Probabilistic evaluation of integrated safety–security protection plans for process facilities

Marroni, G.; Kuipers, S.; Landucci, G.; Casson Moreno, V.

Risk Analysis

WILEY

ORIGINAL ARTICLE

Probabilistic Evaluation of Integrated Safety–Security Protection Plans for Process Facilities

Giulia Marroni[1] | Sanneke Kuipers[2] | Gabriele Landucci[1] | Valeria Casson Moreno[1]

[1]Department of Civil and Industrial Engineering, University of Pisa, Pisa, Italy | [2]Institute of Security and Global Affairs, Leiden University, Leiden, the Netherlands

Correspondence: Gabriele Landucci (gabriele.landucci@unipi.it)

Received: 3 July 2025 | **Revised:** 19 February 2026 | **Accepted:** 19 March 2026

Keywords: Bayesian networks | cost–benefit analysis | process facilities | safety barriers | security barriers

ABSTRACT

The assessment of accident scenarios associated with intentional attacks to chemical and process facilities has garnered the attention of institutions and practitioners because of the exacerbation of conflicts in critical contexts. In this perspective, it is important to create a framework for the integration of conventional safety approaches, dealing with unintentional events, and security science, dealing with the analysis of intentional threats. More specifically, effective protection strategies for industrial facilities require an integrated approach that combines safety and security measures. This work proposes a methodology to evaluate the cost-effectiveness of such strategies using a probabilistic approach based on Bayesian networks (BN). The methodology incorporates attack scenarios, escalation scenarios, and the probabilistic performance of integrated safety–security barriers into a cost–benefit analysis. A dedicated cost–benefit function quantifies the economic benefits of damage reduction relative to the cost of protection strategies. A demonstrative case study evaluates different protection plans, including fireproofing and video motion detection systems. The results highlight the effectiveness of integrated safety–security measures in mitigating damage probability and controlling escalation scenarios. This methodology provides a systematic tool for plant managers and practitioners to assess and compare the economic efficiency of safety and security protection plans. It bridges key gaps in the integration of safety and security analyses, offering insights into the protection of critical infrastructures.

1 | Introduction

Intentional attacks to critical infrastructures, including chemical and process facilities, have become an increasing concern in the last two decades (Khakzad 2023). Several initiatives were introduced to address security risks starting in the early 2000s, including the US Chemical Facility Anti-Terrorism Standard (CFATS) program and the European Program for Critical Infrastructure Protection. However, the CFATS program expired in 2023, and the European Seveso III Directive on the control of major accidents in process facilities still lacks explicit requirements for security assessment. Namely, process facilities, often storing high amounts of hazardous substances, face unique challenges due to the potential for escalation. Escalation scenarios take place when the consequences of accidents affect nearby equipment and assets, thus amplifying the severity of consequences on people, the environment, and assets. The analysis of cascading events triggered by process upsets, malfunctions, and errors, referred to as "safety scenarios," was extensively studied in recent years (Zhao et al. 2024). In this work, safety scenarios are therefore considered to be associated with unintentional events. However, recent works demonstrated how escalation may take place also with "security scenarios" as well (Iaiani et al. 2022). Security scenarios are intended in this work as accidents triggered by an intentional action, such as sabotage, misoperation, and terrorist attack. Escalation scenarios thus make safety and security inter-

connected, and several works have dealt with the integration of safety and security, both considering the conceptual integration (Van Den Berg et al. 2020) and the technical implications (George and Renjith 2021).

Intentional attack scenarios can have complex evolutions, and the consequences can be severe also in terms of asset losses. For this reason, evaluating the cost-effectiveness of protection strategies is fundamental. Cox (2009) provided recommendations on risk-informed decision-making on security protection strategies, stressing the importance of assessing the effectiveness of their risk reduction. Stewart and Mueller (2013) reported an example of cost–benefit analysis (CBA) for security threats in the aviation sector, whereas Hausken (2016) developed a systematic theoretical structure for cost–benefit analyses for terrorist attacks. Game theoretical approaches were also applied to support the allocation of security countermeasures. Advanced probabilistic tools can be of assistance in order to deal with the wide number variables and complex interactions associated to this task.

However, limited works have dealt with identifying the contribution of integrated safety–security measures in the quantification of economic losses, more so when it comes to a detailed description of the attack scenario. Moreover, there is a lack of knowledge when it comes to assessing the cost-effectiveness of protection plans to protect chemical and process facilities from intentional attacks. Finally, the systematic investigation of the performance of integrated safety–security barriers based on sound probabilistic evaluations still needs to be addressed.

For this reason, this work presents a structured approach to assess the cost-effectiveness of integrated safety–security protection strategies. The methodology adopts a probabilistic approach based on Bayesian networks (BN), which allows for the identification of the contribution of different barriers and protection strategies. For each step, we provide specific approaches and quantitative data, which can guide readers and practitioners in tackling each specific issue. The analysis of an industrial case study shows the potential of the methodology in supporting plant managers in decision-making on integrated safety and security issues.

2 | Methodology

2.1 | Overview

The overview of the methodology developed in this work is shown in Figure 1.

Step 1 is dedicated to the evaluation of the accidental chain, which is composed by attack scenarios and escalation scenarios. The attack scenario starts from the intrusion attempt and ends in the final outcome, that is, the event that generates a physical effect in case of successful attack (such as fire and explosion). Selecting an attack scenario entails the selection of a target equipment and an intrusion path, as detailed in Section 2.2. In the case of successful attack, for instance by damaging the equipment and causing a release of hazardous materials, the escalation scenario will be eventually triggered. The escalation scenario involves the assets located near the target equipment. Assessing the final outcomes entails evaluating which assets are damaged from the release of the hazardous materials, as explained in Section 2.2. Step 2 of the methodology is dedicated to the conceptualization and classification of plant protections, with the aim of quantitatively identifying performance parameters for integrated safety–security barriers. Details are provided in Section 2.3. Step 3 is the economic assessment: first, the cost of accidental chains and the related benefits in the implementation of the protection configuration should be identified. Then, a cost–benefit indicator, namely, a cost–benefit function, is defined in order to compare different protection strategies, as shown in Section 2.4. The final step of the methodology is the setup of the BN through the definition and quantification of variables; details are reported in Section 2.5. Additionally, as the costs and benefits defined in Step 3 are subjected to fluctuation, a sensitivity analysis is carried out to test the robustness of the methodology.

2.2 | Accidental Chain Evaluation

The evaluation of the accidental chain begins with the identification of attack scenarios. An attack scenario is defined by specifying the (i) target asset, (ii) intrusion path, and (iii) final outcome. Currently, there are no standardized methodologies for the systematic identification of attack scenarios. Hence, this work relies on expert judgment. Relying on expert judgment is a practical approach commonly adopted for the security of the process industry (Matteini et al. 2019), but also in conventional safety analyses.

A process facility might contain a wide number of potential targets (i). Thus, it is necessary to screen all equipment to identify the critical ones. It should be noted that potential targets include only those assets that store or process hazardous substances, due to their inherent potential for severe consequences. Some of these methods include the use of matrixes (Marroni et al. 2023); moreover, the historical analysis of the site or similar sites can guide the team in choosing critical targets.

Hereby, we propose a method for screening equipment based on the identification of groups of equipment. Groups can be identified based on the physical proximity of the units, such as neighboring or shared catch basins. Within each group, the target assets are identified through different considerations regarding the nature of the equipment. Namely, a piece of equipment may be an attractive target not only for its size or content, but also for its visibility and iconicity (Marroni et al. 2024). For example, a fuel storage tank might be more recognizable than a pipe rack by a potential intruder. A target equipment for each hazardous substance present in each group should be chosen; this implies that there might be multiple target equipment within the same group.

