

# Development Of Advanced Tools For Safety-Security Integration Based On The Implementation Of Site-Specific Protections

Giulia Marroni<sup>a</sup>, Sanneke Kuipers<sup>b</sup>, Valeria Casson Moreno<sup>a</sup>, Gabriele Landucci<sup>a</sup>

<sup>a</sup>*Department of Civil and Industrial Engineering, University of Pisa, Italy*

<sup>b</sup>*Institute of Security and Global Affairs, Leiden University, the Netherlands*

---

## 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. For this reason, it is important to create a framework for the integration of conventional operational safety and security science. The present work proposes a quantitative methodology to combine safety and security aspects in the bow-tie analysis, which is a commonly adopted technique in Quantitative Risk Assessment (QRA) studies. The methodology begins with the identification and classification of safety and security barriers. In this part, the working principles and functions of safety and security barriers are studied. This guides the assessment of quantitative performance parameters of barriers. Then, the barriers are integrated in a probabilistic model based on the event tree analysis. This is done using specific decisional gates tailored to functions and working principles of each barrier. The potentialities of this methodology are shown through the application to a case study. The results show that safety barriers play an important role in mitigating intentional security-related attacks, as their intervention reduces the escalation probability of the scenarios. In this way, the overall vulnerability of the plant is reduced, and a better picture of the criticalities of the facility under analysis can be depicted. The methodology can be readily integrated in conventional QRA studies. Namely, the integration of safety and security using this methodology can grant a homogeneous framework, which could be useful to support a more informed allocation of resources.

*Keywords:* Bow-tie analysis, security vulnerability assessment, safety and security integration, performance assessment, cascading effects

---

## 1. Introduction

In the latest years, topics connected to the security of chemical and process plants have attracted the attention of both researchers and institutions. Namely, plants storing and processing high amounts of hazardous chemicals can become attractive targets of intentional attacks, leading to potentially severe consequences. This has been demonstrated by recent analyses of past accidents (Iaiani et al., 2021). Although the intentionality of human actions plays a significant role in security science, its foundations are connected with the ones of conventional operational safety. Namely, there are intersections among the two disciplines. First of all, the intervention of safety barriers can play a significant role in mitigating security scenarios. Moreover, accidental scenarios deriving from both unintentional and intentional events may escalate generating cascading effects, i.e., the propagation of consequences to other units, causing an amplification of consequences with potentially severe effect on people, assets, and the environment. Hence, the integration of safety and security is a pivotal step to better model and understand cascading effects in process facilities, as well as to better manage the available resources.

There have been several works dealing with the integration of safety and security. Iaiani et al. (2022) used a Bow-Tie approach in order to identify reference release scenarios for intentional attacks to chemical and process facilities. Chen et al. (2019) developed a methodology for the integration of safety and security using a dynamic graph approach. Yuan et al. (2022a) reiterated the importance of integrating safety and security barriers in order

to provide a comprehensive management of process facilities. Nonetheless, no work focused on creating a quantitative methodology that could account for the performance of barriers and be seamlessly integrated in conventional Quantitative Risk Assessment (QRA) studies. Still, we believe that common approaches in QRA can indeed be tailored to assess Integrated Safety and Security (ISS) risks, including cascading effects. For this reason, this work deals with the integration of security barriers and scenarios in a dedicated event tree analysis, which is one of the most common used techniques in QRA studies to determine the probability of accidental scenarios evolution. The methodology is based on the quantification of specific event trees tailored for the implementation of ISS barriers and scenarios. The methodology is then applied to a case study in order to show the potential benefits in the perspective of risk-informed decision making.

