CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648116

Probabilistic Vulnerability Assessment of Chemical Clusters Subjected to External Acts of Interference

Francesca Argenti[a], Gabriele Landucci*[a], Genserik Reniers[b,c]

[a]Dipartimento di Ingegneria Civile e Industriale, Università di Pisa, Largo Lucio Lazzarino 1, 56126 Pisa, Italy.
[b]Safety and Security Science Group, Faculty of Technology, Policy, and Management, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, the Netherlands.
[c]Faculty of Economics and organizational sciences, Campus Brussels, KULeuven, Warmoesberg 26, 1000 Brussels, Belgium.
gabriele.landucci@unipi.it

Acts of interference against chemical facilities or chemical clusters might result in severe consequences in case of a successful attack (major explosions, fires, toxic dispersions or environmental contamination). Although process facilities implement multiple safety barriers to control process hazards that may result in major accidents and plants are mostly well equipped from a safety point of view, the security attention and resources dedicated to the protection of assets against external adversaries are not at all at the same level. The lack of a consolidated practice in the risk-informed implementation of security countermeasures goes hand in hand with the existence of very few systematic procedures for the quantitative performance evaluation of security systems, particularly physical protection systems (PPSs). Therefore, it is crucial to develop a methodology aimed at supporting the assessment of industrial facilities vulnerability to external attacks.
The present contribution addresses the vulnerability assessment using a probabilistic risk analysis approach, supported by a model based on Bayesian Networks (BN). The proposed methodology includes the quantitative performance assessment of the protection systems, intended as both physical protection systems adopted as security countermeasures and safety barriers, in interfering with the progress of a potential attack. A case study is analyzed to exemplify the methodology application.

1. Introduction

Deliberate attacks to chemical facilities and clusters processing large amounts of hazardous chemicals might lead to high impact explosion, fire, toxic dispersion or environmental contamination scenarios (Lou et al., 2003), ultimately resulting in a large number of public fatalities and loss of public confidence (Baybutt and Reddy, 2003). Nonetheless, acts of interference started to be included in the formal risk assessment of chemical industries only after the 9/11 attacks in New York City (Bajpai and Gupta, 2005). In Europe, although directives have been enacted to regulate the prioritization of measures to prevent and respond to terrorist attacks involving Critical Infrastructures (European Commission, 2008) and to guide the enhancement of the security of ship and port facilities used in international trade (European Commission, 2004), no guidelines are yet available for the security of chemical and process plants.
Two recent attacks perpetrated in France in 2015, against a chemical and a petrochemical plant, dramatically confirmed that the security of sites where relevant quantities of hazardous chemicals are stored or processed must be treated as a major concern. Actually, these events showed that industry must address with the greatest urgency the need of increasing the level of security attention and of adopting objective, performance-based methods to verify the adequateness of the resources dedicated to the protection of assets against external attacks. Therefore, it is crucial to develop a structured methodology to assess the vulnerability of industrial facilities and clusters (especially those operating in the chemical sector) to external attacks and to identify weak links.
Early work on assessing the risk of terrorist acts targeting industrial facilities started after 9/11, with the development of the so-called Security Vulnerability Assessment methods in the USA (see for example Center

Please cite this article as: Argenti F., Landucci G., Reniers G., 2016, Probabilistic vulnerability assessment of chemical plants subjected to external acts of interference, Chemical Engineering Transactions, 48, 691-696 DOI:10.3303/CET1648116

