CHEMICAL ENGINEERING TRANSACTIONS
VOL. 111, 2024
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers

ISBN 979-12-81206-11-3; **ISSN** 2283-9216
DOI: 10.3303/CET24111082

Securing Chemical Facilities Against Intentional Attacks: a Bayesian Network Approach for Asset Risk Assessment

Giulia Marroni[a], Valeria Casson Moreno[a], Sanneke Kuipers[b], Marcello Mossa Verre[c], Gabriele Landucci[a,*]

[a] Department of Civil and Industrial Engineering, University of Pisa, Largo Lucio Lazzarino 2, 56126 Pisa, Italy
[b] Institute of Security and Global Affairs, Leiden University, Turfmarkt 99, 2211 DP Den Haag, the Netherlands
[c] Regional Agency for Environmental Protection of Tuscany (ARPAT), Via del Ponte alle Mosse 211, 50144 Firenze, Italy
gabriele.landucci@unipi.it

The consequences of a successful intentional attack to a process facility can be severe and could propagate among units generating the so-called domino effects, with potential effects on people, the environment, and assets. For these reasons, institutions and practitioners have found interest in determining the entity of damages associated with these events and integrating them into conventional safety and economic analyses. Still, approaches devoted to assessing the economic losses associated with intentional attacks have received less attention in the literature. This work presents a methodology to evaluate asset losses associated to intentional attacks. A probabilistic approach based on Bayesian Networks was adopted to include several factors associated to intrusion scenarios and their interdependencies. The developed methodology was then applied to a case study to demonstrate its potentialities. A demonstrational attack scenario was considered to test the methodology. The results show that a successful intentional attack might indeed lead not only to direct consequences on people, but also to relevant economical losses. Moreover, factoring in the synergistic performance of safety and security barriers allows to improve the estimation of asset losses.

1. Introduction

The assessment of scenarios associated with intentional attacks to chemical and process facilities has garnered the attention of both institution and practitioners because of the exacerbation of conflicts in critical contexts. The consequences of a successful intentional attack can be severe and could propagate among units generating the domino effects, with potential effects on people, the environment and assets (George and Renjith, 2021). For these reasons, assessing the entity of damages associated with successful intentional attacks and integrating them into conventional safety and economic analyses is a crucial point to protect installations and citizens, which was extensively studied in the literature. For instance, Shuaiqi et al. (2022) developed a theoretical framework for the integration of safety and security barriers. Still, no works were devoted to the quantitative integration of safety and security, and more specifically of safety and security barriers in scenario assessment. Moreover, methodologies that tackle the assessment of asset losses following an intentional attack are lacking. In this framework, Bayesian Network (BN) are a promising tool for a probabilistic-based assessment of economic losses. Namely, BN are a versatile tool that can include a high number of elements and dependencies. The use of such a tool is not new in security science and process safety, as scenarios tend to be complex and dependent on many different factors (George and Renjith, 2021). For instance, BN was adopted to assess the efficacy of fire-fighting protections (Khakzad et al., 2018) and allocate countermeasures in critical infrastructures (Misuri et al., 2018). Iaiani et al. (2022) used BN to quantitatively assess the vulnerability, i.e., the probability of attack success in Offshore Oil&Gas installations, while BN was adopted to assess the vulnerability of process installations (Marroni et al., 2024). For this reason, this work shows a methodology to assess the economic losses associated to intentional attack scenarios considering the synergistic performance of safety and security barriers and potential domino effects. A probabilistic approach based on Bayesian Network (BN) has been adopted to determine the economic losses associated to intentional attacks.

Paper Received: 27 January 2024; Revised: 12 April 2024; Accepted: 4 July 2024
Please cite this article as: Marroni G., Casson Moreno V., Kuipers S., Mossa Verre M., Landucci G., 2024, Securing Chemical Facilities Against Intentional Attacks: a Bayesian Network Approach for Asset Risk Assessment, Chemical Engineering Transactions, 111, 487-492 DOI:10.3303/CET24111082

2. Methodology

2.1 Overview

Figure 1 shows the proposed methodological approach. Step 1 is detailed in Section 2.2 and entails the simplified assessment of the safety-security related scenario, including probability of attack success and consequence assessment. The second step of the methodology is the evaluation of economic losses using a consequence-based approach presented in Section 2.3. Step 3 of the methodology is the implementation of Steps 1 and 2 in the BN, which is shown in Section 2.4. Finally, Step 4 of the methodology is the application of Steps 1, 2, and 3 to a demonstrational case study, which is presented in Section 3. The results are discussed in Section 4, while Section 5 offers some conclusive remarks.