The intrusion could happen via different attack paths (ii); however, it is beyond the scope of this analysis to identify all potential attack paths. Namely, the experts should identify a single attack path for each target asset, which is (a) credible given site layout and likely adversary resources, and (b) conservative with respect to assumptions about attack times used in the evaluation. If the configuration or effectiveness of security barriers varies over time, such as between daytime and nighttime operations,

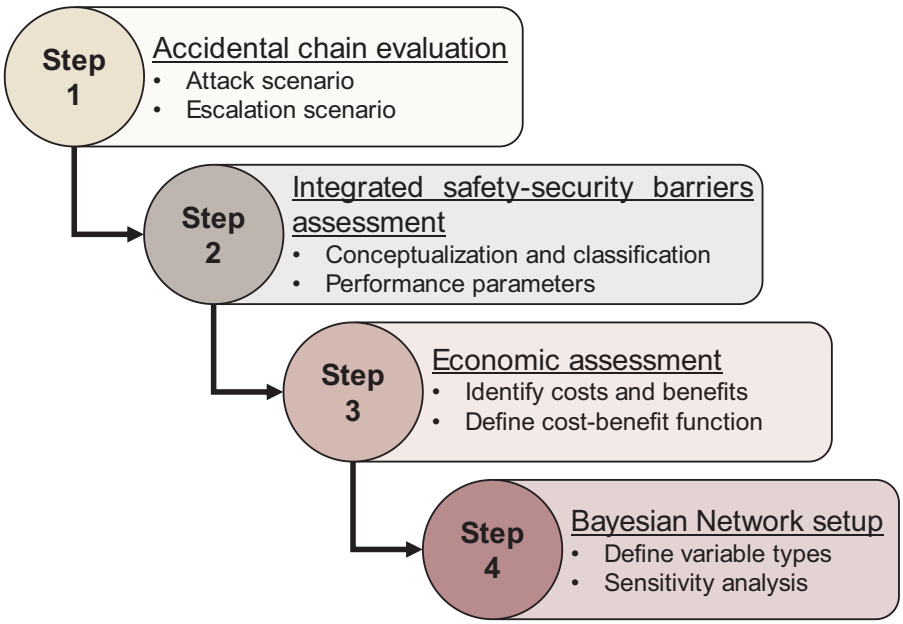

FIGURE 1 | Overview of the methodology developed in this work.

the representative path should be assessed under each relevant operational condition. Still, attack paths are an input to the CBA, and thus more rigorous approaches to path analysis are compatible with the developed framework and can be therefore integrated in the methodology when available.

Then, consequence assessment is carried out in order to identify the final outcome (iii) and estimate its hazard potentially by evaluating the related physical effects. Release diameters and source terms should be characterized. As released diameters for intentional attacks are not currently conventionally established, release diameters are adapted from the available safety standards, such as the risk-based inspection standard from the American Petroleum Institute (2008). More specifically, in this work a catastrophic rupture has been conservatively associated to explosive attacks, given the high damage potential of such weapons in the attacks to storage and process facilities (Wang et al. 2022). The source term associated with the release diameter depends on the nature of the substance and its storage conditions (Van Den Bosch and Weterings 2005). The physical effects associated to the source term are considered for security studies only in the case of immediate ignition, as shown by Iaiani et al. (2022). The physical effects are then simulated using integral models implemented in the software ALOHA (United States Environmental Protection Agency 2025).

Once the attack scenario is quantified, the escalation scenarios can be assessed through the identification of other equipment damaged by the final outcome. The threshold-based approach developed by Cozzani and Reniers (2013) is adopted in this work: A piece of equipment is considered part of the escalation scenario if the intensity of the physical effect exceeds the threshold values. Table 1 shows escalation thresholds for different types of fires as escalation vectors.

It should be noted that the presence of safety barriers might mitigate the dose of physical effect on a target and could therefore avoid its inclusion in the escalation. This mitigative effect is discussed in detail in Section 2.3.2.

2.3 | Integrated Safety–Security Barriers Assessment

2.3.1 | Conceptualization and Classification

In this work, barriers are conceptualized according to the analysis of Sklet (2006) and are thus considered "physical and/or non-physical means to prevent, control, and mitigate undesired events or accidents."

Following this definition of barrier, the classification and schematization of both safety and security barriers adopted in the present work are shown in Figure 2.

Garcia (2005) focuses on security pre-event actions and further distinguishes the function into detection, delay, and response. Detection is the discovery of the adversary action, and typical detection barriers include entry checks, or Closed-Circuit Television (CCTV). Delay consists of all actions that slow the adversary path to the target, and typical barriers include walls or fences. Finally, response includes all the actions taken to interrupt and subsequently neutralize the adversary.

2.3.2 | Performance Parameters

Once barriers are classified according to function and working principle, next step is to characterize their quantitative performance. As the performance of safety barriers is a critical aspect in evaluating the probability of accident chain evolution, its characterization is needed to support the probabilistic assessment of final scenarios. In this study, the following probabilistic parameters are adopted to both evaluate the performance of safety and security barriers, namely (Casson Moreno et al. 2022):

TABLE 1 | Escalation thresholds for different vectors.

Scenario	Escalation vector	Target category	Threshold
Fireball	Heat radiation	AtmosphericPressurized	$Q > 100$ kW/m^{2}Escalation unlikely
Jet firePool fire	Heat radiation	AtmosphericPressurized	$Q > 15$ kW/m$^2 Q > 45$ kW/m^2

Source: Adapted from Cozzani and Reniers (2013).

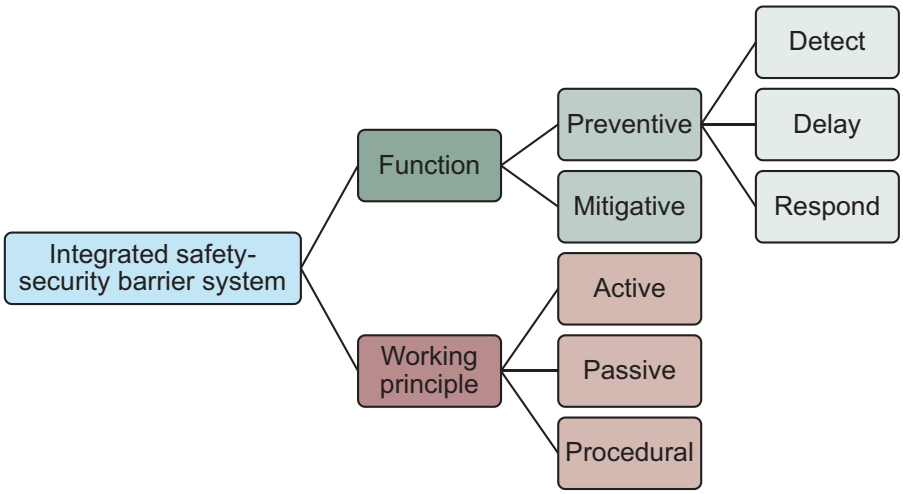

FIGURE 2 | Classification of integrated safety–security barriers adopted in this work, elaborated based on the work from Sklet (2006) and Garcia (2005).

- *Availability* of the barrier: It is defined as the degree to which the barriers are operational. Expressed as the probability of failure on demand (PFD). This term is null for passive barriers, as they are, by definition, always available.
- *Effectiveness* (η) of the barrier: Even if the barrier is operational, there is still the possibility of the barrier not really performing its function.

The barrier correctly performs its function only if it activates on demand and it is effective. Hence, the probability of success, P_s, is evaluated using the following equation, which is adapted from Landucci et al. (2017), Casson Moreno et al. (2022):

$$P_s = (1 - \text{PFD})\,\eta \tag{1}$$

Table 2 shows the classification, as well as the probabilistic parameters for different integrated safety–security barriers. For the emergency response, the model shown in Garcia (2006) and based on attack times can be adopted. The model assumes that both the emergency response time t_{ERT} and the time to complete the attack t_P follow normal distributions. Consequently, their difference $(t_P - t_{\text{ERT}})$ is also normally distributed. An attack can be successfully interrupted only if the emergency response time is shorter than the time required to complete the attack, that is, $(t_P - t_{\text{ERT}}) > 0$. Therefore, the following equation expresses the probability that this condition is valid by integrating the probability density function of the variable $(t_P - t_{\text{ERT}})$ for values greater than zero:

$$\text{PFD}_{\text{ERT}} = 1 - \frac{1}{\sqrt{2\pi\left(\sigma^2_{\text{ERT}} + \sigma^2_P\right)}} \int_0^{\infty} \text{e}^{\frac{-(t-(t_P - t_{\text{ERT}}))^2}{2\left(\sigma^2_{\text{ERT}} + \sigma^2_P\right)}}\, dt \tag{2}$$

where $\sigma^2{}_P$ and $\sigma^2{}_{\text{ERT}}$ are the variance of t_P and t_{ERT}, respectively. The quantitative details on t_P and t_{ERT} are reported in detail in Section 2.5, and a practical application is discussed in the case study (see Sections 4 and 5). In the case of lack of data regarding the probabilistic distribution, a simplified approach is proposed by Casson Moreno et al. (2022): If the average value of $(t_P - t_{\text{ERT}})$ is lower than zero, then the probability of successful interruption P_s can be conservatively set to zero.

The effect of barriers is not only probabilistic. Rather, there are physical effects associated with the correct functioning of barriers. Firefighting systems act on the heat radiated from the fire. More specifically, sprinkler systems can reduce the heat radiation by 40% (Khakzad et al. 2017) by releasing firefighting agents like foam or water directly on the flame.

Fireproof coatings instead reduce the heat-up of equipment exposed to fire and thus extend the time to failure. The extent to which the time is extended depends on various factors, such as the material and quality of the coating; high-quality coatings can provide fire protection from one-half to several hours (Weil 2011).

TABLE 2 | Classification and probabilistic parameters of selected safety and security barriers.