for Chemical Process Safety (CCPS, 2003) and American Petroleum Institute (API, 2003) methodologies) as well as in Europe (Störfallkommission (SFK), 2002). Contributions available in the open literature are mostly qualitative, while Bajpai and Gupta proposed semi-quantitative methodologies for application to the O&G (Bajpai and Gupta, 2007a) and chemical sector (Bajpai and Gupta, 2007b). More recently, Reniers et al. (2015) developed a security protection model for the use in the process industries in Belgium.
Other recent contributions were devoted to the analysis of specific aspects of security risks: Argenti et al. (2015) proposed a semi-quantitative methodology to the attractiveness assessment of chemical facilities; Salzano et al. (2014) investigated the potential of deliberate attacks carried out with home-made explosives to trigger domino effects within process plants.
The present work specifically focuses on outsiders' attacks involving high-consequence loss physical assets within the target facility, whose direct damage may lead to the release of hazardous substances. As element of novelty, it adopts a probabilistic risk analysis (PRA) approach, supported by a model based on Bayesian networks, to address vulnerability assessment quantitatively through the functional analysis of Physical Protection Systems (PPSs) applied to secure process and storage installations.

2. Evaluation of the likelihood contribution to security risk

In case of security risk assessment, risk is usually analysed by using consequences, threats, target attractiveness and vulnerabilities in some combination. Herein, the set of risk variables proposed by the API SRA Methodology (API, 2013) and given in Eq. (1) was adopted as reference, then a probabilistic approach was proposed to characterize the likelihood contributions to security risk and a BN-based model was used to model the relevant influences (not only causal relations).

$$R = L_1 \times L_2 \times C \tag{1}$$

Although Eq. (1) does not explicitly show the conditional dependencies linking the variables, it expresses the concept that the probability that a given act will result in a given consequence (C) can be estimated as the product of the marginal probability of the threat that the attack against the asset is attempted (i.e., L_1, which in turn depends on the threat agents' intent and capabilities and on target attractiveness) times the conditional probability of successful execution of the attack given the attack attempt (i.e., L_2).
The conditions upon which a deliberate attack aiming at directly impacting process equipment is successful are: i) adversaries choose an installation or piece of equipment as target to attack, and ii) the security system protecting the installation is not effective in preventing the accomplishment of the attack. Herein, the effectiveness of PPSs has to be intended as overall performance variable, to be derived through a specific assessment of the system as a whole with respect to its design protection functions, as detailed in Section 4.
Different attack modes, selected within the set presented in (SFK, 2002) as those capable of causing a direct damage to the affected equipment, were adopted to describe in a more detailed, though simplified, manner the attack scenarios that may be foreseen; this allowed a deeper analysis of the credibility of each scenario. According to Norman (2010), adversaries plan to attack according to a certain attack mode, which depends, on one hand, on the type of equipment selected as target and, on the other hand, on adversaries' motivations, available weapons, tools and knowledge of tactics. The latter aspects may vary a lot from case to case; since it is beyond to the purpose of our study to devote efforts to a full characterization of threat actors, we assume that these aspects, and their variation, can be summarized in the definition of "threat actors categories" (i.e. criminals, terrorists, activists etc.), according to the approach suggested in (SFK, 2002).
The above-mentioned considerations were taken into account to build the qualitative structure of the Bayesian Network shown in Figure 1.
A Bayesian Network is a graphical method for reasoning under uncertainty (Jensen, 1996); it was selected as modelling 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).
The proposed network, once quantified according to the approaches presented in Section 3 and Section 4, allowed the evaluation of probability values that represent the quantitative expression of the likelihood contribution to security risk of the analyzed set of attack scenarios. Each attack scenario is represented by one of the possible combinations of the states of nodes N.1, N.2 and N.3; in other words, it is defined by a triplet: attack mode, threat agent category, and target equipment type.
Clearly enough, the qualitative structure of the BN has generalized validity; conversely, the quantification of the network has to be carried out considering the specific location and features of the industrial facility under analysis and may involve the choice of ruling out some attack scenarios as not applicable and considering a reduced number of node states.