## 2. Methodology

Figure 1 shows the methodology developed in the present work. The first step of the methodology (Step 1) is related to the definition of a reference framework, in which security (Step 1a)) and safety (Step 1b)) barriers are examined (see Section 3). Typical barriers are identified, and are classified according to their function and working principle. A literature review is then carried out to the establishment of a common framework among different types of barriers suitable for their synergistic integration in risk studies. Step 2 of the methodology is then dedicated to the assessment of the performance of barriers and is described in Section 4 of the paper. Firstly, relevant performance parameters are defined in Step 2a); then, the quantitative evaluation of the performance parameters is carried out in Step 2b). The third phase (Step 3) of the methodology entails the integration of the barriers in the conventional event tree (ET) analysis. For this purpose, specific decision gates are tailored to the barriers in Section 5 of the paper. The final step of the methodology is dedicated to the application of the tailored ET analysis to a case study

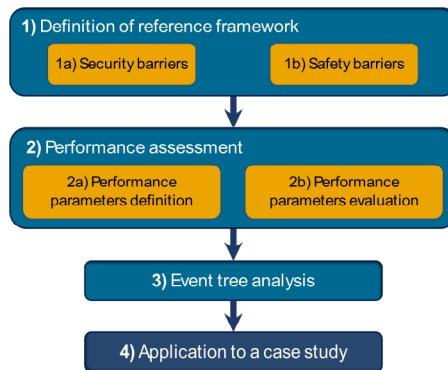


Fig. 1. Methodology adopted in this study.

## 3. Identification and classification of barriers

The concept of “barrier” is commonly applied not only in chemical and process industry, but also in other fields of engineering. For this reason, several definitions of this term have been proposed by researchers and institutions, all highlighting different aspects of the term (Yuan et al., 2022b). Hence, it is necessary to propose an appropriate definition to identify and analyze ISS scenarios.

Compared to operational safety, security science and more so the integration of safety and security are relatively new fields of research. Therefore, there is much to learn based on the principles and techniques of safety science. Namely, the models built in years of research in safety science can be tailored and applied to security science too (Landucci et al., 2020). Hereby, different approaches are discussed.

The “Swiss Cheese” model proposed by British psychologist (Reason, 2016) is one of the first conceptualization of barrier. According to this model, accidents exist due to “holes” in the risk management system, which can be “closed” through proper risk assessment and improvement actions. One of the strengths of this model is its dynamic nature: holes may increase in number or size, but they may also decrease if solid risk management is adopted. This model was initially only declined to operational safety; however, Landucci et al.

(2020) argue that it could indeed be extended to security science. The model developed by Reason is the basis for another relevant framework, which is the Bow-Tie approach. This approach takes the Swiss cheese model one step further, as it is based on the representation of accidental chains in two different sides. The left side of the bow-tie is the Fault Tree (FT), while the right side is referred to as Event Tree (ET) (De Dianous and Fiévez, 2006). The accidental event lays in the middle of the representation, leading to the bow-tie shape. The FT represents all the potential causes of the accidental events, while the ET all the potential consequences. One advantage of this representation is the possibility of visualizing multiple events from different origins: this implies that it allows to visualize conventional process upsets, as well as external events, such as intentional attacks. Hence, the two frameworks detailed above are appropriate for assessing the quantitative performance of safety and security barriers.

Once the framework has been established, then a proper definition of barrier shall be given. This topic has been explored by different researchers. The definition of Sklet (2006) is adopted in the development of this work because it can be applied to both safety and security barriers, and includes their different purposes: “barriers are physical and/or non-physical means to prevent, control, and mitigate undesired events or accidents”. This definition allows to define other key terms related to barriers, such as barrier function. Barrier functions are the purpose of the safety barriers, i.e., the action to be done by the barrier to interrupt the chain of undesired events. To categorize barriers, two different approaches can be used. The first one is to divide barriers according to their working principle. Three main working principles can be identified: active, passive, and procedural. Active barriers need the activation of an engineered system, e.g., interlocks or emergency shutdowns, to perform the safety function (Center for Chemical Process Safety, 2012). Typically, these systems tend to be more complex and are linked to signals and/or detection systems; an example of active barriers are fire protection systems, such as water deluge systems or sprinklers. On the other hand, passive barriers can perform their safety function without external activation, e.g., fireproofing materials, blast walls, or catch basins. Lastly, procedural barriers are all operating procedures, administrative checks, emergency plans that are used to prevent and/or mitigate an accidental event; external and internal emergency plans, employees training are examples of this type or barrier. Although conventionally only applied to safety barriers, Casson Moreno et al. (2022) showed that this classification is applicable to security barriers as well. The second approach is to classify barriers according to the function they are called to perform. A common nomenclature for safety barriers is the one proposed in (Salvi and Debray, 2006), who divide barriers in preventive and mitigative. This classification is shared by other researchers, although the names might differ. Preventive barriers act as pre-event control and are placed of the FT side of the bow-tie, while mitigative barriers act as post-event control and are therefore placed on the ET side of the bow-tie. As for security barriers, they are often referred to in the literature as Physical Protection Systems (PPS), and their functions are also agreed upon by researchers. The classification from SANDIA National Laboratories (Garcia, 2006) is often adopted; PPS are therefore classified according to their preemptive functions: detection, delay, and respond. Detection is the discovery of an adversary action, e.g., entry controls; delay consists in slowing down the adversary, e.g., placing fences; the response function consists in actions taken by the response force to prevent adversary success and include the interruption and neutralization. It should be noted that the focus of these works are on preventive barriers, as security mitigative barriers are the same as safety ones: namely, the firefighting system should activate whether the fire is intentional or accidental. Table 1 summarizes the classification of barriers adopted in this work.