Barrier	Classification	Barrier availability, PFD	Barrier effectiveness, η	Probability of success, P_s	Source
Entry check	Detection, procedural	4.00E − 01	8.00E − 01	0.480	Casson Moreno et al. (2022)
Detection from employees	Detection, procedural	2.33E − 01	2.48E − 01	1.90E − 01	Casson Moreno et al. (2022)
Video motion detection	Detection, active	2.05E − 01	9.70E − 01	7.71E − 01	Casson Moreno et al. (2022)
Emergency response	Response, procedural	See Equation (2)	9.50E − 01	—	Garcia (2006)
Foam sprinkler	Mitigative, active	5.43E − 03	9.54 − 01	9.49E − 01	Landucci et al. (2017)
Fireproofing	Preventive/Mitigative, passive	0.00E + 00	9.99E − 01	9.99E − 01	Landucci et al. (2017)

Abbreviation: PFD, probability of failure on demand.

2.4 | Economic Assessment

The economic assessment is based on the estimation of costs associated with potential damages and the costs of additional countermeasures. The primary objective of this work is to provide a methodological framework to determine the probabilistic-based analysis of safety–security countermeasures. A detailed breakdown of costs is out of the scope of the work, and, thus, the discussion on cost assumptions is intentionally simplified, as the focus lies beyond the scope of economic analysis.

In this work, the considered economic damages for the ith attack scenario are (i) the cost of the kth damaged equipment, $E_{e,i,k}$; (ii) the cost of the stored substance in the kth target, $E_{s,i,k}$, which is considered totally lost and not recoverable in the event of a successful intentional attack; and (iii) the costs associated to the business interruption, $E_{b,i,k}$, intended as the economic impact associated with production downtime, as a damaged asset has to be restored and is thus unproductive. The costs $E_{e,i,k}$ can be retrieved either by manufacturers' data, or by using available simplified correlations in the literature (Peters et al. 2003). The costs $E_{e,i,k}$ can be retrieved from commercial data or price lists, as shown in Section 3.

The costs associated to business interruption $E_{b,i,k}$ are related to the productivity of the site. In this work, a simplified assessment of the business interruption is adopted for the sake of example. More specifically, in the Dow Fire & Explosion Hazard Index Guide (American Institute of Chemical Engineers 2016), a part is dedicated to estimating the business interruption. In the proposed method, the business interruption is estimated on the basis of different factors: (i) The maximum probable days of outage, that is, the length of downtime; (ii) the value of replacing the equipment and its content, for example, the sum of $E_{e,i,k}$ and $E_{s,i,k}$; and (iii) the monthly value of production.

Hence, for the ith attack scenario to the kth piece of equipment, the total associated economic loss $L_{i,k}$ is evaluated as follows:

$$L_{i,k} = E_{s,i,k} + E_{e,i,k} + E_{b,i,k} \tag{3}$$

The cost of protection strategies is evaluated using either vendor data, or sources from the literature: for example, Janssens et al. (2015) provide the costs of typical preventive and mitigative safety barriers, C_{sf}, whereas Villa et al. (2017) report the costs for some security countermeasures, C_{sc}. For the jth protection strategy, the cost C_j can be evaluated as follows:

$$C_j = \sum_{q=1}^{m} C_{\mathrm{sf},j,q} + \sum_{v=1}^{p} C_{\mathrm{sc},j,v} \text{ with } C_j \leq C_b \tag{4}$$

where m and p, respectively, are the total number of safety/and security barriers within the jth protection strategy. The available budget for safety and security measures, C_b, is treated as a constraint throughout the analysis. Each protection strategy C_j must be firstly assessed in relation to the budget, and only those strategies whose cost does not exceed the available budget ($C_j \leq C_b$) are considered feasible and retained for the CBA. It should be noted that the maintenance costs and the downtime associated with maintenance activities are not included in the cost evaluation, as process facilities already allocate scheduled shutdowns and maintenance budgets for safety and security systems. The maintenance of the additional measures considered in this study is therefore assumed to be covered within the existing maintenance framework.

The benefits of implementing barriers are viewed in this work as the reduction in the probability of successfully damaging all equipment in the tank, transitioning from the baseline case (in which a preliminary set of barriers are provided) to the implementation of additional measures with a given protection strategy. The cost–benefit function $\mathrm{CBF}_{i,j}$ for each attack scenario i and each protection strategy j is thus evaluated according to the following equations:

$$\mathrm{CBF}_{i,j} = \frac{\mathrm{ED}_{b,i} - \mathrm{ED}_{p,i,j}}{C_j} \tag{5}$$

$$\mathrm{ED}_{b,i} = \sum_{k=1}^{n} P_{b,i,k} L_{i,k} \tag{6}$$

$$\mathrm{ED}_{p,i,j} = \sum_{k=1}^{n} P_{s,i,j,k} L_{i,k} \tag{7}$$

where $\mathrm{ED}_{b,i}$ represents the baseline expected damage: $P_{b,i,k}$ is the damage probability of the equipment k in the ith scenario with the baseline set of protections; n is the number of damaged equipment in the attack and escalation scenario i. On the other hand, $\mathrm{ED}_{p,i,j}$ represents the expected damage after implementing protection strategy j: $P_{s,i,j,k}$ is the damage probability of the equipment k in the ith scenario after the implementation of the jth protection strategy. $\mathrm{CBF}_{i,j}$ thus represents the obtained reduction in expected losses per cost of implemented strategy: the higher $\mathrm{CBF}_{i,j}$, the more cost-effective the implemented strategy is, because either $P_{s,i,j,k}$ is greatly reduced, or C_j is sufficiently low.

It is worth mentioning that economic losses and the cost 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 CBA (Mishan and Quah 2020), which can incorporate other variables, such as the discount rate, to account for the value of money in time. For a broader perspective on alternative methodologies and applications of CBA in security applications, readers are encouraged to consult the works cited in the Introduction. Nonetheless, the simplified CBF in Equation (5) serves as a practical basis in the context of this specific work and can anytime be modified to reflect a more (or less) rigorous approach, depending on the intended purpose and resource availability within the analysis.

2.5 | BN Setup

The probabilistic dependencies among the variables presented in the previous sections are modeled using BN. BN are directed acyclic graphs, where variables are represented by nodes and the relationships among variables are represented through arcs (Yuan et al. 2014; Hanea et al. 2022). Nodes can be differentiated on the basis of their relationships: nodes with only arcs directed from them are parent nodes, whereas nodes with arcs directed to them are called children. The probability of an occurrence $P(x)$ can be calculated according to Jensen and Nielsen (2007):

$$P(x) = \prod_{z=1}^{l} P(v_z | \mathrm{Pa}(v_z)) \tag{8}$$

where v_z is the parent set of x, and $\mathrm{Pa}(v_z)$ are the parent nodes of v_z. The graphical and mathematical formulation of BN makes them a suitable tool for safety and security evaluations, where expert knowledge deeply intersects with observational data. Moreover, BN exploits Bayes' Theorem in order to update the occurrence probability $P(x)$ once new evidence enters the network. This makes them particularly suitable for decision-making, as different protection strategies can be easily implemented and their impacts on variables evaluated (Hanea et al. 2022). The software GeNIe Modeler (Bayesfusion 2025) is used in this work to develop the BN. GeNIe supports the modeling of different domains of variables: in this work, all variables are discrete; hence, they take on fixed states defined by a label, for example, "success" and "failure." Quantifying a BN implies quantifying all fixed states for variables by populating the CPT (conditional probability tables).

For the implementation of the CBA, the baseline probabilities are first evaluated by modeling the accidental chain within the BN. The network structure follows the key steps outlined in Section 2.2. More specifically, the main factors to be modeled are the choice of target equipment, the operational condition of the plant, the performance of safety and security barriers (see Section 2.3), and the occurrence of damage to the target equipment. The damage probability is calculated using fragility models, which convert the intensity of physical effects into damage probability; the fragility models used in this work are reported in Appendix A. Representing these factors within a BN requires the definition of multiple nodes, with conditional relationships among them.

Once the baseline probabilities are computed, the BN can be further developed by adding specific groups for decision-making. The probabilistic performance of the additional elements included in the protection strategies is modeled through chance nodes, whose CPTs are populated using the availability and effectiveness parameters defined in Section 2.3. The core of this group is a "Decision Node." Unlike other nodes, D1 is deterministic: it represents fixed choices, namely, the protection strategies and the baseline case. The selected strategy determines which additional barriers are implemented in the network, allowing the different combinations of barriers to be represented within a single BN. The so-called switches are also introduced to support the implementation of the protection strategies. As their name suggests, switches are deterministic nodes that can be switched "on" and "off," enabling the differentiation of cases where different barriers are implemented. They act as intermediate variables and allow the simplification of the BN by avoiding redundancies.

Finally, utility nodes are introduced to implement the CBF within the BN. Through utility nodes, numerical values can be assigned to each combination of relevant parent states. This allows the expected value of the cost–benefit function to be evaluated directly for each protection strategy.

