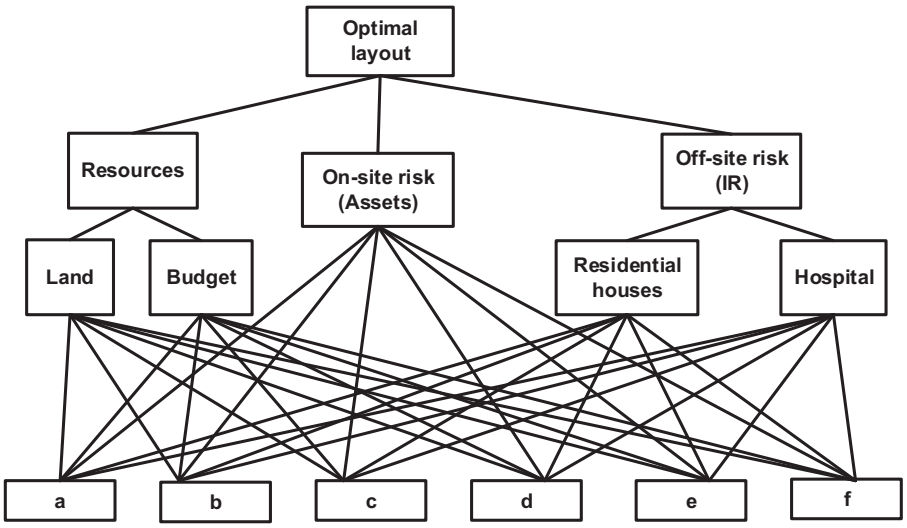


FIGURE 6.1.5 AHP for layouts shown in Fig. 6.1.3.

"resources" and "off-site risk" are subsequently decomposed to subcriteria "land" and "budget," and "residential houses" and "hospital," respectively. It is worth noting that the decision criteria are of different units: the land is in m^2; the budget and the internal risk are in USD; the internal risks are in death probabilities. Next steps are (i) to rank the decision criteria according to the optimal decision, (ii) to rank subcriteria considering their contributions to the criteria, and (iii) to rank decision alternatives considering their importance to decision subcriteria and criteria.

To rank the decision criteria against the decision, it has been assumed that among the criteria, the off-site risk should be given more priority over the on-site risk, and the on-site risk should be emphasized more than required resources. As such, using the fundamental scale table (Saaty, 2008), the weights of the decision criteria have been presented in Table 6.1.5 (columns 2–4). The normalized values of the principal eigenvector of the resulting matrix represent the ranks of the decision criteria according to the decision (column 5 of Table 6.1.5).

Similarly, the pairwise comparison of subcriteria "land" and "budget" against the criterion "resources" along with the pairwise comparison of "residential houses" and

Table 6.1.5 Pairwise comparison of decision criteria and their rank according to the decision.

	Resources	On-site risk	Off-site risk	Priority
Resources	1	1/3	1/7	0.081
On-site risk	3	1	1/5	0.188
Off-site risk	7	5	1	0.731

Table 6.1.6 Pairwise comparison of land and budget according to resources.

	Land	Budget	Priority
Land	1	1/3	0.250
Budget	3	1	0.750

Table 6.1.7 Pairwise comparison of residential houses and hospital according to off-site risk.

	Residential houses	Hospital	Priority
Residential houses	1	1/5	0.167
Hospital	5	1	0.833

"hospital" against the criterion "off-site risk" has been listed in Tables 6.1.6 and 6.1.7, respectively. These weights have been assigned assuming that the initial budget is a more important decisive factor than available land (perhaps due to the availability of extra land but scarcity of the budget) while IR at the hospital is more critical than that at the residential houses (due to a higher population density and relatively higher vulnerability of a hospital compared to residential houses).

To rank decision alternatives, i.e., plant layouts, against the aforementioned criteria and subcriteria, the problem constraints should be taken into account. Without loss of generality, assume that the desired amount of land available for the storage plant is about $7500\ m^2 \pm 10\%$ while the available budget to supply storage tanks is 2,000,000 USD ± 15%.

To set a constraint on the on-site risk, it is decided that the risk of on-site damages should be limited to 3E-5 times the sum of the initial budget (i.e., 2,000,000 USD) and the value of fuel content (24,000 m^3). Considering a value of 315 USD/m^3 for crude oil, the amount of the on-site risk thus should not exceed $3E\text{-}5 \times (2{,}000{,}000 + 24{,}000 \times 315) = 312$ USD. Moreover, following the risk-based approach of LUP suggested by HSE of the United Kingdom (PADHI, 2011), the amount of individual risks at residential houses and the hospital should not exceed 1.00E-05 and 3.00E-07, respectively.

For the sake of exemplification, the results of the pairwise comparison of plants according to "land" have been presented in Table 6.1.8. Having the local ranks of the plants, the overall rank of each plant can be calculated as shown in Fig. 6.1.6. As can be seen, the most three preferable plants are identified as layouts f, e, and a, respectively.

Table 6.1.8 Pairwise comparison of layouts according to land.

	a	b	c	d	e	f	Priority
a	1	5	2	9	9	9	0.421
b	1/5	1	1/3	7	7	7	0.150
c	1/2	3	1	9	9	9	0.335
d	1/9	1/7	1/9	1	1	1	0.031
e	1/9	1/7	1/9	1	1	1	0.031
f	1/9	1/7	1/9	1	1	1	0.031

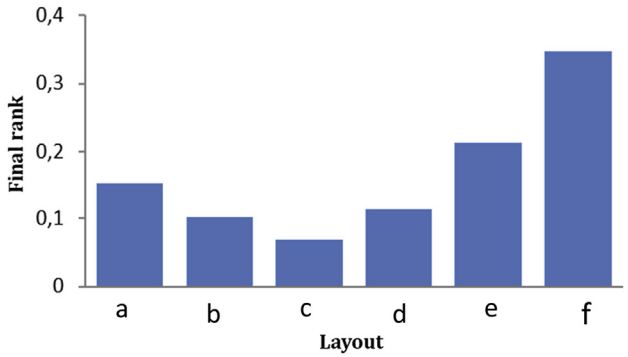


FIGURE 6.1.6 Final rank of plant layouts.

6.2 Security-based design of the industrial control system of process plants w.r.t cyberattacks

6.2.1 Introduction

Under the threat of terrorist attacks aiming at maximal damage, one needs to consider whether domino effects could also be caused intentionally. For instance, when such events could be initiated remotely via computer and network infrastructure, they could become attractive vectors for terrorists. Nowadays, the majority of chemical and process plants have adopted Industrial Control Systems (ICSs) to improve the management of their operation. The widespread adoption of ICSs can be attributed to an increased efficiency, improved safety, and reduction of production costs (Hayden et al., 2014). However, despite their apparent benefits, the adoption of ICSs by the industry has given rise to some criticisms with regard to cyberattacks' possibilities (Casson Moreno et al., 2018).

One of the impacts of ICSs adoption in chemical and process plants is the emergence of the risk of cyberattack to industrial facilities, such as the notorious Stuxnet malware against Iran's nuclear industry (Sanger, 2012), the Germany-based steel mill incident (Lee et al., 2014), and cyberattacks against a Saudi-based petrochemical company

(McMillan, 2018). Some studies have indicated that damages from targeted attacks have been the potential cause of domino effects (Crucitti et al., 2004; Zhao et al., 2004; Wang et al., 2014). More importantly, cyberattacks have been indicated as a potential trigger for domino accident (Srivastava and Gupta, 2010), and it is only a matter of time before adversaries trigger such incidents (Boyes, 2013).

Several countries have demonstrated the urgency to improve the cybersecurity of their critical infrastructures. For instance, the President of the United States signed an order to improve the cybersecurity of the United States' critical infrastructure, in which they declared cyber threats to their critical infrastructures as "the most serious national security challenges" (Schmidt and Perlroth, 2013). These policies have not only hinted the potential adverse impacts of cyberattacks toward critical infrastructure, but more importantly, confirmed the existence of motivated threat actors targeting these facilities.

All in all, the existence of cyber vulnerabilities in chemical and process plants, the possibility of cyberattacks to trigger domino effects, and the indication of threat actors that are motivated to exploit these vulnerabilities may indicate the need for risk assessment and management of cyberattack-related domino effects.

There have been extensive researches on the cybersecurity of ICSs in industrial facilities. For instance, the works of Stouffer et al. (2011) and Knapp and Langill (2014) have offered a comprehensive guideline to secure ICS and its related components by addressing the common vulnerabilities and threats and the control measures to mitigate the risks. ICS-CERT and NCCIC (2016) also present guidance for developing cybersecurity mitigation strategies for ICSs through a concept known as Defense-in-Depth. Byres and Lowe (2004) discussed the security implications of nonproprietary (open standard) technologies adoption in ICS and offered some recommendations to prevent the negative repercussions. Cardenas et al. (2009) elaborated on challenges of securing cyber−physical systems. However, despite the indication that cyberattacks might trigger domino effects in industrial facilities, no study has been attempted to address this issue.

One approach that can be taken to mitigate the risk of cyberattack-related domino effects is network segmentation of ICS networks in chemical and process plants. Network segmentation, also referred to as network segregation (Australian Signals Directorate, 2012) or network compartmentalization (Wagner et al., 2017), can be defined as the practice of partitioning a network architecture into multiple smaller segments, which is already regarded as a common approach used by businesses and organizations to improve their cybersecurity (Nicholas, 2017). By understanding the risk of domino effects and how cyberattacks might translate to accidents in chemical plants, segmentation of ICS networks can be designed in such ways that a primary accident resulting from a cyberattack imposes the least risk of domino effect.

For that purpose, this chapter introduces a risk-based methodology for developing ICS network segmentation in chemical and process plants that may improve the robustness against domino effects from cyberattacks. This way, chemical plants could become inherently securer toward cyberattacks and especially those aiming at triggering domino effects.

6.2.2 ICS network segmentation

Network segmentation can be defined as the partitioning of computer networks into subnetworks with the aim of preventing cyber threats from spreading (Security Roundtable, 2018). The main idea is when a data breach occurs in one of the segments, the attack will be contained within that subnetwork segment and be limited from accessing the other parts of the network (Fig. 6.2.1).

Network segmentation can be implemented using different techniques and technologies including physical segmentation, logical segmentation, and network traffic filtering (Stouffer et al., 2011). Physical segmentation is a method that utilizes separate communication infrastructures for different segments. On the other hand, logical segmentation is implemented logically, e.g., using Virtual LANs (VLANs) or virtual private networks (VPNs). Logical segmentation potentially presents similar security advantages offered by physical segmentation yet provides greater flexibility and lower cost. Lastly, network traffic filtering provides segmentation by restricting certain parts of the system from communicating with others.

Network segmentation has been recognized as a common practice in both IT networks and ICS networks to increase the security of systems (Nicholas, 2017). In the present study, the segregated partitions of the network will be referred to as "network segments" or simply "segments." An example of ICS network segmentation implementation in a tank farm is illustrated in Fig. 6.2.2.

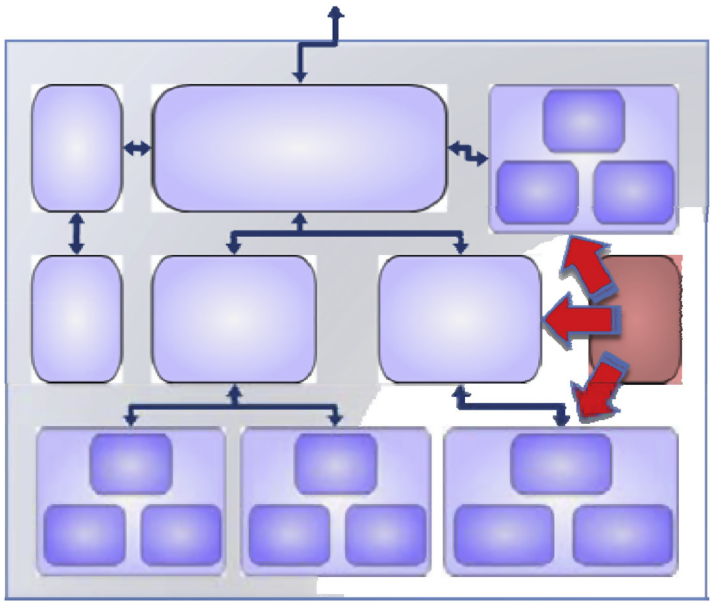


FIGURE 6.2.1 Illustration of a security breach in a segmented system. The segment highlighted in red (black in print version) is assumed to be under security breach. *Adopted from Siemens., 2008. Security Concept PCS 7 and WinCC—Basic Document (Whitepaper). Retrieved from: https://cache.industry.siemens.com/dl/files/131/26462131/att_80283/v1/wp_sec_b.pdf.*

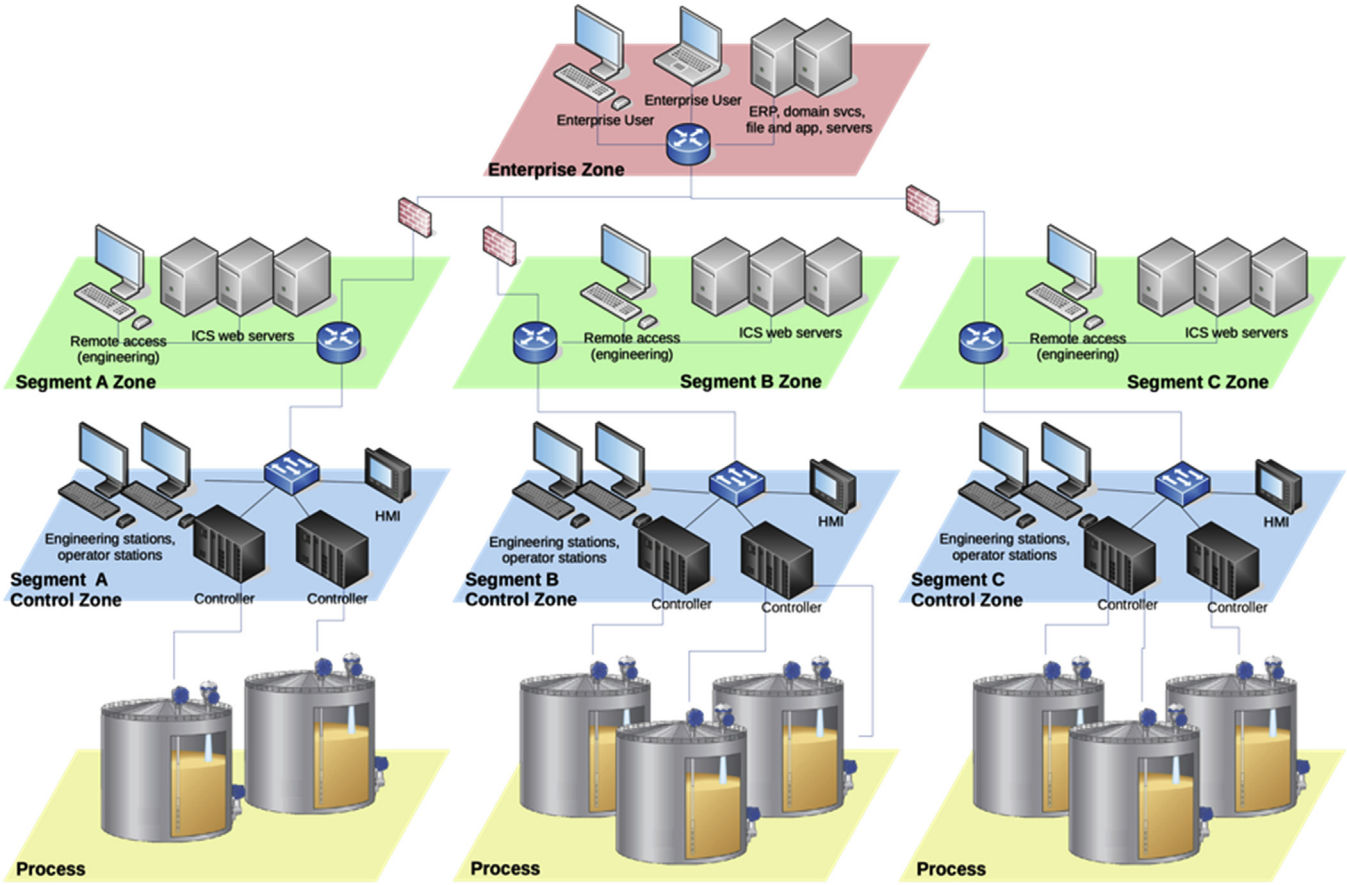


FIGURE 6.2.2 An example of a network segmentation in a tank farm.

6.2.3 Minimax strategy

In the case of adversarial risk analysis, game theory can be employed to improve the outcome of risk analysis (Cox, 2009). In the context of game theory, cyberattacks to a process plant can be considered as an attacker–defender game. An attacker–defender game is a setting where the defenders move first by allocating resources to their defense before the attackers deploy an attack to respond to the defender's strategy with the goal of gaining the optimal outcome; finally each player receives a payoff or consequence (Cox and Anthony, 2009).

In such an adversarial game, the minimax analysis can be an alternative when the attackers' payoff is unknown to the defenders (Cox and Anthony, 2009). Minimax can be useful for handling uncertainties in situations where probabilities are not available (Aghassi and Bertsimas, 2006). Through this minimax analysis, the defenders try to minimize the maximum possible damage by anticipating the worst attack scenarios.

With regard to domino effects, it can be assumed that the attackers' motivation would be inflicting maximum damage to the plants. Based on this argument, the payoff sought by the attackers can be deemed equivalent to the amount of damage to the facility. In other words, the attackers can be assumed to pursue an attack scenario with the highest risk of domino accident.

It is also assumed that the attackers are only capable of attacking a single segment. Realistically speaking, in a situation where the attacker is highly skilled, and the system is improperly defended, it is possible that the attacker can penetrate the entire system despite the implemented segmentation. However, under such circumstances, it can be argued that the system owners should be dealing with an entirely different issue as the addition of network segmentation would add little to no security benefit.

The application of minimax analysis can be described using the example presented in Table 6.2.1, considering two defense strategies A and B and two attack strategies X and Y. In this example, the numbers in Table 6.2.1 present the loss incurred by the defenders for each defend–attack pair. Considering the maximum loss for each defense strategy, it can be seen that defense strategy B would result in a lower amount of maximum loss. By anticipating the worst attack scenario for every segmentation alternative (defense strategy), the alternative that would yield the least maximum damage can be identified as the optimal defense strategy, resulting in the least maximum risk of domino effects.

Table 6.2.1 Example of minimax strategy.

	Attacker strategy		
Defender strategy	**X**	**Y**	**Maximum loss**
A	900	600	900
B	750	700	**750**

This is the lowest maximum loss.

6.2.4 An illustrative example

In this section, the network segmentation and the impact of attack scenarios will be demonstrated using a tank farm of six gasoline atmospheric storage tanks, T1−T6, as depicted in Fig. 6.2.3. All the tanks are identical with a diameter of 33 m, a height of 9 m, and volume of 8000 m^3.

For illustrative purposes, assume that the central control system is divided into two segments: Segment A (SgA) and Segment B (SgB). Hence, the goal is to determine the network segmentation alternative that exhibits the highest robustness against the risk of cyberattack-related domino effects. Now, consider a segmentation alternative where SgA comprises T1, T3, and T4 while SgB comprises T2, T5, and T6 (Fig. 6.2.4).

Further, since there are two control centers to control the tank farm, two attack scenarios against the tank farm could be envisaged: the first attack scenario, At_1, where the control center of SgA is attacked, and the second attack scenario, At_2, where the control center of SgB is attacked. Attacks to SgA or SgB could compromise the safety of the storage tanks controlled within that network segment (unwanted opening of drain valves, overflow of the tank, etc.). These attack scenarios will be considered when calculating the risk of domino effects for each segmentation alternative.

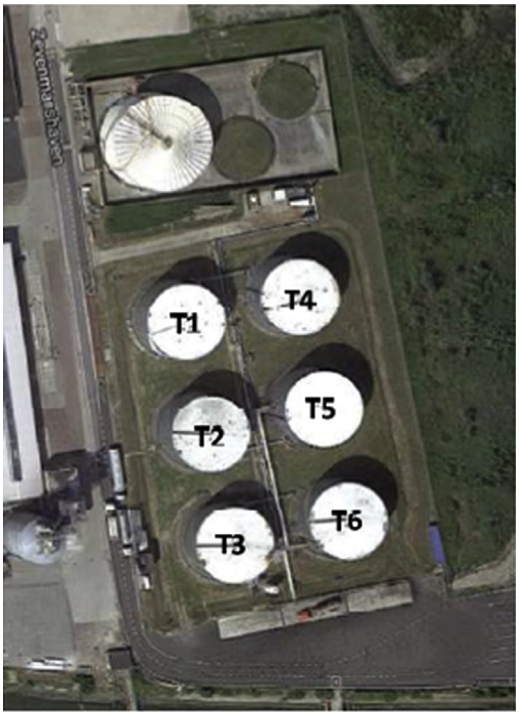


FIGURE 6.2.3 Layout of a gasoline tank farm.