Table 1. Classification of barriers based on working principle and function.

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

Thus, a reference framework and classification has been defined. This will support the next steps of the methodology, i.e., the development of a quantitative technique based on ET analysis to integrate safety and security barriers.

#### 4. Performance assessment of barriers

The evaluation of the probabilistic performance of barriers is ordinarily carried out as a part of QRA studies; nonetheless, the assessment neglects the assessment of cascading events and the evaluation of ISS scenarios. Therefore, this part of the methodology (Step 2 in Fig. 1) is devoted to assess what parameters can be adopted to describe the quantitative performance of barriers in order to include the aforementioned factors. The work of

Landucci et al. (2016) can be used as a reference to determine the main parameters used to assess the performance of safety barriers. Casson Moreno et al. (2022) extended the use of the same parameters to security barriers. In particular, the identified probabilistic parameters are:

- Availability of the barrier (*PF**D*), expressing the probability of failure on demand;
- Effectiveness ( $\eta$ ), expressing the probability of the barrier of preventing the escalation of the scenario once successfully activated;

Namely, even if a barrier successfully responds on demand, there is still the possibility that the barrier will not fully perform its function; the effectiveness term is here considered to account for this factor.

An additional performance parameter to be considered is related to the attenuation of physical effect once the barrier successfully performs its task. Namely, an attenuation factor  $\phi$  can be defined for different mitigative barriers. Although it is not a probabilistic parameter,  $\phi$  represents the amount of physical effect actually received by other equipment in case of successful activation of the barrier. It is essential to evaluate the probability of failure of equipment, so to determine the credibility of the accident propagating other units.

To obtain performance quantities for both safety and security barriers, different techniques, such as FT, human error analysis, or suppliers data can be used. For the sake of exemplification, the performance assessment of a door is shown. A door is a passive PPS and its function is to delay the adversary, as it can block a potential threat from entering areas such as control room or storages. Hence, the quantitative performance of a door is described by a *PF**D* and  $\eta$  value;  $\phi$  is not defined as the door is not a mitigative barrier. A door is a fixed installation, so the *PF**D* can be considered null, as the barrier is always available. The effectiveness of the door can instead be related to two main factors: i) correctly assembling the door, and ii) locking it. For both actions, the SPAR-H method for human reliability analysis (Gertman et al., 2005) can be adopted. According to the definitions of the methodology, assembling the door can be classified as an action; on the other hand, locking the door has a diagnostic and an action component: the operator needs to remember to check whether the door is locked and then lock it. By assessing the value of the performance shaping factors, we obtain a probability of wrong assembling  $HEP_A = 2.5 \times 10^{-5}$  and a probability of wrongly locking the door  $HEP_L = 2.25 \times 10^{-5}$  leading to an overall human error probability of  $HEP = HEP_A + HEP_L = 4.75 \times 10^{-5}$ . The effectiveness of the door can be derived from HEP as follows:

$$\eta_{door} = 1 - HEP = 9.9995 \cdot 10^{-5} \quad (1)$$

A similar procedure was adopted for other safety and security barriers in previous studies. The overview of the barriers considered in the present study, along with their performance parameters and related reference source, is shown in Table 3 in Section 5.

