Assessment of integrated safety-security barriers performance to support the management of industrial installations

Casson, Moreno V.; Marroni, G.; Guarguaglini, M.; Kuipers, S.L.; Landucci, G.

CHEMICAL ENGINEERING TRANSACTIONS
VOL. 116, 2025
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Bruno Fabiano, Valerio Cozzani

ISBN 979-12-81206-18-2; **ISSN** 2283-9216
DOI: 10.3303/CET25116067

Assessment of Integrated Safety-Security Barriers Performance to Support the Management of Industrial Installations

Valeria Casson Moreno[a], Giulia Marroni[a], Michela Guarguaglini[a], Sanneke Kuipers[b], Gabriele Landucci[a,*]

[a]Department of Civil and Industrial Engineering – University of Pisa, Largo Lucio Lazzarino n.2, 56126 Pisa (Italy)
[b]Institute of Security and Global Affairs, Leiden University, Turfmarkt n.99, 2511 DP Den Haag, the Netherlands
gabriele.landucci@unipi.it

The assessment of accident scenarios linked to intentional attacks on chemical and process facilities has gained significant attention due to escalating conflicts in critical contexts. This work presents a methodology for the quantitative integration of safety and security aspects within the Event Tree Analysis (ETA), a widely used tool in Quantitative Risk Assessment (QRA). Firstly, the conceptual framework is established: safety and security barriers are identified, and classified based on the functions and working principles. Then, the performance of the barriers is studied in terms of availability and efficiency. This support the incorporation of the barriers into the ETA using tailored decisional gates and quantifying the probability of escalation due to external attacks. The application of the methodology to a demonstration case study next shows its potential: safety barriers effectively mitigate the escalation probability of intentional attacks, reducing plant vulnerability and providing a clearer understanding of facility criticalities. The proposed methodology can seamlessly integrate into existing QRA studies, offering a unified framework to enhance risk-based decision-making and resource allocation.

1. Introduction

In recent years, the protection of chemical and process plants from intentional attacks has garnered significant attention from researchers, institutions, and the industry. Namely, plants storing and processing hazardous chemicals are shown to be attractive targets of intentional attacks (Iaiani et al., 2022). The intentionality of actions is essential to security science, but the discipline is also linked to conventional process safety, as safety barriers can play a crucial role in preventing and/or mitigating security risks. Additionally, accidental scenarios resulting from both unintentional and intentional events can escalate, creating cascading effects that amplify consequences and could severely impact people, assets, and the environment. For this reason, the integration of safety and security is essential to understand, model and manage cascading effects in process facilities.
Several studies have approached the Integration of Safety and Security (ISS). Yuan et al. (2022) emphasized the importance of combining safety and security barriers for a comprehensive management of process and chemical facilities. Iaiani et al. (2022) applied a Bow-Tie approach to identify reference release scenarios for intentional attacks. Chen et al. (2019) developed an approach for the integration of safety and security through dynamic graphs. The mentioned work tackle concepts that are often adopted in conventional Quantitative Risk Assessment (QRA). However, current literature has not yet focused on developing a quantitative methodology to evaluate the performance of barriers that could be readily integrated in QRA.
Therefore, this work proposes a methodology that quantitatively integrates safety-security barriers and cascading effects in the conventional Event Tree Analysis (ETA), with the aim of comprehensively describing the evolution of complex accidental chains caused by ISS events. The performance of barriers is studied and specific decision gates are tailed to security barriers. The methodology is applied to a case study discussing the potential benefits and drawbacks of the application for risk-informed decision-making.

Paper Received: 15 December 2024; Revised: 31 January 2025; Accepted: 15 April 2025
Please cite this article as: Casson Moreno V., Marroni G., Guarguaglini M., Kuipers S., Landucci G., 2025, Assessment of Integrated Safety-security Barriers Performance to Support the Management of Industrial Installations, Chemical Engineering Transactions, 116, 397-402 DOI:10.3303/CET25116067

2. Methodology

The methodology developed in this work consists of three main steps:

1) Conceptual framework development
2) Performance assessment of Integrated Safety-Security barriers
3) Development of the demonstrational case study

Step 1 is dedicated to the development of the conceptual framework, which is presented in Section 2.1. Relevant literature has been examined in order to assess the main definitions related to both safety and security barriers. This guides Step 2 (see Section 2.2), where typical safety and security barriers are identified, and their performance is quantitatively assessed. Finally, the potentialities of the method have been demonstrated in Step 3 (see Section 3) through the application to a case study.

