Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4629-cd

Quantitative Analysis of Economic Losses Induced by Malevolent Acts of Interference to Process Facilities

Giulia Marroni, Michela Guarguaglini

Department of Civil and Industrial Engineering, Università di Pisa, Italy
E-mail: giulia.marroni@phd.unipi.it, michela.guarguaglini@phd.unipi.it

Wout Broekema, Sanneke Kuipers

Institute of Security and Global Affairs, Universiteit Leiden, the Netherlands
E-mail: w.g.broekema@fgga.leidenuniv.nl; s.l.kuipers@fgga.leidenuniv.nl

Dino Dentone

DataCH Technologies, Italy
E-mail: dino.dentone@datach.it

Valeria Casson Moreno, Gabriele Landucci

Department of Civil and Industrial Engineering, Università di Pisa, Italy
E-mail: valeria.cassonmoreno@unipi.it; gabriele.landucci@unipi.it

Intentional attacks on chemical and process installations have intensified in recent years due to the exacerbation of conflicts in critical areas. These attacks can escalate affecting nearby areas, potentially triggering domino effects with severe impact on assets, people, and the environment. Existing security studies primarily focused on impacts to people, with limited focus on economic losses and the combined effect of safety and security barriers in managing external attack scenarios. This work addresses this gap by assessing the extent of damages from such threats and integrating these findings into safety and economic analyses. To achieve this, a cost-benefit analysis tool was developed. The tool is based on a probabilistic approach and evaluates different protection strategies against intentional attacks to process facilities. A Bayesian Network (BN) model is used to handle the complexity of attack scenarios. Damages are incorporated in the BN, along with the cost of safety and security barriers, through a dedicated cost-benefit function. A demonstrative case study highlights the benefits and limitations of the methodology, showing the influence of barriers on economic losses, and driving the selection of the more effective protection strategy for industrial facilities. This research addresses key gaps in integrating safety and security within industrial risk management and provides a flexible tool for optimizing resources when facing complex threats.

Keywords: Physical security, Security management, Economic losses, Bayesian Networks, Cascading events, cost-benefit analysis, domino effects

1. Introduction

The study of intentional attacks to chemical and process facilities is a topic that gained relevant attention in the last two decades. Namely, these attacks can have severe consequences, which could escalate towards neighbouring units, generating intentional domino effects, ultimately affecting people, assets, and the environment (George and Renjith, 2021).

Intentional attacks are intrinsically dynamic in nature, and have a complex escalation potential. For this reason, interest should be taken not only on the potential effects on people, but also on asset and property. For example, Khakzad et al. (2017) explored the propagation of domino effects using graph-based methods. In this framework, Bayesian Networks (BN) are a promising tool to address the effects on property, because of the wide range of parameters than can be considered and the possibility of updating the network once new evidence is available. BN have been often employed to support decision making

in critical infrastructures. Misuri et al. (2019) developed an influence diagram using BN to evaluate the efficacy of different types of barriers. Witte et al. (2022) developed a method to assess the uncertainties related to cost-benefit design for civil structures, such as airports. Roy (2022) studied a risk-based strategy for the optimization of conventional safety barriers. Villa et al. (2017) developed a model to evaluate the feasibility of security countermeasures through the formulation of a constrained optimization problem. However, limited studies (Misuri et al., 2019; Witte et al., 2022) were devoted to consolidating the potentialities of BN in supporting cost-benefit analyses to allocate safety and security protections in chemical facilities.

The aim of this work is to explore cost-benefit analysis when it comes to protecting chemical and process plants from integrated safety and security threats. More specifically, the economic feasibility of the installation of safety and security measures has been investigated.

The developed methodology is of probabilistic nature. While intentional attacks have a non-probabilistic component—such as predicting when they will occur—they also involve decision-making processes that often follow recognizable patterns. Assuming that an attack has already taken place, a probabilistic approach is therefore suitable. Considering the various factors influencing both the attack's characteristics and the effectiveness of barriers in mitigating its success, Bayesian Networks (BN) have been employed.

2. Methodology

The methodology we used consists of three consecutive steps, as shown in Fig. 1.