## 5. Integration of barriers

How do the organizational factors, as safety culture, influence security performance in customs? A literature review in Event TreesThe quantitative performance of the barriers can be implemented in the ET analysis by means of specifically developed logical gates. These gates have been developed in a past study (Landucci et al., 2016) and were tailored for the purpose of security barriers in a recent work (Casson Moreno et al., 2022). An overview of the gates adopted in this methodology is shown in Table 2.

The operators represent the possible types of probabilistic functions obtained through the combination of availability and effectiveness of a barrier. For example, single point estimates or continuous or discrete distribution can be considered, leading to gate types A, B and C respectively. Gate D in Table 2 is crucial for the representation of escalating scenarios. In fact, Gate D represents the physical integrity of the target equipment: based on the received physical effect (e.g., heat radiation, overpressure), the probability of failure  $P_d$  can be computed using equipment vulnerability models available in the literature. In this gate, the attenuation factor  $\phi$  is considered in order to compute the reduced physical effects, in case mitigation of successful operation of the barrier.

Now, all required information has been gathered in order to integrate safety and security barriers in the ET analysis to determine the vulnerability of the plant. Table 3 sums up the main information of barriers adopted in this work. It should be noted that the developed approach is flexible: if more precise information on barriers is available, then the performance parameters value can be varied accordingly.

## 6. A case study

The methodology is applied to a demonstration case study in order to highlight its potentialities. The facility under analysis is a chemicals storage facility, the layout of which is shown in Figure 2.

The facility is constituted by two main parts. The first part is constituted by an indoor storage of hazardous material, the majority of which is hydrazine. The hydrazine is stored in 25 L plastic jerrycans, which are grouped in pallets and stored in racks. Then, there is an open storage part where gas cylinders are stored. One part is devoted to storing empty cylinders, one part stores cylinders containing acetylene dissolved in acetone, and one part storing refrigerants cylinders. The total amount of acetylene that can be stored in the site is 4000 cylinders, which amounts to roughly 25000 m<sup>3</sup> of acetylene and 50 ton of acetone.

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



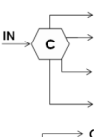

Gate type & representation	Description
 $OUT_1 = IN \times [ PFD + (1 - \eta) \times (1 - PFD) ]$ $OUT_2 = IN \times (1 - PFD) \times \eta$	Simple composite probability: availability is multiplied by a single probability value expressing the probability of barrier success in the prevention of the escalation.
 $OUT_1 = IN \times [ PFD + (1 - \eta) \times (1 - PFD) ]$ $OUT_2 = IN \times (1 - PFD) \times \eta$	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.
 $OUT_1 = IN \times PFD$ $OUT_2 = IN \times (1 - PFD) \times \eta_2$ $OUT_i = IN \times (1 - PFD) \times \eta_i$ $OUT_M = IN \times (1 - PFD) \times \eta_M$	Discrete probability distribution: depending on barrier effectiveness, three or more events may originate from the gate describing the barrier performance.
 $OUT_1 = IN \times P_d$ $OUT_2 = IN \times (1 - P_d)$	Vessel fragility gate: based on the status of the target equipment, the damage probability ( $P_d$ ) is computed through equipment vulnerability models.

Table 3. Overview of the safety and security barriers used in the present work, adapted from (Casson Moreno et al., 2022; Landucci et al., 2016); AIT: adversary intrusion time; ERT: emergency response time.