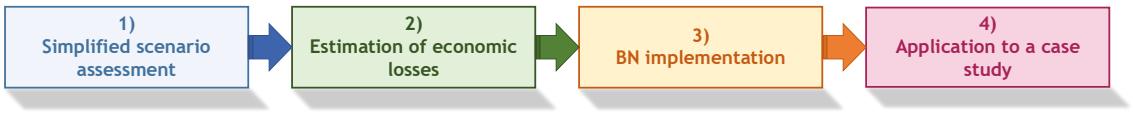


Figure 1: Proposed methodology for assessing the economic losses associated with intentional attacks

2.2 Simplified scenario assessment

The first step (see Figure 1) is aimed at the quantitative evaluation of the intentional attack scenario, from intrusion to final outcomes. Hence, it is firstly necessary to assess potential threats, and their attack paths. Although some more structured methodologies are available, in this work we used a simplified method, i.e., expert judgement, to determine the attack path of the demonstrational case study in Section 3. Then, the vulnerability of the plant to the attack scenarios should be evaluated. There are two main factors influencing the probability of an intentional attack being successful: the performance of security barriers in place and the fragility of the target equipment, i.e., its physical resistance to an attack vector. For security barriers, the performance of three main functions associated to a correctly functioning system are evaluated: intrusion assessed detection, communication to emergency response system, and its timely intervention to neutralize the attack (Garcia, 2006). As for the physical resistance of the equipment, specific fragility models tailored to the attack mode are used in order to determine the probability of the equipment being damaged based on the intensity of physical effects; see (Marroni et al., 2024) for more details.
Once the vulnerability of the scenarios has been evaluated, consequence assessment was carried out. The release scenarios were defined by tailoring conventional release diameters (API, 2008) to security scenarios. More in detail, a small release diameter of 1'' (25.4 mm) was associated to sabotage, while a catastrophic rupture was the outcome of explosive attacks. The release scenarios were then simulated through integral models using the software ALOHA®. A threshold-based approach was used to assess potential domino effects: if the intensity of the physical effect is higher than the threshold values, then the equipment is involved in the domino chain. Fragility models are then used to calculate the damage probability of such equipment (Marroni et al., 2024). Instead, if the physical effect is below the threshold, the equipment is excluded from the domino scenario. The threshold values are extensively discussed and reported elsewhere (Reniers and Cozzani, 2013).

2.3 Estimation of economic losses

To estimate the economic losses, two factors were taken into consideration: the price of the damaged equipment, and the price of the stored substance. To estimate the price of equipment, different approaches can be used. In this work, the total cost of the equipment is composed by price of materials, installation, instrumentation and controls, auxiliary piping, electrical system, and manufacturing. While the price of materials can be easily retrieved from suppliers' data, the other costs are more difficult to evaluate, hence they were scaled on the price according to Table 1.

Table 1: Multiplying factors for the evaluation of equipment costs.

Cost item	Percent of cost of materials [%]	Source
Installation	47.00	(Peters et al., 2013)
Instrumentation & Control	36.00	(Peters et al., 2013)
Piping	68.00	(Peters et al., 2013)
Electrical Systems	11.00	(Peters et al., 2013)
Manufacturing	100.00	Assumption
Safety factor	100.00	Assumption

The manufacturing costs were assumed 100% of the price of materials, to conservatively cover for all operations required to treat the materials; the same assumption was made for the safety factor: namely, there are many uncertainties connected to these cost items, thus a higher safety factor was considered. Suppliers' data can be consulted to obtain the retail price of the stored substance, while official sources may provide commodities costs. In this work, the price of not only primary equipment, but also secondary equipment involved in the accidental scenario has been considered.