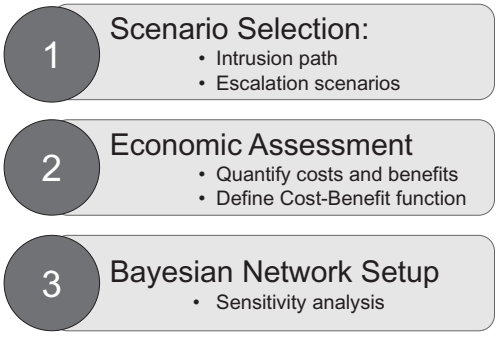

Fig. 1. Methodology used for the economic analysis

Step 1 is dedicated to the selection of the scenario; this includes both the intrusion scenario, as well as potential domino effects generated by a successful attack. Step 2 is the economic assessment based on two sub-steps. Firstly, the costs associated with a successful attack are evaluated along with the costs of different sets of countermeasures. Then, a Cost-Benefit function is developed to study the effectiveness of protection plans. In Step 3, Step 1 and 2 are implemented in the BN model: different nodes are selected to represent the scenario and the cost-benefit analysis. As the economic assessment can be subjected to uncertainty, a sensitivity analysis is carried out by varying the costs of the different protection strategies adopted.

2.1. *Scenario selection*

The first step of the methodology in Fig. 1 is devoted to the quantitative evaluation of the attack scenario, which was adapted from Marroni et al. (2024a).

First, intrusion paths are determined. Credible intrusion paths were determined using expert judgement; a multi-disciplinary group of experts merged their know-how to identify critical paths for the case study in Section 3. Then, the probability of attack success should be evaluated. The probability of attack success is composed of two factors: the performance of security barriers, and the fragility of the equipment, i.e., its resistance to the attack vector. The performance of security barriers is modelled following the approach from Garcia (2008): the attack can be successfully interrupted only if it is firstly detected, and the emergency response team successfully acts to stop the action. The physical resistance of the target to the attack can be evaluated using specific fragility models, which allow for the evaluation of the probability of damage based on the dose of attack vector. The Reader is referred to Marroni et al. (2024b) for more details.

Then, consequence assessment is carried out. As release diameters for security scenarios are not available, conventional release diameters are adapted from API (2008). More specifically, an equivalent release diameter of 1'' (25.4 mm) can be considered for sabotages, while a catastrophic rupture is conservatively considered for explosive attacks. The physical effects are

simulated using integral models implemented in the software ALOHA® (United States Environmental Protection Agency, 2024).

A threshold-based approach is adopted to evaluate potential domino scenarios following a successful intentional attack. Namely, a piece of equipment is considered affected by an accident scenario triggered by the attack, thus participating in the domino effect chain, if the intensity of the physical effect at the target equipment is above the threshold value. In that case, fragility models are used to evaluate the probability of damage (Marroni et al., 2024b). A comprehensive explanation of threshold-based approaches in domino effect assessment is reported in Cozzani and Reniers (2013).

It should be noted that the presence of safety barriers can mitigate the dose of physical effect. For example, a sprinkler system, if correctly working, might mitigate the heat radiated from a fire. This effect is accounted for by introducing an attenuation factor, φ. The attenuation factor indicates the percentual reduction of dose of physical effect on a target equipment and it can vary according to the different type of barrier.

2.2. *Economic assessment*

The first part of Step 2 of the methodology in Fig. 1 is the assessment of economic losses and of the costs of additional protection solutions. To evaluate the economic losses, the expenditure on stored substance E_s, as well as the expenditure on the equipment E_e are considered. The retail price of substances can be retrieved directly from suppliers'; in case of commodities (natural gas, gasoline, etc.), official sources may be used to retrieve the price.

Different strategies can instead be adopted to estimate the price of the equipment; firstly, vendor data can be used. If vendor data are hard to retrieve, then the cost of the equipment can be scaled on the price of the materials: the cost for manufacturing, instrumentation, auxiliary piping etc., can be scaled on the price of equipment using appropriate factors, as shown in Marroni et al. (2023). The economic loss L_{ik} associated to attack scenario i and equipment k is thus evaluated according to Eq.(1):

$$L_{ik} = \sum_{k=1}^{n} E_{s,ik} + E_{e,ik} \quad (1)$$

where n is the number of equipment actually damaged in scenario i.