Barrier	Function	Working Principle	Gate type	PFD	$\eta$	Source
Entry Gate	Delay	Passive	A	2.00E-02	9.98E-01	(Casson Moreno et al., 2022)
Door	Delay	Passive	A	0	9.9995E-01	This work
Detection by site personnel	Detect	Procedural	A	Day: 2.33E-01 Night: 4.00E-01	2.48E-01	(Casson Moreno et al., 2022)
Emergency Team	Respond	Procedural	C	7.52E-01	1 if AIT > ERT 0 if AIT ≤ ERT	(Casson Moreno et al., 2022)
Water/Foam Sprinkler system	Mitigate	Active	B	5.43E-02	9.54E-01	(Landucci et al., 2016)

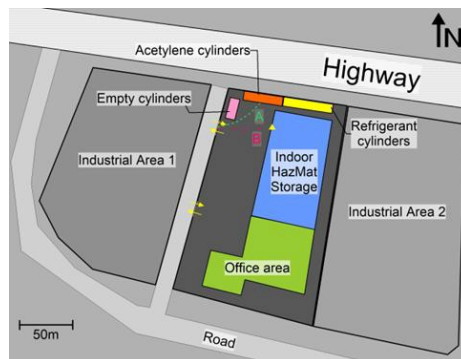


Fig. 2. Layout of the case study.

Figure 2 also shows the demonstrational attack paths chosen for this study. In path A, the threat trespasses the entry gate during the day, runs for 43m and then detonates 10 kg of triacetone triperoxide (TATP) near the acetylene cylinders storage.

The open storage is protected by a sprinkler system that activates in case of fire detection. In path B, the attacker trespasses the entry gate at night, runs at the indoor storage, picks the door, and then detonates 10 kg of TATP targeting the hydrazine pallets. The indoor storage is also protected by a foam system, which has the aim of preventing the evaporation of flammable and toxic materials inside the storage.

## 7. Results and discussion

Figure 3 shows the bow-tie developed for the attack scenario A introduced in Section 6. The scenario associated with the failure of the barrier is represented in the top exit in Figure 3.

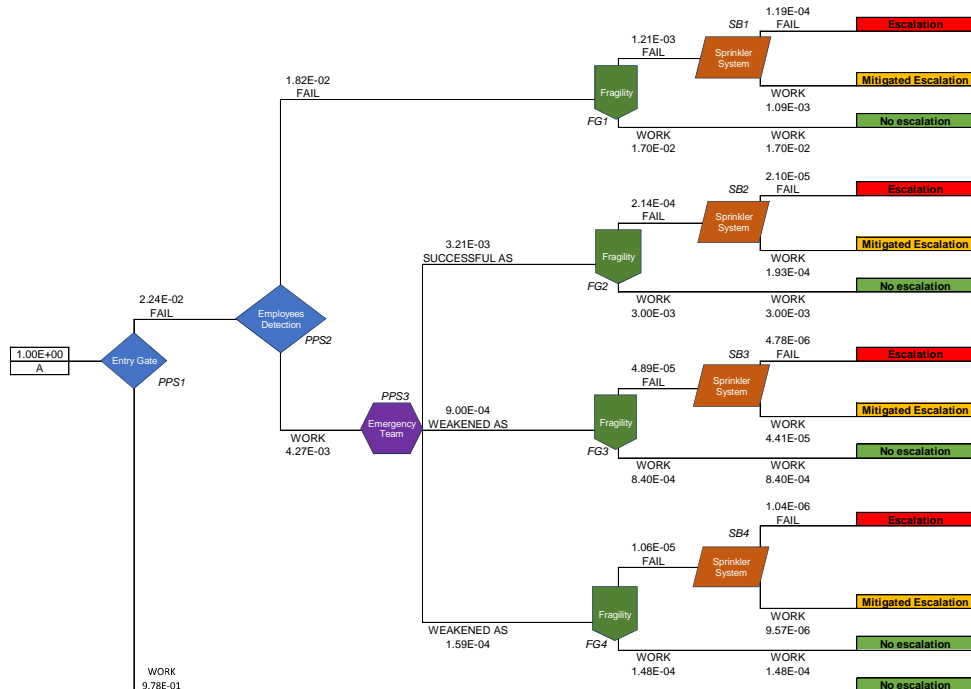


Fig. 3. Bow-tie for attack path A shown in Figure 2.