2.1 Conceptual framework development

The concept of "barrier" is applied in numerous engineering fields, hence many definitions are available, each one emphasizing different concepts. For this reason, before moving to the quantitative evaluation of barriers, it is necessary to establish a conceptual framework, stating our interpretation of barriers, their functions and working principles. In this work, the conceptual framework adopted is based on the ARAMIS approach (De Dianous and Fiévez, 2006) that is extended to both safety and security events to define the function of the barriers, intended as the action to be done by the barrier to interrupt the chain of undesired events. For safety barriers, the function could be either to prevent the accidental event, or to mitigate its consequences. Security barriers, often referred to as Physical Protection Systems (PPS) are either aimed at detecting the intrusion, delaying the adversary, or responding, e.g., neutralizing it. Another important characteristic of the barriers is the way the function is carried out, e.g., the working principle. This classification can be applied to both safety and security barriers; namely, active barriers require external activation, and are typically connected to engineered systems, e.g., water deluge systems or Closed Circuit Television (CCTV). Passive barriers instead do not require external activation, e.g., fire walls or doors. Finally, procedural barriers refer to specific operating procedures, such as emergency response or evacuation.

Table 1 sums up the main concepts related to the established framework. The Reader is directed to (Securdomino, 2024) for the extensive discussion on the conceptual framework.

Table 1: Classification of ISS barriers based on working principle and function

	Security barriers (PPS)	Safety barriers
Function	Detect, delay, respond	Preventive, mitigative
Working principle	Active, passive, procedural	

2.2 Performance Assessment of ISS barriers

The classification of barriers carried out in Section 2.1 supports the assessment of the parameters that are needed to quantitatively describe their performance. In particular, the probabilistic parameters adopted in this work are: i) the availability the barriers, expressed in terms of the probability of failure on demand (*PFD*); ii) the effectiveness (η) expressing the probability of the barrier of preventing the escalation of the scenario once successfully activated. An additional performance parameter is the attenuation factor φ, which is used to evaluate the decrease of physical effects by action of mitigative barriers; despite not being a probabilistic parameter, it is essential in order to assess potential cascading effects. Different techniques can be used to evaluate the numerical values of PFD, η, and φ, such as fault trees, human error, or suppliers data. For the sake of exemplification, the assessment of the performance of a fence door is hereby explained. A fence door is a passive PPS, that has the function to delay the adversary; so, its performance is described only by PFD and η. Since the door is a fixed installation, its availability is constant, leading to a PFD_{door} = 0.00. For what concerns the effectiveness, in this application we consider that the door might be not well locked by an operator; to evaluate the probability of not locking the door, the SPAR-H methodology from (Gertman et al., 2005) can be adopted. According to the definition from the SPARH-H methodology, not locking the door can be seen as a task requiring only an action. Since this is a relatively simple action, it is assumed that the procedures do not clearly emphasize it, and that trainings are not specifically focused on this specific action. This results in a value of 1.50 actions failed per 100 total actions, thus leading to η_{door} = 1.000 – 0.015 = 0.985.

The parameters defined above can be thus implemented in the ETA by means of specific logical gates. These gates have been adapted from the work of (Casson Moreno et al., 2022) and are summarized in Table 2. Namely, the probabilistic parameters are combined according to the type of distribution (single for gate A, composite for gate B, and discrete for gate C). Gate D instead represents the physical integrity of the targeted

equipment: namely, the failure probability of the equipment P_d is evaluated based on the received dose of physical effects, e.g., overpressure or heat radiation, through the use of fragility models found in the literature. Table 3 sums up the information on the barriers that are going to be used in the demonstrational case study in Section 3.