The quantitative implementation of the network and the detailed discussion of its application are presented in Section 4.

3 | Case Study Definition

The methodology developed in Section 2 is applied to a case study, consisting in a petroleum products depot located in Italy. The layout of the case study is shown in Figure 3. The facility is composed of 5 tanks: T1 is an atmospheric floating roof tank storing gasoline, whereas T2, T3, T4, and T5 are fixed roof tanks storing diesel. Table 3 contains the geometrical features of the tanks and relative catch basins, as well as the cost.

The costs of tanks can be retrieved from vendor data (Matches 2025), whereas the price of fuels in Italy can be retrieved from official Italian sources (MASE—Italian Ministry of Environment and Energetic Security 2024). The average price between 2010 and 2025 was considered for the analysis, which amounts to €1.63/L for gasoline and €1.53/L. To evaluate the business interruption,

TABLE 3 | Characterization of the tanks featured in the case study in Figure 3.

ID	Type	Content	Diameter (m)	Height (m)	Volume (m)	S_{CB} (m)	L (m)
T1	Floating roof	Gasoline	54.00	3.60	8244.80	5625	18,000
T2–T5	Fixed roof	Diesel	16.77	9.40	2076.27	625	3130

Note: S_{CB} is the surface of the catch basin, and L is the cost.

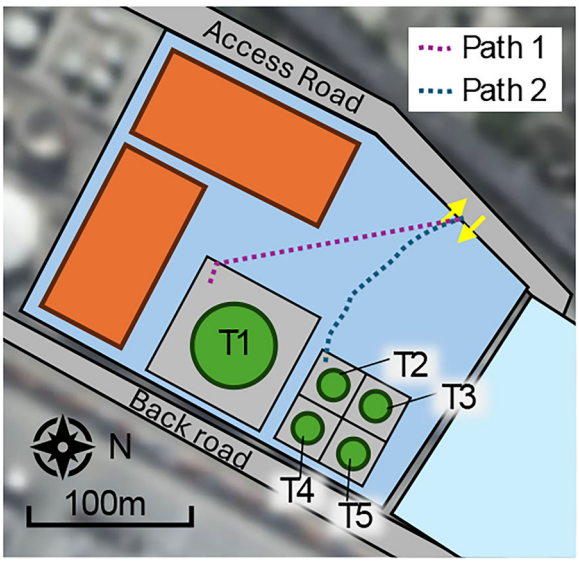

FIGURE 3 | Layout of the case study; the dashed blue line shows the analyzed attack path.

a monthly value of production equivalent to the capacity of the tanks was considered. For T1, this led to 26 days of outage, with an estimated nominal business interruption of €6340k, for T2, T3, T4, and T5, 6 days of outage were considered, with a business interruption of €354 k. Applying Equation (3), the cost of T1 amounts to €18.00M, whereas the cost of T2, T3, T4, and T5 is €3.13M.

All tanks are protected by foam sprinklers. The facility is protected by an external wall 4 m high and manual control at the entry gate; additionally, employees received a security training, hence they are aware of potential unauthorized persons in the plant, but they are not present in the plant at night.

Concerning the attack paths, trespassing from the perimetral wall is not considered a credible way to enter the plant, given its height (4 m). Hence, the attack paths for T1 and T2 shown in Figure 3 both start from the entry gate.

During the day, the attacker eludes the entry controls, whereas at night it trespasses the closed gate. Then it runs in the catch basin (160 m to T1, 120 m to T2) and detonates a homemade explosive device made of 10 kg of triacetone triperoxide (TATP). Namely, past works in the literature confirmed that explosive attacks are among the most frequent for the process industry (Casson Moreno et al. 2018) and hold significant damage potential (Iaiani et al. 2022).

If the attack is successful, T2 fails catastrophically. Through the analysis of past events (Iaiani et al. 2022), a pool fire constitutes a credible outcome of the accidental chain, and thus it is considered the final outcome of the attack scenario. A representative wind speed of 5 m/s with a Pasquill stability condition D was considered.

The plant manager is considering the introduction of additional safety–security protections: a CCTV with video motion detection (VMD) system and fireproofing the tanks. On the basis of a plant of similar size (Janssens et al. 2015), a budget of €3500k was allocated for safety and security protection. The considered protection strategies are shown in Table 4; A is security-based, B, C, and D are safety-based, whereas E, F, and G are integrated safety–security protection strategies.

Table 4 also shows the cost of the protection alternatives. On the basis of suppliers' data (Atexshop 2025), the retail price of a high-quality VMD camera for explosive atmospheres application is around €3k. For a complete system composed of multiple cameras, video management system, monitors, and alert system, a conservative price of €100k has been considered. Different types of fireproofing with different grades of quality are available. For this application, a good-quality fireproofing priced €410/m^2 (Paltrinieri et al. 2012) was chosen.

4 | Results

The BN used for the assessment is built according to the methodology shown in Section 2.5 and is represented in Figure 4. For clarity, variables have been divided in different groups and distinguished with labels and colors. Identifying the variable groups helps in understanding the functioning of the BN: to this purpose, we advise the reader to pinpoint the parent nodes and then move further toward the children nodes. All the CPT related to the BN is reported in the Supporting Information. Table 5 summarizes the quantitative results.

Group N1 (in orange in Figure 4) is devoted to the calculation of the probability of attack success. N1.1 represents the probability of a target asset being attacked; as a baseline value, T1 and T2 are considered equally probable, leading to a probability of 50% each. N1.2 represents the operation time, which influences the security asset of the site under analysis. We considered that the depot is open for a total of 8 h: considering 24 h in the day, we define a day state (plant closed) with a 33% probability (8 h out of 24) and a night state (depot closed) with a 67% probability (16 h out of 24). According to Garcia (2006), the attack can be prevented only if successfully detected and interrupted by the emergency response. The CPT for N1.3 and N1.4 are filled according to the data in

TABLE 4 | Protection strategies considered for implementation in the case study; VMD = video motion detection.

ID	Description	Price (k€) (source)
A	Video motion detection	100 (Atexshop 2025)
B	Fireproofing on T1	250 (Paltrinieri et al. 2012)
C	Fireproofing on T2–T5	812 (Paltrinieri et al. 2012)
D	Fireproofing on all	1062 (Paltrinieri et al. 2012)
E	Video motion detection + fireproofing on T1	350
F	Video motion detection + fireproofing on T2–T5	912
G	Video motion detection + fireproofing on all	1162