2.4 Bayesian Network implementation

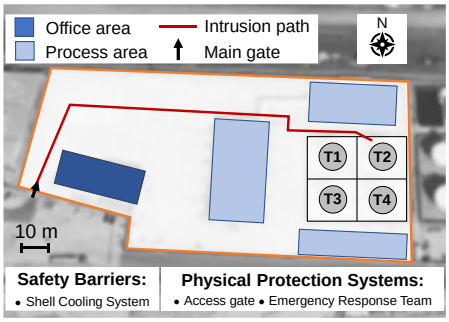
BN are a tool to model probabilistic dependencies among a set of variables. It is composed of nodes, which represent the variables, and arcs, which represent the relations among nodes. Nodes with arcs directed from them are called parents, while nodes with arcs directed to them are called children. The probability of an occurrence *P(A)* can be evaluated based on the conditional probabilities of parent nodes, according to Eq. 1:

$$P(A) = \prod_{i=1}^{n} P(G_i|Pa(G_i)) \quad (1)$$

where G_i are parents nodes of *A*, and $Pa(G_i)$ are the parents of G_i. BN are an appropriate tool to handle a wide range of variables with complex inter-dependencies; moreover, the network can be updates using Bayes theorem, once new evidence enters the network. The software GeNIe Modeler was used in this work to model the BN. More in detail, all variables were considered as discrete, hence the BN is quantified if all Conditional Probability Tables (CPTs) of variables are complete. Four main groups of variables have been modeled in the BN proposed in this work. The first group is composed by all nodes that represent the performance of security barriers, the modelling of the CPTs of this group of nodes has been object of several works, hence the Reader is referred to (Marroni et al., 2024) and (Securdomino, 2024) for more details. The second group represents all equipment involved in the analysis; to complete the CPTs of this group, it is necessary to compute the probability of the equipment being damaged following the approach shown in Section 2.2. The third group represents the safety barriers; the CPTs for these group account for the availability and effectiveness of the barriers following the approach proposed by (Khakzad et al., 2018). The last group is composed by a utility node, which is a special type of node used to assess the value of a utility function. In our work, the utility function is the total economic losses expressed in M$. The CPT of this group can be thus filled by evaluating the total economic losses for each combination of parent nodes. Considering the complexity of BN and the wide range of information needed, the Reader is referred to the literature suggested above. However, a more detailed analysis of quantitative data is available in Section 4 related to the results of the case study.

3. Application to a case study

The methodology has been applied to a demonstration case study consisting of a depot of petroleum products located in the Netherlands. Figure 2 shows the layout of the plant.



ID	Content	Height [m]	Diameter [m]	Capacity [m^3]	Filling Level [%]	Dike Height [m]
T1	Gasoline	12.00	11.00	912	60.00	3.00
T2	Gasoline	12.00	11.00	912	100.00	3.00
T3	Gasoline	12.00	11.00	912	40.00	3.00
T4	Gasoline	12.00	11.00	912	20.00	3.00

Figure 2: Layout of the demonstration case study and information on target equipment

T1-T4 are four gasoline fixed-roof atmospheric tanks made of carbon steel. Figure 2 also shows the characteristics of the equipment. All four tanks are protected by a shell cooling system, which activates in case of external fire. The plant is protected by an external wall, which has only one access gate. A site emergency response is available to protect the facility, and its intervention time is assumed to be 240s (Garcia, 2006).

Figure 2 also shows the intrusion path. The intrusion scenario takes place at night, while the atmosphere is in stability condition F and the wind blows from west at 2 m/s. The intruder trespasses the main gate, and targets T2 using 15 kg of triacetone triperoxide, an explosive which can be home made. In case of successful attack, T2 undergoes catastrophic rupture with instantaneous release of its content. The ignition of the gasoline pool leads to a pool fire, which heat radiation affects tanks T1, T3, and T4.

4. Results and discussion

In order to assess the contribution of the different types of barriers included in the analysis, three different BN were created, as shown in the three panels of Figure 3.