Table 2: Gate types and representation (adapted from (Casson Moreno et al., 2022))

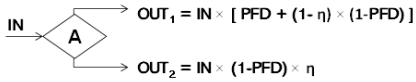
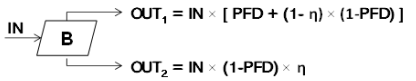
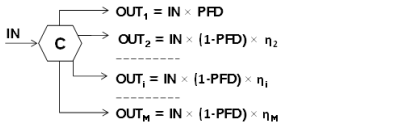
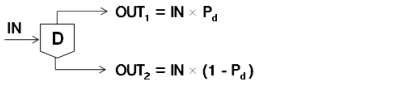
Gate type & representation	Description
	Simple composite probability: availability is multiplied by a single probability value expressing the probability of barrier success in the prevention of the escalation.
	Composite probability distribution: availability is multiplied by a probability distribution expressing the probability of barrier success in the prevention of escalation, thus obtaining a composite probability of barrier failure on demand.
	Discrete probability distribution: depending on barrier effectiveness, three or more events may originate from the gate describing the barrier performance.
	Vessel fragility gate: based on the status of the target equipment, the damage probability (P_d) is computed through equipment vulnerability models.

Table 3: Performance of barriers used in this work. AIT: adversary intrusion time; ERT = emergency response time. For gate types, see Table 2

Barrier name	Function	Working Principle	Gate type	PFD	η	Source
Entry Control	Procedural	Detect	A	4.00E-01	8.00E-01	(Casson Moreno et al., 2022)
Fence door	Passive	Delay	A	0.00	9.85E-01	This work
Detection by site personnel- daytime	Procedural	Detect	A	2.00E-01	2.48E-01	(Casson Moreno et al., 2022)
Emergency team	Procedural	Respond	C	7.52E-01	1.00 if AIT>ERT 0.00if AIT≤ERT	(Casson Moreno et al., 2022)
Water Deluge System (WDS)	Active	Mitigate	B	4.33E-02	1.00	(Securdomino, 2024)

3. Case study

The methodology presented in Section 2 is applied to a case study. In particular, a Liquefied Petroleum Gas (LPG) depot is studied; the layout is shown in Figure 1.

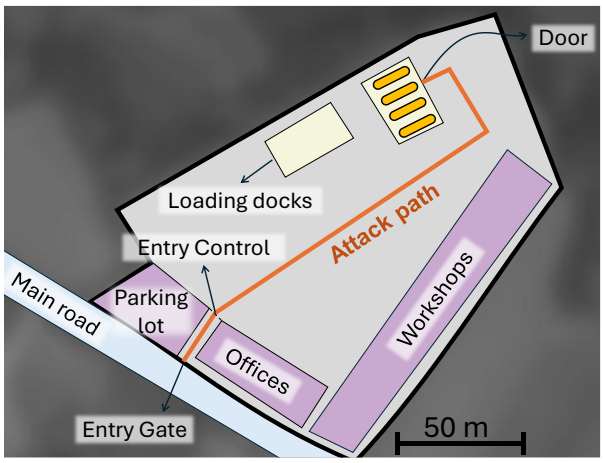


Figure 1: Layout of the case study

The facility stores LPG in four horizontal cylindrical vessels, each of one storing a maximum of 100 m^3 of LPG. The LPG vessels are isolated through a fence, that can be accessed through an entry road located on the opposite side of the loading docks; moreover, a Water Deluge System (WDS) is available to cool off the vessels in case of fire. Road tankers access the facility to load the LPG through the loading docks, while filling of the LPG vessels happens once per day. During the day, the entry gate is open, and visitors are identified at the entry control, which is conducted by dedicated personnel, which is also in charge of the intervention inside the plant in case of intrusion. For the exemplification of the methodology, the following attack scenario is studied: an intruder enters the facility during the day, walks 20 m, successfully passes the entry controls, walks 170 m to the LPG fence, find the door open, and uses an incendiary weapon on one of the tanks for 90 s.

4. Results and discussion

The Event Tree (ET) obtained for the attack scenario presented in Section 3 is shown in Figure 2.