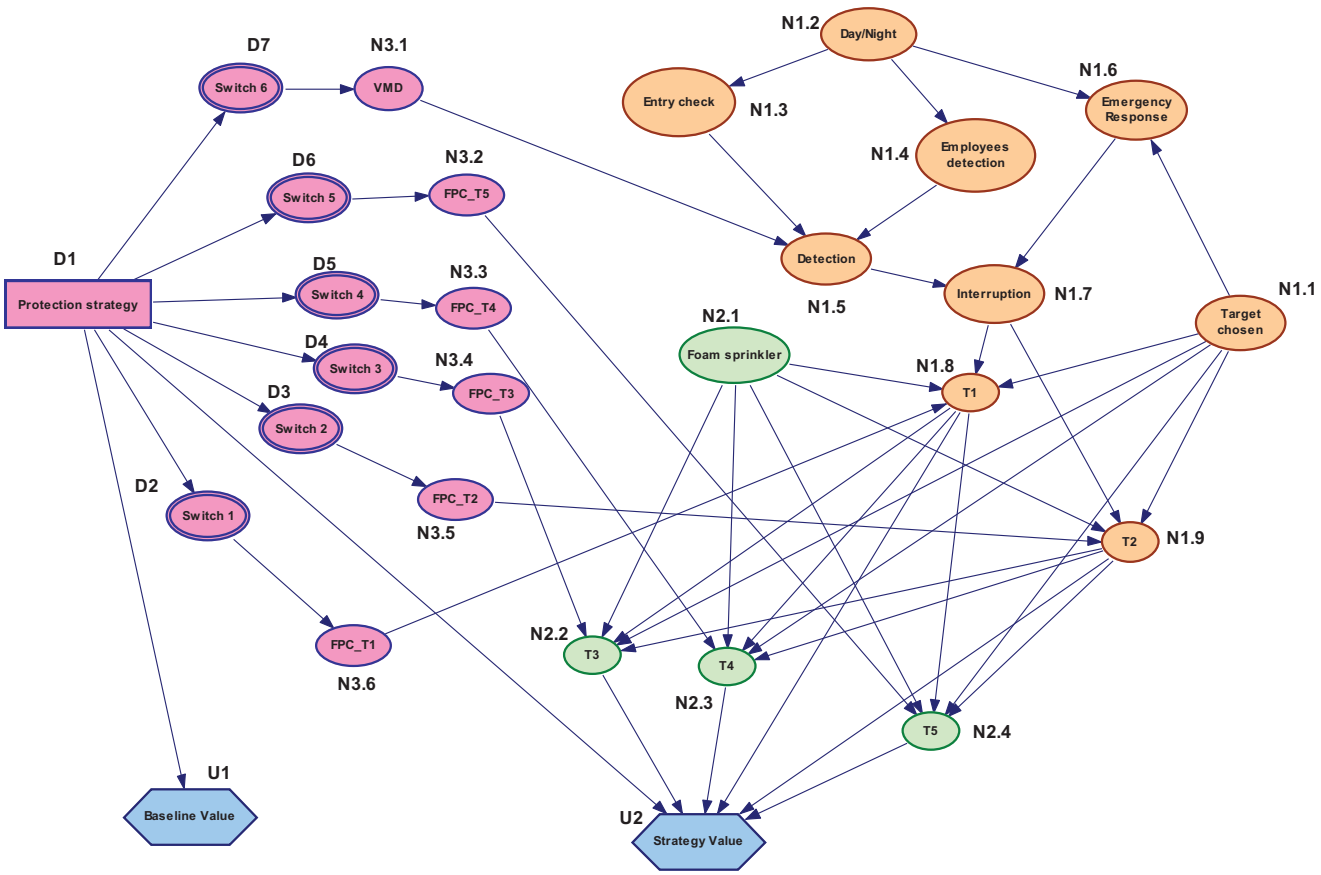

FIGURE 4 | Bayesian network developed for the case study. VMD, video motion detection.

Table 2; their value does not change depending on the protection strategy (see Table 5) because they are baseline barriers. Detection (Node N1.5) is successful only if at least one detection measure is available: during the night, employees are not available, nor is the entry check; thus, there is no detection at night in the baseline case.

Then, the probability of successful emergency response (Node N1.6) is evaluated using Equation (2): delay values for the evaluation of t_P include the time to walk to the target and the time set to complete all tasks and can be retrieved in literature (Garcia 2006; Argenti et al. 2018; Casson Moreno et al. 2022; Marroni, Casini, et al. 2024). The assumptions made for the quantification of node N1.6 are reported in the Supporting Information (see Sheet "Group N1"). N1.7 and N1.8 are related to the probability of damaging the target, and their CPT can be filled using fragility models (see Appendix A). For instance, the probability of damaging the atmospheric tank T2 using 10 kg of TATP from 15 m is 63%.

Group N2 (in green) in Figure 4 represents the escalation scenario. First, the intensity of the final outcome is assessed. The pool fire in the catch basin caused by the successful attack is evaluated using the "burning puddle" model in ALOHA: The surface of the pool is assumed equal to the corresponding catch basin surface S_{CB}, which is reported in Table 3. ALOHA is a simplified tool for consequence assessment, and fuels are a complex hydrocarbon mixture; for this reason, diesel is modeled as pure n-octane,

TABLE 5 | Case study results: prior probability values for the Bayesian network (BN).

Node id	State	Baseline	Protection strategy						
			A	B	C	D	E	F	G
N1.1	"T1"	0.500	0.500	0.500	0.500	0.500	0.500	0.500	0.500
N1.2	"Day"	0.330	0.330	0.330	0.330	0.330	0.330	0.330	0.330
N1.3	"Success"	0.144	0.144	0.144	0.144	0.144	0.144	0.144	0.144
N1.4	"Success"	0.057	0.057	0.057	0.057	0.057	0.057	0.057	0.057
N1.5	"Success"	0.174	0.811	0.174	0.174	0.174	0.811	0.811	0.811
N1.6	"Success"	0.287	0.287	0.287	0.287	0.287	0.287	0.287	0.287
N1.7	"Success"	0.082	0.240	0.082	0.082	0.082	0.240	0.240	0.240
N1.8	"Damaged"	0.498	0.411	0.293	0.498	0.293	0.238	0.411	0.238
N1.9	"Damaged"	0.726	0.599	0.726	0.300	0.300	0.599	0.253	0.253
N2.1	"Works"	0.956	0.956	0.956	0.956	0.956	0.956	0.956	0.956
N2.2	"Damaged"	0.466	0.387	0.465	0.005	0.005	0.386	0.005	0.005
N2.3	"Damaged"	0.499	0.412	0.499	0.006	0.006	0.412	0.005	0.005
N2.4	"Damaged"	0.249	0.303	0.003	0.003	0.249	0.003	0.003	0.303
N3.1	"Active"	0.000	0.771	0.000	0.000	0.000	0.771	0.771	0.771
N3.2, N3.3, N3.4, N3.5	"Active"	0.000	0.000	0.000	0.999	0.999	0.000	0.999	0.999
N3.6	"Active"	0.000	0.000	0.999	0.000	0.999	0.999	0.000	0.999
U1	—	—	152.000	60.700	18.700	14.300	43.400	16.700	13.100
U2	—	—	−125.441	−45.966	−12.225	−5.882	−26.914	−8.999	−4.399
D1	—	—	26.559	14.734	6.475	8.418	16.486	7.701	8.701

Note: For node labels refer to Figure 4; Node D1 is the decision node for each protection strategy.
Abbreviation: VMD, video motion detection.

whereas gasoline is modeled as *n*-heptane. If T1 is chosen on a target, a severe pool fire takes place; in the absence of protection, the heat radiated on T2 is 83.0 kW/m^2, on T3 it is 47.7 kW/m^2, on T4 it is 83.0 kW/m^2, and on T5 it is 47.7 kW/m^2. If T2 is chosen as a target, the heat radiated in absence of protection on T1 is 35.5 kW/m^2, on T3 it is 72.2 kW/m^2, on T4 it is 53.3 kW/m^2, and on T5 it is 31.5 kW/m^2. Hence, the physical effects are above the threshold for atmospheric tanks exposed to pool fire (see Table 1). To calculate the probability of damage, fragility models require the evaluation of the time to failure of the tank, as detailed in Appendix A; the time to failure depends on the heat received, as well as the volume of the tank. In the case of correct functioning of the sprinkler system (N2.1), the obtained 40% reduction in heat radiation is not sufficient to exclude any tank from the escalation scenario. The probabilistic performance of the sprinkler (N2.1) can be retrieved from Table 2.

The protection strategies in Table 4 are implemented in the BN through nodes D1 to D6. Nodes N3.1 to N3.5 represent the performance of the protection strategies, and their CPTs can be filled according to the performance data in Table 2. For the VMD (N3.1), the performance parameters from Table 2 are implemented in the BN for strategies A, E, F, and G. For what concerns fireproofing, on the basis of indications reported in literature (Weil 2011), the minimum extension of 30 min is assumed. These considerations allow the completion of the CPTs for nodes N3.2–N3.5, as well as calculating the damage probabilities for different combinations of effective protection measures in Nodes N1.5, N1.7, N1.8, N2.2, N2.3, and N2.4.

Finally, U1 and U2 are the utility nodes, which represent the two terms of the CBF, as per Equation (5).

More specifically, U1 (baseline value) represents the ratio between $ED_{b,i}$ (see Equation 6) and C_j. It is used to represent the first term of $CBF_{i,j}$ (see Equation 5), that is, the minuend, and it is populated considering the combinations of baseline expected damage and the cost of the protection strategy. On the other hand, U2 (strategy value) represents the negative value of the ratio between $ED_{p,i,j}$ (see Equation 7) and C_j. U2, hence, represents the subtrahend term of the $CBF_{i,j}$, and therefore it holds a negative value. Populating U2 implies evaluating the expected damages ED_p for all combinations of protection strategies and equipment state using Equation (6). The probabilistic-weighted value of the $CBF_{i,j}$ is then computed on the basis of the different protection strategies: The total value of the $CBF_{i,j}$ can be read using GeNIe by clicking on Node D1 once calculations are complete. U1 and U2 values for each strategy are in Table 5, and the last row of the table is the value of the CBF (namely, node D1).

Figure 5 shows the results in terms of probability of damage of the tanks and of CBA. This, coupled with the probability evaluations in Table 5, provides some key insights. The probability of detection (N1.5) and of successfully interrupting the attack (N1.7) changes with the protection strategy. The probability value for these nodes is higher when the VMD is implemented (Strategies A, E, F, and G in Table 4). More specifically, strategy A, involving only VMD, increases the probability of successful detection (N1.3) from 0.174 in the baseline to 0.811. The improvement is considerable because, for the baseline configuration of barriers, an attack during the night could not be detected. It significantly reduces the likelihood of a successful attack, even though it does not act on the escalation scenario. Strategies incorporating fireproofing demonstrate a significant reduction in the damage probability of secondary equipment. For example, in Strategy D (fireproofing all tanks), the probability of damage to T1 and T3 (N2.2 and N2.3) decreases from 0.466 to 0.499 in the baseline case to 0.005 and 0.006, respectively. From a probabilistic standpoint, integrated safety–security protection strategies (E, F, and G) achieve the highest reduction in damage probability of tanks, as they simultaneously act on the attack scenario and on the escalation scenario. This trend is also partially reflected by the CBA. For better clarity, the values of D1 have been plotted in Figure 5.