The cost of countermeasures is evaluated using either vendor data or literature sources: for example, Janssen et al. (2015) provided the cost of safety barriers, C_{Saf}, while in Villa et al. (2017) the costs for some security countermeasures, C_{Sec}, are available. The total cost for protection strategy j, C_j, is:

$$C_j = C_{Saf,j} + C_{Sec,j} \quad (2)$$

Once losses and costs have been evaluated, a The Cost-Benefit Function (CBF) has been implemented for each protection strategy associated with an attack scenario. The CBF is obtained combining Eq. (3), Eq. (4) and Eq. (5).

$$CBF_{ij} = CBF_{B,ij} - CBF_{P,ij} \quad (3)$$

$$CBF_{B_{ij}} = \frac{\sum_{j=1}^{n} P_{B,ik} \cdot L_{ik}}{C_j} \quad (4)$$

$$CBF_{Pij} = \frac{\sum_{j=1}^{n} P_{P,ijk} \cdot L_{ik}}{C_j} \quad (5)$$

where $P_{B,ik}$ is the probability of damaging asset k in the baseline case, and $P_{P,ijk}$ is the probability of damaging it with protection strategy j implemented. Hence, CBF_{ij} represents the reduction in expected losses per cost of implemented strategy. An high value of CBF_{ij} represents a favourable protection strategy, because $P_{P,ijk}$ is greatly reduced and/or C_j is low. This type of CBF is meaningful when both the economic losses L_i and the cost C_j of different strategies are of comparable magnitude. This ensures that extreme CBF values are not driven by disproportionate inputs, such as exceptionally low costs or excessively high losses. This approach is less comprehensive compared to other metrics adopted in Cost-Benefit analysis (Mishan and Quah, 2020), which can incorporate other variables, such as an available budget for the protection strategies, and the discount rate to account for the value of money in time. For a broader perspective on alternative methodologies and applications of Cost-Benefit Analysis in security applications, readers are encouraged to consult the works cited in the Introduction. Nonetheless, the simplified CBF in Eq.(3) serves

as a practical basis in the context of this specific work.

2.3. *BN setup*

BN are employed in this work to model the probabilistic dependencies among the variables introduced in Section 2.1 and 2.2. In BN, such variables are represented through nodes, and the relationships among variables are represented through nodes. Nodes with only arcs directed from them are called parent nodes, while nodes with arcs directed to them are called children. The probability of an occurrence *P(x)* can be calculated according to Eq.(6).

$$P(x) = \prod_{k=1}^{m} P(v_k | Pa(v_k)) \quad (6)$$

where v_k is the parent set of x, and $Pa(v_k)$ are the parent nodes of v_k. The network can be updated using Bayes Theorem once new evidence enters the network, which allows to study the influence of different parameters on the overall network. In this work, the software GeNIe Modeler (Bayesfusion LLC, 2024) was used to build the BN. GeNIe supports the modelling of different variable domains; in this analysis, all variables were considered discrete. Discrete variables can take on fixed states, such as "damaged" or "safe". To fully quantify the BN, it is necessary to populate the Conditional Probability Table (CPT) for all variables. Next, the variables modelled in the BN can be grouped based on their roles in the analysis.

The first group of variables is the baseline set of barriers, i.e., those barriers that are already in place; this group includes both safety and security barriers in their working or failure state. The CPTs of these variables can be filled using reliability data available either in literature or in commercial databases. The second group of variables represents the status of the equipment involved in the analysis, e.g., if the equipment is damaged by the attack or safe; the CPTs of these can be populated using the fragility approach shown in Section 2.1.

In addition to these, there are variables related to the decision-making. Decision alternatives are represented in the BN through a "Decision Node," which influences other nodes by allowing different CPTs to be defined for each option. The barriers considered in the decision alternatives are represented as children of the Decision Node.

Finally, the Cost-Benefit Function (CBF) is implemented in the BN using the "Utility Node," which is connected to the Decision Node and to nodes representing the tanks. Populating the Utility Node requires evaluating all combinations of decision options and damaged equipment states. More specifically, Utility Nodes were implemented, one for each term of CBF_{ij} in Eq. (3).