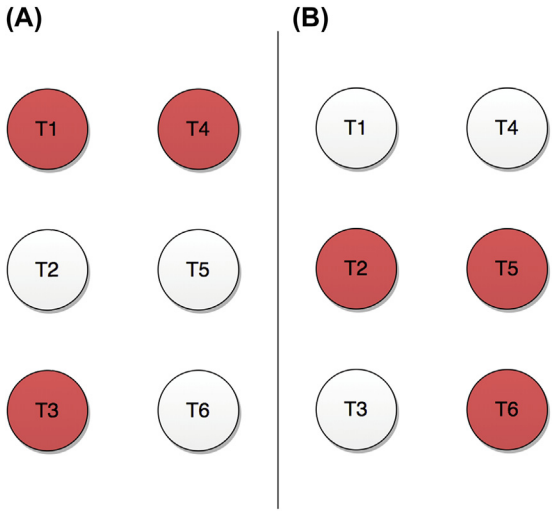


FIGURE 6.2.4 The units in (A) Segment A and (B) Segment B considering the plant layout reported in Fig. 6.2.3.

For illustrative purposes, in the present study, the considered attack scenario is considered a cyberattack to the ICS within the tank farm, which may lead to a major release of flammable materials and subsequently a pool fire (PF) given ignition (with a certain probability).

To estimate the risk of domino effects for each segmentation alternative, the damage probability of every storage tank for both attack scenarios must be calculated. To achieve that, the BN methodology developed by Khakzad et al. (2013) could be employed. Table 6.2.2 presents the amount of radiated heat the storage tanks would receive from pool fire at an adjacent tank. Fig. 6.2.5 displays the potential domino effect triggered by attack scenario At_1.

To calculate the conditional probabilities required for the quantification of the BN, P(Release | Cyberattack) is assumed 1.00E-01, and P(Ignition | Release) is estimated as 5.00E-02 (Rew and Daycock, 2004), resulting in P(Primary pool fire | Cyberattack) = P(Release | Cyberattack) × P(Ignition | Release) = 5.00E-03. Having the probabilities of

Table 6.2.2 Heat radiation intensity tank T_j receives from tank T_i (kW/m^2).

$T_i\downarrow$ $T_j\rightarrow$	T1	T2	T3	T4	T5	T6
T1	–	38	–	22	–	–
T2	38	–	38	–	22	–
T3	–	38	–	–	–	22
T4	22	–	–	–	38	–
T5	–	22	–	38	–	38
T6	–	–	22	–	38	–

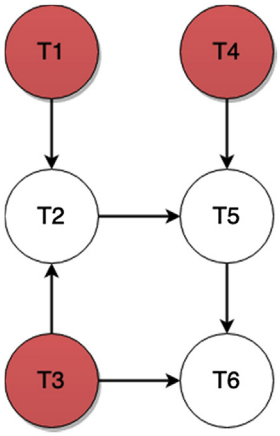


FIGURE 6.2.5 Application of BN for modeling domino effect triggered by At_1 scenario.

Table 6.2.3 Marginal probability of accident at the storage tanks.

	Probability of accident	
Storage tank	***At*$_1$ scenario**	***At*$_2$ scenario**
T1	5.00E-03	1.60E-05
T2	3.43E-05	5.00E-03
T3	5.00E-03	1.72E-05
T4	5.00E-03	1.60E-05
T5	1.60E-05	5.00E-03
T6	3.32E-07	5.00E-03

the primary events and the escalation probabilities of the other units, the developed BN was quantified to calculate the marginal probability of accident at each storage tank as presented in Table 6.2.3.

The risk of damage to each storage tank is the product of the probability of damage and the value of the tank without considering loss of life, off-site damages, reputation loss, etc. Considering that all the tanks are identical, a monetary value of €3.1M is assigned to each storage tank (Matches, 2014). For instance, considering the probabilities of accidents in Table 6.2.3, the risks sustained by T1 and T2 in the attack scenario toward Segment A are €15,500 and €106, respectively. Table 6.2.4 presents the estimated risks of damage to the storage tanks for both attack scenarios.

Based on the assumption that attackers aim to maximize the amount of damage to the system, and the attackers are only able to target a single segment, it can be understood that the attackers would pursue an attack scenario with the highest risk in any network segmentation alternative. Accordingly, the risk of domino effects for a segmentation alternative would be equal to the risk of domino effects for its highest attack scenario. For example, since the risk level of At_1 is higher than that of At_2, it can be determined as a more credible attack scenario and thus its risk as the risk of domino accident.

Table 6.2.4 Risk of damage to the storage tanks.

	Risk	
Unit	**Attack scenario At_1**	**Attack scenario At_2**
T1	€15,500	€50
T2	€106	€15,500
T3	€15,500	€53
T4	€15,500	€50
T5	€50	€15,500
T6	€1.0	€15,500
Total	€46,657	€46,653

The process of examining the robustness of network designs can be lengthy and complicated in the case of large process plants with tens and even hundreds of process units; hence, the number of design alternatives that can be examined should be limited. In this regard, segmentation of units based on their criticality could be investigated as a viable approach.

Criticality of the units based on graph metrics can be a useful criterion to help develop robust segmentation designs. Critical units refer to the units whose failure would contribute the most to the initiation and continuation of domino effects. It has been demonstrated that the graph centrality metrics are applicable for identifying critical units. More specifically, accidents on units with higher out-closeness score would result in a higher probability of domino effects, whereas units with higher betweenness score would contribute more to the propagation of domino effects (Khakzad and Reniers, 2015a,b).

For demonstration purposes, the vertex-level centrality score of each tank (node) in Fig. 6.2.3 is calculated. When calculating the centrality scores, it is important to note the difference in the weight of the edges: larger weights represent a longer distance, hence weaker connectivity. However, in domino effects modeling, larger weights (i.e., larger heat intensity) represent stronger connectivity. To manage this difference, the weight of the edges will be presented as a ratio of the threshold value and the value of the escalation vector. For instance, the weight of the edge between T1 and T2 is $15/38 = 0.395$. To obtain the centrality scores of the units, a directed graph based on Table 6.2.2 is developed and modeled using the igraph package in RStudio (Csardi and Nepusz, 2006). The results are presented in Table 6.2.5.

Table 6.2.5 Centrality metrics for storage tanks in Fig. 6.2.5.

Attack to node	**T1**	**T2**	**T3**	**T4**	**T5**	**T6**
Vertex-level out-closeness	0.226	0.276	0.226	0.226	0.276	0.226
Risk	€15,550	€15,600	€15,550	€15,550	€15,600	€15,550

Table 6.2.6 Graph-level centrality for single accident scenarios.

Attack to node	T1	T2	T3	T4	T5	T6
Graph-level out-closeness	0.180	0.423	0.180	0.180	0.423	0.180
Risk	€15,550	€15,600	€15,550	€15,550	€15,600	€15,550

In Table 6.2.5, it can be seen that both T2 and T5 have the largest vertex-level out-closeness score and also would result in the highest risk if selected as the primary units initiating domino effect. Having the vertex-level centrality scores of the units, the graph-level out-closeness can be calculated as an indication of the vulnerability of the storage plant to domino effect (Khakzad and Reniers, 2015a,b, 2018). As presented in Table 6.2.6, it can be seen that primary events at T2 and T5 have resulted in the highest graph-level out-closeness, which is consistent with the result from the vertex-level out-closeness.

Khakzad and Reniers (2018) demonstrated that an attack to two of the most critical units (i.e., those with the largest vertex-level out-closeness) would result in the most severe domino accidents compared to an attack to any other pair of units. Accordingly, it may be implied that by separating these units into different segments, a scenario in which both of these units fail at the same time can be avoided. Hence, it can be hypothesized that by identifying the most critical units using their out-closeness score and allocating them into separate segments, more robust network segmentation alternatives can be developed.

6.2.5 Application of methodology

Fig. 6.2.6 displays a tank farm consisting of eight storage tanks of different size and volume. The potential heat radiation intensities between the tanks are presented in Table 6.2.7. The costs of the storage tanks are presented in Table 6.2.8.

Based on the amount of the escalation vectors in Table 6.2.7, a directed graph illustrating potential domino effects through the storage tanks can be created. Using the directed graph and the heat radiation intensities, the vertex-level out-closeness score of the storage tanks can be computed.

However, not all factors that affect the risk of domino effects can be represented by vertex-level out-closeness. For instance, although the volume of flammable chemicals of the storage tanks plays an important role, it is not considered in the vertex-level out-closeness score. To consolidate the tank's volume into its criticality score, geometric mean of the tank's out-closeness score and its volume can be used:

$$Cr = \sqrt{C_{out} \cdot V} \tag{6.2.1}$$

where Cr is the modified criticality, C_{out} is the vertex out-closeness, and V is the volume. The out-closeness scores and the modified criticality score of the tanks in Fig. 6.2.6 are presented in Table 6.2.9.

FIGURE 6.2.6 Layout of a storage tank farm consisting of eight storage tanks.

Table 6.2.7 Heat radiation intensity (kW/m^2) T_j receives from T_i in Fig. 6.2.6.

$T_i\downarrow$ $T_j\rightarrow$	T1	T2	T3	T4	T5	T6	T7	T8
T1	–	34	34	–	–	–	–	–
T2	34	–	19	34	–	–	–	–
T3	34	19	–	19	34	–	–	–
T4	–	29	15	–	30	–	–	–
T5	–	–	30	30	–	15	15	–
T6	–	–	–	–	15	–	15	32
T7	–	–	–	–	15	15	–	32
T8	–	–	–	–	–	30	30	–

Table 6.2.8 Approximate cost of tanks in Fig. 6.2.6 (Matches, 2014).

Tank	T1	T2	T3	T4	T5	T6	T7	T8
Vol (m^3)	39,700	39,700	39,700	25,400	25,400	25,400	25,400	17,600
Cost (Euro)	2,057,500	2,057,500	2,057,500	1,638,400	1,638,400	1,638,400	1,638,400	1,354,500

Table 6.2.9 The criticality of the tanks in Fig. 6.2.6.

Tank	T1	T2	T3	T4	T5	T6	T7	T8
V (m^3)	39,700	39,700	39,700	25,400	25,400	25,400	25,400	17,600
C_{out}	0.110	0.112	0.138	0.126	0.156	0.106	0.106	0.087
Cr	66.01	66.77	73.98	56.54	62.86	51.91	51.91	39.19

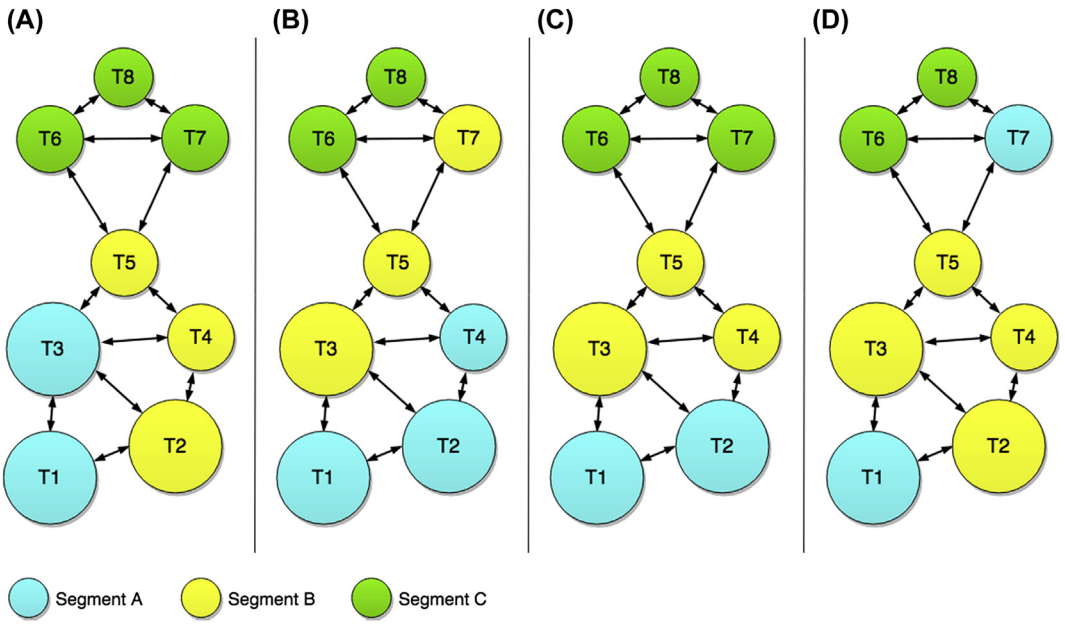


FIGURE 6.2.7 Illustrations of four network segmentation alternatives for the tank farm in Fig. 6.2.6: (A) NSD-1, (B) NSD-2, (C) NSD-3, and (D) NSD-4.

Using the C_{out} exclusively, T5, T3, and T2 would be identified as the most critical units. On the other hand, considering the Cr, T3, T2, and T1 would be identified as the most critical nodes.

As previously discussed, the most critical units must be distributed into separate segments. Based on the criticality scores presented in Table 6.2.9, units T3 and T2 can be considered as the most critical storage units descendingly. Hence, for the design alternatives to be made, the T2 and T3 units must be placed in separate segments.

For the present case, three design alternatives with an identical number of segments are considered as presented in Fig. 6.2.7: panel (A) NSD-1, panel (B) NSD-2, and panel (C) NSD-3. For the sake of demonstration, one additional segmentation alternative is considered without separating the critical units, namely, NSD-4 as in Fig. 6.2.7D, which is expected to perform not so effectively as the other alternatives. Now that the segmentation alternatives have been developed, the next step is to analyze their respective risk of domino effect to determine the most robust segmentation alternative.

To evaluate the robustness of the alternatives, each one must be assessed using the developed risk-based method. Firstly, the attack scenarios for every design alternative

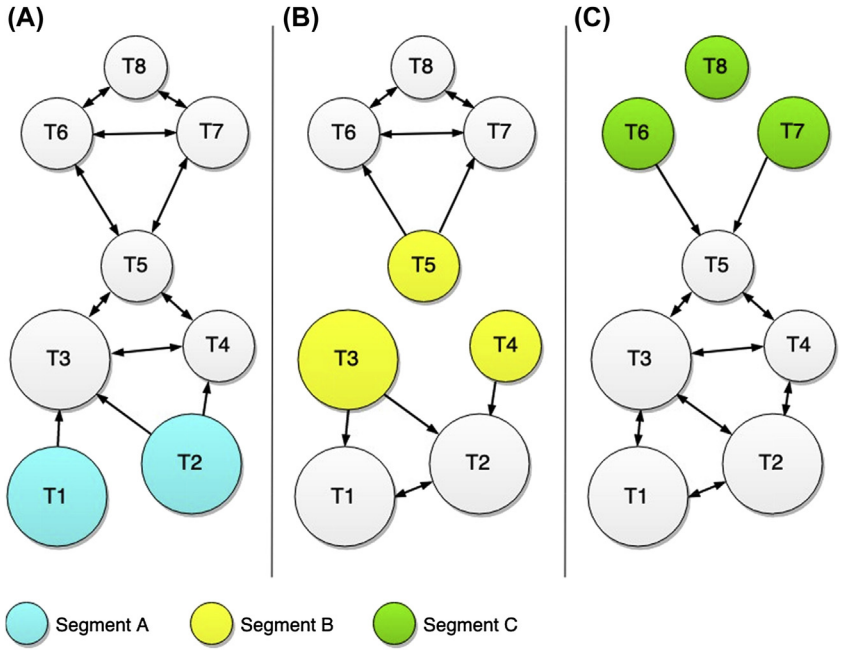


FIGURE 6.2.8 The graphs illustrating the primary units attacked according to segmentation in Fig. 6.2.7C. (A) Attack to Segment A, (B) attack to Segment B, (C) attack to Segment C.

must be defined. In this case study, there are three attack scenarios for each design alternative. For instance, Fig. 6.2.8 illustrates the primary units that may be attacked with regard to segmentation in Fig. 6.2.7C.

The BN methodology can be applied to every attack scenario on each design alternatives to model the domino effects and estimate the risks. Once the risk values of all attack scenarios are obtained, the minimax analysis can be utilized to select the optimal segmentation alternative; the results are summarized in Table 6.2.10.

As can be seen, NSD-3 (Fig. 6.2.7C) has the lowest risk compared to the other alternatives and hence can be selected as the most robust design alternative. On a side note, it can also be seen that the design alternative developed without separating the critical units, i.e., NSD-4, exhibits the least robustness than the other alternatives.

Table 6.2.10 The risk of each network segmentation alternative in Fig. 6.2.7.

		Risk			
Design	**Panel of Fig. 6.2.7**	**Segment A**	**Segment B**	**Segment C**	**Maximum**
Nonsegmented network		–	–	–	€68,557
NSD-1	A	€21,629	€28,133	€23,158	€28,133
NSD-2	B	€29,774	€27,669	€15,042	€29,774
NSD-3	C	€21,627	€28,031	€23,158	**€28,031**
NSD-4	D	€20,195	€38,647	€15,042	€38,647

This is the lowest maximum damage.

6.3 Add-on (safety and) security measures: an in-depth discussion

6.3.1 Protection of industrial facilities: the concept of safety barriers and layers of protection

Barriers, defenses, safeguards constitute layers of protection aimed at avoiding the propagation of a hazard toward a target and occupy a key position in high-technology systems (Reason, 2000). Therefore, standards, design practice, and regulations critically focus on their introduction and assessment in the design of industrial facilities and, more specifically, chemical and process facilities. An in-depth conceptualization of "safety" and "security" is out of the scope of this chapter (see (Amundrud et al., 2017) for more details); following the approach described in Chapter 5, a functional and practical distinction is adopted in this chapter to specifically support the discussion of critical layers of protections of industrial facilities:

- "Safety" barriers constitute hardware, operations, procedures, design strategies, etc., aimed at reducing the risk arising from unintentional accidents affecting an industrial facility. Safety barriers can be directed toward reducing the likelihood of incidents (incident frequency), or reducing the magnitude of the loss, injury, or damage should an incident occur (incident consequences), or some combination of both.
- "Security" barriers and, specifically "physical security measures," constitute the protection against external acts of interference, i.e., intentional damages to the plant operation.

In the specific field of physical security, the study by Nunes-Vaz et al. (2011) shed light on the concepts of security functions, security layers, and security barriers to be adopted with reference to physical protection systems (PPSs), thus clarifying the concept of layered security (security-in-depth) and its implications in terms of resource allocation objectives. The more rigorous framework to security-in-depth and the related principles were then applied to provide practical guidance for the design of physical security in complex infrastructures (Nunes-Vaz and Lord, 2014).

Although methodologies and tools are available for the development of security risk assessments and security plans to be implemented at industrial facilities, no specific guidelines on the selection and on the performance assessment of security countermeasures have been established to date. Only general guidance of security risk mitigation through the adoption of recommended security countermeasures is currently available (Garcia, 2008; Norman, 2010). This induces two relevant issues:

(i) the merits of effectiveness of security countermeasures and the estimation of the effects of their use are not systematically addressed in the specific field of chemical and process plants protection

(ii) the integration/synergy between "safety" and "security" barriers is not systematically undertaken.

In the following, these specific issues, which were introduced in Section 5.1, are discussed in depth with some examples of applications. A dedicated analysis of physical security systems aimed at the protection of chemical and process facilities is firstly outlined (Section 6.3.2). Specific data gathered in a previous research study (Argenti et al., 2017) are illustrated in order to provide an example of quantitative estimation of PPS effectiveness. Safety barriers that are commonly adopted in process plants are then briefly presented (Section 6.3.3), in order to highlight their potential integration and synergy with security systems in protecting industrial facilities against the escalation of cascading events triggered by external acts of interference.

6.3.2 Protection of chemical facilities against external acts of interference: a focus on physical security

In recent years, the definition of strategic objectives to enhance the security of the chemical and process industry was based on the perspective that considers security throughout its timeline from emergence of the threat, through the occurrence of a defined security event, to its effects and downstream consequences. Hence, each security countermeasure may act as a pre-event or as a post-event control and have a contribution to overall risk reduction (Talbot and Jakeman, 2009).

The aforementioned timeline perspective induced the establishment of the rigorous framework for physical security based on the concept of layered security (security-in-depth) (Nunes-Vaz et al., 2011). Layers require the coordination of one or more security functions, which synthetize the accomplishment of protection objectives. The layers and functions are implemented by security barriers: a security barrier (also security control or countermeasure) is therefore a physical, procedural, technical, or other device that performs or contributes to one or more security functions (Garcia, 2006; Nunes-Vaz et al., 2011).