Namely, one of the three most cost-effective strategies integrates safety and security barriers: Strategy A (VMD), Strategy E (VMD and fireproofing T1), and Strategy B (fireproofing T1). The least cost-effective options, with very similar CBF values (see Table 4), are F (VMD and fireproofing T2, T3, T4, and T5) and option C (fireproofing T2, T3, T4, and T5).

The VMD emerges as the most cost-effective component, which is reasonable considering the low cost of the protection plan (see Table 4) and the improvement in detection capability (Node N1.5 in Table 5). This makes all integrated protection strategies more cost-effective than the safety-only alternative. For example, comparing Strategy B and E shows that Strategy E is slightly more cost-effective than B, which only features fireproofing. It is also interesting to note that the expensive strategies are among the least cost-effective options. These protection strategies focus on the smaller tanks in the depot (T2, T3, T4, and T5). However, T1 is one of the critical targets, and its loss entails an economic loss that is higher than losing the four tanks together. Consequently, even if there is a consistent reduction of escalation on T2, T3, T4, and T5, T1 is still prioritized. Furthermore, escalation on T1 is expected if T2 is successfully damaged, reinforcing again the strategies that protect T1. The results highlight the contribution of safety barriers to security scenarios. It should also be noted that the integration of the VMD with the fireproofing grants a good balance in damage reduction and investment, demonstrating the necessity and the effectiveness of implementing safety and security measures.

4.1 | Sensitivity Analysis

A sensitivity analysis is carried out to evaluate how the variation of the input reflects on the outputs. Among the different types of sensitivity analysis that can be used to our purpose (Saltelli et al. 2007), we adopt a one-at-a-time (OAT) sensitivity analysis. In OAT sensitivity analysis, one input variable is changed while keeping others at their nominal values; then, returning the variable to its nominal value, and the process is repeated for each of the other inputs in the same way. This choice is appropriate at the current stage, as the objective is to explore the individual effect of each parameter and to identify the most influential variables before considering more complex, potentially nonlinear dependencies (Saltelli et al. 2007).

The effect of the following variables and parameters was investigated as follows:

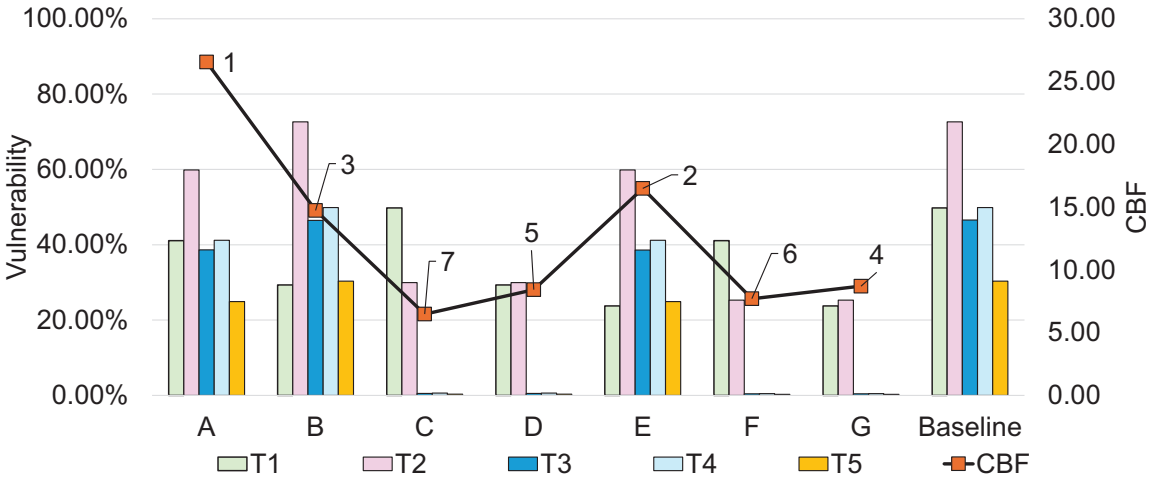

FIGURE 5 | Results using nominal values. The bars represent the vulnerability of the tanks (left axis), the line represents the trend on the CBF (right axis); the labels on the CBF show the ranking in optimality, highest (1) to lowest (7).

- The cost of the protection strategies, C_{sf} and C_{sc}. We assumed a ±20% variation, as data regarding such fluctuations is difficult to retrieve in literature.
- The cost of the stored substance E_s. Credible ranges of variation depend on the substance; however, for commodities, credible values can be retrieved through historical analyses, which are publicly available.
- The losses attributed to the business interruption E_b. Dow also offers a range of variation of maximum probable days of outage (American Institute of Chemical Engineers 2016), which was used to define the credible variation range of the business interruption. It should be noted that the business interruption according to Dow's approach depends on E_e and E_s. To avoid introducing artificial dependencies in the sensitivity analysis, the business interruption term E_b is treated independently from E_e and E_s. The latter are kept at their baseline. This also reflects the practical consideration that, in industrial evaluations, such estimates are typically based on representative market values rather than on short-term values.
- The probability of choosing a target asset, which populates node N1.1 in Figure 4. Namely, if a target is preferred, this could influence the optimality of the protection strategies.

The range of variation is shown and discussed in Table 6. For all the cases in Table 6, the BN in Figure 4 was updated, and consequently the ranking of the cost-effectiveness of the strategies. Figure 6 shows the results of the sensitivity analysis: the protection strategies are ranked from most cost-effective (corresponding to rank number 1), to least cost-effective (rank number 7).

Although the individual values of the CBF change by varying the prices of C_j, E_s, and E_b, there is no change in the order of cost-effectiveness of the protection strategies. This implies that the methodology is robust with respect to the fluctuation of economic parameters.

However, results vary when the probability of choosing a target changes, as shown in Figure 6. Even though the ranking of the various protection options changes as a function of assumptions about target choice, only three protective options (B, E, and F) are ever ranked highly. More in detail, although Strategy A (VMD only) remains the most cost-effective across all four cases, there are significant variations in other parts of the ranking. If only T2 is chosen as a target (Case AA4 in Table 6 and Figure 6), then the three most cost-effective strategies remain the same as the baseline case, although the ranking between Strategies E and B switches: this could be because T1 is at this point a secondary target, and the mitigation (fireproof) becomes more important than the prevention (VMD).

If only T1 is chosen as a target (Case AA3 in Table 6 and Figure 6), then the protection strategies tend to focus on the protection of T2, T3, T4, and T5, making Strategies F and C rise in cost-effectiveness. This is explained by the fact that fireproofing T1 has no direct effect on the prevention of the intentional attack, thus putting them to the bottom of the cost-effectiveness ranking.

If T1 is the preferred target (Case AA1 in Table 6 and Figure 6), then Strategy F becomes the third most-effective, because the T1 escalation scenario reasonably raises in credibility. Finally, if T2 is the preferred target (Case AA2 in Table 6 and Figure 6) or the only target (Case AA4 in Table 6 and Figure 6), it makes T1 a more credible target of an escalation scenario. This means that fireproofing T1 might prove more cost-effective, as demonstrated by the rise of cost-effectiveness of Strategy B. Overall, this confirms the deep interdisciplinary nature of security studies and proves the importance of assessing the attractiveness of targets during the analysis. Still, even adopting a basic sensitivity analysis, the methodology can be effective in the evaluation of protection strategies in different contexts where different targets might be prioritized.

5 | Discussion

The application of the methodology to a case study showed the effectiveness of coupling safety–security measures in reducing

TABLE 6 | Range considered in the sensitivity analysis for the different variables; each case is labeled in order to discuss the results (see Figure 6).

Variable	Baseline value	Max value (case id)	Min value (case id)	Range (%) (source)	Comment
Fireproofing price	€410/m^2	€492/m^2 (PP1)	€328/m^2 (PP4)	±20%	Absence of reference market values
VMD price	€100k	€120 (PP2)	€80 (PP3)	±20%	
Diesel price	€1.53/L	€1.81/L (RP1)	€1.24/L (RP4)	±19% (MASE 2025)	Prices in the last 15 years in Italy
Gasoline price	€1.63/L	€1.89/L (RP2)	€1.37/L (RP3)	±16% (MASE 2025)	
Business interruption (E_b) for T2, T3, T4, and T5	€354k (26 days)	€598k (BIP1)	€190k (BIP4)	+68% (+43 days), −46% (−13 days) (American Institute of Chemical Engineers 2016)	Considering maximum probable days of outage
Business interruption (E_b) for T1	€6340k (6 days)	€10,700k (BIP 3)	€3376k (BIP2)	+68% (+10 days), −46% (−3 days) (American Institute of Chemical Engineers 2016)	
Probability of choosing T1	0.5	1.0 (AA3), 0.7 (AA1)	0.0 (AA4), 0.3 (AA2)	±100%	Only one target is chosen (AA3 and AA4). One target is preferred to the other (AA1 and AA2)

Abbreviation: VMD, video motion detection.