Given the complexity of the BN and the extensive data required for its quantification, the Reader is directed to the references cited earlier. Additionally, the quantitative analysis is detailed in Section 4, which discusses the results of the case study defined in Section 3.

3. Case Study

The methodology showed in Section 2 is applied to a case study, consisting in a depot of petroleum products located in Italy. The layout of the case study is shown in Fig. 2.

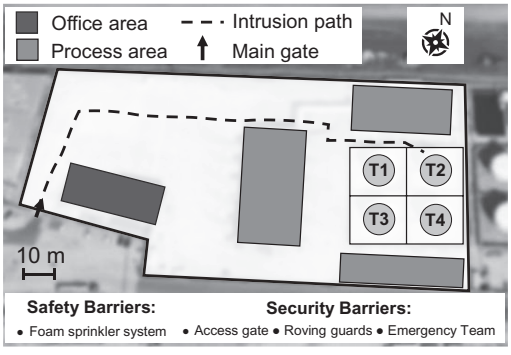

Fig. 2. Layout of the case study, adapted from (Marroni et al., 2024)

T1-T4 are fixed-roof atmospheric tanks, made in carbon steel, with a total volume of 1140 m^3 and a total capacity of 912 m^3; T1 and T2 store gasoline, while T3 and T4 store diesel fuel. According to suppliers' data (Matches, 2024), the cost of fixed-roof carbon steel tank is around 200 k€, while the average cost of gasoline and diesel is retrieved from Ministero dell'ambiente e della sicurezza energetica (2024). The total cost of a gasoline tank (T1 and T2) is therefore 1800 k€,

while the cost of a diesel tank (T3 and T4) is 1700 k€.

All tanks are protected by a foam sprinkler system. The facility is protected by an access gate, and also has roving guards.

The following attack scenario is studied: the attacker trespasses main gate using bolt cutters, walks 200 m towards T2 and detonates 15 kg of tricetone triperoxide, a home-made explosive. The intrusion scenario takes place during the day, and a condition of wind blowing at 5m/s and Pasquill stability class D is considered for consequence assessment. In the event of a successful attack, T2 undergoes a catastrophic rupture, with immediate ignition of the gasoline pool, leading to a pool fire, which could affect the nearby T1, T3, and T4. In relation to this scenario, the plant manager is considering the implementation of different protection strategies, which are shown in Table 1.

Table 1. Protection strategies studied in this work

Protection strategy	Barrier list	Price (k€)
A	VMD	150
B	SCS on T1 and T2	400
C	SCS on all tanks	800
D	VMD + SCS on T1 and T2	550
E	VMD + SCS on all tanks	900
F	Baseline set of barriers	-

VMD = Video Motion Detection
SCS = Shell Cooling System

The strategies in Table 1 are either security-based (A), safety based (B, C) or integrated safety and security (D, E) and are obtained through the combination of Video Motion Detection system, VMD) and a Shell Cooling System (SCS). The retail price of a high-quality VMD camera for ATEX applications is around 3 k€ based on suppliers' data (Atexshop, 2024). Considering the installation of a complete system, with multiple cameras, and the related electrical equipment, a conservative price of 150k€ is considered. For the SCS, the data from Janssen et al. (2015).

4. Results

The BN used for the cost-benefit analysis is shown in Fig. 3.

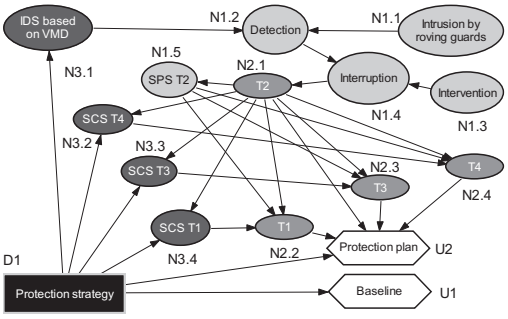

Fig. 3. BN used for economic assessment in this work

Nodes N1.1 to N1.4 are related to the security measures in place. N1.1 can be quantified using the data from Argenti et al. (2017): the probability of successful detection is 39.6%.The CPT of node N1.2 is populated assuming that the attack is detected only if at least one detection measure is effective.