In this section, the ultimate objective of a PPS is considered to prevent the accomplishment of malevolent actions against assets. The protection functions are summarized in the following, based on the indications reported in (Garcia, 2008) and incorporating elements of the aforementioned "5D" principle (see Chapter 5):

- *Detection*: discovery of an adversary action through sensing adversary actions, alarm transmission, and alarm assessment;
- *Delay*: slowing down of adversary progress toward the target equipment to provide additional time to respond;
- *Response:* action taken by the response force to prevent the adversary from reaching and damaging the target.

A fourth function, namely the *deterrence*, is considered in the study by (Nunes-Vaz et al., 2011). The concept of deterrence is related to the implementation of measures that are perceived by the potential adversary as too hard to defeat, thus decreasing the facility attractiveness (see Section 3.2) and possibly convincing the adversary not to attempt an attack. Since this measure is dependent on adversaries' perceptions, the

effectiveness of the deterrence may introduce relevant uncertainties in a quantitative assessment (Nolan, 2008). Hence, in this section, deterrence was not analyzed, leading to a conservative treatment of the subject (in other words, once an adversary is identified, there will be an attack).

Fig. 6.3.1 illustrates more details on the functions and components of each preventive layer of physical security. This characterization sets the basis of the quantitative assessment of the overall effectiveness of PPSs object of this section and that was adopted in Section 4.2 to carry out the quantitative study based on Bayesian Networks.

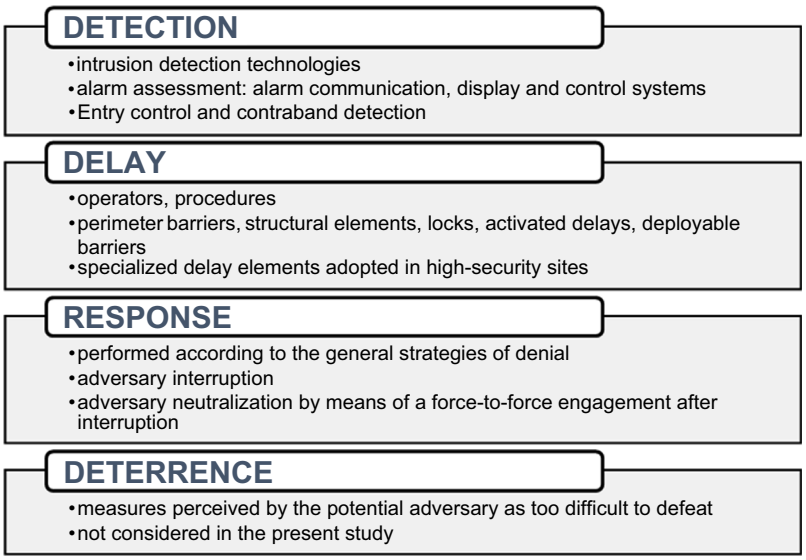


FIGURE 6.3.1 Details on the security protection functions as described by (Nunes-Vaz et al., 2011). *Adapted from Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Quantitative performance assessment of physical security barriers for chemical facilities, in: Safety and Reliability—Theory and Applications—Proceedings of the 27th European Safety and Reliability Conference, ESREL 2017. CRC Press/Balkema, Boca Raton, FL, pp. 1279–1288.*

6.3.2.1 Defining the performance of PPS

The direct measure of PPS effectiveness derives from the assessment of the effectiveness measures pertaining to the three functions of detection, delay, and response (see Fig. 6.3.1). In the present study, the metrics for physical protection system effectiveness that was proposed by the Sandia vulnerability assessment model was adopted (Garcia, 2008).

The Sandia model makes use of the concept of "timely detection" to measure PPS overall effectiveness. The principle of timely detection states that system effectiveness is measured by the cumulative probability of the detection at the point where there is still enough time remaining for the response force to interrupt the adversary. The probabilistic terms of interest to express the PPS overall performance are defined in Table 6.3.1 together with the correspondent mathematical expressions.

Table 6.3.1 Summary of quantitative relationships to support the estimation of PPS effectiveness.

Item	Description	Relationship
P_I	Probability of adversary interruption, namely the effectiveness of the considered protection layer	$P_I = P_{AD} \times P_C \times P_T$
P_T	Probability of response force intervening on time to prevent attack success assuming normal distribution of time parameters	$p_T = \frac{1}{\sqrt{2\pi\left(\sigma_{RFT}^2+\sigma_D^2\right)}} \int_0^T e^{-\frac{T^2}{2\left(\sigma_{RFT}^2+\sigma_D^2\right)}} dT$
P_{AD}	Probability of successful assessed detection of a security breach	$P_{AD} = \left[1 - \prod_{i=1}^{k}(1 - P_{D,i})\right] \times P_{AS}$
P_{AS}	Probability of successful alarm assessment	Single point probability
P_C	Probability of successful communication	Single point probability
$P_{D,i}$	Probability of detection by the sensor system present at the *i*-th ring of protection	Single point probability
T	Penetration time for *i*-th delay barrier	$T = \sum_{i=k+1}^{m} T_{Di} - RFT > 0$
T_{Di}	Penetration time along adversary's path toward the target	Single point value
RFT	Response force time	Single point value

Adapted from 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.

It is worth noticing that the relationships summarized in Table 6.3.1 need to be applied given a specific adversary's path. Pathway analysis consists in determining the ordered series of a potential adversary's actions and locate them on the corresponding areas and perimeters of the site under analysis (see Section 3.3). Indeed, the previous identification of credible adversary paths toward a potential target equipment item allows to identify which security controls may actually pose an obstacle to adversary progress as they are physically located along the path.

In order to apply the set of equations summarized in Table 6.3.1, reliable quantitative data are needed. The Sandia metric may be considered as a reference guideline in the definition of performance variables and, whenever possible, in security controls performance quantification (this is the case for data on the normal distribution of penetration time for delay barriers, derived from field tests and available in (Garcia, 2006)). However, there is not a specific standard dataset for process and chemical facilities. Therefore, Argenti and coworkers (Argenti et al., 2017) elaborated a methodology based on expert consultation to seek quantitative performance estimates.

6.3.2.2 Methodology for gathering PPS quantitative performance data

The methodology for gathering PPS quantitative performance data is based on the following four phases:

1. Definition of security functions required to PPS effective action
2. Identification of security controls contributing to each security function
3. Identification of influencing factors and variables
4. Probabilistic performance assessment.

Table 6.3.2 List of experts that cooperated and of industrial sites that were analyzed in the study.

Expert	Expert position	Analyzed site type
A	Site security manager	Chemical production site
B	Company security manager	Petrochemical production sites (company-owned sites)
		Petroleum products depots (company-owned sites) – Large scale
		Petroleum products depots (company-owned sites) – Small scale
C	Security consultant	LNG regasification terminal + shore base
D	Security consultant	Chemical production site
E	Site manager	Seveso plant
F	Safety manager	Chemical production site

Adapted from 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.

Considering the lack of applicable experimental data and available literature information on the effectiveness of security barriers and controls, the performance quantification study was translated into an expert judgment exercise. Six experts provided information on the effectiveness of PPS elements applied to secure different types of industrial sites, as summarized in Table 6.3.2.

The security functions required to PPS effective action were identified in the preparatory study, as documented in Section 6.3.1. Then, the first phase of experts' consultation was based on a standardized checklist, which was sent to each expert before the interview, which allowed completing phases 2 and 3.

The last phase (phase 4) consists of the elicitation of probabilistic performance variables through a simplified approach and supported by the use of a preprepared questionnaire tailored on the results of the previous phases of consultation.

The postelicitation phase mainly regarded the combination of expert assessments. Herein, an equal weighting aggregation scheme was applied. The simplest weighting scheme was adopted due to the lack of literature data on physical protection systems that might be used as seed variables to determine experts' performance as subjective probability assessors to be translated into global calibration scores to support performance-based weighing of experts.

During the elicitation of quantitative PPS performance estimates, the security barriers that constitute a functional subsystem were considered one by one, as separate modules. The term "PPS functional sub-system" is herein used to represent a security barrier made up of hardware elements, software elements, and/or procedural elements implementing in itself one of the primary functions of the preventive PPS.

The quantification regarded the overall performance variables, as defined according to Sandia effectiveness metric, together with all identified variables and situational factors affecting the performance (see Table 6.3.1). In the majority of cases, the influencing factors identified by the experts were considered as independently affecting the successful accomplishment of a security function; when interdependencies needed to be included, they were evidenced and quantitatively characterized through the elicitation of conditional probabilities.

Table 6.3.3 Summary of query variables obtained through experts' elicitation.

ID	Definition/Relationship
P_m	Marginal probability of occurrence of the favorable state of each relevant IF
P_0	Conditional probability of the security barrier successfully performing the design security function, being the IF in favorable state (namely, the "baseline" state of the functional subsystem)
r_i	Impact index, measuring the impact of the i-th IF on P_0, if it changes from the favorable to the unfavorable state

IF, influencing factor.

Adapted from 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.

The selection of query variables pertaining to each module was based on the adoption of a simplified approach, which required the elicitation of three probability values, as summarized in Table 6.3.3.

This allowed to reduce the number of conditional probabilities to be elicited and to quantify the probability of success of each security barrier P_{SB}, given all possible combinations of states of its influencing factors, as follows:

$$P_{SB} = P_0 \Pi_{i=1}^{N} X_i r_i \tag{6.3.1}$$

where N is the number of factors and variables that (independently) affect the performance of the security barrier, P_0 and r_i are defined in Table 6.3.3, and $X_i = 1$ if the i-th influencing factor is in its unfavorable state, while $X_i = 1/r_i$ if the i-th influencing factor is in its favorable state. A scale to translate from a verbal description to a measure of impact was used during the interview to aid the expert in eliciting numerical values to capture impact factors, r_i, on baseline probabilities. The scale is defined in Fig. 6.3.2.

Qualitative impact	None	Small	Medium	Significant	Large
Impact index, r_i	1	0.75	0.5	0.25	0.1

FIGURE 6.3.2 Conversion of qualitative verbal impact classification to r_i impact factors in Eq. (6.3.1).

6.3.2.3 Identification of security "typicals" and performance data

The preliminary phase of expert consultation, which was carried out asking experts to fill a checklist (see Section 6.3.2), indicating the security barriers in place in the sites summarized in Table 6.3.2, allowed the identification of the typical security barriers (or security "typicals", see Section 5.4 for a more extended description) used in a representative set of European chemical facilities, as summarized in Table 6.3.4, where security barriers are classified based on their function.

During the first part of the interviews, consultation was finalized at the identification of the influencing factors or variables that may affect the success of PPS barriers in performing their function. An agreed set of influencing factors for the security barriers representing a PPS functional subsystem was extracted from interviews, an example is reported in Table 6.3.5, while the complete set of influencing factors is reported elsewhere (Argenti et al., 2017).

Table 6.3.4 Summary of typical security barriers adopted in European chemical facilities.

Function	Relevant security barriers
Detection	External IDS based on VMD
	Intrusion detection by roving guards
	Intrusion detection by employees
	Entry control, supervised automatic credentials check (people)
	Entry control, unsupervised automatic credentials check (people)
	Entry control, manual credentials check (people)
	Entry control, unsupervised automatic biometrics check (people)
	Entry control, supervised automatic credentials check (vehicles)
	Entry control, manual credentials check (vehicles)
	Manual machine-aided contraband detection on people
	Manual machine-aided contraband detection on baggage/items
	Manual contraband detection for vehicles
Alarm assessment	Alarm assessment through CCTV system
	Alarm assessment by roving guards
	Alarm assessment by employees
Alarm communication	Communication to/among response force

Adapted from 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; Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Quantitative performance assessment of physical security barriers for chemical facilities, in: Safety and Reliability—Theory and Applications—Proceedings of the 27th European Safety and Reliability Conference, ESREL 2017. CRC Press/Balkema, Boca Raton, FL, pp. 1279–1288.

Table 6.3.5 Performance influencing factors for relevant security barriers summarized in Table 6.3.4.

Security barrier	Relevant influencing factors	Favorable state	Unfavorable state
Intrusion detection by EMP	EMP presence	True	False
	EMP level of security training	High	Low
Alarm assessment by EMP	EMP level of security training	High	Low

EMP, employees.

Adapted from Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Quantitative performance assessment of physical security barriers for chemical facilities, in: Safety and Reliability—Theory and Applications—Proceedings of the 27th European Safety and Reliability Conference, ESREL 2017. CRC Press/Balkema, Boca Raton, FL, pp. 1279–1288.

Expert elicitation, conducted through the procedure described in Section 6.3.2, allowed for the quantitative probabilistic assessment of PPS performance, with the support of a questionnaire specifically prepared. A satisfying percentage of the questions (higher than 85%) received an answer, providing a quantitative estimate of performance.

For the sake of brevity, only the analysis of questionnaire results concerning the modules summarized in Table 6.3.5 is described in detail. The results are illustrated in Fig. 6.3.3, where expert estimates are presented in the aggregate form of a box plot, to provide a synthetic visualization of the different judgements.

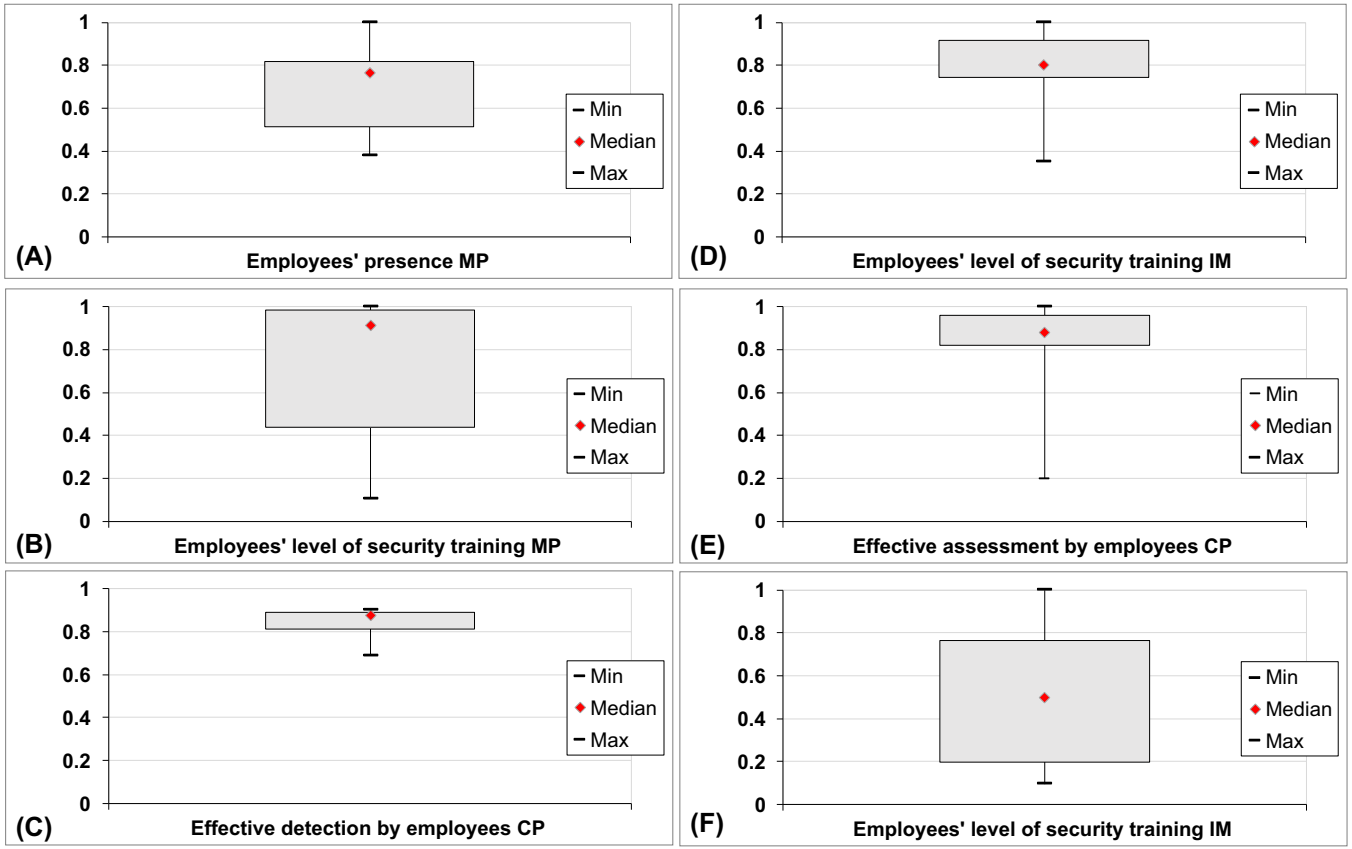


FIGURE 6.3.3 Performance estimates provided by experts with respect to the security functions summarized in Table 6.3.3. (A) MP of employees' presence; (B) MP of employees having a high level of security training; (C) CP of having effective detection given all IFs in favorable state; (D) IM that a low level of security training has on the probability of effective detection; (E) CP of having effective alarm assessment given all IFs in favorable state; (F) IM that a low level of security training has on the probability of effective alarm assessment. MP: marginal probability; *CP*, conditional probability; *IM*, impact measure. *Adapted from Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Quantitative performance assessment of physical security barriers for chemical facilities, in: Safety and Reliability—Theory and Applications—Proceedings of the 27th European Safety and Reliability Conference, ESREL 2017. CRC Press/Balkema, Boca Raton, FL, pp. 1279—1288.*

As shown in Table 6.3.5, in the case of intrusion detection by employees working on site, the main influencing factors are the employees' presence and their level of security training. All experts agreed that if employees are not present at the location where intrusion occurs, there cannot be detection. The estimates of marginal probabilities of employees being present at the location where intrusion occurs shown in Fig. 6.3.3A were derived taking into account that intrusion may occur at any location of the site and considering the different number of employees present during day shift and night shift. When experts were asked to provide the marginal probability of employees having received a high level of security training, which represents the favorable state, the estimates obtained spanned almost the entire range (from 0 to 1). However, a high median value is shown in Fig. 6.3.3B, since four of six estimates were equal or higher than 0.85.

As shown in Fig. 6.3.3C, there was a rather good agreement among the experts in the assessment of employees' performance in detecting intruders or, more in general, any suspect person, activity, or behavior. However, this agreement did not hold for the case of employees' performance in assessing and thus reporting the detected anomaly (see Fig. 6.3.3D). Finally, Fig. 6.3.3E,F show the measures of the unfavorable impact that a low level of security training of employees has respectively on the detection and the assessment functions. Five of six experts agreed that the level of training is more important to the success of the assessment function rather than the detection function.

Although founded on a structured definition of physical security functions and barriers, the present dataset was extensively based on the use of expert judgment. Hence, it has all the limitations of expert judgment studies and may not be immune from biases. More specifically, the results are to be intended as descriptive of the European geopolitical context. However, the need of quantitative data is of utmost importance for supporting quantitative studies, as exemplified in Chapter 4, and the present approach is aimed at the selection of the best performance estimates based on the actual operative conditions.

6.3.3 (Add-on) safety barriers and their effect on security scenarios

6.3.3.1 Safety barriers classification

As introduced in Section 5.3, the concept of safety barrier is used within the process industry referring to measures to protect vulnerable assets (e.g., people, environment, reputation, etc.) against hazards posed by failures or deviations of systems (Rausand, 2011).

There is a considerable amount of scientific and technical literature dedicated to barriers and barrier management (Bucelli et al., 2018; Janssens et al., 2015; Landucci et al., 2016, 2015; Paltrinieri et al., 2017; Sklet et al., 2006; Vinnem et al., 2012). Safety barriers may be generically defined as physical and nonphysical means planned to prevent, mitigate, or control undesired events or accidents (Sklet, 2006). They constitute layers of protection between the hazard and the people, property, and surrounding environment to be protected (CCPS—Center of Chemical Process Safety, 2001a).