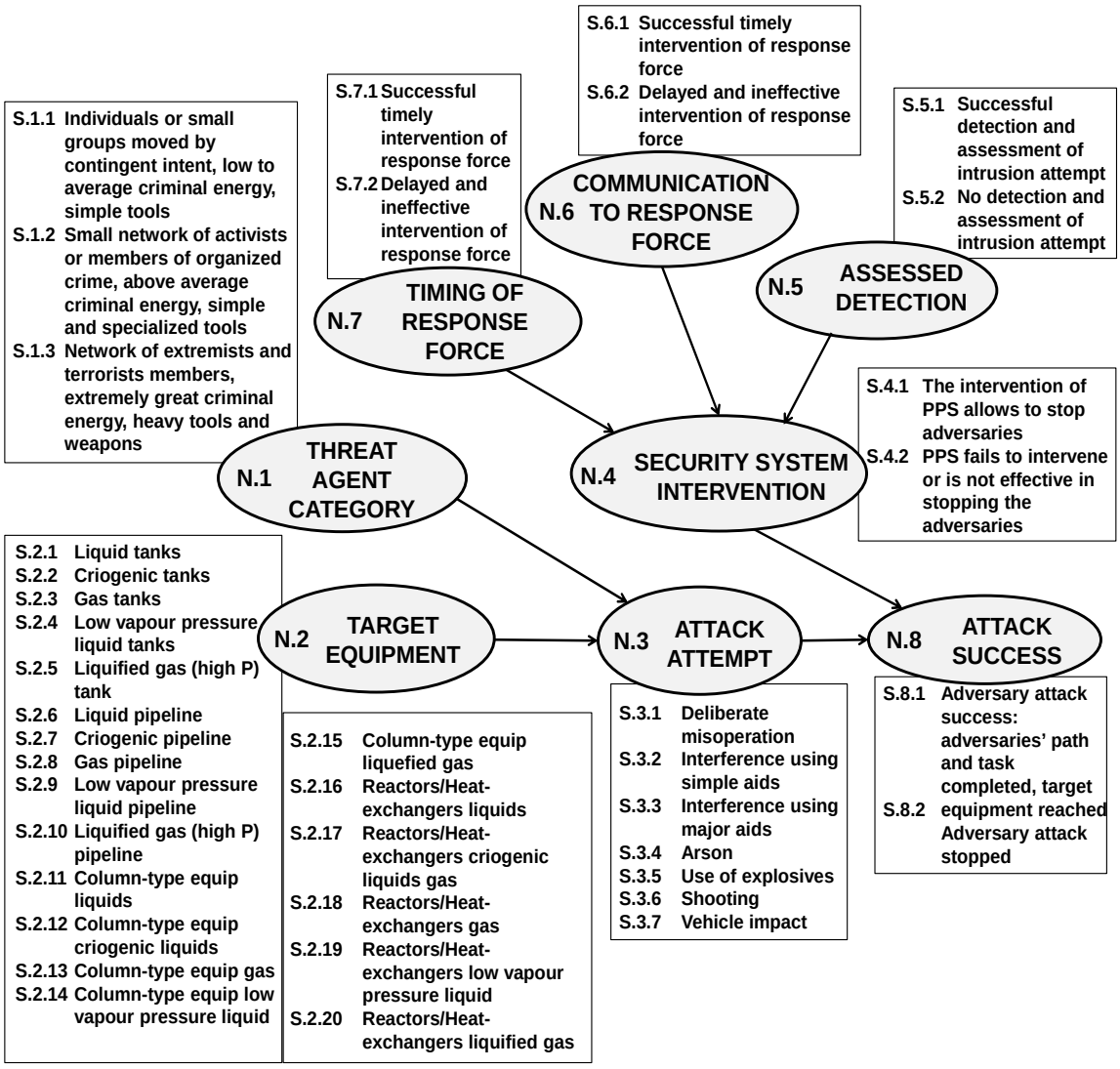

Figure 1: Bayesian network for the estimation of the likelihood contribution to security risk

3. Evaluation of the likelihood of attack

The likelihood of an attack was characterized through the quantification of the Conditional Probability Tables (CPTs) of node N.3 and its parent nodes (N.1 and N.2 in Figure 1).

The marginal probability of the threat being posed by the three categories listed as the possible states of node N.1 can be derived from statistical data on criminal and terroristic activities prepared by law enforcement and intelligence agencies.