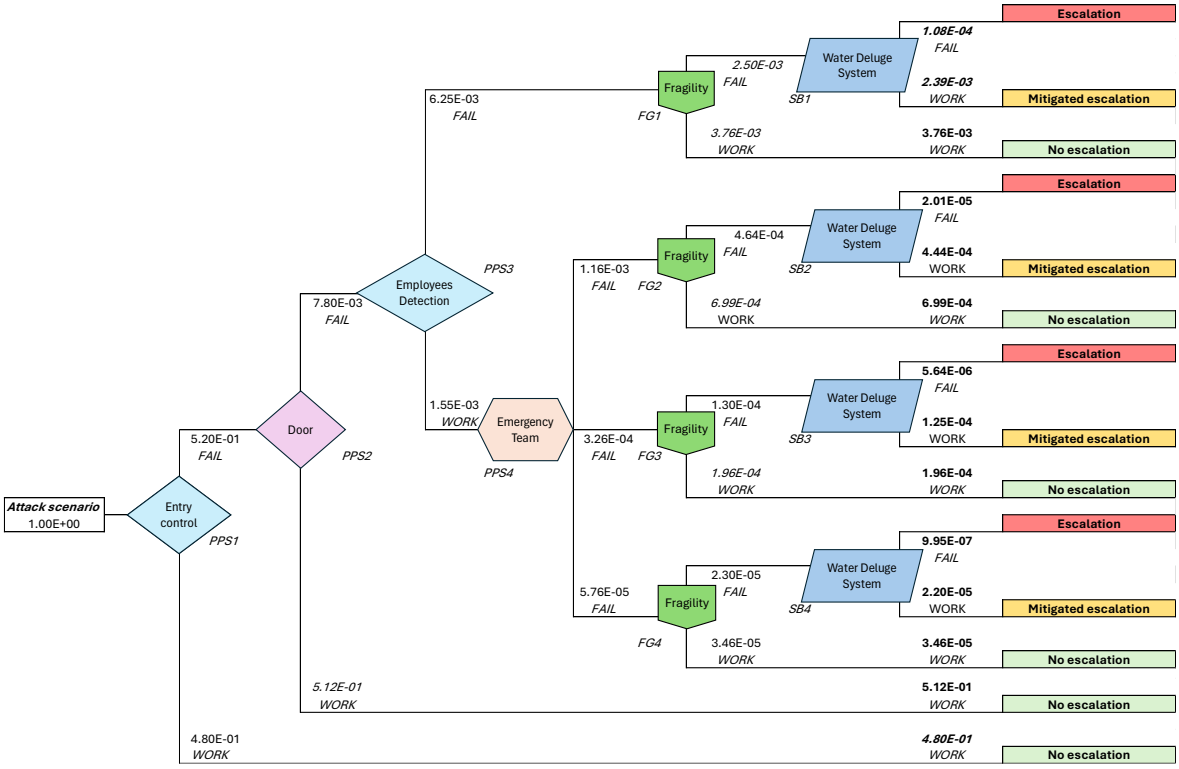


Figure 2: Event tree for the attack scenario presented in Section 3. For gate types and barriers data refer to Table 2 and Table 3, respectively

The first PPS encountered by the adversary is the entry control (*PPS1*), located at the access point of the plant. The attack scenario moves forward only if the adversary successfully eludes the guards; otherwise, no escalation is considered (lower branch from *PPS1* in the ET). The next PPS is the fenced door of the LPG storage; the attack scenario is interrupted if the adversary finds a locked door. While inside the facility, the adversary can be detected by the employees working on the site (*PPS3*). The performance of PPS1, PPS2, and PPS3 can be evaluated using the values in Table 3 combined with the appropriate gate in Table 2. The emergency team (*PPS4*) can intervene and block the attack only if the detection is successful. To determine the efficacy of the emergency team, the Adversary Intrusion Time (AIT) should be evaluated: a total distance of 190 m travelled at a fast walking speed (3 m/s) yields 60 seconds to reach the target, while 90 s are necessary to use the weapon, resulting in 150 s to complete the scenario. According to the sources cited in Section 2.2, a well-trained team acts in ERT_H = 240 s, while a low-trained team in ERT_L = 360 s. Applying the formulas in Table 2 and 3, no team is able to stop the attacker, because the AIT is higher than both ERT_H and ERT_L. This implies that, if the intruder finds the door open, it is always able to successfully reach the target. The fragility of the equipment should be evaluated through gates *FG1*, *FG2*, *FG3*, and *FG4*. By applying the model presented in (Marroni et al, 2024) for incendiary attacks, the probability of failure P_d is around 40%. If the pressure vessel resists, then the attack scenario is not considered successful; this is represented by the lower branches