The first barrier encountered by the threat is the entry gate, which can be quantified using the data in Table 3. If the attacker cannot pass the entry gate, then the scenario is interrupted and there is no escalation. If the attacker successfully passes the gate, then it could be detected by employees of the facility. The performance of this gate is once again quantifiable using the data in Table 3. In case the threat is not detected, then the attacker can detonate the explosive and damage the target. In case the targets are not damaged, then the scenario does not escalate. In the opposite case, the acetylene cylinders might then ignite, potentially generating a fire. To quantify this gate, a few steps shall be taken. Firstly, the overpressure generated by the detonation of 10 kg of TATP is evaluated using the models proposed in (Landucci et al., 2015). It should be noted that the 4000 cylinders all have a different distance from the detonation point in Figure 2; however, they are very close to each other, meaning that a single equipment can be considered, and the overpressure was evaluated at an average distance from the detonation point. The overpressure on the targets is estimated to be 21.8 kPa. Fragility models based on probit relationships are then used to quantify the probability of successfully damaging the cylinders. In particular, the model for elongated equipment discussed in (Marroni et al., 2024) is used, obtaining a damage probability of 6.88%, which is used in the fragility gate (see gates FG1, FG2, FG3 and FG4 in Figure 3). The scenario has full escalation potential in case of failure of the sprinkler system, the performance of which can be

retrieved from Table 3. In case of correct activation of the sprinkler system, then a mitigated cascading scenario will take place, since the physical effects associated to the fire are mitigated. In case the attacker is detected by employees, the bottom part of the tree departing from Employees Detection gate (gate PPS3 in Figure 3) shall be followed. In particular, if the intrusion is detected, then the emergency response team is deployed. To quantify this gate, it is necessary to compute AIT, i.e., the adversary intrusion time. This can be done by assessing the time needed for each task. A time to overcome the gate of 90s is assumed. Then, the threat has to run towards the target. The running rates available in (Garcia, 2006) can be used to evaluate the time: if the lowest running rate is chosen (3.18 m/s), a running time of 13.5s is obtained. Then, the threat has to place and detonate the explosive. According to (Garcia, 2006), around 17s are needed to place and detonate the explosive. Hence, the total time for the scenario is around 120s. Considering that a well-trained emergency team can respond in 240s (Casson Moreno et al., 2022), this means that the attack cannot be interrupted or neutralized, as the attacker is faster in carrying out the actions. Hence, all outputs of the purple gate in Figure 3 lead to the same event sequence with fragility gate and sprinkler system, as outlined earlier.

Figure 4 shows the Bow-tie developed for attack path B, which can be read in a similar way of the bow-tie presented in Figure 3 for attack path A. As for the quantitative assessment of the bow-tie, some considerations shall be done. The value of  $PF D$  and  $\eta$  can be retrieved from Table 3. To quantify the AIT, the same time to trespass the gate as attack path A is considered. Also the running rate is the same, meaning the attacker needs around 16s to reach the door. From (Garcia, 2006) an average time for picking a door is gathered (150s). Then, 17s are needed to place and detonate the explosive. In this way, the total AIT is around 273s. This implies that a well-trained emergency team can neutralize the attack, while a low-trained team will not (ERT = 360s). Finally, as there are not fragility models specifically addressing the probability of failure of jerrycans exposed to overpressure, the failure of the equipment was considered with a unitary probability (thus, avoiding the use of the fragility gate).