The marginal probability of a specific type of equipment being selected as target was attributed on the basis of the equipment attractiveness level. The attractiveness level of different types of process equipment was attributed according to the taxonomy and qualitative evaluation proposed by Sabatini et al. (2009); a probability value was then associated to each qualitative level of attractiveness following the guidelines provided in (API, 2013), as summarized in Table 1. Finally, the marginal probability of each equipment type being selected as target was calculated through a normalization to 1 with respect to the sum of probability values associated to all equipment types present at the facility under analysis.

The conditional probability values to be applied to quantify the CPT of node N.3 in Figure 1 can be determined through expert judgment to represent the credibility of each attack mode being chosen as preferred strategy given the threat actors' category and the type of target equipment.

Table 1: Probabilistic attractiveness assessment to support the characterization of the conditional probability table for node N.2 (see Figure 1). PLG = pressurized liquefied gas

Node State	State Description	Qualitative attractiveness level	Attractiveness-based probability estimate
S.2.1	Tanks for liquid storage	Very high	0.9
S.2.2	Tanks for cryogenic storage	High	0.7
S.2.3	Tanks for gas storage	High	0.7
S.2.4	Tanks for low vapour pressure liquid storage	Medium	0.5
S.2.5	Tanks for liquefied pressurized gas storage	Low	0.3
S.2.6	Large diameter pipelines (liquids)	Very high	0.9
S.2.7	Large diameter pipelines (cryogenic liquids)	High	0.7
S.2.8	Large diameter pipelines (gases)	Medium	0.5
S.2.9	Large diameter pipelines (volatile liquids)	Medium	0.5
S.2.10	Large diameter pipelines (PLG)	Low	0.3
S.2.11	Column-type equipment processing liquids	High	0.7
S.2.12	Column-type equipment processing cryogenic liquids	Medium	0.5
S.2.13	Column-type equipment processing gases	Medium	0.5
S.2.14	Column-type equipment processing low vapour pressure liquids	Medium	0.5
S.2.15	Column-type equipment processing PLG	Low	0.3
S.2.16	Reactors/ heat-exchangers processing liquids	High	0.7
S.2.17	Column-type equipment processing cryogenic liquids	Medium	0.5
S.2.18	Reactors/ heat-exchangers processing gases	Low	0.3
S.2.19	Reactors/ heat-exchangers processing low vapour pressure liquids	Low	0.3
S.2.20	Reactors/ heat-exchangers processing PLG	Low	0.3

4. Evaluation of the likelihood of attack success through the assessment of Physical Protection Systems

The proposed approach evaluates the probability of attack success as the complement to 1 of the probability of the physical protection system being effective against the attack. In the present study, the considered assets potentially targeted are process and storage equipment; hence, the relevant security countermeasures against an attack are mainly Physical Protection Systems (PPSs). The primary functions for which PPSs are designed are (Garcia, 2008): i) detection, which is the discovery of an adversary action followed by an alarm notification and proper alarm assessment ; ii) delay, which is the slowing down of adversary progress; and iii) response, which consists of the action taken by the response force to prevent adversary success. For the PPS to be effective, all the three functions must be performed in the given order: in other words, the overall system is effective if timely interruption of attacker's path of actions occurs (Garcia, 2006).

The metric used in the Sandia model (Garcia, 2006) was adopted to define overall performance variables that characterize the effectiveness of the functional sub-systems of PPS in terms of probability and the probability of attack success (P_{AS}) was calculated according to Eq. (2):

$$P_{AS} = 1 - (P_{AD} \times P_C \times P_{TR}) \tag{2}$$

where P_{AD} is the probability of assessed detection, which is calculated according to Eq. (3) as a cumulative probability, if *i* independent Ring of Protections where detection can occur are in place; P_C is the probability of effective communication to response force; P_{TR} is the probability of having a timely intervention of the response force, which is calculated according to Eq. (4) assuming normal distributions for time parameters characterizing the response force intervention and adversary's tasks duration, where T_{Di} = time duration of task *i*, and RFT= response force intervention time:

$$P_{AD} = 1 - \prod_{1=1}^{k} \left(1 - P_{AD,i}\right) \tag{3}$$

$$P_T = \int_0^T \frac{1}{\sqrt{2\pi\left(\sigma_{RFT}^2 + \sigma_D^2\right)}} e^{-\frac{T^2}{\sigma_{RFT}^2 + \sigma_D^2}} dT; \quad T = \sum_{i=k+1}^{m} T_{Di} - RFT \tag{4}$$