Node 1.3 is related to the intervention and can be populated using the EASI approach proposed by Garcia (2008). To use the mentioned approach, delay times for the adversary should be evaluated using the data available in the original source: a total time for the attack of 214 s is obtained. On the other hand, the response time of the emergency team is assumed to be 240s. By comparing the attack time with the response time using the EASI approach, a 35% probability of intervention is obtained. The attack is halted (Node N1.4) only if the detection and the intervention are both successful. Node N1.5 is related to the performance of the sprinkler system (SPS), which is quantified using the probabilistic data available in Securdomino (2024): the probability of failure is 5.12%.

Node D1 is the decision node, which contains protection strategies A-E and the baseline case F (see Table 1). N3.1-N3.4 are the barriers to be implemented. The probability of failure of the VMD is 40% (Argenti et al., 2017). The performance of the SCS can be retrieved from Securdomino (2024) and the probability of failure is 4.43%. If a barrier is not contemplated in a protection strategy, then it is assumed to be in the failure state. This allows the completion of the CPTs of N3.1-N3.4. Nodes N2.1-N2.4 represent

the tanks. T2 is the target of the intentional attack, and its CPT can be evaluated using the fragility model for explosive attacks found in Marroni et al., 2024); for this attack scenario, the probability of damaging the equipment is 80.8%. To quantify N2.2, N2.3, and N2.4, the pool fire following the catastrophic release of gasoline is modelled in ALOHA® as pure n-hexane, and the release of the whole content of the tank is simulated. Hence, a confined rectangular pool the size of the catch basin (see Fig. 2) is simulated using the "Burning Puddle" model. ALOHA then computes the value of the heat radiation at given target positions. The outcome is that, without mitigation measures, all targets are involved in the domino effect chain. T4 is hit by the highest unmitigated radiation (44.5 kW/m^2), while T3 by the lowest (27.9 kW/m^2).

The mitigated radiation is evaluated using the attenuation factors: an attenuation factor of 40% is considered for the sprinkler system, while a reduction of 50% is considered for the shell cooling system (Securdomino, 2024). To populate the CPTs of N2.2, N2.3, N2.4, the probability of failure using the models in Marroni et al. (2024a) should be evaluate for the different dose of physical effects obtained combining the performance of the safety barriers. The SCS of T2 does not participate in the scenario because its function is to protect the target rather than act on the originating fire. Nonetheless, as a protection strategy, it is reasonable to implement the same level of protection for tanks of the same type and content.

Nodes U1 and U2 implement respectively $CBF_{B,ij}$ and $CBF_{P,ij}$, according to Eq. (4) and Eq. (5). $CBF_{B,ij}$ is thus evaluated for each protection strategy, $CBF_{P,ij}$ is evaluated for each combination of protection strategy and damaged tanks. The total CBF value can be retrieved in GeNIe through node D1.

Fig. 4 shows the results of the analysis. The bars represent the probabilistic outcomes, while the line indicates the values of the CBF.

As demonstrated in previous works (Marroni et al., 2024b), the contribution of safety barriers to reducing the likelihood of domino scenarios generated by intentional attack is relevant. Namely, the likelihood of T1, T3, and T4 being damaged reduces by an order of magnitude when comparing the baseline case (F in Fig. 3) with protection strategies that include the SCS.

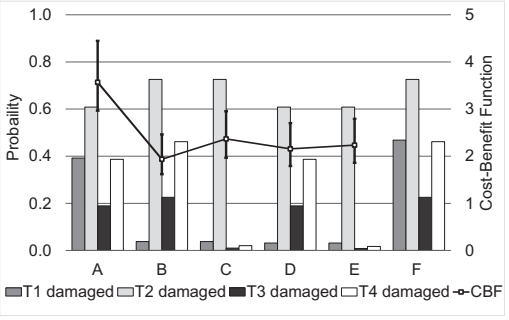

Fig. 4. Probabilistic values and CBF (cost benefit function) for different protection strategies; refer to Table 1 for the list of protection strategies

This is due to the good probabilistic performance of the SCS. For example, the probability of damaging tank T3 reduces from 22.57% in the baseline case F to 0.99% in case C, and to 0.83% in case E.