stemming from *FG1-4* in the ET in Figure 2. Otherwise, the scenario is successful, and its escalation degree is determined by the performance of the WDS (*SB1*, *SB2*, *SB3*, and *SB4*), which can be also quantified using the values shown in Section 2.2. Namely, a full escalation happens in case of failure of the WDS (upper branch from *SB1-4* in Figure 2*)*, with potential cascading effects involving the other vessels found inside the fence. On the other hand, a mitigated escalation takes place is case of correct functioning of the WDS, represented by the lower branches of *SB1-4* in Figure 2.
The result of the probabilistic assessment is shown in Figure 3. The synergistic performance of barriers is labeled as ISS in Figure 3. Additionally, the same scenario is analyzed under two specific conditions: excluding the performance of security barriers (NO PSS in Figure 3) and neglecting the contribution of safety barriers (NO SB in Figure 3). These cases aim to better isolate and highlight the individual contributions of each type of barrier. The same event tree in Figure 2 can be used to evaluate these cases, by setting *PFD* values to unitary, and η values to null for the omitted barriers.

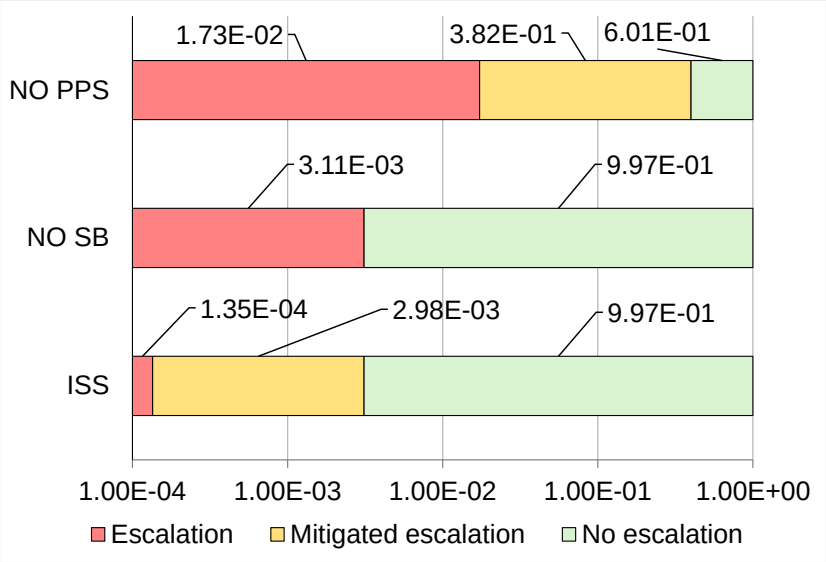


Figure 3: Results of the probabilistic assessment; PPS= security barriers; SB = Safety barriers, ISS= Integration of safety and security barriers