The so defined overall performance variables are those applied in the quantitative characterization of the nodes N.5, N.6, N.7 in Figure 1. Prior to apply Eqs. (2-4), path analysis has to be conducted to identify the possible paths that adversaries may use to enter the site and reach the selected target equipment and the PPS elements present along each of those paths. It should be noted that the use of Eq. (2) implies that, in order to successfully execute the attack, the adversary has to devote efforts to entering the site and going in close proximity of the target. This formulation matches well with the types of PPS and protections functions implemented in industrial sites; however, it is not applicable to the analysis of attack scenarios that involve the use of remotely controlled or long distance heavy weapons or other technologically sophisticated tools (e.g. RPG, drones).

5. Illustrative case study

In order to exemplify the application of the proposed approach to an industrial facility, a petroleum product terminal was considered. The scheme of the facility layout is given in Figure 2. The available PPSs consist in: i) a single line rigid fence with outriggers along the perimeter; ii) Access control based on shipment schedules, preannouncement of visitors and use of credentials (ID badges); iii) video motion detection system based the use of cameras mounted along the fence line, integrated with a display and control system that allows the remote assessment of an intrusion alarm by the security guard at the security post; iv) radio communication among security guards and to local law enforcement agencies with backup communication means; v) direct intervention of security guards working on site only in case of evidence of unarmed intruders.
For the sake of brevity, the numerical results obtained for an attack carried out by a terrorist acting alone (assimilated to a threat agent of category 2) through the path indicated by the dashed arrow in Figure 2 are reported in Table 2. The presented results were derived by quantifying the BN shown in Figure 1 through HUGIN Expert™ Software version 8.1.

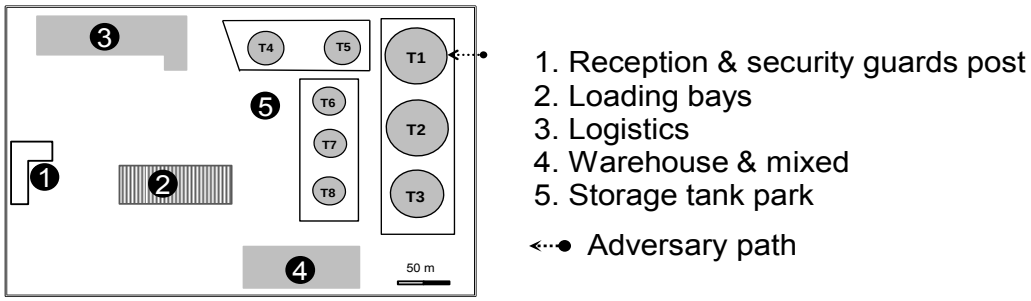

Figure 2: Simplified layout of the petroleum product terminal considered for the illustrative case study

Table 2: Prior probabilities for the illustrative case study

Node	State	Prior probability	Notes
Threat agent category	S.1.1, S.1.3	0	Assumed scenario
	S.1.2	1	Assumed scenario
Target equipment	S.2.1	1	From facility characterization
	S.2.2 to S.2.20	0	From facility characterization
Attack attempt	S.3.4	1	Assumed scenario
	S.3.1, 2, 3, 5, 6, 7	0	Assumed scenario
Security system intervention	Success	0.059	Calculated
	Failure	0.941	Calculated
Assessed Detection	Success	0.900	Data from (Garcia, 2008)
	Failure	0.100	Calculated
Communication to response force	Success	0.950	Data from (Garcia, 2008)
	Failure	0.050	Calculated
Timing of response force	Success	0.069	Calculated according to Eq. (4), task time data from (Garcia, 2008)
	Failure	0.931	Calculated
Attack success	True	0.941	Calculated
	False	0.059	Calculated