The installation of the VMD has also a satisfactory performance, and a reduction in damage probabilities for all tanks can be observed by comparing the baseline case F with strategies A, D, and E. For example, there is a 16% reduction in probability of damaging the tanks when strategy A is implemented compared to the baseline case.

The biggest reduction in damage of all tanks is observed in strategy E, as it is the most complete protection strategy.

The value of the CBF (right axis in Fig. 4) provides a complementary perspective to the probabilistic assessment. Protection strategies protecting T1 and T2 (B and D) rank among the least cost-effective, with a CBF of 1.93 and 2.16 respectively.

In contrast, the installation of the VMD alone (case A) achieves the highest CBF, approximately 3.5, making it the most favourable strategy from an economic perspective.

Installing a SCS on all tanks (strategy C) and coupling this with a VMD (strategy E) are the second most convenient strategies, with a CBF value of 2.36 and 2.23, respectively.

Protecting all tanks is also slightly more convenient than protecting just two tanks (strategies B and D); this suggests that the higher reduction in damage probability can compensate for the higher cost of the strategies.

These results highlight the potential benefits of integrating safety and security measures for a more comprehensive risk mitigation approach,

while also showing the trade-offs between effectiveness and cost-efficiency across different strategies.

5. Discussion and future developments

While the CBF effectively highlights the economic efficiency of each strategy, a few considerations should be noted regarding the findings in Section 4.

The first observation concerns costs' variability. The cost of protection measures is subject to fluctuation. Hence, a sensitivity analysis on the CBF has been carried out varying the price of the SCS and the VMD in a ±20% range. The results of the sensitivity analysis are shown in Fig. 4 through the error bar.

Strategy A remains the most cost-effective, despite being the most sensitive to price fluctuation. The other strategies have lower variability, but their variation range overlap. This is due to the fact that the price of the VMD and the SCS are close. Moreover, a significant difference in price is observed among strategy A and the others, making it more susceptible to any alterations.

The variability of the results could be addressed by further improving the economic analysis. Namely, the barriers should be characterized not only by installation costs, but also by operating costs. This would help in making a more informed decision, as some barriers might be affordable to install, but more expensive to maintain. Additionally, as discussed in Section 2.2, a more detailed CBF could be implemented, taking into consideration additional variables such as an available budget to spend on countermeasures. For instance, while installing an SCS on all tanks may be the most cost-effective solution overall, its feasibility would depend on the available budget for these additional countermeasures.

Another consideration should be made on the SCS. While the SCS contributes to reducing the damage probability, its high cost compared to the achieved probability reduction results in a less favourable cost-benefit balance. This suggests that, from a purely economic perspective, the installation of the SCS on tanks T1 and T2 may not justify the investment. That said, it is also important to recognize that SCS could be required to address conventional process safety concerns beyond the specific scenario analysed here. In this sense, the natural progression of this methodology is to have it coupled with a conventional safety analysis. In that way, it would be possible to integrate safety and security in a comprehensive analysis, and understand the contribution to the overall safety of the plant.

Extending the methodology might also lead to some drawbacks. Namely, one issue with Bayesian Network is the so-called curse of dimensionality; namely, the more nodes and dependencies included in the analysis, the more onerous the BN becomes to quantify. Moreover, the amount of data needed considerably rises. For this reason, this approach should be coupled with other approaches based on graph theory (Khakzad et al., 2017). In this way, the most relevant domino scenarios are evaluated at a lower computational cost and then implemented in the BN for a comprehensive analysis.

6. Conclusions

This work shows an exploratory cost-benefit analysis for intrusion scenarios in chemical and process facilities. A probabilistic cost-benefit analysis is setup using BN as a tool. Next, a Cost-Benefit Function is evaluated through the ratio of the damages and the costs. Safety and security barriers are integrated within a Bayesian Network (BN) approach.

The application of the methodology to a case study yields diverse results. While advanced strategies like those involving the Shell Cooling System (SCS) or combinations such as the Video Motion Detection (VMD) with the SCS can significantly reduce the likelihood of damage, they also bring notable cost considerations. For instance, standalone solutions like the VMD are identified as economically favourable due to their high CBF, emphasizing their utility for budget-conscious scenarios. Nonetheless, strategies combining multiple measures showed potential for broader risk mitigation, although with diminishing economic returns.