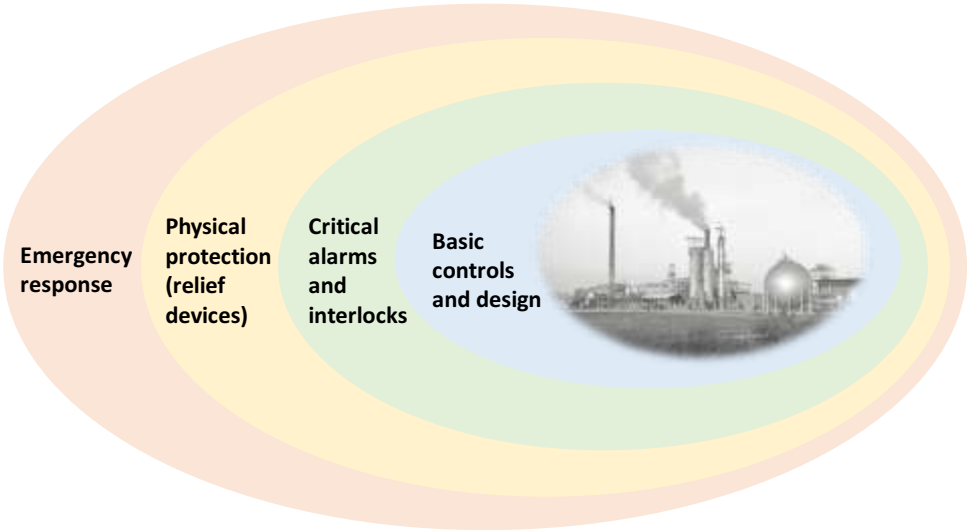


FIGURE 6.3.4 Example of a layer of protection system in chemical industry, as reported in CCPS – Center of Chemical Process Safety (2001a).

Fig. 6.3.4 illustrates the layers of protection concept (CCPS – Center of Chemical Process Safety, 2001a) and includes examples of some layers that might be found in a typical chemical plant. This approach can be highly effective, and its application has resulted in significant improvement in the safety record of the chemical industry.

However, the approach of imposing barriers between a hazard and potentially impacted people, property, and environment has significant disadvantages:

- The layers of protection are expensive to build and maintain throughout the life of the process. Factors include initial capital expense, operating costs, safety training cost, maintenance cost, and diversion of scarce and valuable technical resources into maintenance and operation of the layers of protection.
- The hazard remains, and some combination of failures of the layers of protection may result in an accident. Since no layer of protection can be perfect, there is always some risk that an incident will occur.

In the following, specific examples of add-on safety measures are reported and their integration in the design of security protection system are discussed.

6.3.3.2 Safety barriers as protection measures: the example of escalation triggered by fire

Technical and procedural measures, which constitute the safety layers needed to reduce the risk of accident propagation, are systematically applied in different chemical and process facilities where hazardous substances are stored, processed, and transported. Reniers and Faes (2013) report a list of the possible technological solutions that can be used for managing and/or preventing damages to process equipment induced by safety-related events and discuss procedural and managerial aspects related to risk reduction.

As introduced in Section 6.3.3.1, passive systems do not require external activation to perform the protective action. A typical example in the framework of equipment protection against external fires is the application of a heat-resistant insulation on process equipment in order to reduce the incoming heat flux due to fire and, consequently, the vessel heat-up (Bradley et al., 2017; Scarponi et al., 2018, 2017; 2016; Scarponi and Heymes, 2018). This allows to delay the time to reach the critical conditions leading to the failure of the exposed target (Birk, 1995; Birk et al., 2006). Another widely applied type of passive fire protection system consists of an emergency relief device, such as a pressure safety valve, aimed at avoiding the pressure buildup and consequent mechanical stress increment in equipment exposed to the fire (Lees, 1996; Moodie, 1988; Roberts et al., 2000; Van Den Bosh, 1989).

Active systems require external automatic and/or manual activation and hence, feature lower robustness than passive systems. Nevertheless, they may be effective and are often compulsory in technical standards (NFPA — National Fire Protection Association, 2009; NORSOK-standards, 2008; Roberts, 2004a,b). Active protections may be aimed at either preventing or mitigating potential accident chains triggered by fire. Emergency shutdown (ESD) and emergency blowdown (EBD) are usually adopted to prevent domino effect reducing the escalation potential of the primary scenarios (Lees, 1996). ESD systems act isolating the process units, thus reducing the severity of fires and vapor cloud explosions (VCEs), by limiting the inventory of released flammable materials. EBD systems depressurize the process units venting their content to the flare, thus reducing the potential loss and the pressure in the target equipment.

Active mitigation barriers may as well aim at protecting the target from the effects of the primary event. Typical examples are water deluge systems (WDS) and foam/water sprinklers (Finucane and Pinkney, 1988; Frank et al., 2013; Shirvill, 2004). WDS mitigate the fire exposure of the target, providing a water film on the exposed surfaces to absorb radiant heat and to lower the temperature of the metal shell, thus preventing loss of strength. They are typically installed on pressurized vessels (e.g., separators, horizontal storage units, pressure buffers, etc.) (Frank et al., 2013). Sprinkler systems instead may provide an effective control of the primary fire and may prevent fire spread in nearby units delivering fire-fighting agents such as water or foam. Sprinklers are typically installed on atmospheric storage vessels (Necci et al., 2014).

Since active mitigations typically have a significant time lag of intervention, mitigation actions aimed at protecting the target vessels are usually ineffective for primary scenarios as fireballs (which feature characteristic time ranges typically between 1 and 20 s (Birk, 1995; Lees, 1996; Van Den Bosh and Weterings, 2005)) and overpressure due to VCEs or mechanical explosions (that are phenomena lasting few tens to hundreds of milliseconds). These times are typically less than characteristic response times of any active protection equipment (Hølset et al., 1998).

Finally, procedural and emergency measures may support the management and control of fire scenarios having an escalation potential by their integration with passive

and/or active measures (Lees, 1996). Emergency response can be provided by internal and/or external emergency teams (Lees, 1996). These teams can be composed of expert fire fighters as well as of volunteers or workers who receive a specific training. For this type of barriers, the characteristic response time may be longer by one or two orders of magnitude compared to active measures. Therefore, no procedural measures are usually applicable to fast-evolving scenarios (fireball, mechanical explosions, VCE, etc.). However, emergency management of scenarios involving steady fires (e.g., pool or jet fires) can be crucial in preventing escalation and worsening of events associated with the damage of multiple equipment.

6.4 Conclusions: some reflections on the currently applied protection strategies

As discussed in Section 5.1.4, the fundamental basis of security management can be expressed in a similar manner to the Layers of Protection used in modern chemical process plants for addressing safety-related, accidental events. In the similar security-related concept of rings-of-protections (American Institute of Chemical Engineers — Center for Chemical Process Safety (AIChE-CCPS), 2003), the spatial relationship between the location of the target asset and the location of the physical countermeasures is used as a guiding principle, as discussed in Section 5.1.4. Moreover, the safety barriers discussed in Section 6.3.3, despite designed to cope with unintentional events in order to protect process equipment, may serve as a valiant defense resource to stop potential cascading events triggered by external acts of interference.

Reniers et al. (2008) reflected on this strategy in which safety and security elements are integrated in order to prevent cascading events in clusters of chemical and process facilities. When eliminating terrorist groups and intentional attacks seems impossible, minimizing the potential consequences of intentional attacks can be considered as an effective approach to protect industrial plants against terrorist attacks (Reniers and Audenaert, 2014).

However, minimizing the potential consequences is challenging, not only due to the interactions among different installations, but also because the evolution of complex chain of events, such as domino effect, is a dynamic process. Therefore, it is important to design rings-of-protection in a way that also takes domino effect scenarios into account, accounting for their complex and dynamic features, such as synergistic effects (Khakzad et al., 2017, 2013). More generally, the security management at single site and/or at cluster level by means of the ring-of-protection concept should adopt a number of measures, combining physical security equipment, people, and procedures but, at the same time, verify if the installed “safety” provisions may be able to cope with potential cascading events triggered by external attacks. This may be seen as a key strategy in order to offer the best chance of adequate asset protection against a variety of threats.

References

Aghassi, M., Bertsimas, D., 2006. Robust game theory. Math. Program. 107 (1–2), 231–273.

American Institute of Chemical Engineers–Center for Chemical Process Safety (AIChE-CCPS), 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. AIChE-CCPS, New York.

Amundrud, Ø., Aven, T., Flage, R., 2017. How the definition of security risk can be made compatible with safety definitions. Proc. Inst. Mech. Eng. O J. Risk Reliab. 231, 286–294.

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.

Australian Signals Directorate, 2012. Network Segmentation and Segregation. Information security advice for all levels of government, Department of Defence, Australian Government.

Basta, C., Neuvel, J., Zlatanova, S., Ale, B., 2007. Risk-maps informing land-use planning processes A survey on The Netherlands and the United Kingdom recent developments. J. Hazard. Mater. 145, 241–249.

Bernechea, E., Arnaldos, J., 2014. Optimizing the design of storage facilities through the application of ISD and QRA. Process Saf. Environ. Prot. 92, 598–615.

Birk, A., 1995. Scale effects with fire exposure of pressure-liquified gas tanks. Loss Prev. Process Ind. 8, 275–290.

Birk, A.M., Poirier, D., Davison, C., 2006. On the thermal rupture of 1.9 m^3 propane pressure vessels with defects in their thermal protection system. J. Loss Prev. Process. Ind. 19, 582–597.

Boyes, H., 2013. Trustworthy Cyber-Physical Systems-A Review.

Bradley, I., Scarponi, G.E., Otremba, F., Cozzani, V., Birk, A.M., 2017. Experimental analysis of a pressurized vessel exposed to fires: an innovative representative scale apparatus. Chem. Eng. Trans. 57, 265–270. https://doi.org/10.3303/CET1757045.

Bucelli, M., Landucci, G., Haugen, S., Paltrinieri, N., Cozzani, V., 2018. Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment. Ocean. Eng. 158, 171–185.

Byres, E., Lowe, J., 2004. The myths and facts behind cyber security risks for industrial control systems. In: Paper Presented at the Proceedings of the VDE Kongress.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., Sastry, S., 2009. Challenges for securing cyber physical systems. In: Paper Presented at the Workshop on Future Directions in Cyber-Physical Systems Security.

Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Prot. 116, 621–631.

CCPS–Center of Chemical Process Safety, 2001a. Layer of Protection Analysis: Simplified Process Risk Assessment. American Institute of Chemical Engineers–Center of Chemical Process Safety, New York, NY.

CCPS–Center of Chemical Process Safety, 2001b. Guidelines for Engineering Design for Process Safety. American Institute of Chemical Engineers–Center of Chemical Process Safety, New York, NY.

Christou, M., Amendola, A., Smeder, M., 1999. The control of major accident hazards: the land-use planning issue. J. Hazard. Mater. 65, 151–178.

Christou, M., Gyenes, Z., Struckl, M., 2011. Risk assessment in support to land-use planning in Europe: towards more consistent decisions? J. Loss Prev. Process. Ind. 24, 219–226.

Christou, M.D., Struckl, M., Iermann, T., 2006. Land Use Planning Guidelines in the Context of Article 12 of the Seveso II Directive 96/82/EC. Institute for the Protection and Security of the Citizen. European Commission, Ispra, Italy. Available online at: http://ec.europa.eu/environment/seveso/pdf./landuseplanning_guidance_en.pdf.

Cox, L.A., 2009. Game theory and risk analysis. Risk Anal. Int. J. 29 (8), 1062–1068.

Cozzani, V., Antonioni, G., Landucci, G., Tugnoli, A., Bonvicini, S., Spadoni, G., 2014. Quantitative assessment of domino and NaTech scenarios in complex industrial areas. J. Loss Prev. Process. Ind. 28, 10–22.

Cozzani, V., Tugnoli, A., Slazano, E., 2009. The development of an inherent safety approach to the prevention of domino effects. Accid. Anal. Prev. 41, 1216–1227.

Cozzani, V., Bandini, R., Basta, C., Christou, M., 2006a. Application of land-use planning criteria for the control of major accident hazards: a case-study. J. Hazard. Mater. A136, 170–180.

Cozzani, V., Gubinelli, G., Salzano, E., 2006b. Escalation thresholds in the assessment of domino accidental events. J. Hazard. Mater. 129 (1), 1–21.

Crucitti, P., Latora, V., Marchiori, M., Rapisarda, A., 2004. Error and attack tolerance of complex networks. Phys. A Stat. Mech. Appl. 340 (1), 388–394.

Csardi, G., Nepusz, T., 2006. The igraph software package for complex network research. Int. J. Complex Syst. 1695 (5), 1–9.

Demichela, M., Pilone, E., Camuncoli, G., 2014. Land use planning around major risk installations: from EC directives to local regulations in Italy. Land Use Policy 38, 657–665.

Finucane, M., Pinkney, D., 1988. Reliability of Fire Protection and Detection Systems, SRD R431. United Kingdom Atomic Energy Authority. University of Edinburgh, Edinburgh (UK).

Flammable Liquids Bulk Storage Regulations, 2014. Published by the Minister of Justice of Canada. Available online at: http://laws-lois.justice.gc.ca.

Frank, K., Gravestock, N., Spearpoint, M., Fleischmann, C., 2013. A review of sprinkler system effectiveness studies. Fire Sci. Rev. 2 (6), 1–19.

Franks, A., 2004. A Review of HSE's Risk Analysis and Protection-Based Analysis Approaches for Land-Use Planning. Available online at: http://www.hse.gov.uk/landuseplanning/hseriskanalysis.pdf.

Garcia, M., 2006. Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann, Newtown, MA.

Garcia, M., 2008. The Design and Evaluation of Physical Protection Systems, second ed. Butterworth–Heinemann, Burlington, MA, USA.

Hauptmanns, U., 2005. A risk-based approach to land-use planning. J. Hazard. Mater. A125, 1–9.

Hayden, E., Assante, M., Conway, T., 2014. An abbreviated history of automation & industrial controls systems and cybersecurity. Available online at: https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf.

Hølset, S., Hjertager, B.H., Solberg, T., Malo, K.A., 1998. Properties of simulated gas explosions of interest to the structural design process. Process Saf. Prog. 17, 278–287.

HSE, 1989. Risk Criteria for Land-Use Planning in the Vicinity of Major Industrial Hazards. HSE Books, 1989. ISBN 9780118854917.

HSE, 2014. HSE's Current Approach to Land Use Planning (LUP). Available online at: http://www.hse.gov.uk/landuseplanning/lupcurrent.pdf.

ICS-CERT, & NCCIC, 2016. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-In-Depth Strategies. Retrieved from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

Janssens, J., Talarico, L., Reniers, G., Sörensen, K., 2015. A decision model to allocate protective safety barriers and mitigate domino effects. Reliab. Eng. Syst. Saf. 143, 44–52.

Khakzad, N., Khan, F., Amyotte, P., Cozzani, V., 2013. Domino effect analysis using Bayesian networks. Risk Anal. 33 (2), 292–306.

Khakzad, N., Reniers, G., 2017. Cost-effective allocation of safety measures in chemical plants w.r.t land-use planning. Saf. Sci. 97, 2–9.

Khakzad, N., Reniers, G., 2015a. Risk-based design of process plants with regard to domino effects and land use planning. Hazard. Mater. 299, 289–297.

Khakzad, N., Reniers, G., 2015b. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. Reliab. Eng. Syst. Saf. 143, 63–73.

Khakzad, N., Reniers, G., 2019. Low-capacity Utilization of Process Plants: A Cost-Robust Approach to Tackle Man-Made Domino Effects, 191. Reliability Engineering & System Safety, p. 106114. https://www.sciencedirect.com/science/article/abs/pii/S0951832017309158.

Khakzad, N., Landucci, G., Reniers, G., 2017. Application of dynamic Bayesian network to performance assessment of fire protection systems during domino effects. Reliab. Eng. Syst. Saf. 167, 232–247.

Knapp, E.D., Langill, J.T., 2014. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems: Syngress.

Kontic, D., Kontic, B., 2009. Introduction of threat analysis into the land-use planning process. J. Hazard. Mater. 163, 683–700.

Laheij, G., Post, J.G., Ale, B., 2000. Standard methods for land-use planning to determine the effects on societal risk. J. Hazard. Mater. 71, 269–282.

Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Quantitative performance assessment of physical security barriers for chemical facilities. In: Safety and Reliability–Theory and Applications–Proceedings of the 27th European Safety and Reliability Conference, ESREL 2017. CRC Press/Balkema, Boca Raton, FL, pp. 1279–1288.

Landucci, G., Argenti, F., Spadoni, G., Cozzani, V., 2016. Domino effect frequency assessment: the role of safety barriers. J. Loss Prev. Process. Ind. 44, 706–717.

Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab. Eng. Syst. Saf. 143, 30–43.

Lee, R.M., Assante, M.J., Conway, T., 2014. German steel mill cyberattack. Ind. Contr. Syst. 30.

Lees, F.P., 1996. Loss Prevention in the Process Industries, second ed. Butterworth–Heinemann, Oxford.

Matches., 2014. Retrieved from: http://matche.com/equipcost/Tank.html.

McMillan, R., January 19 , 2018. New type of cyberattack targets factory safety systems. Wall Str. J. Retrieved from: https://www.wsj.com/articles/hack-at-saudi-petrochemical-plant-compromised-a-safety-shut-off-system-1516301692.

Moodie, K., 1988. Experiments and modelling:- an overview with particular reference to fire engulfment. J. Hazard Mater. 20, 149–175.

Necci, A., Argenti, F., Landucci, G., Cozzani, V., 2014. Accident scenarios triggered by lightning strike on atmospheric storage tanks. Reliab. Eng. Syst. Saf. 127, 30–46.

NFPA-National Fire Protection Association, 2009. NFPA 15–Standard for Water Spray Fixed Systems for Fire Protection. NFPA, Quincy (MA).

Nicholas, P., 2017. Mind the Air Gap: Network Separation's Cost, Productivity and Security Drawbacks. Retrieved from: https://www.microsoft.com/en-us/cybersecurity/blog-hub/mind-the-air-gap-network-separation.

Nolan, D.P., 2008. Safety and Security Review for the Process Industries. Elsevier Inc., Amsterdam, The Netherlands.

Norman, T.L., 2010. Risk Analysis and Security Countermeasure Selection. CRC Press, Boca Raton, FL.

NORSOK-standards, 2008. Standard S-001–Technical Safety, fourth ed. NORSOK, Lysaker, NO.

Nunes-Vaz, R., Lord, S., 2014. Designing physical security for complex infrastructures. Int. J. Crit. Infrastruct. Prot. 7, 178–192.

Nunes-Vaz, R., Lord, S., Ciuk, J., 2011. A more rigorous framework for security-in-depth. J. Appl. Secur. Res. 6, 372–393.

PADHI, 2011. HSE's Land Use Planning Methodology. Available online at: http://www.hse.gov.uk/landuseplanning/padhi.pdf.

Paltrinieri, N., Grøtan, T.O., Bucelli, M., Landucci, G., 2017. A case of dynamic risk management in the subarctic region. In: Walls, L., Revie, M., B.T. (Eds.), Risk, Reliability and Safety: Innovating Theory and Practice–Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016. CRC Press/Balkema, p. 127.

Papazoglou, I., Bonanos, G., Nivolianitou, Z., Jan Duijm, N., Rasmussen, B., 2000. Supporting decision makers in land use planning around chemical sites. Case study: expansion of an oil refinery. J. Hazard. Mater. 71, 343–373.

Papazoglou, I., Nivolianitou, Z., Bonanos, G., 1998. Land use planning policies stemming from the implementation of the SEVESO-II Directive in the EU. J. Hazard. Mater. 61, 345–353.

Pasman, H., Reniers, G., 2014. Past, present and future of quantitative risk assessment (QRA) and the incentive it obtained from land-use planning (LUP). J. Loss Prev. Process. Ind. 28, 2–9.

Rausand, M., 2011. Risk Assessment. Theory, Methods and Applications. Wiley.

Reason, J., 2000. Human error: models and management. BMJ 320, 768–770.

Reniers, G., Faes, R., 2013. 13–managing domino effects in a chemical industrial area. In: Cozzani, G.R. (Ed.), Domino Effects in the Process Industries. Elsevier, Amsterdam, pp. 272–295.

Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures w.r.t. domino effects. Process Saf. Environ. Prot. 92, 583–589.

Reniers, G.L.L., Dullaert, W., Audenaert, A., Ale, B.J.M., Soudan, K., 2008. Managing domino effect-related security of industrial areas. J. Loss Prev. Process. Ind. 21, 336–343.

Rew, P., Daycock, L., 2004. Development of a Method for the Determination of On-Site Ignition Probabilities, HSE Contractor Report WSA/226. HSE Books, London, UK.

Roberts, A., Medonos, S., Shirvill, L.C., 2000. Review of the Response of Pressurised Process Vessels and Equipment to Fire Attack OFFSHORE TECHNOLOGY REPORT–OTO 2000 051. Health and Safety Laboratory, Fire and Explosion Group, Buxton UK.

Roberts, T.A., 2004a. Directed deluge system designs and determination of the effectiveness of the currently recommended minimum deluge rate for the protection of LPG tanks. J. Loss Prev. Process. Ind. 17, 103–109.

Roberts, T.A., 2004b. Effectiveness of an enhanced deluge system to protect LPG tanks and sensitivity to blocked nozzles and delayed deluge initiation. J. Loss Prev. Process. Ind. 17, 151–158.

Saaty, T., 2008. Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World. RWS Publications, Pittsburgh, Pennsylvania. ISBN 0-9620317-8-X.