The obtained prior probabilities (see Table 2) show that the effectiveness of physical security systems in stopping the execution of an attack is low if not questionable (probability of success equal to 0.059). This is due to the fact that multiple security functions have to be executed in a timely manner in order to interrupt the adversary chain of actions, which requires few minutes to be completed. A worsening factor in the analyzed case study, which is however representative of real installations, is the absence of multiple detection and assessment elements (only a single ring of protection is in place) to defend outdoor process equipment that may actually represent an attractive target.

6. Conclusions

The evaluation of the likelihood contribution to security risk through a probabilistic approach has been discussed and exemplified. A BN-based model has been developed to support the assessment through the integration of quantitative statistical and performance data with probability estimates from expert elicitation.
The analysis of the case study evidenced that only a low level of protection against intentionally induced losses can be obtained if the “Defence in Depth” principle (IAEA, 1996) is not applied in the design of physical security elements. In fact, a highly effective countermeasure deploys concentric rings of protection to defend critical targets, where each ring represents an independent defence layer that accomplishes or triggers the success of primary protection functions of assessed detection, delay and response.

Reference

American Petroleum Institute (API), National Petrochemical and Refinery Association, 2003. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries. American Petroleum Institute, Washington, DC.Lou H.H., Muthusamy R., Huang Y., 2003. Process Security Assessment: Operational Space Classification and Process Security Index. Proc. Saf. Env. Protection, 81(B), 418-429.

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

Argenti F., Landucci G., Spadoni G., Cozzani V., 2015. The assessment of the attractiveness of process facilities to terrorist attacks. Safety Science, 77, 169-181.

Bajpai S., Gupta J.P., 2005. Site security for Chemical Process Industry. J. Loss. Prev. Process. Ind., 18 (4–6), 301–309.

Baybutt P., Reddy V., 2003. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homeland Defence Journal, 2, 1.

Bajpai S., Gupta J.P., 2007a. Securing oil and gas infrastructure. J. of Petroleum Sci Eng. 55, 174-186.

Bajpai S., Gupta J.P., 2007b. Terror proofing chemical process industries. Process Saf Environ, Trans IChemE, Part B, 85 (B6), 559-565.

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

European Commission, 2004. Regulation (EC) n. 725/2004 of the European Parliament and of the Council of 31 march 2004 on enhancing ship and port facility security. Off. J. Eur. Union L129, 6–91.

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. Union L345, 75–82.

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

Garcia M. L., 2008. The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, Newtown, MA.

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

Jensen F.V., Nielsen T.D., 2007. Bayesian networks and decision graphs. 2nd ed. Springer, New York, NY.

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

Reniers G., Van Lerberghe P., Van Gulijk C., 2015. Security Risk Assessment and Protection in the Chemical and Process Industry. Process Saf Progr,34, 1, 72-83.

Sabatini M., Zanelli S., Ganapini S., Bonvicini S., Cozzani V., 2009, Ranking the attractiveness of industrial plants to external acts of interference. Safety, Reliability and Risk Analysis: Theory, Methods and Applications - Proceedings of the Joint ESREL and SRA-Europe Conference, 2, 1199-1205.

Salzano E., Landucci G., Reniers G., Cozzani V., 2014, Domino effects related to home-made explosives, Chemical Engineering Transactions, 36, 349-354 DOI: 10.3303/CET1436059

Störfallkommission (SFK), 2002. SFK – GS – 38, Report of the German Hazardous Incident Commission. Störfallkommission, Baden, Germany.

Weber P., Medina-Oliva G., Simon C., Iung B., 2012. Overview on Bayesian Networks applications for dependability, risk analysis and maintenance area. Eng App Artif Intel, 25, 671-682.