Sensitivity analysis confirmed the economical favourability of the VMD system, while a higher variability is obtained for safety-based and integrated safety-security strategies.

The methodology we developed could be expanded by including the incorporation of operational costs and indirect economic losses.

This would provide a more nuanced understanding of the long-term implications of each strategy. Moreover, challenges such as the computational complexity inherent in the BN approach and the need for extensive data highlight opportunities for methodological refinement, such as integrating graph theory-based techniques or extending the framework to cover a wider array of attack scenarios.

In conclusion, this research bridges critical gaps in the integration of safety and security within industrial risk management and offers a versatile tool for optimizing resource allocation in the face of complex threats. By addressing its limitations and broadening its scope, future applications of this framework could further advance the resilience and sustainability of chemical plants and similar industrial systems.

Acknowledgement

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

American Petroleum Institute (2008). *ANSI/API Standard 581 – Risk-based Inspection Technologies*. API Publishing Services.

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

Atexshop. (2024). "MAXIMUS MVXHD Camera Full HD, 1080p, 60fps Product Page". Accessed December 26, 2024. https://www.atexshop.com/maximus-mvxhd-camera-full-hd-1080p-60fps.html

Bayesfusion LLC. (2024). "GeNIe Modeler: Complete Modeling Freedom". Accessed December 26, 2024. https://www.bayesfusion.com/genie/

Cozzani, V., and G. Reniers (2013). *Domino Effect in the Process Industries*. Elsevier.

Garcia, M.L. (2008). *The Design and Evaluation of Physical Protection Systems*. Elsevier.

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

Janssen, J., L. Talarico, G. Reniers, and K. Sörensen (2015). A decision model to allocate protective safety barriers and mitigate domino effects. *Reliability Engineering & System Safety 143*, 44-52.

Khakzad, N., G. Landucci, and G. Reniers. (2017). Application of Graph Theory to Cost-Effective Fire Protection of Chemical Plants During Domino Effects. *Risk Analysis 37*, 1652-1667.

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

Marroni, G., V. Casson Moreno, S. Kuipers, M. Mossa Verre, and G. Landucci (2024b). Securing Chemical Facilities Against Intentional Attacks: a Bayesian Network Approach for Asset Risk Assessment. *Chemical Engineering Transactions 111*, 487-492.

Matches. (2024). "Tank Cost Estimate". Accessed December 26, 2024. https://www.matche.com/equipcost/Tank.html

Ministero dell'ambiente e della sicurezza energetica. (2024). "Prezzi mensili carburanti". Accessed December 25 https://sisen.mase.gov.it/dgsaie/prezzi-mensili-carburanti

Mishan, E.J., and E. Quah (2020). *Cost-Benefit Analysis* (6th ed.), Routledge

Misuri, A., N. Khakzad, G. Reniers, and V. Cozzani. (2019). A Bayesian network methodology for optimal security management of critical infrastructures. *Reliability Engineering & System Safety 191*, 106112

Roy S. (2022). Optimizing safety budget allocation in process industry using risk metrics. *Journal of Loss Prevention in the Process Industries 79*, 104832

Securdomino. (2024). Open Web Repository of Models and Barriers Data. Accessed December 26, 2024. https://securdomino.eu/open-web-repository/

United States Environmental Protection Agency. (2024). "ALOHA Software". Accessed December 26, 2024. https://www.epa.gov/cameo/aloha-software

Villa, V., G.L.L. Reniers, N. Paltrinieri, and V. Cozzani (2017). Development of an economic model for the allocation of preventive security measures against environmental and ecological terrorism in chemical facilities. *Process Safety and Environmental Protection 109*, 311-319

Witte, D., D. Lichte, and K.D. Wolf. (2022). An Approach to the Consideration of Uncertainties in Cost-Benefit Optimal Design of Physical Security Systems. In M.C. Leva, E. Patelli, L. Podofillini, and S. Wilson (Eds.), *Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)*, 1542-1549.