Sanger, D.E., 2012. Obama Order Sped up Wave of Cyberattacks against Iran. The New York Times, 2012.

Scarponi, G.E., Heymes, F., 2018. CFD study of the behavior of LPG tanks exposed to forest fires. Chem. Eng. Trans. 67, 181–186. https://doi.org/10.3303/CET1867031.

Scarponi, G.E., Landucci, G., Birk, A.M., Cozzani, V., 2018. LPG vessels exposed to fire: scale effects on pressure build-up. J. Loss Prev. Process. Ind. 56, 342–358. https://doi.org/10.1016/j.jlp.2018.09.015.

Scarponi, G.E., Landucci, G., Ovidi, F., Cozzani, V., 2016. Lumped model for the assessment of the thermal and mechanical response of LNG tanks exposed to fire. Chem. Eng. Trans. https://doi.org/10.3303/CET1653052.

Scarponi, G.E., Landucci, G., Tugnoli, A., Cozzani, V., Birk, A.M., 2017. Performance assessment of thermal protection coatings of hazardous material tankers in the presence of defects. Process Saf. Environ. Prot. 105. https://doi.org/10.1016/j.psep.2016.10.009.

Schmidt, M.S., Perlroth, N., 2013. Obama Order Gives Firms Cyberthreat Information. Retrieved from: http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html.

Sebosa, I., Progiou, A., Symeonidis, P., Ziomas, I., 2010. Land-use planning in the vicinity of major accident hazard installations in Greece. J. Hazard. Mater. 179, 901–910.

Security Roundtable, 2018. 'Tried and True' Network Segmentation Can Come to the Rescue. Retrieved from: https://www.securityroundtable.org/tried-true-network-segmentation-can-come-rescue/.

Shirvill, L.C., 2004. Efficacy of water spray protection against propane and butane jet fires impinging on LPG storage tanks. J. Loss Prev. Process. Ind. 17, 111–118.

Siemens, 2008. Security Concept PCS 7 and WinCC–Basic Document (Whitepaper). Retrieved from: https://cache.industry.siemens.com/dl/files/131/26462131/att_80283/v1/wp_sec_b.pdf.

Sklet, S., 2006. Safety barriers: definition, classification, and performance. J. Loss Prev. Process. Ind. 19, 494–506.

Sklet, S., Vinnem, J.E., Aven, T., 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part II: results from a case study. J. Hazard. Mater. 137, 692–708.

Srivastava, A., Gupta, J., 2010. New methodologies for security risk assessment of oil and gas industry. Process Saf. Environ. Prot. 88 (6), 407–412.

Stouffer, K., Falco, J., Scarfone, K., 2011. Guide to industrial control systems (ICS) security. NIST Special Public. 800 (82), 16–16.

Talbot, J., Jakeman, M., 2009. Security Risk Management Body of Knowledge. Wiley, Hoboken, NJ.

Taveau, J., 2010. Risk assessment and land-use planning regulations in France following the AZF disaster. J. Loss Prev. Process. Ind. 23, 813–823.

Van Den Bosh, C.J.H., 1989. Green Book, Methods for the Determination of Possible Damage. CPR 16E. Committee for the Prevention of Disasters, the Hague (NL).

Van Den Bosh, C.J.H., Weterings, R.A.P.M., 2005. Methods for the Calculation of Physical Effects (Yellow Book), third. ed. Committee for the Prevention of Disasters, the Hague (NL).

Vinnem, J.E., Bye, R., Gran, B.a., Kongsvik, T., Nyheim, O.M., Okstad, E.H., Seljelid, J., Vatn, J., 2012. Risk modelling of maintenance work on major process equipment on offshore petroleum installations. J. Loss Prev. Process. Ind. 25, 274–292. https://doi.org/10.1016/j.jlp.2011.11.001.

Wagner, N., Sahin, C.S., Pena, J., Streilein, W.W., 2017. A nature-inspired decision system for secure cyber network architecture. In: Paper Presented at the Computational Intelligence (SSCI), 2017 IEEE Symposium Series on.

Wang, J., Jiang, C., Qian, J., 2014. Robustness of Internet under targeted attack: a cascading failure perspective. J. Netw. Comput. Appl. 40, 97–104.

Yellow Book, Van Den Bosh, C.J.H., Weterings, R.A.M.P., 1997. Methods for the Calculation of Physical Effects. Committee for the Prevention of Disasters, The Hague, NL.

Zhao, L., Park, K., Lai, Y.-C., 2004. Attack vulnerability of scale-free networks due to cascading breakdown. Phys. Rev. 70 (3), 035101.

7 Economic aspects of security decisions

7.1 Introduction to basic economic parameters

In general, the most evident and most employed economic approach for decision-making is based on costs and benefits of certain options that the decision-maker needs to choose from. Reniers and Van Erp (2016) indicate that if a company uses a cost–benefit analysis, the recommendation whether to accept or to reject an investment project is based upon the following processes:

(1) Identification of costs and benefits
(2) Calculation of the present values of all costs and benefits
(3) Comparison of the total present value of costs and total present value of benefits

In order to compare the total costs and the total benefits, composed out of costs and benefits occurring at different points in time, one needs to take a discount rate into account in the calculation to obtain the present values. Thus, during a cost–benefit analysis, all cash flows, from both costs and benefits in the future, need to be converted to values in the present. This conversion is carried out by discounting the cash flows by a discount rate. The discount rate represents the rate at which people (or companies) are willing to give up consumption in the present in exchange for additional consumption in the future. Another definition is that in a multiperiod model, people value future experiences to a lesser degree than present ones, as they are sure about present events and not sure about future events, which are subject to the environment. Thus, the higher the discount rate they choose, the lower the present values of the future cash flows (Campbell and Brown, 2003).

An investment project is recommended when the total Net Present Value (NPV) of all cash flows is positive, and an investment project is usually rejected when the NPV is negative. To calculate the NPV related to project management, all cash flows are determined, and future cash flows are recalculated to today's value of money by discounting them by the discount rate. The formula usually mentioned to calculate the NPV is:

$$\mathrm{NPV} = \sum_{t=0}^{T} \frac{X_t}{(1+r)^t}\,, \tag{7.1.1}$$

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00007-X

where X_t represents the cash flow in year t, T is the time period considered (usually expressed in years), and r is the discount rate.

Applied to operational safety, the NPV of a project expresses the difference between the total discounted present value of the benefits and the total discounted present value of the costs (see Fig. 7.1.1). A positive NPV for a given safety investment indicates that the project benefits are larger than its costs. On the contrary, a negative value of NPV indicates that the costs of the project are larger than its benefits and the safety investment is recommended to be rejected (see Fig. 7.1.1).

It is evident that the cash flows, that is, prevention costs and especially expected hypothetical benefits (due to non events), may be uncertain. Different approaches can be used in this regard. The cash flows can, for example, be expressed as expected values, taking the uncertainties in the form of probabilities into consideration and also increasing the discount rate to outweigh the possibilities for unfavorable outcomes. In case of type II security risks (that is, terrorist attacks, see Chapter 5), it is recommended to use scenario analyses, determining cash flows for different scenario cases (e.g., worst-case and most-credible case) and using a security Disproportion Factor (DF — see later in this section).

There can be different categories of costs related to a security countermeasure (OPER) investments, e.g., initial costs, installation costs, operating costs, maintenance costs, inspection costs, etc. These costs are evidently represented by negative cash flows. Some costs (e.g., initial costs and installation costs of countermeasures) occur in the present and thus do not have to be discounted, while other costs (e.g., operating, maintenance, and inspection costs of countermeasures) occur throughout the whole remaining lifetime of the facility and thus will have to be discounted to the present. There may also be different categories of benefits linked to a security investment, such as supply chain benefits, damage benefits, legal benefits, insurance benefits, human and environmental benefits, intervention benefits, reputation benefits, and other benefits. The benefits represent positive cash flows, which all occur throughout the entire remaining lifetime of the facility and thus will all have to be discounted to the present.

In order to clarify the discount rate principle, all cash flows (for both costs and benefits) are assumed to occur on an arbitrarily chosen date, which can, for example, be chosen to be the last day of the calendar year in which they occur. This assumption converts the continuous cash flows to a discrete range of cash flows, occurring at the end of each year. Then the cash flows at the end of each year have to be discounted to a

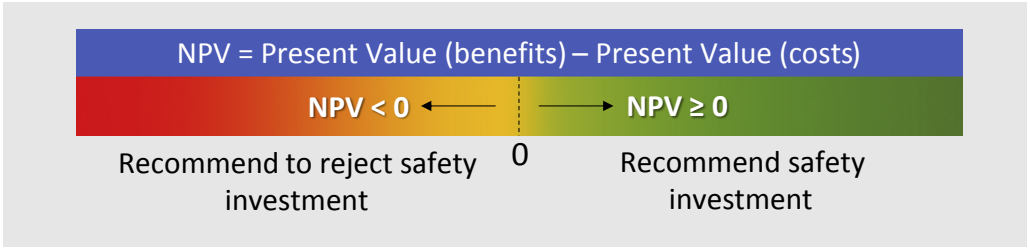


FIGURE 7.1.1 Definition of net present value and evaluation of operative safety investments.

present value, using a discount factor. As stated before, cash flows occurring in the current year do not have to be discounted. Therefore, the current year is called "year 0," and the following years "year 1," "year 2," …, "year *n*." Costs and benefits occurring in year 1 are discounted back one period, those occurring in year 2 are discounted back two periods, those occurring in year n are discounted back n periods. The implicit assumption is made that the discount rate remains the same throughout the entire remaining lifetime of the facility (Campbell and Brown, 2003).

Thus, for calculating the present value of a benefit occurring in year 1, it needs to be discounted for one period to come to a present value in year 0. Similar to the calculation of a benefit occurring in year 1, the present values of benefits occurring in year 2 and year 3 are obtained by discounting them respectively 2 and 3 periods. Similar to the previous calculations, the present value (*PV*) of a benefit occurring in year n is obtained by discounting it n periods. These calculations can be found in the following range:

$$\begin{aligned} \text{PV of a benefit in year 1} &= \frac{\text{Benefit}}{(1+r)} \\ \text{PV of a benefit in year 2} &= \frac{\text{Benefit}}{(1+r)^2} \\ &\vdots \\ \text{PV of a benefit in year } n &= \frac{\text{Benefit}}{(1+r)^n} \end{aligned} \tag{7.1.2}$$

Now that the concept and method of discounting future cash flows are clarified, suppose a safety investment project has a cost in year 0 and then the same level of costs and benefits at the end of each and every subsequent year for the whole remaining lifetime of the facility. Thus this means that the costs in year i are the same for all i, i.e., $C_i = C$, likewise, the benefits in year i are the same for all i, i.e., $B_i = B$. This concept is called an "annuity." The PV of such an annuity is given by the following formula, with n the remaining lifetime of the facility:

$$\text{PV(Annuity of a cost)} = C + \frac{C}{(1+r)} + \frac{C}{(1+r)^2} + \cdots + \frac{C}{(1+r)^n} \tag{7.1.3a}$$

$$\text{PV(Annuity of a benefit)} = B + \frac{B}{(1+r)} + \frac{B}{(1+r)^2} + \cdots + \frac{B}{(1+r)^n} \tag{7.1.3b}$$

C and B are the equal annual costs (cost categories where costs are made in the future) and benefits (all benefits categories) respectively that occur at the end of each year and are assumed to remain constant. This assumption is valid as long as inflation is omitted from the calculations and as long as the annual costs are assumed not to increase over time due to aging. These assumptions can be made to keep it rather simple while explaining the cost–benefit approach. Each term in the aforementioned formula is formed by multiplying the previous term by "$1/(1+r)$." As the aforementioned formulas

can become very long, the formula for calculating the PV of annuities can be rewritten, by way of the series solution:

$$1+\frac{1}{(1+r)}+\frac{1}{(1+r)^2}+\cdots+\frac{1}{(1+r)^n}=1+\frac{1}{r}-\frac{1}{r(1+r)^n} \tag{7.1.4}$$

as follows:

$$\mathrm{PV(Annuity)}=A+\frac{A}{r}-\frac{A}{r(1+r)^n} \tag{7.1.5}$$

where A is the yearly cost or benefit of a cost/benefit category. Note that this general annuity goes to "$(n+1)\times A$" as the discount ratio r goes to zero. The term $\frac{1}{r}-\frac{1}{r(1+r)^n}=\frac{(1+r)^n-1}{r(1+r)^n}$ of the series solution is called "the annuity (discount) factor" and is applicable whenever the annuity starts from year 1 (Campbell and Brown, 2003).

Using this model, the benefits and costs in the future are assumed to be constant, and inflation is not included into the future costs and benefits, as already mentioned. Inflation is the process that results in a rise of the nominal prices of goods and services over time. Therefore, in this (simplified) model, the real rate of interest[1] should be used as the discount rate instead of the money rate of interest.[2] Since the money rate of interest m includes two components, the real rate of interest r, and the anticipated rate of inflation i:

$$m=r+i \tag{7.1.6}$$

the anticipated rate of inflation is built into the money rate of interest. Inflation not being included into the numerator of the formula for calculating the PV of annuities (as the costs and benefits are constant throughout the entire remaining lifetime), it can also not be included into the denominator.

7.2 Different cost–benefit ratios

Several approaches are possible for presenting the cost–benefit principle, and different cost–benefit ratios can be calculated. Remark that sometimes benefits are divided by costs, then a benefit–cost ratio is obtained, and sometimes costs are divided by benefits, and a cost–benefit ratio is obtained. In case of a benefit–cost ratio, the ratio should ideally be higher than 1, and as high as possible, while in case of a cost–benefit ratio, it should ideally be lower than 1, and as low as possible. The following ratios are mentioned by Fuller and Vassie (2004):

- Value of an averted loss:

$$\text{Benefit}-\text{cost ratio}=\text{value of averted losses}(=\text{hypothetical benefits})/\text{Security measures' costs over their lifetime}$$

[1]Real rate of interest (r): does not include the anticipated rate of inflation (i).

[2]Money rate of interest (m): includes two components, the f real rate of interest (r) and the anticipated rate of inflation (i): $m=r+i$.

- Value of equivalent life:

$$\text{Benefit} - \text{cost ratio} = \text{value of equivalent lives saved over the lifetime of the security measures} / \text{Security measures' costs over their lifetime}$$

- Value of risk reduction:

$$\text{Benefit} - \text{cost ratio} = [(\text{liability of the original security risk}) - (\text{liability of the residual security risk})] / \text{Security measures' costs over their lifetime}$$

7.3 Calculating security countermeasure costs

The purpose of implementing security countermeasures is to reduce present and future security risks. By "reducing the security risk," the prevention of threats and attacks is indicated, as well as the mitigation of consequences if an attack would occur after all. Security measures can be costly. The different types of security measures were discussed in Chapters 5 and 6 and were summarized under the OPER acronym.

As already mentioned, four types of security countermeasures are available, summarized in the OPER acronym (see Chapter 5). In order to be able to implement new security measures and upgrade existing security countermeasures, a company has to reserve substantial funding. In this section, the various costs related to new security countermeasures that a company may decide to implement are discussed. The following list provides a clear overview of the different kinds of costs of countermeasures (see also Reniers and Van Erp, 2016 for a more extensive discussion of the different categories):

A. Initiation of security measure
B. Installation of security measure
C. Operation of security measure
D. Maintenance of security measure
E. Inspection of security measure
F. Security of logistics and transportation activities
G. Contractor security
H. Other security costs

For each of the aforementioned costs, formulas were elaborated to calculate every subcategory of costs.

7.3.1 Initiation of security measure

Under the initiation costs of security measures, five different kinds of security costs can be grouped:

i. Investigation costs
ii. Selection and design costs
iii. Material costs
iv. Training costs
v. Changing guidelines and informing costs

These various costs will not have to be discounted to PVs, as they will occur in the present. [Hence in the basic year (=year 0)]. Each of the different types of costs is explained more in depth hereafter.

7.3.1.1 Investigation costs

The investigation, carried out by the so-called "investigation team" studying the potential of a security countermeasure project, brings along costs related to the investigation and audit activities, internally or externally, or both. The purpose of this effort is to check whether additional security measures or upgrades to the existing security system are possible and necessary. The costs can be estimated or/and calculated through multiplying the hourly wage of an employee by the number of hours the investigation/audit takes and again by the number of employees participating in this investigation or audit. If, however, employees with significantly varying wage levels participate, the investigation team costs can be calculated separately for each category of employees. Another possibility is to take the average wage level of all employees participating, in order to simplify the work and only have to work with one category.

7.3.1.2 Selection and design costs

If the investigation or audit points out that upgrades in the security system are possible or necessary, a prevention and/or mitigation measure will have to be selected and designed. Such a measure is of course accompanied by costs, which can be calculated by multiplying the hourly wage of all employees involved by the number of hours they work on the design and then again multiplied by the number of employees participating. They can also be calculated separately for categories of employees with varying wage levels.

7.3.1.3 Material costs

The actual countermeasure, and the components out of which it is made, also sometimes require budget (e.g., a wall that needs to be built, a reinforced door, or a special fence). On the one hand, the material costs and costs related to the creation of the security measure can be calculated by multiplying the price per unit of the necessary materials by the units the company requires to create the security measure.

7.3.1.4 Training costs

In order to calculate these security costs, the assumption is made that the company provides training to its employees working in the facility related to the new security measure, if this is needed. It is assumed that some employees or external consultants or coaches will be given the task to disseminate the necessary information and to explain how to work with the security measure (as already mentioned, if applicable). The costs occurring because of this assignment to some employees or external consultants or coaches can be calculated and estimated through multiplying the hourly wage of an employee by the number of hours this process takes and again by the number of employees participating in this assignment. If, however, employees with significantly varying wage levels participate, the training costs can also be calculated separately for each category of employees. Another possibility is estimating the costs by taking the average wage level of all employees participating, in order to only have to work with one category.

7.3.1.5 Changing guidelines and informing costs

In case of organizational countermeasures ("O" from OPER), some specific guidelines and informing costs can be mentioned. In order to calculate the costs resulting from the needed changes to guidelines and from the necessary disseminating activities, the assumption is made that in addition to training, the company informs the personnel of the new countermeasure through some kind of brochure, newsletter, or guide. This brochure will also contain the changed guidelines and security instructions. These costs can be calculated by multiplying the price per unit of brochures/guides by the number of them needed. One unit can in this case represent 1 brochure or 1 pack of brochures that may contain, for example, 100 brochures. This will depend on which price is used, the price per brochure or per batch of brochures (/procedures).

7.3.2 Installation of security measure

The installation costs are made up of several subcosts:

i. Production loss costs
ii. Start-up costs
iii. Equipment costs
iv. Installation team costs

Similar to the initiation security costs, the installation security costs will not have to be discounted to PVs, as they will occur only in the present. (Hence in the basic year (=year 0)). Each of the different types of costs is explained more in depth hereafter.

7.3.2.1 Production loss costs

When a countermeasure is implemented, in some cases the production has to be stopped temporarily, resulting in a production loss. This production loss is accompanied

by costs because of the nonproducing status of the facility or installation. Production loss security costs can be calculated by the multiplication of the production capacity/rate of the facility by the duration of the stop and again by the profit per unit sold (Gavious et al., 2009).

7.3.2.2 Start-up costs

The implementation of a new security measure can cause a temporary slowdown in production due to the needed restart of the facility (because of the required production stop due to security measure implementation). The costs related to the temporary slowdown in production due to security-related reasons are called start-up security costs and can be calculated by multiplying the difference in production rate before and after the halt in production, by the duration from the time the production line is reactivated after the implementation of the new measure to the time when the production line goes back to the initial production rate, and again by the profit per unit sold (Gavious et al., 2009).

7.3.2.3 Equipment safety costs

The installation of a new countermeasure usually requires equipment (to be bought or to be rented). Equipment indicates all kinds of working tools, but also, for example, machinery and modes of transportation. These equipment costs can be calculated by multiplying the price per unit of the equipment by the number of units needed to install the countermeasure.

7.3.2.4 Installation team costs

The installation team costs are related to the employees taking care of actually installing the new security measure in the facility. These can be calculated and estimated through multiplying the hourly wages of participating employees by the number of hours the installation takes and again by the number of employees participating in this installation. If, however, employees with significantly varying wage levels participate, the installing team costs can be calculated separately for each category of employees. Another possibility is to take the average wage level of all employees participating, in order to only have to work with one category.

7.3.3 Operation security costs

Utility countermeasure costs will have to be discounted to PVs, as they will not only occur in the present (that is, in the basic year (=year 0)), but throughout the entire remaining lifespan of the facility. Active security systems (especially measures of the Electronic and Reporting type, cfr. OPER), for example, need energy sources and other utilities external or internal to the system, to perform their function. Without these utilities, the active safety system will not be able to function. Examples of external energy sources include electric power, hydraulic power, manpower, system pressure. In a

cost–benefit analysis, one may choose to calculate the yearly utility security costs by multiplying the price per unit of a utility by the units needed per year.