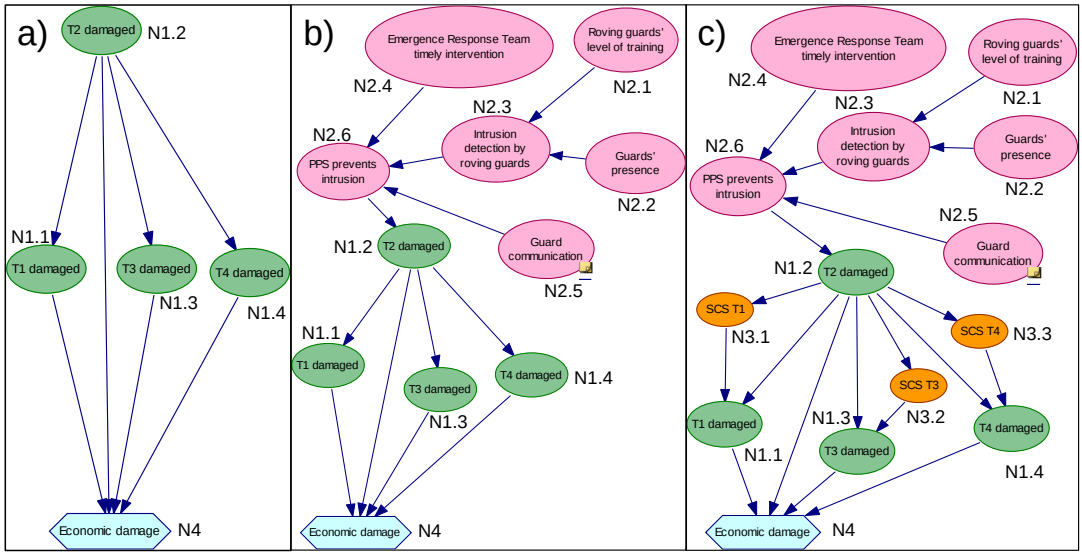


Figure 3: BN built for the demonstrational case study. a) case with no barriers; b) case with only security barriers and c); SCS = shell cooling system; PPS = security barriers

In the first BN (Figure 3a), the contribution of any barriers was neglected. This constitutes a baseline, very conservative case, in which a unitary probability of the threat successfully reaching the target is considered. Hence, the only present nodes are the one related to the equipment (N1-1-N1.4, the green nodes) and the utility node to assess the economic losses (N4, the blue node). The second BN (Figure 3b) only accounts for the performance of security barriers. So, the pink nodes N2.1-N2.6 are added to the network. Finally, the third BN (Figure 3c) is build considering the performance of both safety and security barriers. In this case, the orange nodes N3.1-N3.3 are added. Nodes N1.1 to N1.4 represent the damage state of the equipment. To quantify them, the physical effects associated to the intentional attack should be firstly quantified; the explosive attack leads to the instantaneous release of the gasoline in T2, with a consequent pool fire. Gasoline was modelled on ALOHA as n-heptane, and the source term was modeled as a “burning puddle”. ALOHA then computes heat radiation point values at target positions; for example, the heat radiation on T3 is 42.6 kW/m^2. T3 is therefore part of the domino chain, as the threshold value suggested in (Reniers and Cozzani, 2013) for atmospheric vessels is 15 kW/m^2. The same calculations were carried out for T1 and T4, resulting in both tanks also being involved in the domino chain. To consequently quantify the damage probability, specific fragility models were used (Marroni et al., 2024), and the CPTs of the specific targets were filled using the obtained damage probabilities. More specifically, a fragility model for explosive attacks was used to quantify N1.2 related to T2, while a fragility model for heat radiation was used to quantify N1.1, N1.3, and N1.4. For example, the probability of T3 being in the damaged state due to the heat radiation is 92%. Nodes N2.1 to N2.6 represent the performance of security barriers. To quantify N2.1, N2.2, and N2.3, the performance and probability dataset from (Argenti et al., 2017) was used. N2.4 is instead quantified based on the comparison between the time needed by the attacker to perform the attack, and the time needed by the emergency team to intervene, as suggested by (Garcia et al., 2006). The attack can be stopped only if the time needed by the threat is higher than the one needed by the emergency team. As for Node 2.5, a standard value of 95% is suggested by (Garcia et al., 2006). As for Node 2.6, it can be quantified considering an AND gate among all parent nodes: security barriers are successful only if all three functions are completed. To quantify Nodes N3.1 to N3.3, the data from (Khakzad et al., 2018) were used; it was assumed that all three barriers have the same performance parameters.