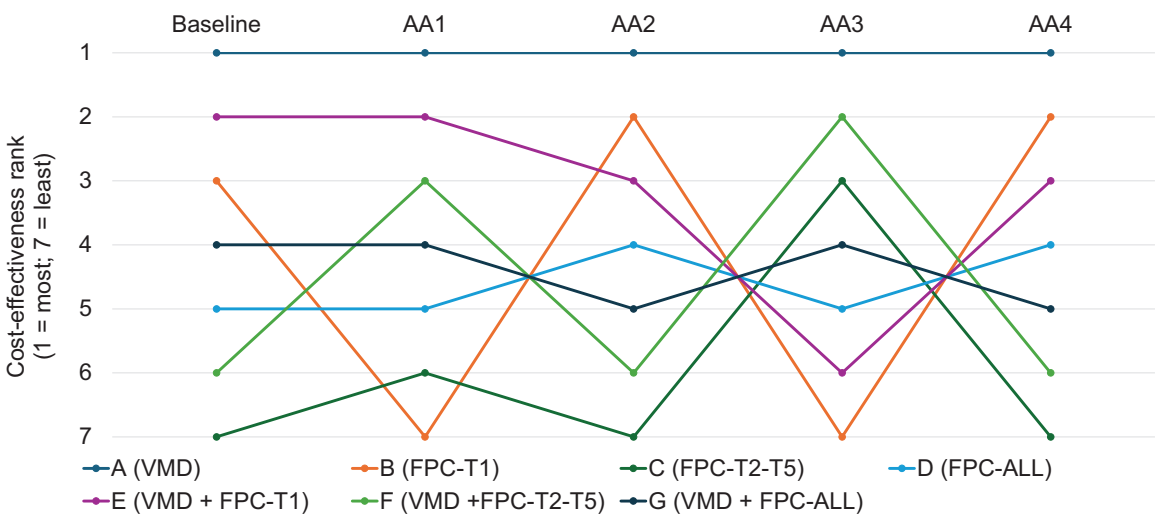

FIGURE 6 | Results of the sensitivity analysis in terms of ranking of the strategies shown in Table 4 for different probabilities of choosing a target (see Table 6); 1 = most cost-effective strategy; 7 = least cost-effective strategy. VMD, video motion detection.

and controlling escalation scenarios, while still being convenient price-wise.

We can validate the analysis using the methods proposed by Lee et al. (2019): reality check, benchmarking, and peer review. The reality check supports the preliminary hazard identification performed in Step 2 of the methodology. For benchmarking, no comprehensive methodology exists for integrated safety–security CBA. We therefore benchmarked only individual steps of the

methodology by using established tools from physical security of process facilities. Finally, submission to this journal and the response to reviewers' comments directly fulfill the peer-review validation step.

Nonetheless, the methodology, whereas sufficiently robust, can still be improved. The main focus of the work was to define necessary steps to tackle CBA for integrated safety–security scenarios: each step contains simplifying assumptions. Still, it should be noted that more detailed models can still be employed in the framework we developed; for example, more rigorous consequence modeling can be adopted for final outcomes adopting tools, such as DNV Phast. Additionally, the economic analysis of the study could benefit from further refinement, to capture the evolution in time of the cost-effectiveness. Namely, through a dynamic BN, the CBF could be evaluated over time. Moreover, it is possible to integrate metrics, such as the net present value (NPV), within the methodology. However, for the sake of demonstration of the proposed methodology, we opted for an approach that is independent from the lifetime of the facility and that calculates the costs associated with a given security scenario. Similar approaches can be found in literature (Misuri et al. 2019).

The extension of the methodology with the points mentioned above might also lead to some drawbacks, especially with the potential implementation of the above-mentioned improvements. One of the main issues of BN is the so-called curse of dimensionality (Chandra et al. 2023): namely, the more nodes, states, and dependencies included in the BN, the more onerous it comes to quantify. To overcome this, this approach could be coupled with a preliminary analysis to identify the most relevant escalation scenarios. For example, approaches based on graph theory have a much lower computational cost than BN (Khakzad et al. 2017) and could support the preliminary analysis of relevant escalation scenarios.

Finally, it is worth mentioning that process safety practice often relies on heuristic or semi-quantitative methods due to resource constraints. Hence, the approach we propose may be not routinely applied but rather adopted in specific high-risk or geopolitically sensitive contexts requiring robust quantitative support for decision-making. Beyond its direct application, this work aims to stress the need for integrated safety–security evaluations and to stimulate more systematic approaches in future practice.

6 | Conclusions

Threats to chemical and process facilities have become sophisticated and multi-faceted in the last few years. Thus, protecting these installations against external attacks has become a matter of interest for practitioners, as well as the scientific community. For this reason, this work deals with cost-effective selection of protection strategies to protect process facilities from integrated safety–security threats through a probabilistic-based methodology based on BN. First, we provide a characterization and classification of barriers, in order to define the quantitative performance parameters required for the analysis. Then, a cost–benefit function is defined by comparing the damages deriving from the intentional attacks with the cost of protection strategies. The protection strategies and cost-benefit function are implemented in the BN using decision and utility nodes. The application of the methodology to a petroleum depot shows the effectiveness of coupled safety–security measures in reducing and controlling escalation scenarios, while still being convenient price-wise. The developed approach can guide plant managers and practitioners in obtaining a practical overview of the cost-effectiveness of different protection strategies and in investing in additional protection plans.

Acknowledgments

This work is supported by PNRR M4C2—HPC, Big data and Quantum Computing (simulazioni, calcolo e analisi dei dati e altre prestazioni—CN1)—CUP I53C22000690001 SPOKE 6 Multiscale modelling & Engineering applications and by the National Recovery and Resilience Plan (NRRP).

Data Availability Statement

The data that supports the findings of this study are available in the supplementary material of this article.

References

American Institute of Chemical Engineering. 2016. *Dow's Fire and Explosion Index Hazard Classification Guide*. 7thed. John Wiley & Sons.

American Petroleum Institute. 2008. "*API Recommended Practice*." In *Risk-Based Inspection Technology*. 2nd ed. American Petroleum Institute.

Argenti, F., G. Landucci, G. Reniers, and V. Cozzani. 2018. "Vulnerability Assessment of Chemical Facilities to Intentional Attacks Based on Bayesian Network." *Reliability Engineering & System Safety* 169: 515–530. https://doi.org/10.1016/j.ress.2017.09.023.

Atexshop. 2025. *MAXIMUS MVXHD Camera Full HD, 1080p, 60fps*. Atexshop. https://www.atexshop.com/maximus-mvxhd-camera-full-hd-1080p-60fps.html.

Bayesfusion LLC. 2025. GeNIe Modeler: Complete Modeling Freedom. Bayesfusion LLC. https://www.bayesfusion.com/genie/.

Casson Moreno, V., G. Marroni, and G. Landucci. 2022. "Probabilistic Assessment Aimed at the Evaluation of Escalating Scenarios in Process Facilities Combining Safety and Security Barriers." *Reliability Engineering & System Safety* 228: 108762. https://doi.org/10.1016/j.ress.2022.108762.

Casson Moreno, V., G. Reniers, E. Salzano, and V. Cozzani. 2018. "Analysis of Physical and Cyber Security-Related Events in the Chemical and Process Industry." *Process Safety and Environmental Protection* 116: 621–631. https://doi.org/10.1016/j.psep.2018.03.026.

Chandra, N. K., A. Canale, and D. B. Dunson. 2023. "Escaping the Curse of Dimensionality in Bayesian Model-Based Clustering." *Journal of Machine Learning Research* 24: 1–42. https://jmlr.org/papers/v24/21-1276.html.

Cox, L. A. 2009. "Improving Risk-Based Decision Making for Terrorism Applications." *Risk Analysis* 29: 336–341. https://doi.org/10.1111/j.1539-6924.2009.01206.x.

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

Garcia, M. L. 2005. *Vulnerability Assessment of Physical Protection Systems*. Elsevier.

Garcia, M. L. 2006. *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann.

George, P. G., and V. Renjith. 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. https://doi.org/10.1016/j.psep.2021.03.031.

Hanea, A. M., A. Christophersen, and S. Alday. 2022. "Bayesian Networks for Risk Analysis and Decision Support." *Risk Analysis* 42, no. 6: 1149–1154. https://doi.org/10.1111/risa.13938.

Hausken, K. 2016. "A Cost–Benefit Analysis of Terrorist Attacks." *Defence and Peace Economics* 29, no. 2: 111–129. https://doi.org/10.1080/10242694.2016.1158440.