The assumption is made that the utility security costs represent the same level of costs at the end of each year for a specific time interval. As mentioned earlier, the cost stream C_1, C_2, …, C_n with n the remaining lifespan of the facility in years, where $C_i = C$ for all i, is termed an annuity. The total PV is not just the sum of the utilities' costs of each year such as it was calculated in the previous cost sections, because the utilities' costs occur throughout the whole remaining lifetime of the facility and thus have to be calculated taking into account a discount factor.

7.3.4 Maintenance security costs

i. Material costs
ii. Maintenance team costs
iii. Production loss costs
iv. Start-up costs

These countermeasure costs will have to be discounted to PVs, as they will not only occur in the present (in the basic year (=year 0)), but throughout the entire remaining lifespan of the facility. Each of the different types of countermeasure costs is explained more in depth hereafter.

7.3.4.1 Material costs

Maintenance of security measures requires replacements for decrepit materials. It should be noted that besides the material itself composing a countermeasure, "materials" should be seen as security devices, -infrastructure, -equipment, etc. The material costs of the replacement materials can be calculated by multiplying the price per unit of the materials by the units needed for the maintenance of the security measure per year.

These costs represent the maintenance material costs of one maintenance period, which can be defined as 1 year. Thus if it is assumed that maintenance occurs on a yearly basis and the yearly cost is always the same, the total PV of all maintenance materials needed during the lifetime of the countermeasure can be calculated by taking into account a discount factor, because the maintenance material costs occur throughout the whole remaining lifetime of the facility.

7.3.4.2 Maintenance team costs

The maintenance team costs are related to the maintenance activities of employees for the installed countermeasure(s). These can be calculated and estimated through multiplying the hourly wage of such an employee by the number of hours the maintenance takes and again by the number of employees participating. If, however, employees with significantly varying wage levels participate, the maintenance team costs can be

calculated separately for each category of employees. Another possibility is to take the average wage level of all employees participating, in order to only have to work with one category.

These costs represent the maintenance team costs for one maintenance period, which is defined as 1 year. Thus if we assume that maintenance occurs on a yearly basis and the yearly cost is always the same, the total PV of all maintenance teams needed during the lifetime of the safety measure can be calculated by taking into account a discount factor, because the maintenance team costs occur throughout the whole remaining lifetime of the facility.

7.3.4.3 Production loss costs

When maintenance is periodically necessary for the optimal functioning of the security measure, sometimes the production has to be stopped temporarily, resulting in a production loss. This production loss (if applicable) is accompanied by costs because of the nonproducing status of the facility. Production loss costs per maintenance period can be calculated by the multiplication of the production rate of the factory by the duration of the stop and again by the profit per unit sold (Gavious et al., 2009).

These countermeasure costs represent the maintenance production loss costs of one maintenance period, which is defined as 1 year. Thus if it is assumed that maintenance occurs on a yearly basis and the yearly cost is always the same, the total PV of all maintenance production loss during the lifetime of the countermeasure can be calculated by taking into account a discount factor, because the maintenance production loss costs occur throughout the whole remaining lifetime of the facility.

7.3.4.4 Start-up costs (after maintenance)

Maintenance of a new security measure can cause a temporary slowdown in production due to the restart of the facility occurring because of the stopping of the production that was necessary for the maintenance. The costs accompanied by the temporary slowdown in production are called start-up costs and can be calculated by multiplying the difference in production rate before and after the halt in production by the duration from the time the production line is reactivated after the maintenance period of the safety measure to the time when the production line goes back to the initial production rate and again by the profit per unit sold (Gavious et al., 2009).

Notice that if the production rate at the time of the start-up is exactly the same as the production rate before the halt in production, the start-up costs will be zero.

Remark that the aforementioned countermeasure costs represent the maintenance start-up costs of one maintenance period, which can be defined as 1 year. Thus if it is assumed that maintenance occurs on a yearly basis and the yearly cost is always the same, the total PV of all maintenance start-ups during the lifetime of the countermeasure can be calculated by taking into account a discount factor, because the maintenance start-up costs occur throughout the whole remaining lifetime of the facility.

7.3.5 Inspection team security costs

This cost will have to be discounted to a PV, as it will not only occur in the present (in the basic year (=year 0)), but throughout the entire remaining lifespan of the facility.

The inspection team security costs are related to the periodic inspection and audit activities of the security department of the company or of an external auditing company, to check whether the security countermeasures are effective (Brijs, 2013). Carrying out periodic risk assessments can also be considered to be part of these security costs. These inspection team costs can be calculated and estimated through multiplying the hourly wage of an employee by the number of hours the inspection takes and again by the number of employees participating. If, however, employees with significantly varying wage levels participate, the inspection team costs can be calculated separately for each category of employees. Another possibility is to take the average wage level of all employees participating, in order to only have to work with one category.

These costs, however, represent the inspection team security costs of one inspection period, defined as 1 year. Thus if it is assumed that these costs occur on a yearly basis and the yearly cost is always the same, the total PV of all teams needed during the lifetime of the safety measure is calculated by considering a discount factor, because the inspection team costs occur throughout the whole remaining lifetime of the facility.

7.3.6 Security costs related to logistics and transportation activities

Materials need to be transported and stored in a secure way. Security documents need to be drawn, filled in, and updated. The subcategories of this cost category are the following:

i. Transport and loading/unloading of hazardous materials costs
ii. Storage of hazardous materials costs
iii. Security documents costs

7.3.6.1 Transport and loading/unloading of hazardous materials costs

The transportation of materials and of substances, such as transport of gas cylinders, entails costs due to existing legislation and due to extra measures for security. Transport indeed requires compliance with existing regulations (e.g., part of ADR legislation regarding security) during transportation and during loading and unloading of goods, and sometimes extra security measures are needed.

The transport costs of materials can be calculated by determining the security cost for the transportation of a material unit or good and multiplying this with the number of units or goods transported, for all materials that need to be transported. These costs, however, represent the transport security costs of all materials transported during 1 year for an organization. Thus if it is assumed that these costs occur on a yearly basis and the yearly cost is always the same, the total PV of all transport costs can be determined using parameters such as the remaining lifespan of the facility and the discount rate.

7.3.6.2 Storage of hazardous materials costs

The storage costs can be determined by multiplying the storage security cost per material unit or good with the number of units or goods stored, for all materials that need to be stored. These costs, however, represent the storage security costs of all materials stored during 1 year. Thus if it is assumed that these costs occur on a yearly basis and the yearly cost is always the same, the total PV of all storage costs can be determined.

7.3.6.3 Security documents costs

Security documents periodically need to be filled in by employee(s) (Reniers and Audenaert, 2009). The cost accompanying the filling in of security documents can be determined by multiplying the hourly wage of those employees with the number of hours needed to fill in the documents and again by the number of employees participating. If, however, employees with significantly varying wage levels participate, the security documents costs can be calculated separately for each category of employees. Another possibility is to take the average wage level of all employees participating, in order to only have to work with one category.

These costs, however, represent the security document costs of one period, which are, for instance, defined as 1 year. Thus if it is assumed that these costs occur on a yearly basis and the yearly cost is always the same, the total PV of all teams needed during the filling in of security documents can be calculated by considering a discount factor and the remaining lifetime of the facility under consideration.

7.3.7 Contractor security costs

If a company works with contractors, they need to be selected, taking security into account. The selection process, as well as the contractor training aimed at company security, represents a security cost. Moreover, a loss of working time training the contractors should also be considered. Therefore, contractor security costs include:

i. Contractor selection costs
ii. Training costs

7.3.7.1 Contractor selection costs

Contractor firms need to be chosen with "security" as one of the most important selection parameters. The selection is conducted by employees of the company, and thus, the costs can be determined by taking these employee costs into consideration.

These costs, however, represent the contractor selection security costs of one period, which are, for instance, defined as 1 year. Thus if it is assumed that these costs occur on a yearly basis and the yearly cost is always the same, the total PV of all contractor selection procedures is calculated by considering a discount factor and taking the remaining lifetime of the facility under consideration. If the contractor selection costs

only need to be incurred once, there is evidently no need to use a discount factor and calculate an NPV. If another time period is used for the selection, e.g., a 5-year period, the formula needs to be adjusted to this.

7.3.7.2 Training costs

Contractor employees, when selected by a company, often need to receive security training within the company, as well as receive instructions and guidelines for working at or with certain installations. These extra costs, which are related to security, should also be taken into consideration.

These costs, however, represent the training costs of one period, which are, for instance, defined as 1 year. Thus if it is assumed that these costs occur on a yearly basis and the yearly cost is always the same, the total PV of all security training needs is calculated by considering a discount factor and the remaining lifetime of the facility.

7.3.8 Other security costs

Security costs that cannot be assigned to one of the discussed categories of security costs in the previous sections are listed under "other security costs" and can/should be mentioned in this category.

7.4 Calculating benefits (avoided security incident costs)

The purpose of implementing security measures is to reduce present and future security risks. By "reducing the security risk," the prevention of security incidents is indicated, as well as the mitigation of the consequences if an incident would occur after all. Thus, the benefits of a security investment/countermeasure can be regarded as the difference in consequences without and with a security investment/countermeasure, and taking into account the difference in likelihood, if an incident would occur. The "consequences without security countermeasure" can be seen as potential (hypothetical) consequences of incident scenarios. The "consequences with security countermeasure" indicate those consequences still possible after taking a specific security measure for the incident scenario. In this section, the various financial aspects of consequences related to an incident (scenario) will be discussed, as well as the formulas to calculate these aspects.

The research outcomes in the framework of the safety literature (due to the lack of security literature) mention a number of safety accident cost categories and taxonomies, the most used and well-known incident cost categories being direct and indirect costs. These cost categories can be investigated and eventually used for security incident cost categories. We will further in this section apply safety-related accident cost information to security.

Direct incident costs represent costs that are immediately visible and tangible. They can be seen as "logical, common sense consequences of an incident." Conversely,

indirect costs are those security incident costs that are difficult to assess and are often intangible and invisible.

In case of safety-related accidents, costs are often much higher than merely the direct and visible costs. The same observation holds true in case of security incidents. In fact, indirect costs usually represent a multiple of the direct costs, and therefore, they are a very important factor while analyzing incidents and making decisions on security investments for dealing with type I as well as type II security risks (see Chapter 5). As was also indicated in Chapter 5, different researchers tried to draft ratios of direct over indirect costs for safety-related accidents, and a variety of ratios can be found in safety literature, depending on the nature of the study (e.g., depending on the industrial sector where the research was conducted). A well-known and much used ratio for type I accident costs is that of Heinrich, the already mentioned father of industrial safety. Based on a study of 75,000 type I accidents, Heinrich (1959) concluded that indirect costs are four times higher than direct costs. But, as mentioned, other studies have found different ratios. Some examples of direct and indirect costs are: (i) direct costs: damage to installations, equipment, buildings, products, medical costs (for instance, evacuation, used material for first aid, hospitalization, paying fines, wage costs of injured employees being at home, etc.); and (ii) indirect costs: production delays/stops, production decrease and problems, planning problems with clients and suppliers, costs of replacements of employees, costs of carrying out security incident investigation, etc.

A number of different avoided security incident cost categories can thus be derived from safety literature and can therefore be mentioned. Such costs can be used in a cost−benefit analysis and/or a cost-effectiveness analysis tool in order to calculate the benefits linked with type I security risks and type II security risks. If there would be no accurate variables available about some of the subcategories, information derived from previous executed projects within the company can be employed, or another option is to use estimated consequences given by an independent partner company. If needed, this information can then eventually be employed to determine one or more flat-rate amounts representing one or more of the avoided cost subcategories from Table 7.4.1.

Since the consequences of a security incident only become reality when the incident actually occurs, the frequency of occurrence should be taken into account in the calculation of the expected hypothetical benefits in some way. Therefore, the consequences will have to be multiplied by the likelihood of occurrence in some way, in order to obtain the expected hypothetical benefits due to an incident scenario (see Chapter 3 and 4 for examples of calculations). Thus if the hypothetical different kinds of consequences are considered to be spread out on a yearly basis, and the yearly cost coming from these consequences is considered to always be the same, the total PV of all hypothetical costs of an accident scenario during the remaining lifetime of the facility can be calculated by taking into account both the remaining lifetime and a discount factor.

This calculation has to be executed for both the cases with and without the implementation of the security countermeasure. The difference between the two PVs of

Table 7.4.1 Avoided security incident cost categories.

Type of avoided security incident cost	Subcategory of avoided security incident cost
Supply chain	Production-related (type I + type II)
	Start-up (type I + type II)
	Schedule-related (type I + type II)
Damage	Damage to own material/property (type I + type II)
	Damage to other companies' material/property (type II)
	Damage to surrounding living areas (type II)
	Damage to public material property (type II)
Legal	Fines (type I + type II)
	Interim lawyers (type II)
	Specialized lawyers (type II)
	Internal research team (type II)
	Experts at hearings (type II)
	Legislation (type II)
	Permit and license (type II)
Human and environmental	Compensation victims (type I + type II)
	Injured employees (type I + type II)
	Recruitment (type I + type II)
Personnel	Productivity of personnel (type I + type II)
	Training of new or temporary employees (type I + type II)
	Wages (type I + type II)
Medical	Medical treatment at location (type I + type II)
	Medical treatment in hospitals and revalidation (type I + type II)
	Using medical equipment and devices (type I + type II)
	Medical transport (type I + type II)
Intervention	Intervention (type I + type II)
Reputation	Share price (type II)
Other	Accident investigation (type I + type II)
	Manager working time (type I + type II)
	Cleanup (type I + type II)

consequence costs represents the maxmax hypothetical security benefit resulting from the implementation of the new security investment.

Maxmax hypothetical security benefits = Total present value of consequence costs (without security investment) − Total present value of consequence costs (with security investment).

This calculation is identical for all of the following discussed consequences.

If the probabilities of incident scenarios are used, the expected hypothetical security benefits can be determined. Indeed, the costs as elaborated further in this section need to be multiplied by the frequency of occurrence or the probability of the event, in order to obtain the yearly expected avoided costs. Afterward, this yearly avoided cost is used in the formula for annuities in order to obtain the PV of the consequences for the remaining lifetime of the facility. This needs to be carried out for both the situation without and

with the new security measure, and the difference between the two PVs represents the expected hypothetical security benefits with regard to that specific subcategory. This calculation is identical for all defined subcategories of consequences and has to be carried out for every one of them.

It should be noted that "Maxmax hypothetical security benefits" can be calculated and used for type II security incidents, while the "Expected hypothetical security benefits" can be employed in case of type I security incidents.

7.4.1 Supply chain avoided costs

7.4.1.1 Production-related avoided costs

When a security incident occurs, it is possible that (a part of) the production stops, resulting in a production loss. This production loss is accompanied by costs because of the nonproducing status of (a part of) the factory or plant. Production loss costs can be calculated by the multiplication of the production capacity/rate of the facility by the estimated duration of the stop and again by the profit per unit sold (Gavious et al., 2009).

7.4.1.2 Start-up avoided costs

When the production is started again after the occurrence of a security incident, a temporary slowdown in production due to the restart of the facility can occur. The costs accompanied by the temporary slowdown in production are called start-up costs and can be calculated by multiplying the difference in production rate before and after the halt in production by the duration from the time the production line is reactivated after the accident occurred to the time when the production line goes back to the initial production rate and again by the profit per unit sold (Gavious et al., 2009). Notice that if the production rate at the time of the start-up is exactly the same as the production rate before the halt in production, the start-up costs will become zero.

7.4.1.3 Schedule-related avoided costs

If a serious incident occurs, this will also affect the timetable schedule of the factory, and this can cause problems with clients. The possibility exists that clients may cancel one or more contracts or may demand a lower price due to the delay. A solution may be to hire a contractor that can help the company to provide the necessary products to handle the company's time schedule. However, a schedule problem will arise not only toward clients and customers but also toward partners and suppliers. If the company produces part of a product and a partner company finishes the partly completed product, the partner company will also face supply chain costs, as the company will have to wait longer for the partly completed products to arrive. Toward suppliers, the problem is that if the company cannot produce, its inventory stays the same. Because of the latter, the company will not need fresh suppliers at the normal rate, and thus the agreements with suppliers will have to be changed/canceled, which will also bring the suppliers some scheduling problems.

Costs accompanying these scheduling problems can be calculated by adding up three factors. The first one is the multiplication of the fine for a canceled order/contract by the number of canceled orders/contracts. The second one is the multiplication of the fine due to delays in deliveries per day by the number of days of tardiness of the orders and again by the number of orders that have a delay. Finally, the third cost can be calculated by multiplying the number of units given by the contractor with the difference between the cost per unit asked by the contractor and the in-house cost per unit (Gavious et al., 2009).

7.4.2 Damage avoided costs

7.4.2.1 Material and property damage avoided costs

An incident may lead to damage to buildings, infrastructure, products, raw materials, finished goods, equipment, machines, etc. These costs are labeled as "damage costs" and are usually taken into account in any cost–benefit analysis.

7.4.2.2 Other companies' damage avoided costs

A major security incident of type II might cause damage to other companies' material and property, besides damage to the own assets. The company needs to pay for the damage incurred by other companies, as they will likely file claims toward the company where the security incident was initiated (Brijs, 2013). These costs are also labeled as damage costs and should be taken into account in an economic analysis.

7.4.2.3 Surrounding area damage avoided costs

An incident of type II sometimes may cause damage to residential properties. The company will have to pay for the damage, as the inhabitants possibly will file claims toward the company where the incident originated. These costs are also labeled as damage costs and should be taken into account in the cost–benefit analysis.

7.4.2.4 Public material and property damage avoided costs

An incident of type II in some cases causes damage to public material and property. The company needs to pay for that damage as well, as the local government probably will file claims toward the company that caused the accident (Brijs, 2013). These costs are also labeled as damage costs.

7.4.3 Legal consequences avoided costs

The different types of legal consequences due to an incident are explained more in depth in this section. The legal aspects may turn out to be an important part of the hypothetical benefits, especially in case of type II security incident scenarios. One can imagine that whenever a major security incident occurs, the legal department of a company will be put under focus and stress. In the case of a type II security incident, for instance, a successful large-scale terrorist attack, a lot of financial resources will have to be spent for

hiring additional workforce and experts to deal with the complexity of such an incident. In addition, the legal environment in which the company operates will change according to the occurrence of such catastrophes, and the company will need to make sure that it complies with these changes.

7.4.3.1 Fines-related avoided costs

If an incident occurs, the government and other organizations will look for responsible individuals or a responsible group of individuals. In some cases, the company as a whole will be held responsible for the accident, in other cases employees, managers, or other persons may be held responsible (Moeyersoms, 2013).

Responsible persons or the responsible organization may be exposed to civil liability, administrative liability, and/or criminal liability for the major accident. Having both administrative and criminal liability carries the obligation of paying fines. The difference between the two types of liabilities is explained hereafter. Criminal liability on the one hand is when someone or some organization has hurt or killed people, or if property has been destroyed on purpose. Administrative liability on the other hand comes into play when one has not operated and handled according to the law (in this case security-related legislation such as ISPS or EPCIP) and prescribed procedures and methods. Thus if an incident is caused due to violations of security procedures or not following the law, the organization may be exposed to fines and claims given by the authorities due to the administrative liability (Gavious et al., 2009; Moeyersoms, 2013). Another difference is that the importance and weight of the sentence are significantly different. On top of the fine, criminal liability will be put on the criminal record and may have serious punishment as a consequence such as jail time. This is not the case with administrative liability, which only includes a fine.

7.4.3.2 Lawyers avoided costs

If a major security incident occurs, the government will assemble a research team to know what caused the incident and what the consequences are on all aspects for the country, society, and environment. A company lawyer will also be assigned to be a part of this research and therefore he will not be able to do his usual work for his company. Therefore, the company will probably need to hire an interim lawyer for the full duration of the research.

The costs related to the hiring of interim lawyers due to the occurrence of a major event can be calculated and estimated through multiplying the daily wage of such a lawyer by the number of days he will be hired and again by the number of lawyers that the company wishes to hire. If, however, the company decides to hire both junior and senior interim lawyers, the user may want to calculate the costs separately for both categories of lawyers.

In the event of a trial regarding major incidents, companies will also hire lawyers who are specialized in law related to disaster. These lawyers require substantial salaries, and are expensive for any organization, even, for example, for a large multinational, as trials

about major incidents can take several years. However, the costs of specialized lawyers vary widely depending on the country in which the accident occurs or the trial takes place. Often a deal is made between the two parties or a flat-rate amount is used. In any case, trials and lawsuits due to major security incidents taking several years might easily cost several millions of euros to the company who hires specialized lawyers (Moeyersoms, 2013).