Finally, to quantify Node N4, the economic evaluations were carried out. Using suppliers' data on carbon steel, the price of materials was estimated around 0.03 M$. Considering all the pricing factors in Table 1, a total price of 0.17 M$ for each equipment was estimated. As for the content, the average retail price of gasoline in January 2024 in the Netherlands was retrieved from (Centraal Bureau voor de Statistiek, 2024). Namely, the highest losses are around 1.90 M$ for tank T2 (see Figure 2), because the tank is completely filled. Table 4 reports the prior probabilities of the main nodes related to barriers in the analysis.

Table 4: Prior probabilities of selected nodes of the quantified BN. For case descriptions refer to Figure 3.

Node ID	N2.1	N2.2	N2.3	N2.4	N2.5	N2.6	N3.1	N3.2	N3.3
Case	b), c)	b), c)	b), c)	b), c)	b), c)	b), c)	c)	c)	c)
State	High	Present	Detection	Success	Success	Success	Success	Success	Success
Prior Probability	0.85	0.40	0.30	0.38	0.95	0.11	0.96	0.96	0.96

As it can be seen, the prior probabilities of safety barriers (Nodes 3) are higher than that of security barriers (Nodes 2). This is due to the fact that the considered security barriers are strongly based on human action, which tends to be less reliable than an automated system such as a shell cooling system. The detection function of security barriers could be improved by the use of automatic systems, such Closed Circuit Television or Intrusion Detection Systems. However, the bottleneck of the process still remains the intervention of the emergency team (Node 2.4), which cannot be substituted by automated systems. Hence, the management should invest not only in automated detection systems, but also in the training of the emergency team.
Figure 4 reports the values of Nodes N1.1, 1.2, 1.3, 1.4 and N4 in the three different cases shown in Figure 3.

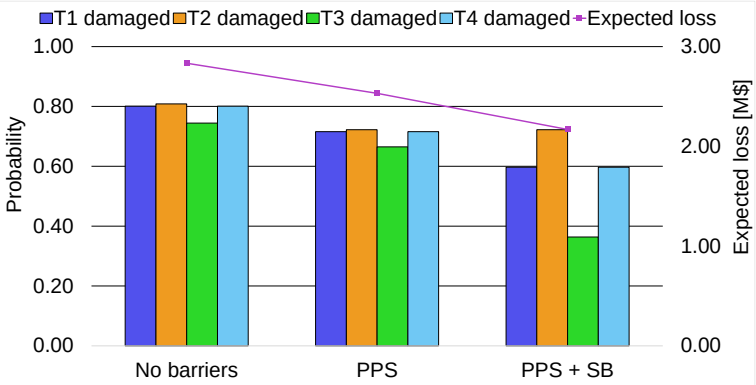


Figure 4: Results of the application of the methodology to the case study; PPS = Security barriers; SB = Safety barriers

The first thing that can be noticed is that all vessels are included in the scenario, meaning that there is a severe domino effect escalation. In the case without barriers, all vessels have more than 70% probability to be damaged. In case the performance of safety barriers is considered, the probability of damaging the tanks reduces by 10%. A higher impact is observed considering the synergistic effect of safety and security barriers. Namely, the successful intervention of the shell cooling system significantly mitigates the received heat radiation, causing a 50% decrease in the damage probability of T3. For T1 and T2, a reduction of 25% in vulnerability can instead be observed. This shows how considering the intervention of safety barriers in security scenarios is essential in order to better identify the vulnerabilities of process facilities. As for the economic losses, they are in the order of 3M$ in all three cases; this is reasonable as gasoline tends to be a very profitable product, hence the majority of the losses are associated with the loss of product, rather than to the loss of the equipment. A different result could be obtained if a less profitable but still hazardous chemical is stored in the tanks. Also, some tanks might be more sophisticated than the ones in this work, contributing to more significant costs. More specifically, economic losses have a 10% drop if only security barriers are considered; instead, the synergistic performance of safety and security barriers causes an almost 25% reduction of economic losses compared to the case with no barriers.
A better understanding of which barriers impact both the vulnerability and the economic losses associated to intentional attacks can guide plant managers in choosing correct defense strategies.