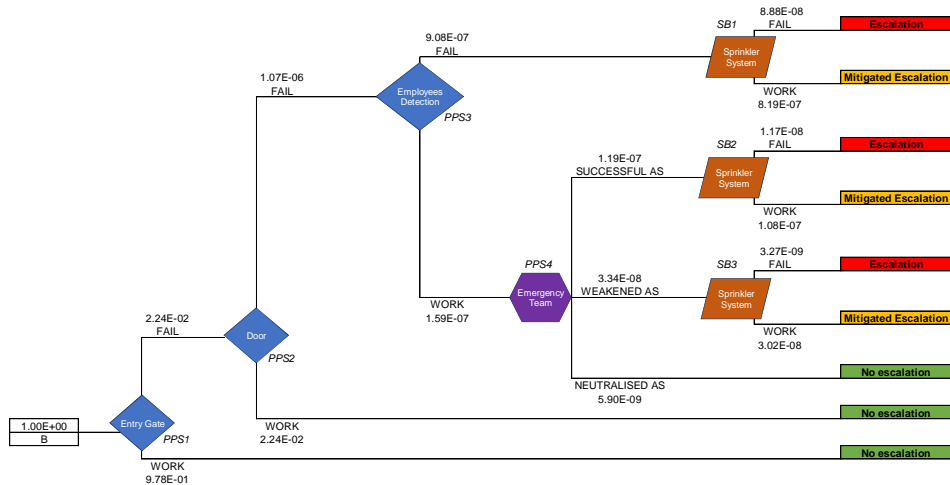


Fig. 4. Bow-tie for attack path B shown in Fig. 2.

Figure 5 shows the results of the probabilistic assessment in different cases. The blue bars represent the outcomes of the scenario considering the intervention of ISS barriers, the green bars represent the outcomes in case of neglect of the performance of safety barriers, while the yellow bars show the outcomes in case of neglect of security barriers. To obtain these two results, it is sufficient to set the  $PF D$  value as unitary and the  $\eta$  value as null.

The neglect of safety barriers in both Fig. 5a and 5b does not change the likelihood of the “no escalation” scenario, but it allows us to better understand and describe the nature of the escalation. Namely, accounting for safety barriers allows to distinguish between mitigated escalation and escalation scenarios, instead of considering only one type of escalation. This is essential in order to prioritize the likelihood and severity of the different scenarios. Because of this, the probability of escalation is 94% lower for attack path A (Fig. 5a) and 90% lower for attack path B (Fig. 5b) if the synergistic performance of ISS is considered. In case of the neglect of PPS, different results are obtained. Namely, for attack path A, there is still a residual probability of the scenario being prevented because of the consideration of the fragility of the target: if the equipment does not fail as a result of

the attack, then there is no escalation scenario. On the other hand, for attack path B, the neglect of PPS causes the scenario to never be mitigated, as the failure of the equipment is assumed as certain. This underlines the importance of actively accounting for the fragility of the target when dealing with escalation scenarios. Nonetheless, for path A, the accounting for PPS diminishes the probability of escalation by 97%: this shows that the contribution of safety and security barriers can be in some case comparable, highlighting once again the importance of the synergistic effect of ISS barriers.

Other considerations can be made on the nature of the barriers considered in the study. Namely, the comparison of the results of Figure 5a and 5b shows that there the escalation scenarios have dramatically different orders of magnitude. This is due to the fact that the attacker in attack path B has to overcome two different fixed PPS, namely the entry and the door. These PPS have a better performance because they rely less on human action when compared to PPS such as employees detection or emergency team response.

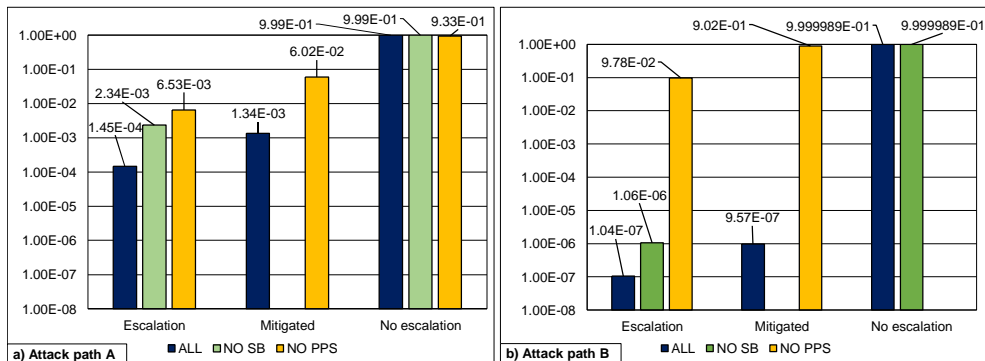


Fig. 5. Results of the probabilistic assessment; (a) attack path A; (b) attack path B.