The costs related to the hiring of specialized lawyers due to the occurrence of a major accident can be calculated and estimated through multiplying the hourly wage of such a lawyer by the number of hours he/she will be hired and again by the number of lawyers that the company wishes to hire. If, however, the company decides to hire specialized lawyers with widely varying wage levels, the user may want to calculate the avoided costs separately for those categories of lawyers.

7.4.3.3 Internal research team avoided costs

Independently of the research team assembled by the government and separately from any investigation done by other organizations involved in the major security incident, a research team will probably also be assembled by the company itself. This research team will evidently mainly consist of security and HSE-experts, but other company specialists such as process engineers etc., will also need to be present, and its purpose is to analyze available information to identify how the incident could have happened and to make sure there is no possibility that it can be repeated in any of the company's plants in the future, by making recommendations to take adequate countermeasures (Moeyersoms, 2013; BP, 2010).

The costs related to the internal investigation team due to the occurrence of a major security incident can be calculated and estimated through multiplying the daily wage of people participating by the number of days they will be hired and again by the number of people that the company wishes to assemble. If, however, employees with significantly varying wage levels participate, it may be necessary to calculate the internal investigation team costs separately. Another possibility is to take the average wage level of all employees participating.

7.4.3.4 Experts at hearings avoided costs

In addition, experts in their field will sometimes be invited to testify and state their opinion in court. The party that is held accountable for a type II security incident will pay the salary of these experts. The company will also sometimes need the possibility to hire additional experts, to challenge the findings of the initial experts.

The costs related to the hiring of experts due to the occurrence of a major accident can be calculated and estimated through multiplying the hourly wage of experts participating by the number of hours they will be hired and again by the number of experts that the company wishes to hire. If, however, experts with significantly varying wage levels participate, the user may want to calculate the experts' costs separately. Another possibility is to take the average wage level of all experts participating.

7.4.3.5 Legislation changes avoided costs

Companies all over the world have invested some of their resources in the fields of safety as a response to legislation and directives. For instance, in Europe, the major industrial accident prevention legislation is called the Seveso Directive, of which the first version was issued in 1982 as a result of the major accident that occurred in Seveso, Italy, 6 years before, in 1976. Vierendeels et al. (2011) indicate that there are two drivers for safety legislation changes: (i) scientific progress and societal changes and (ii) a shock effect (that is, safety-related major accidents).

However, the exact relationship between the occurrence of a major accident and a changing legislation is not unambiguous, an occurrence of a major security incident, say, a terrorist attack, would undoubtedly change legislation. Due to 9/11, for instance, the most well-known type II security event worldwide that ever happened, new international legislation, called the International Ship and Port facility Security code (ISPS for short), among others, was worked out and imposed on harbors globally. If a successful terrorist attack with thousands of fatalities would materialize at a chemical industrial area situated somewhere in the Western World, there is no doubt whatsoever that national and international legislations would be revisited and much more stringent regulations would be imposed, much like how safety legislation came about.

In the beginning of the 19th century, more specifically the year 1810, the first regulation regarding major risks was born, caused by an accident in 1794 in Grenelle located in France in which about 1000 people died. In the following decades, similar catastrophes occurred in Europe, triggering the decree of similar legislations regarding major industrial risks in those countries. In 1982, the first European Directive concerning major risks, Seveso I, was issued as a response for the occurrence of the major accidents in Flixborough in the United Kingdom in 1974 and in Seveso in Italy in 1976. The legislation has changed several times since, mainly because of the occurrence of new major industrial accidents. For example, the accident that occurred in Bhopal in India in 1984 and the Rhine pollution in Basel in Switzerland in 1986 directly caused new amendments in 1987 and 1988. Together with the major accidents in 1984 in Mexico City and in 1987 in Piper Alpha, these accidents caused legislation to change, and in 1996, the Seveso II Directive was approved. However, major accidents kept on occurring and mainly because of shock effects such as the accidents in Baia Mare in Romania in 2000, in Enschede in the Netherlands in the same year, and in Toulouse in France in 2001, the legislation was changed and amended again in 2003. On the 1st of June 2015, a new version of the legislation for major risks, the Seveso III Directive, entered into force in Europe. Hence, legislation is subject to frequent changes as new accidents and new challenges arise. This is the case for the safety domain, as is illustrated earlier, but it is also true for the security domain, as was seen after the 9/11 terrorist attack and the legislation changes it brought with it. This is not only a time-consuming and costly process for governments, but also for private companies, as they need to analyze and implement the changed regulation in order to comply (Vierendeels et al., 2011).

Future changes in security legislation will be accompanied by a large financial, administrative, and operational burden. However, costs related to legislation changes due to the occurrence of a major security incident are difficult to quantify directly. Nonetheless, they can be calculated indirectly through multiplying the total security budget of the type of facility under consideration by the estimated increase (in percentage) of the security budget (due to the occurrence of a scenario that will cause the legislation to change and become more elaborated).

7.4.3.6 Permits and licenses avoided costs

It will become harder for a company to obtain the necessary exploitation permits and operation licenses in the country where a major security incident of the company would occur. In general, companies (especially with activities in the fields of petrochemicals, energy, and chemicals) need to obey the rules for obtaining permits and licenses very well. They cannot afford to lose operating and exploitation permits through behaving in a reckless way, as this would cause a financial disaster for the company.

The costs related to obtaining new permits and licenses due to the occurrence of a major security incident are difficult to quantify. However, they can be estimated through multiplying the total costs of having to close down the facility by the possible likelihood that the company will lose the operating permit due to the security event.

7.4.3.7 Lawsuit avoided costs

The amount of costs accompanying lawsuits and trials can become substantial and can pose a significant threat to the liquidity of the company. This is primarily caused by the fact that such lawsuits and trials can last multiple years, even more than a decade. Thus, it would be in the best interest of any company to avoid such time- and money-consuming trials.

Companies operating in certain areas, such as the chemical, oil, and gas industry, should always remember that it takes years building up a good image. On the contrary, a good reputation can be destroyed in just one brief moment, after which it will take at least several years to regain a good reputation.

7.4.4 Human and environmental avoided costs

7.4.4.1 Compensation victims avoided costs

Whenever an incident causes casualties, usually the company will compensate the families for their losses (Brijs, 2013). These costs are also labeled as compensation victims costs and should be taken into account in any cost–benefit analysis. These consequences can, for instance, be calculated by multiplying the Value of Statistical Life by the expected number of fatalities.

7.4.4.2 Injured employees avoided costs

Whenever an accident causes injuries, both minor and major injuries, the company usually will compensate the injured people for their injuries in some way (Brijs, 2013). These consequences can, for instance, be calculated by multiplying the cost of light and serious injured workers by the expected number of light and heavily injured people.

7.4.4.3 Avoided recruitment costs

As some employees can be injured or killed or leave the company due to a security incident, new employees will have to be recruited. The recruiting cost is thus the cost of hiring new workers, which includes the time invested in recruiting and training the new workers. The recruitment consequences are calculated by multiplying the sum of the hiring and training cost by the number of newly recruited employees. Hiring costs include advertising, interviews and assessments, and other costs (Gavious et al., 2009).

7.4.5 Personnel-related avoided costs

A major security incident will often result in situations where employees are temporary, for a short or a long period of time, or sometimes even indefinitely, not able to carry out their job and daily activities. Otherwise, employees may sometimes also be obliged to do other activities than those they are used to. Such situations entail avoided accident costs related to personnel and their productivity.

7.4.5.1 Lowered/lost productivity avoided costs

Productivity of employees often decreases due to an incident or accident (of any kind). This productivity loss is not merely the result of the employee who is actively involved in the accident, but also other employees may display lower productivity patterns. Furthermore, irrespective of the fact that due to an accident an employee can be incapable to work for a certain period of time, also when he returns, often a lower productivity can be observed. It is indeed sometimes possible that physical problems and restrictions or/and a changing risk perception (this is the so-called Hawthorne effect (cfr. Miller, 1997; Sun et al., 2006)) may lead to different behavior and may entail lower productivity. If "adapted work" is foreseen for the employee, productivity will most likely be lower as well. If the employee needs to be replaced, productivity levels will also be lower, especially initially, due to a lack of experience and expertise (Simmonds, 1951; LaBelle, 2000).

7.4.5.2 Training of temporary workforce avoided costs

Training people who have to replace those employees that suffered an incident represents also a cost. The most important part of this cost is time. The time needed by the trainer having to train the person who replaces the injured employee, as well as the

training time of the substitute, needs to be counted. The latter can also be seen as lowered productivity, since during the training period, the substitute does not attain his/her optimal productivity (Simmonds, 1951; LaBelle, 2000; Jallon et al., 2011).

7.4.5.3 Wage avoided costs

Incidents always go hand in hand with a lot of loss of time. The "wage cost" represents the amount of time that company employees cannot devote to their regular tasks due to a security incident. This may be the result of a necessary medical treatment at the company's first aid department, in which case the corresponding wage cost may be negligible. However, in the case that the accident leads to a longer period of work incapability, the wage cost can be significant (Gavious et al., 2009; Simmonds, 1951; Miller, 1997; LaBelle, 2000; Head and Harcourt, 1998). There may also be a wage cost due to colleague employees having to work extra if an incident happens.

7.4.6 Medical-related avoided costs

This category of avoided costs only applies to accidents involving one or more injured persons. Medical expenses often are an important part of the total cost of an accident, but they are mostly considered as insured costs. The level to which such costs are in fact indeed insured depends on the insurance policy.

7.4.6.1 Medical treatment at location avoided costs

Large companies usually have their own medical service department, so that in case of any kind of incidents, medical personnel of the organization may offer first aid. Sometimes, it is necessary for the medical service to travel onsite of an incident, leading to a possible cost.

7.4.6.2 Medical treatment in hospitals and revalidation avoided costs

Some of the more severe security incidents may need to be treated in hospitals by specialized personnel. This may also represent a substantial avoided cost.

7.4.6.3 Medical equipment and devices avoided cost

Avoided costs related to used medical equipment and devices is mainly applicable to companies having their own medical services. Depending on the incident nature and the severity of the incident, employees can be treated in the medical facilities of the organization, and medical equipment, devices, and material can be consumed in such case. First, well-educated medical personnel needs to be present in case of certain equipment. Such personnel and their training and education represent an avoided cost. Second, medical material may include bandages, painkillers, etc.

7.4.6.4 Medical transport avoided cost

If an incident requires employee(s) to be treated in hospital instead of by the organization's medical services, he/she/they need(s) to be transported to the hospital. This transportation cost can be taken into consideration in a cost–benefit analysis.

7.4.7 Intervention avoided costs

Whenever a security incident occurs, and certainly in case of a major one, different types of intervention personnel will be necessary. Intervention types can be as wide as from fire department services, law enforcement and police department services, ambulance services, and special unit services if, for instance, toxic materials are involved in the accident. The option to include fire and police department costs should at least be considered, as in some cases the company will have to pay an amount of money for their services, although these interventions by the fire and police department are public services (Brijs, 2013). The intervention avoided costs can be calculated by taking the sum of the avoided costs for the specified intervention types.

7.4.8 Reputation avoided costs

Financial consequences related to the reputation of the company subject to a major security incident are evidently very hard to quantify, although they will be extremely important. One possible way to do so is by considering the share price consequences, as share prices display the investors' image of the current performance and future expectations of the company, which can be seen as the "reputation."

To clarify this consequence, the example of the BP share price drop due to the Deepwater Horizon drilling rig major accident of 20 April 2010 can be given. Following the oil rig disaster, BP share prices dropped more than 50% in value. On the 20th of April, the day when the major accident occurred, the share price was GBP 655.40. As information regarding the severity and consequences of the disaster became widespread known, the share price plunged, reaching a low of GBP 302.90 on the 29th of June, a decline of 53%, 78% in comparison with the share price on the 20th of April. The total decline in market value of BP between the 19th of April and the 29th of June was approximately $100 billion (Fodor and Stowe, 2010). From this day on, the share price gradually increased back. The price seems to have stabilized around GBP 450.00, a recovery of some 50% of its loss, although still some 30% decline in comparison with the preaccident share price and preaccident market value of about $190 billion.

The share price avoided costs can be calculated through multiplying the current total market value of the company by the expected drop in the share price. A company can, for example, use a rule of thumb for the expected drop in share price and anticipate an expected decrease of share price (expressed in percentage), depending on the consequences of a security disaster scenario.

7.4.9 Other avoided costs

7.4.9.1 Incident investigation avoided cost

When an incident occurs, a person or a team is assigned to investigate the accident (not necessarily related to any legal affairs). Organizations often desire to determine and map the causes of accidents to take the necessary preventive measures to avoid future similar incidents and accidents. Literature thus mentions a variety of incident investigation approaches, each displaying pros and cons. The costs of accident analyses result from time that employees have to devote to the investigation and sometimes also from technical studies.

The time-related costs are composed of the wages of people carrying out the incident investigation. This cost can be determined by using the wage per employee category involved in the investigation. Sometimes, certain additional employee-related costs are present that should be added to the costs. Such additional costs, for instance, involve the further processing of the incident investigation file and sending the report to all concerned parties.

7.4.9.2 Manager work-time avoided cost

Managers of all levels (middle management, higher management, and board of directors) will be forced to invest time if an incident occurs. They will have to spend time for the incident, guide the employees, possibly deal with press attention, and in certain cases attend lawsuits and other legally required processes (Gavious et al., 2009). The manager work-time consequences can be calculated and estimated through multiplying the total number of hours lost by all managers of a certain manager category by the cost per hour of the lost work-time of managers of that category. As the work of managers with significantly varying wage levels will be affected, the manager work-time consequences can be calculated separately for each category of managers.

7.4.9.3 Cleanup avoided cost

An avoided cost often forgotten is the cleanup cost resulting from an incident. Before rebuilding and restoring the initial situation, the whole incident area needs to be cleaned up. Besides the employees, an independent cleaning company may sometimes need to be hired to execute this cleaning up assignment. The avoided cleanup costs can for instance be calculated and estimated through multiplying the hourly wage of an employee by the number of hours the cleaning will take and again by the number of employees participating.

7.5 Investment analysis — economic concepts related to type I security risks

In case of type I security risks, certain economic concepts exist that are linked with the costs and the benefits and help to make an investment analysis to steer a

recommendation for the security investment. The economic concepts are "Internal Rate of Return" (IRR) and "Payback Period" (PBP).

7.5.1 Internal rate of return

The Internal Rate of Return (IRR) can be defined as the discount rate at which the PV of all future cash flows (or monetized hypothetical benefits) is equal to the initial investment, or in other words, it is the rate at which an investment breaks even. Generally speaking, the higher an investment's IRR, the more desirable it is to carry on with the investment. As such, the IRR can be used to rank several possible investment options an organization is considering. Assuming that all other factors are equal among the various investments, the safety investment with the highest IRR would then be recommended to have priority.

An organization should, in theory, undertake all security investments available with IRRs that exceed a minimum acceptable rate of return predetermined by the company. Investments may of course be limited by availability of funds or security budget to the company.

Because the IRR is a rate quantity, it is an indicator of the efficiency, quality, or yield of an investment. This is in contrast with the NPV, which is an indicator of the value or magnitude of an investment.

A rate of return for which the NPV, expressed in function of the rate of return, is zero is the internal rate of return r^*. This can be expressed as follows:

$$\mathrm{NPV}(r^*) = \sum_{n=0}^{N} \frac{C_n}{(1+r^*)^n} = 0 \tag{7.5.1}$$

In cases where a first security investment displays a lower IRR but a higher NPV over a second security investment, the first investment should be accepted over the second investment. Furthermore, remark that the IRR should not be used to compare investments of different duration. For example, the NPV added by an investment with longer duration but lower IRR could be greater than that of an investment of similar size, in terms of total net cash flows, but with shorter duration and higher IRR.

7.5.2 Payback period

The payback period is calculated by counting the time (usually expressed in a number of years) it will take to recover an investment. Hence, a break-even point of investment is determined in terms of time. The payback period of a certain investment for type I security risks is a possible determinant of whether to go ahead with the security project or not, as longer payback periods are typically not desirable for some companies. It should be noted that the PBP ignores any benefits that occur after the determined payback period and, therefore, does not measure profitability. Moreover, the time value of money

is not taken into account in the concept, and neither is the opportunity cost considered. The PBP may be calculated as the cost of security investment divided by the annual benefit inflows.

Note that the payback calculation uses cash flows, not net income. The payback period simply computes how fast a company will recover its cash investment.

7.5.3 Cost–benefit analysis for type I security investments

It is possible to determine whether the cost of a security countermeasure outweighs – or not – its benefits. In the approach explained in this section, the benefits are expressed as the "reduced security risk," taking into account the costs of incidents with and without the security measure implementation. The following equation, which is based on safety-related literature, may be used for this approach (OGP, 2000):

$$[C_{\text{no count}} \times L_{\text{no count}} - C_{\text{with count}} \times L_{\text{with count}}] \times L_{\text{count}} > \text{Cost of countermeasure} \quad (7.5.2)$$

Or, if no sufficient information regarding the likelihood of the security event scenario is available for using the previous equation:

$$[C_{\text{no count}} - C_{\text{with count}}] \times L_{\text{security incident}} \times L_{\text{count}} > \text{Cost of countermeasure} \quad (7.5.3)$$

with:

- $C_{\text{no count}}$ = cost of security incident without security countermeasure
- $C_{\text{with count}}$ = cost of security incident with security countermeasure
- $L_{\text{no count}}$ = likelihood of the security event if the countermeasure is not implemented
- $L_{\text{with count}}$ = likelihood of the security event if the countermeasure is implemented
- $L_{\text{security incident}}$ = Likelihood of security incident
- L_{count} = Likelihood that the countermeasure will perform as required

The aforementioned formulas show immediately why this approach may only be carried out for (type I) risks where sufficient data is available: in case of type II security risks, the required "likelihoods" are not known, and rough estimates (more or less *guesses*) should be used, leading to unreliable results. If sufficient information is available, results from using these equations for determining the cost–benefit of a security countermeasure are reliable.

7.6 Cost–benefit analysis for type II security investments

Type II security incidents such as terrorist attacks are related to extremely low frequencies and a high level of uncertainty. To take this into account, the cost–benefit analysis preferably involves a so-called "Disproportion Factor" in order to reflect an

intended bias in favor of security above costs. This security mechanism is vital in the calculation to determine the adequate level of investment in countermeasures, as on the one hand the likelihood influences the hypothetical benefits substantially through the number of years over which the total incident costs can be spread out, and on the other hand the uncertainty regarding the consequences is high (Goose, 2006).

Usually cost–benefit analyses state that the investment is not encouraged if the costs are higher than the benefits. If, however, a disproportion factor is included, an investment in security is reasonably practicable unless its costs are grossly disproportionate to the benefits. If the following equation is true, then the countermeasure under consideration is not reasonably practicable, as the costs of the measure are disproportionate to its benefits.

$$\text{Costs/Benefits} > \text{Disproportion Factor (DF)} \rightarrow \text{Costs} > \text{Benefits} \times \text{DF} \tag{7.6.1}$$

In order to give an idea about the size of the disproportion factor, some guidelines and rules of thumb are available. They state that disproportion factors are rarely greater than 10, and that the higher the risk, the higher the disproportion factor must be in order to stress the magnitude of those risks in the cost–benefit analysis. This means that in cases where the risk is very high, it might be acceptable to use a disproportion factor greater than 10 (Goose, 2006). However, a value greater than 10 is allowed, Rushton strongly advices not to use a disproportion factor greater than 30 (Rushton, 2006).

In brief, companies can, for instance, demonstrate governments and other people that additional countermeasures are not reasonably practicable, based on cost–benefit analyses taking a disproportion factor into account. An advantage of using a disproportion factor in the analysis is that the company can claim to be biased in favor of security above costs. Remark that in theory it would also be possible to use the Disproportion Factor for type I risks, if company security management wishes to pursue certain security investments for this type of risks.

The decision-making process in practice is preferably not one of simply balancing costs and benefits of measures but, rather, of always implementing the security measures (due to the high Maxmax hypothetical benefits in case of type II security risks), except where they are ruled out because they involve so-called “grossly disproportionate” sacrifices. Security-related decisions indeed ideally should be justified based on some form of economic analysis. Moreover, when comparing the sacrifice (investment cost of security countermeasure) and the risk reduction (hypothetical benefit of the countermeasure), the usual rule applied by a CBA model is that the investment should be made if the benefit outweighs the costs. However, the rule is that the security measure should be implemented unless the sacrifice is “grossly disproportionate” to the risk. By using this successful practice, the investment costs are allowed to outweigh the benefits, and the security investment is pursued. However, the question remains how much costs can outweigh benefits before being judged “grossly disproportionate.” The answer to this question depends on factors that are summarized by the Disproportion Factor.