Neglecting the performance of the WDS (*SB1-4*) does not reduce the probability of the “No escalation” scenario; still, it allows to better characterize the intensity of the evolution of the scenario, as it is a mitigative barrier, reducing the probability of the “Escalation” scenario by 95%. This severely downsizes the likelihood of cascading scenarios, allowing for an improvement in the prioritization of different scenarios. Another important consideration is to be made regarding the performance of security barriers. For the analyzed attack scenario, the emergency team always fails in neutralizing the adversary, because the facility is relatively small and the intervention times are not optimized. Additionally, the overall performance of the detection (both employees and entry controls) is not very high compared to the performance of the safety barrier (see Table 3); this is a reasonable result because in this case, detection is only enforced with procedural PPS, which are thus based on human action. Still, when security barriers are neglected, the probability of escalation rises sharply to 1.73×10^{-2}, which is approximately 128 times higher than in the ISS case. This shows how an effective layering of PPS can still be effective, even though the installation of active detection systems, e.g., a CCTV system, should be taken into consideration.
The developed methodology could support the determination of the likelihood of intentional attacks, which could then be implemented in quantitative risk studies, as well as in more complex risk assessment techniques, including three-dimensional and real-time risk assessment (Marroni et al., 2023). Another area of application could be the evaluation of the potential economic losses associated to ISS scenarios, leading also to economic risk assessment. A benefit of the present approach is its flexibility; namely, the established conceptual framework allows the characterization of several barriers. Moreover, the performance of the already characterized barriers can still be refined, for example by using data directly supplied by the facility under analysis.
Nonetheless, further improvements can be made to the methodology. The first improvement can be made by including the dynamic evolution of the attack path according to the performance of the barriers; referring to

Figure 2, another tree branch could be added regarding to the action of the intruder if they find the door correctly locked. They could, for example, decide to target another point of the facility, e.g., the loading docks. This would refine even more the accidental scenarios that can be captured by the methodology. Another development may be related to a more detailed analysis of the interactions and potential interferences between safety and security barriers, and how they impact the overall credibility of escalation of scenarios. Finally, the methodology could be seamlessly integrated in the Bow-Tie approach (De Dianous and Fiévez, 2006); this approach can be applied to both safety and security events and puts the accidental or intentional event in the middle of the representation. The left side of the tree is a Fault Tree (FT), while the right side is the ET. For ISS events, the left side of the tree should include the motivation from a potential attacker, socio-economic factors, as well as security culture and management within the site under analysis, which could be modeled using the approach shown in this work. Still, in its current form, the methodology can assist in understanding complex accidental chains and prioritizing critical scenarios.

5. Conclusions

The rising tensions in the current geopolitical space has led to an increase in attention to security aspects not only for civil structures, but also for critical infrastructures. This work deals with the integration of safety and security aspect in conventional tools for QRA. More specifically, typical safety and security barriers were identified, quantified and integrated in the Event Tree Analysis using specific decisional gates. The application to a demonstrational case study shows that considering the synergistic performance of safety and security is beneficial for multiple reasons. The first one is that the overall probability of attack success is significantly reduced. Moreover, the severity of the escalating scenarios can be better characterized. This methodology can be seamlessly integrated in conventional safety analyses and could be used both by practitioners and plant managers. The ability of capture the synergistic performance of barriers additionally boosts risk-based decision making on the allocation of resources, as well as cost-benefit economic evaluations.

Acknowledgments

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

References

Casson Moreno, V., Marroni, G., Landucci, G., 2022, Probabilistic assessment aimed at the evaluation of escalating scenarios in process facilities combining safety and security barriers. Reliability Engineering and System Safety 228, 108762.

De Dianous V., Fiévez C., 2006, ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. Journal of Hazardous Materials 130(3), 220-233.

Chen C., Reniers G., Khakzad N., 2019, Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach. Reliability Engineering and System Safety (191), 106470.

Gertman, D., Blackman, H., Marble, J., Byers, J., Smith, C., 2005, The SPAR-H Human Reliability Analysis Method. US Nuclear Regulatory Commission, Washington DC.

Iaiani M., Tugnoli A., Cozzani V., 2022, A Bow-Tie Approach for the Identification of Scenarios Induced by Physical Intentional Attacks to Chemical and Process Plants, Chemical Engineering Transactions, 90, 403-408

Marroni G., Casini L., Kuipers S., Dentone D., Mossa Verre M., Overdijk W., Casson Moreno V., Landucci G., 2023, Real-Time Assessment of Integrated Safety-Security Scenarios Triggering Cascading Events in the Process Industries, Chemical Engineering Transactions, 99, 349-354.

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

Securdomino, 2024, Open repository of models and barriers data <https://securdomino.eu/open-webrepository/>, accessed 28.11.2024.

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