The definition of a common framework and methodology hence allows to consider the synergistic performance of safety and security barriers through the ET analysis. The developed methodology can be of support in better determining and defining the likelihood of intentional attacks, which could then be implemented in conventional risk studies, as well as more complex risk assessment techniques. A potential application is in a three-dimensional tool to assess the risks connected to ISS scenarios and related cascading effects (Marroni et al., 2023). Additionally, the methodology is flexible, as the performance of different types of barriers can be customized according to the data available, which could also be directly supplied by the facility under analysis.

Nonetheless, the methodology can be further improved. An interesting development is related to the interaction of barriers with physical effects. For example, more sophisticated fragility models could be adopted to the analysis in order to account for the potential mitigation of fixed barriers such as dike walls (Marroni et al., 2024). Another interesting study is related to a more deep study of the interaction among safety and security barriers aimed at identifying potential interferences, i.e., when the functions of safety and security barriers clash. Finally, this methodology could be of support to practitioners and plant managers to understand the interactions between safety and security, and thus to prioritize critical scenarios and decide the appropriate countermeasures.

## 8. Conclusions

The integration of security issues with conventional operational safety is a topic that raised the attention of researchers as the attractiveness of chemical and process facilities to intentional attacks has risen in the last years. Still, the development of tools to integrate safety and security scenarios is lacking in current literature.

Hence, this work presents a quantitative approach for integrating ISS scenarios using the well-known event tree analysis. The first step of the methodology aimed at identifying a framework for the analysis including a definition of barriers and working principles and functions of ISS barriers. Then, parameters associated to the quantitative performance of the barriers were identified, along with specific decisional gates to be implemented in the event trees.

The methodology is then applied to a demonstrational case study. Two different attacks paths on a facility storing both flammable and toxic substances were examined. The results show that safety and security barriers are both crucial elements to better describe the escalation of intentional attack scenarios. Moreover, accounting



for the performance of safety barriers allows to distinguish between the severity of the escalation scenarios, and thus to identify mitigated scenarios. In this way, cascading scenarios can be ranked in severity, allowing for a more rigorous assessment.

The developed methodology could be thus implemented in conventional QRA studies in order to guide practitioners and plant managers in identifying critical attack scenarios and critical barriers, as well as guiding potential improvements and allocation of resources.

## Acknowledgements

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.
- Center for Chemical Process Safety. 2012. *Guidelines for Engineering Design for Process Safety*. John Wiley and Sons inc, Hoboken NJ
- 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.
- 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.
- Garcia, M.L. 2006. *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann, Burlington MA.
- 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., Casson Moreno, V., Reniers, G., Tugnoli, A., Cozzani, V. 2021. Analysis of events involving the intentional release of hazardous substances from industrial facilities. *Reliability Engineering and System Safety* 212, 107593.
- Iaiani, M., Tugnoli, A., Cozzani, V. 2022. Identification of reference scenarios for security attacks to the process industry. *Process Safety and Environmental Protection* (161), 334-356.
- Landucci, G., Reniers, G., Cozzani, V., Salzano, E. 2015. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. *Reliability Engineering & System Safety* 143, 53-62.
- Landucci, G., Argenti, F., Spadoni, G., Cozzani, V. 2016. Domino effect frequency assessment: The role of safety barriers 44, 706-717.
- Landucci, G., Khakzad, N., Genserik, R. 2020. *Physical Security in the Process Industries*. Elsevier, Amsterdam.
- 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 and System Safety* (243), 109880.
- Reason, J. 2016. *Managing the risks of organizational accidents*. Routledge, New York NY.
- Salvi, O., Debray, B. 2006. A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive. *Journal of Hazardous Materials* 130(3), 187-199.
- Sklet, S. 2006. Safety barriers: Definitions, classification, and performance. *Journal of Loss Prevention in the Process Industries* 19(5), 494-506.
- Yuan, S., Reniers, G., Yang, M. 2022a. The Necessity of Integrating Safety and Security Barriers in the Chemical Process Industries and its Potential Framework. *Chemical Engineering Transactions* (91), 13-18
- Yuan, S., Yang, M., Reniers, G., Chen, C., Jiansong, W. 2022b. Safety barriers in the chemical process industries: A state-of-the-art review on their classification, assessment, and management. *Safety Science* 148, 105647.