In the following, a formula is presented to derive the value of the DF, which makes the NPV of a security investment equal to zero. Using the results of such simulation exercise, it is possible to compare alternative security measures. It is important to judge whether the DF associated to each security measure "behaves" in a reasonable way.

With every security investment, three main features are associated as shown in Table 7.6.1 (see also Reniers and Van Erp, 2016).

The cost of a security investment can be divided into M, corresponding to the initial investments (e.g., purchasing cost of new equipment and materials directly *related* to the intervention) and m, the yearly recurring costs due to maintenance, energy costs, yearly equipment, depreciation and interest expenses, material and training costs. A security investment is evaluated considering a time horizon n that should be defined by the investor. More specifically the time horizon should be compatible with the asset life of the security measure to be analyzed. Hence, within n years, the security investment is supposed to maintain its effectiveness, without any significant deterioration of its performance.

In order to assess the financial impact of a security investment, the NPV equation should be adapted to the evaluation of the cost/effectiveness of a security countermeasure by explicitly including the disproportion factor DF. More specifically, the investment is represented by the cost of the security measure to be evaluated (i.e., M). This cost is supposed to be entirely sustained in the initial year (year 0) when the investment needs to be evaluated. Due to the characteristics of the measure, yearly recurring costs (due, e.g., to maintenance activities) might be required over the time horizon in which the investment is evaluated. These recurring costs are needed to maintain the functionality of a security measure and keep its effectiveness at its initial level. These costs are expressed as a percentage of the measure's initial cost and assumed to be sustained starting from year 1 until n, where n represents the time horizon in which the investment is evaluated. Therefore, the cost value C_t to be considered in the formula of the NPV assumes the following form:

$$C_t = \begin{cases} M, & \text{if } t = 0 \\ M \cdot m, & \text{otherwise} \end{cases} \tag{7.6.2}$$

On the other side, consistent with what was previously explained in this section, the benefits are quantified as the monetary savings, which can be achieved if the disruptions

Table 7.6.1 Features associated with a security investment to be evaluated.

Symbol	Description
e	Effectiveness of the security investment expressed as a percentage
M	Initial cost of the security investment including the installation expressed in a specific currency
m	Yearly recurring cost expressed as a percentage of the initial investment's cost M

caused by a security incident, that might happen with a certain likelihood, are avoided or mitigated thanks to the security investment that has been pursued. To quantify the savings, risk is seen as an index of potential economic loss, human injury, or environmental damage, which is measured in terms of both the incident probability and the magnitude of the loss, injury, or damage. The risk associated with a specific (unwanted) event is thus expressed as the product of two factors: the likelihood that the event will occur (p) and its consequences (V) considering both financial and human aspects. A risk in this approach therefore is an index of the "expected consequence" of the unwanted event. Two types of losses (financial loss f and human loss h) are considered to quantify the value of V (see (Talarico et al., 2015) for more details) where c represents a factor translating human loss into financial terms:

$$V = f + c \cdot h \tag{7.6.3}$$

Moreover, the risk aversion of a decision-maker toward a high consequence incident scenario is also considered by using the risk aversion factor a. Together with the DF, the risk aversion factor a can be used as a parameter to balance the risk awareness of the decision-maker as a way to incentive investments in security.

Assuming further that a security investment, whose effectiveness is represented by the letter e, is adopted, then the risk of an accident can be decreased. In fact, the probability of an accident that might trigger consequences estimated to be equal to V can be lowered due to the security investment as follows:

$$R_{\text{with measure}} = (1 - e) \cdot p \cdot V^a \tag{7.6.4}$$

Assuming that no security investment is pursued to prevent a potential security incident, the expected risk is measured by $R = p \cdot V^a$. Therefore, the profit of having a security measure can be measured as the marginal savings that can be obtained compared to a case in which no investments in security are made. More specifically, the marginal savings are represented by the avoided expected losses in case of accident due to a lower overall risk. In the following equation, the marginal gain is shown:

$$R_{\text{No security investment}} - R_{\text{with security investment}} = p \cdot V^a - (1 - e) \cdot p \cdot V^a = e \cdot p \cdot V^a \tag{7.6.5}$$

Finally, assuming that the security investment allows to decrease the risk of incidents during a fixed time horizon whose length is n, the total effect of the safety measure on the risk reduction can be estimated by multiplying the probability p by n. As a result, the potential benefits quantified in the year 0 can be assumed to have the following form:

$$B_0 = e \cdot p \cdot n \cdot V^a \tag{7.6.6}$$

Furthermore, during the security risk assessment phase, risk experts analyze the features of a system that might potentially be affected by a type II security incident. Incident types are investigated and possible consequences are calculated. These consequences can also be estimated from a financial point of view, as described before. The likelihoods of the incident scenario(s) are also estimated. Using this information, the expected risk associated to an incident scenario(s) can be quantified. In Fig. 7.6.1,

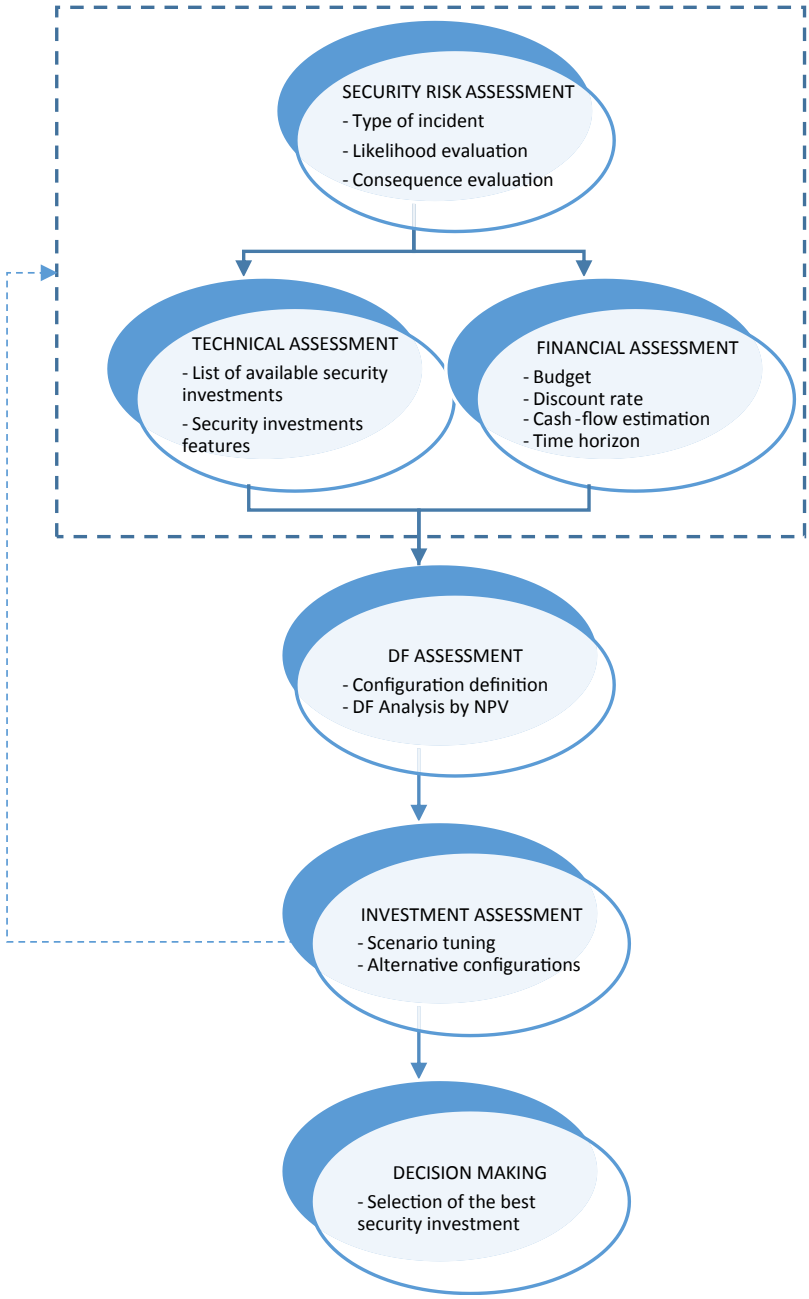


FIGURE 7.6.1 General schema of the decision model for evaluating security investments based on the DF.

a decision model is presented that can be followed within an organization to assess, evaluate, and decide about a security investment regarding a type II incident scenario.

As can be seen in Fig. 7.6.1, this security risk assessment approach serves as an input for both a technical and a financial assessment. These phases can be executed in parallel, based on the findings of the previous step. The technical assessment is focused on the definition of the most suitable security investments, based on the security risks that might affect the system. A list of possible security investments is drafted, and for every possible investment some basic features are determined (e.g., installation cost, maintenance, effectiveness, duration). Moreover, some of the available investments might be not compatible, from a technical point of view, with the system that needs to be protected. For this reason, the incompatible measures should be discarded from the following steps of the analysis. Furthermore, the goal of the financial assessment is to define the security budget, for example, discarding some security investments being too expensive. In addition, some of the parameters required to estimate the benefits of the security investments need to be defined, such as the discount rate and the time horizon to analyze the investment.

For every feasible security investment, an evaluation is subsequently performed to analyze its financial impact and to determine the DF to make the security investment profitable. A specific configuration might be required by the financial and technical assessment phase to evaluate the investment. This configuration provides specific information in term of features of the selected security investment, time horizon, discount rate, etc., which can be used to evaluate the investment. Moreover, several scenarios can be analyzed by carrying out a sensitivity analysis whereby the consequences and probabilities of incident scenarios are used as test parameters. Therefore, the main goal of the investment assessment is to assess the robustness of the choice under different scenarios and assumptions. More specifically, different configurations might be tested to explore how the DF, which is associated to the security investment to be evaluated, is affected by changing one of the test parameters. Sometimes, the financial and the technical assessment needs to be reiterated in order to realign the technical and the financial elements included in the decision model. For every possible security investment, the proposed process can be repeated. In addition, other investments can be analyzed and compared with each other. In some cases, especially for type II security incident scenarios, where there is no consensus between risk experts, alternative scenarios, presenting, e.g., higher or lower incident probabilities (cfr. difference between worst-case scenario, worst-credible scenario, most-credible scenario, etc.), might be considered. Afterward, the whole decision approach is repeated to assess the impact on the security investments to be selected.

The final step is represented by the decision-making in which alternative investments are evaluated on the basis of elements such as the DF for which the NPV is equal to zero. Substituting Eqs. (7.6.2) for the costs and (7.6.6) for the benefits into Eq. (7.6.1) and going from an inequality to an equality, we obtain the formula for the break-even DF_{be}:

$$DF_{be} = C_t/B_0 = C_t/(e \cdot p \cdot n \cdot V^a) \tag{7.6.7}$$

The lower the *DF*, the better the investment from a financial point of view. Different simulations can be carried out such as comparing security investments given an incident scenario (consequence and likelihood) and/or configuration such as the time horizon.

7.7 The Borda algorithm approach

To show a possible economic approach, besides a cost–benefit analysis or an investment analysis, that can be employed for decision-making regarding security investment options, the user-friendly Borda algorithm approach is explained and illustrated in this section.

The Borda algorithm is mainly used in voting problems (Klamler, 2005; Koch and Mitlöhner, 2009). The Borda rule assigns linearly decreasing points to consecutive positions, e.g., for three alternatives the points would be 3 for the first place, 2 for the second place, and 1 for the third place. The Borda algorithm can be found in literature on group decision-making and social choice theory. Readers interested in applications of the algorithm are, e.g., referred to Martin et al. (1996), Zarghami (2011), and Sobczak and Berry (2007). The algorithm is employed to develop an ordinal ranking of preferences. The Borda rule can also be employed in a risk management context (e.g., Garvey, 2009; Ni et al., 2010). In the context of security decision-making, the Borda Algorithm can be employed to develop an ordinal ranking of security investment options, thereby using several security investment criteria (Reniers and Audenaert, 2014).

In the security investment context, the algorithm can, for example, work as follows. All security investment options are ranked by a number of criteria. In case of type I security risks, criteria can be, for example, the absolute cost of security (investment amount), the expected hypothetical benefit of security (expected avoided security incident cost), the payback period of the security investment, and the internal rate of investment. In case of type II security risks, criteria can, for example, be the cost of the security investment, the Maxmax hypothetical benefit, the variability related to the incident scenarios avoided, and the information availability related to the security investment. Let us, for example, explain it for type I risks and their security investment. If there are n security investment options to be compared, then the first-place option (for instance, according to the absolute cost of security) receives $(n - 1)$ points, the second-place option receives $(n - 2)$ points, and so forth, until the last-place option, which receives zero points. The same rule is used for assigning points according to the expected hypothetical benefit of security, the PBP, and the IRR. All the points obtained for the five criteria are summed for all installations, and the option with the most points is ranked first, etc.

Fig. 7.7.1 reports an illustrative example of the present methodology.

The sole concern of the developed approach is the investigation of a security investment option's position relative to other security investment options if one looks simultaneously at the five criteria for, in the case of the illustrative example of Fig. 7.7.1, the type I security risks. This ranking information may lead to optimizing the allocation of security budget resources within an organization.

Consider four Security Investment (SI) options: SI1, SI2, SI3, and SI4. Suppose that the rank-order positions are as follows:

Absolute cost of security (investment amount): ***SI3 > SI2 = S1 > SI4***

Expected hypothetical benefit: ***SI1 > SI3 = S2 = SI4***

Payback period: ***SI1 > SI3 > S2 = SI4***

Internal rate of investment: ***SI2 > SI4 > S1 > SI3***

When ties occur, e.g. in case of the absolute cost of security *SI2* and *SI1* are tied, points allocated to these positions are derived from the average.

That is, *SI2* and *SI1* each will receive: $\frac{(n-2)+(n-3)}{2}$

In case of the expected hypothetical benefit, *SI3*, *SI2*, and *SI4* will each receive $\frac{(n-2)+(n-3)+(n-4)}{3}$

The resulting point distribution is summarized in the following Table together with the total Borda index for the four security investment options, and based on four criteria:

Criteria:	Security Investment options			
	SI1	*SI2*	*SI3*	*SI4*
1. Absolute cost of security	1.5	1.5	3	0
2. Expected hypothetical benefit	3	1	1	1
3. Payback period	3	0.5	2	0.5
4. Internal rate of return	1	3	0	2
Total Borda index	8.5	6	6	3.5

From the above Table, it can be concluded that Security Investment option number 1 (SI1) has the highest Borda count and, therefore, ranks first and is the best security investment according to the criteria used.

The overall rank-order of all four security investment options employing the five criteria is as follows:

SI1 > SI2 = S3 > SI4

FIGURE 7.7.1 Illustrative example for four security investment options to be considered to secure from type I security risks using the Borda Algorithm.

7.8 Conclusions

The present chapter discussed the economic aspects of security decisions, introducing specific methods for the evaluation of security investments based on cost-benefit analysis. Specific details were given in order to identify the typical operative and investment costs related to security. At the same time, potential benefits, for instance related to avoided damages, legal and insurance aspects, reputation, etc., were illustrated. The chapter introduced specific methods and algorithms in order to guide the evaluation of security decision with worked examples.

References

BP Incident Investigation Report, 2010. Deepwater Horizon Accident Investigation Report. BP.

Brijs, T., 2013. Cost-benefit Analysis and Cost-Effectiveness Analysis Tool to Evaluate Investments in Safety Related to Major Accidents. Master thesis. University of Antwerp, Antwerp, Belgium.

Campbell, H.F., Brown, R.P.C., 2003. Benefit-cost Analysis. Financial and Economic Appraisal Using Spreadsheets. Cambridge University Press, New York, USA.

Fodor, A., Stowe, J., 2010. The BP oil disaster: stock and option market reactions. SSRN Electron. J. https://doi.org/10.2139/ssrn.1631970.

Fuller, C.W., Vassie, L.H., 2004. Health and Safety Management. Principles and Best Practice. Prentice Hall, Essex, UK.

Garvey, P.R., 2009. Analytical Methods for Risk Management. Chapman and Hall/CRC Press, Boca Raton, FL, USA.

Gavious, A., Mizrahi, S., Shani, Y., Minchuk, Y., 2009. The cost of industrial accidents for the organization: developing methods and tools for evaluation and cost-benefit analysis of investment in safety. J. Loss Prev. Process. Ind. 22 (4), 434–438.

Goose, M.H., 2006. Gross disproportion, step by step – a possible approach to evaluating additional measures at COMAH sites. In: Institution of Chemical Engineers Symposium Series, vol. 151. Institution of chemical engineers, p. 952, 1999, 2006.

Head, L., Harcourt, M., 1998. The direct and indirect costs of work injuries and diseases in New Zealand. Asia Pac. J. Hum. Resour. 36, 46–58.

Heinrich, H.W., 1959. Industrial Accident Prevention. A Scientific Approach. McGraw Hill Publishing Co, London (UK).

Jallon, R., Imbeau, D., De Marcellis-Warin, N., 2011. Development of an indirect cost-calculation model suitable for workplace use. J. Saf. Res. 42, 149–164.

Klamler, C., 2005. On the closeness aspect of three voting rules: Borda Copeland maximin. Group Decis. Negot. 14 (3), 233–240.

Koch, S., Mitlöhner, J., 2009. Software project effort estimation with voting rules. Decis. Support Syst. 46, 895–901.

LaBelle, J.E., 2000. In: What Do Accidents Truly Cost, vol. 45. Professional safety, pp. 38–43.

Martin, W.E., Shields, D.J., Tolwinski, B., Kent, B., 1996. An application of social choice theory to USDA forest service decision making. J. Policy Model. 18, 603–621.

Miller, T., 1997. Estimating the cost of injury to U.S. employers. J. Saf. Res. 28, 1–13.

Moeyersoms, G., January 7, 2013. Legal Aspects of Major Accidents (Brijs, T, interviewer). Brussels, Belgium.

Ni, H., Chen, A., Chen, N., 2010. Some extensions on risk matrix approach. Saf. Sci. 48, 1269–1278.

OGP, 2000. Fire System Integrity Assurance. Report No. 6.85/304. International Association of Oil and Gas Producers (OGP), London, UK.

Reniers, G.L.L., Audenaert, A., 2009. Chemical plant innovative safety investments decision-support methodology. J. Saf. Res. 40, 411–419.

Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures wrt domino effects. Process Saf. Environ. Prot. 92, 583–589.

Reniers, G.L.L., Van Erp, H.R.N., 2016. Operational Safety Economics. A Practical Approach Focused on the Chemical and Process Industries. John Wiley and sons, Chichester (UK).

Rushton, A., April 4, 2006. CBA, ALARP and Industrial Safety in the United Kingdom. UK.

Simmonds, R.H., 1951. Estimating industrial accident costs. HBR 29 (January, no. 1), 107–118.

Sobczak, A., Berry, D.M., 2007. Distributed priority ranking of strategic preliminary requirements for management information systems in economic organizations. Inf. Softw. Technol. 49, 960–984.

Sun, L., Paez, O., Lee, D., Salem, S., Daraiseh, N., 2006. Estimating the uninsured costs of work-related accidents. Theor. Issues Ergon. Sci. 7 (3), 227–245.

Talarico, L., Reniers, G., Sörensen, K., Springael, J., 2015. Mistral: a game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. Reliab. Eng. Syst. Saf. 138, 105–114.

Vierendeels, G., Reniers, G., Ale, B., 2011. Modeling the major accident prevention legislation change process within Europe. Saf. Sci. 49, 513–521.

Zarghami, M., 2011. Soft computing of the Borda count by fuzzy linguistic quantifiers. Appl. Softw. Comput. 11, 1067–1073.

8

Conclusions

Intentional events associated with malicious acts of interference and/or cyber-physical terroristic attacks to industrial facilities may lead to the escalation of catastrophic events. Chemical and process industry represents a vulnerable sector, due to the large amounts of hazardous materials, which may be used as a potential mean for amplifying the damage potential of attackers.

Hence, chemical and process industries must address with the greatest urgency the need of increasing the level of security, adopting objective, performance-based methods to verify the adequateness of the resources dedicated to the protection of assets against external attacks. The methods and tools described in this book have the crucial aim of evaluating security risk and vulnerability for industrial facilities and clusters operating in the chemical sector, supporting the identification of weak links and the prioritization of resources. On one side, conventional methods based on international standards are presented; on the other side, advanced quantitative tools are introduced.

This book thus well represents the ongoing discussion within academia, but it is also projected toward industrial stakeholders and decision-makers, due to the practical nature of the case studies discussed to apply the methods. It also constitutes a useful guide for students in the framework of quantitative safety and security studies.

Physical Security in the Process Industry. https://doi.org/10.1016/B978-0-444-64054-3.00008-1