Iaiani, M., A. Tugnoli, and V. Cozzani. 2022. "Identification of Reference Scenarios for Security Attacks to the Process Industry." *Process Safety and Environmental Protection* 161: 334–356. https://doi.org/10.1016/j.psep.2022.03.034.

Janssens, 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. https://doi.org/10.1016/j.ress.2015.05.022.

Jensen, F. V., and T. D. Nielsen. 2007. *Bayesian Networks and Decision Graphs*. 2nd ed. Springer.

Khakzad, N. 2023. "Reducing the Risk of Intentional Domino Effects in Process Plants: A Risk-Based Minimax Strategy." *Process Safety Progress* 42, no. 2: 281–289. https://doi.org/10.1002/prs.12443.

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, no. 9: 1652–1667. https://doi.org/10.1111/risa.12712.

Landucci, G., S. Bonvicini, and V. Cozzani. 2017. "A Methodology for the Analysis of Domino and Cascading Events in Oil & Gas Facilities Operating in Harsh Environments." *Safety Science* 95: 182–197. https://doi.org/10.1016/j.ssci.2016.12.019.

Lee, S., G. Landucci, G. Reniers, and N. Paltrinieri. 2019. "Validation of Dynamic Risk Analysis Supporting Integrated Operations across Systems." *Sustainability* 11, no. 23: 6745. https://doi.org/10.3390/su11236745.

Marroni, G., L. Casini, A. Bartolucci, S. Kuipers, V. Casson Moreno, and G. Landucci. 2024. "Development of Fragility Models for Process Equipment Affected by Physical Security Attacks." *Reliability Engineering & System Safety* 243: 109880. https://doi.org/10.1016/j.ress.2023.109880.

Marroni, G., L. Casini, S. Kuipers, et al. 2023. "Real-Time Assessment of Integrated Safety-Security Scenarios Triggering Cascading Events in the Process Industries." *Chemical Engineering Transactions* 99: 349–354. https://doi.org/10.3303/CET2399059.

Marroni, G., V. Casson Moreno, A. Tortolini, F. Tamburini, and G. Landucci. 2024. "Assessing the Attractiveness of Chemical and Process Facilities to Terrorism Using a Situational Crime Prevention Approach." *Journal of Loss Prevention in the Process Industries* 89: 105321. https://doi.org/10.1016/j.jlp.2024.105321.

MASE—Italian Ministry of Environment and Energetic Security. 2024. *Montly costs of fuels in Italy*. MASE https://sisen.mase.gov.it/dgsaie/prezzi-mensili-carburanti.

MASE—Italian Ministry of Environment and Energetic Security. 2025. Open data on energy and fuels. https://sisen.mase.gov.it/dgsaie/open-data.

Matches. 2025. *Tank Cost Estimate*. Matches. https://www.matche.com/equipcost/Tank.html.

Matteini, A., F. Argenti, E. Salzano, and V. Cozzani. 2019. "A Comparative Analysis of Security Risk Assessment Methodologies for the Chemical Industry." *Reliability Engineering & System Safety* 191: 106083. https://doi.org/10.1016/j.ress.2018.03.001.

Mishan, E., and E. Quah. 2020. *Cost-Benefit Analysis*. Routledge. https://doi.org/10.4324/9781351029780.

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. https://doi.org/10.1016/j.ress.2018.03.028.

Paltrinieri, N., S. Bonvicini, G. Spadoni, and V. Cozzani. 2012. "Cost-Benefit Analysis of Passive Fire Protections in Road LPG Transportation." *Risk Analysis* 32, no. 2: 200–219. https://doi.org/10.1111/j.1539-6924.2011.01654.x.

Peters, M. S., K. D. Timmerhaus, and R. E. West. 2003. *Plant Design and Economics for Chemical Engineers*. McGraw-Hill Education.

Saltelli, A., M. Ratto, T. Andres, et al. 2007. Global Sensitivity Analysis. *The Primer*. Wiley. https://doi.org/10.1002/9780470725184.

Sklet, S. 2006. "Safety Barriers: Definition, Classification, and Performance." *Journal of Loss Prevention in the Process Industries* 19, no. 5: 494–506. https://doi.org/10.1016/j.jlp.2005.12.004.

Stewart, M. G., and J. Mueller. 2013. "Terrorism Risks and Cost-Benefit Analysis of Aviation Security." *Risk Analysis* 33: 893–908. https://doi.org/10.1111/j.1539-6924.2012.01905.x.

United States Environmental Protection Agency. 2025. *Aloha Software*. United States Environmental Protection Agency. https://www.epa.gov/cameo/aloha-software.

Van Den Berg, B., P. Hutten, and R. Prins. 2020. "Security and Safety: An Integrative Perspective." In *Advanced Sciences and Technologies for Security Applications*. Springer. https://doi.org/10.1007/978-3-030-42523-4_2.

Van Den Bosch, C. J. H., and R. A. P. M. Weterings. 2005. *Methods for the Calculation of Physical Effects*, Yellow Book. 3rd ed. Hague Committee for the Prevention of Disasters.

Villa, V., G. 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: 311–339. https://doi.org/10.1016/j.psep.2017.03.023.

Wang, Z., K. Hu, and Y. Zhao. 2022. "Doom-Roof Steel Tanks Under External Explosion: Dynamic Responses and Anti-Explosion Measures." *Journal of Constructional Steel Research* 190: 107118. https://doi.org/10.1016/j.jcsr.2021.107118.

Weil, E. D. 2011. "Fire-Protective and Flame-Retardant Coatings—A State-of-the-Art Review." *Journal of Fire Sciences* 29, no. 3: 259–296. https://doi.org/10.1177/07349041103954.

Yuan, Z., N. Khakzad, F. Khan, and P. Amyotte. 2014. "Risk Analysis of Dust Explosion Scenarios Using Bayesian Networks." *Risk Analysis* 35, no. 2: 278–291. https://doi.org/10.1111/risa.12283.

Zhao, Y., B. Cai, V. Cozzani, and Y. Liu. 2024. "Failure Dependence and Cascading Failures: A Literature Review and Investigation on Research Opportunities." *Reliability Engineering & System Safety* 256: 110766. https://doi.org/10.1016/j.ress.2024.110766.

Supporting Information

Additional supporting information can be found online in the Supporting Information section.

Supporting information: risa70230-supp0001-SuppMat

Appendix A

Table A1 and A2, respectively, summarize the fragility models used for the quantitative assessment of the explosive attack and fired escalation scenarios.

TABLE A1 | Fragility model for equipment exposed to explosive attack scenarios.

Item	Definition	Value/Equation
$P_{f,P}$	Probability of failure of atmospheric tanks exposed to overpressure	$P_{f,P} = \phi(Y_P - 5)$ where $\phi(.)$ is the normal distribution
Y_P	Probit value for atmospheric tanks exposed to overpressure	$Y_P = -18.96 + 2.44\ln(\Delta P)$ Probit equation for atmospheric equipment subjected to overpressure ΔP
ΔP	Peak overpressure (Pa) at the target location caused by the TATP explosion	$\Delta P = 10^5\left(\frac{m_{\mathrm{TNT,eq}}^{\frac{1}{3}}}{r} + 4.4\frac{m_{TNT,\mathrm{eq}}^{\frac{2}{3}}}{r^2} + 14.0\frac{m_{\mathrm{TNT,eq}}}{r^3}\right)$
r	Scaled distance (m/kg$^{1/3}$)	$r = \frac{R}{m_{\mathrm{TNT,eq}}^{1/3}}$ where R is the distance (m) of the target equipment from the explosion
$m_{\mathrm{TNT,eq}}$	Equivalent TNT amount (kg) to a given mass of TATP homemade explosive	$m_{\mathrm{TNT,eq}} = \eta_{\mathrm{TNT}} \times m_{\mathrm{TATP}}$ where $\eta_{\mathrm{TNT}} = 0.61$ is the TNT efficiency and m_{TATP} is the mass of TATP used to attack the equipment (i.e., 10 kg in the case study)

Source: Adapted from Marroni, Casini, et al. (2024).

TABLE A2 | Fragility model for fired escalation scenarios.

Item	Definition	Value/Equation
$P_{f,F}$	Probability of failure of atmospheric tanks exposed to fire	$P_{f,F} = \phi(Y_F - 5)$ where $\phi(.)$ is the normal distribution
Y_F	Probit value for atmospheric tanks exposed to fire	$Y_F = 9.25 - 1.85\ln(\mathrm{ttf}/60)$ Probit equation for atmospheric equipment subjected to fire
ttf	Time to failure (s) of atmospheric tanks exposed to heat radiation due to fire	$\ln(\mathrm{ttf}) = -1.13\ln(Q) - 2.6710^{-5}V + 9.9$ Time to failure correlation, where Q is the received heat radiation in kW/m^2, and V is the volume of the tank in m^3

Source: Adapted from Marroni, Casini, et al. (2024).