5. Conclusions

Although the interest of institutions and researchers to intentional attacks to process facilities has risen in the last years, there is still a lack of methodologies that account for the economic losses associated with such critical events. Moreover, available approaches are not able to cope with the synergic performance of safety and security barriers. For this reason, this work explored a BN methodology to evaluate economic losses considering the combined performance of safety and security barriers. The application to the case study demonstrated that safety barriers play a key role in the de-escalation of release scenarios associated to intentional events, which can be more severe compared to unintentional accidents. The presented methodology can be further improved. First of all, the expression of the economic losses can be refined by including factors such as plant expected downtime, reputational losses, and insurance costs. Then, by adding other utility gates, e.g., costs of barriers, the BN can be turned into a proper tool to easily carry out cost-benefit analyses. One drawback is that the so-obtained BN might become very extensive, implying the need for some time to properly build and quantify it. Moreover, more efforts are needed in order to gather all necessary data for the methodology, which might be hard to retrieve. To conclude, the combined performance of safety and security should be considered to better define asset losses, and to avoid over-conservative estimations. The developed methodology can thus support plant managers practitioners in choosing where defence resources should be allocated.

Acknowledgments

This study was in part developed within the project LIFE20 ENV/IT/000436 –LIFE SECURDOMINO “Seveso sites: assessment of integrated safety-security hazards and risks and related domino effects” with the contribution of LIFE program of the European Union.

References

API (American Petroleum Institute), 2008, ANSI/API Standard 581 – Risk-based Inspection Technologies, American Petroleum Industry, Washington DC; USA.

Argenti F., Landucci G., Cozzani V., Reniers G., 2017, A study on the performance assessment of anti-terrorism physical protection systems in chemical plants, Safety Science, 94, 181-196

Centraal Bureau voor de Statistiek, 2024, Pump prices motor fuels; location petrol station, type fuel, https://www.cbs.nl/en-gb/figures/detail/81567ENG, accessed 29.02.2024

Iaiani M., Tugnoli A., Cozzani V., Reniers G., Yang M., 2023, Quantitative Evaluation of the Probability of Success of Deliberate Attacks in the Offshore Oil&Gas Industry, Chemical Engineering Transactions, 99, 121-126

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

George P.G., Renjith V.R., 2021, Evolution of Safety and Security Risk Assessment methodologies towards the use of Bayesian Networks in Process Industries, Process Safety and Environmental Protection, 149, 758-775

Khakzad N., Landucci G., Cozzani V., Reniers G., Pasman H., 2018, Cost-effective fire protection of chemical plants against domino effects, Reliability Engineering & System Safety, 169, 412-421.

Marroni G., Casini L., Bartolucci A., Kuipers S., Casson Moreno V., Landucci G., 2024, Development of fragility models for process equipment affected by physical security attacks, Reliability Engineering & System Safety, 243, 109880

Misuri A., Khakzad N., Reniers G., Cozzani V., 2018, Security Management of Process Plants by a Bayesian Network Methodology, Chemical Engineering Transactions, 67, 247-252

Peters M.S., Timmerhaus K.D., West R.E., 2013, Plant design and economics for chemical engineers, McGraw-Hill Education, New York NY, USA

Reniers G., Cozzani V., 2013, Domino Effect in the Process Industries, Elsevier, Amsterdam, The Netherlands

Securdomino, 2024, Open repository of models and barriers data <https://securdomino.eu/open-web-repository/>, accessed 28.02.2024.

Shuaiqi Y., Reniers G., Yang M., 2022, The Necessity of Integrating Safety and Security Barriers in the Chemical and Process Industries and its Potential Framework, Chemical Engineering Transactions, 91, 13-18.