

# The Role of Safety Barrier Performance Depletion in the Escalation of Natech Scenarios

Alessio Misuri<sup>a</sup>, Gabriele Landucci<sup>b</sup>, Valerio Cozzani<sup>a,\*</sup>

<sup>a</sup> Laboratory of Industrial Safety and Environmental Sustainability – DICAM, University of Bologna, Bologna, Italy

<sup>b</sup> Department of Civil and Industrial Engineering, University of Pisa, Pisa, Italy  
[valerio.cozzani@unibo.it](mailto:valerio.cozzani@unibo.it)

Natural hazards can cause severe damages to chemical and process facilities, triggering technological scenarios involving hazardous materials. The risk related to this type of cascading events, defined Natech accidents, is expected to grow in the foreseeable future due to the enhanced severity of some categories of natural phenomena brought by climate change. A critical feature of Natech events is that the safety systems implemented might undergo some extent of depletion and performance reduction due to the natural event, and this might heavily influence the likelihood and the features of accident escalation. While methodologies have been proposed to perform a quantitative assessment of Natech risk, the role of the safety system concurrent depletion has been only recently investigated and has not been addressed systematically yet. Hence, a comprehensive framework to assess the risk related to the escalation of Natech scenarios and to possible domino effects due to concurrent safety barrier depletion is presented. A specific three-level approach was conceived to evaluate barrier performance according to system complexity and impact uncertainty. A straightforward analysis (L0) based on a Boolean approach is applied for simple barriers when their missing action can be assessed with a low uncertainty. A more detailed analysis (L1) leveraging specific performance modification factors to express the likelihood that similar reference barriers will fail is applied in case of relevant uncertainty. For the analysis of complex barriers and situations when system architecture differs from reference configurations, a further level (L2) based on fault tree analysis is introduced to consider barrier subsystem failure during natural events and to update the overall unavailability of the system. A dedicated event tree approach is then used to embed barrier performance into the quantitative risk assessment of Natech scenarios. The methodology was applied to a test case demonstrating that the quantification of the updated performance of the considered set of safety barriers during natural hazards leads to a relevant increase in overall Natech risk figures.

## 1. Introduction

When impacting chemical and process installations, natural disasters can lead to the release of hazardous materials producing severe technological accidents usually referred to as Natech events (Krausmann et al., 2017). Natech events are particularly critical since also safety barriers implemented for accident prevention and mitigation might be damaged by natural hazards, and their performance might be reduced, as demonstrated by past accident analysis. For instance, during the Kocaeli earthquake that hit Turkey in 1999, several Natech scenarios were triggered and safety systems were damaged leading to extremely severe consequences (Girgin, 2011). Indeed, the propagation of fires involving a petrochemical storage could hardly be managed due to the unavailability of firefighting systems, and a massive release of toxic acrylonitrile could not be retained due to the failure of containment dikes exposed to the intense seismic load (Girgin, 2011). Also during Hurricane Harvey, in 2017, many industrial facilities reported multiple chemical spills and damages to safety barriers and auxiliary systems (Misuri et al., 2019). Among the others, the accident progression of the severe accident that involved the Arkema plant in Crosby, TX, was determined by the failure of utility systems and safety measures implemented to guarantee the control of unstable chemicals (Misuri and Cozzani, 2021) It is thus clear that quantifying the risk associated with Natech scenarios can be complex, although of extreme importance. In the literature, several methodologies have been proposed to perform the Natech quantitative risk assessment

(QRA) (Mesa-Gómez et al., 2020). Nonetheless, these methodologies do not consider neither the possible depletion of the safety barriers implemented for accident prevention and mitigation nor its implications for Natech risk figures (Antonioni et al., 2015). Therefore, the aim of this study is to present a novel methodology to assess the performance of safety barriers during natural hazards and to include them in a comprehensive QRA procedure, producing a more realistic characterization of accident escalation. The overview of the methodology is shown in Section 2, while the barrier assessment approach is described in detail in Section 3. Section 4 is dedicated to the tools needed to include barrier performance into the QRA. As an example of application, a case study is shown in Section 5. The conclusions of the study are then summarized in Section 6.

## 2. Methodology

The novel QRA methodology including the role of safety barriers into the assessment of the escalation of Natech scenarios is shown in the flowchart of Figure 1. As shown in the figure, the methodology shares common features with the established approaches for Natech QRA (Antonioni et al., 2015), and for the evaluation and characterization of further scenarios due to domino effect (Cozzani et al., 2014). However, important modifications involve the development of specific approaches to assess barrier performance (Steps 4 and 5) and their inclusion in the frequency assessment of final outcomes (Step 6), as discussed in the following.

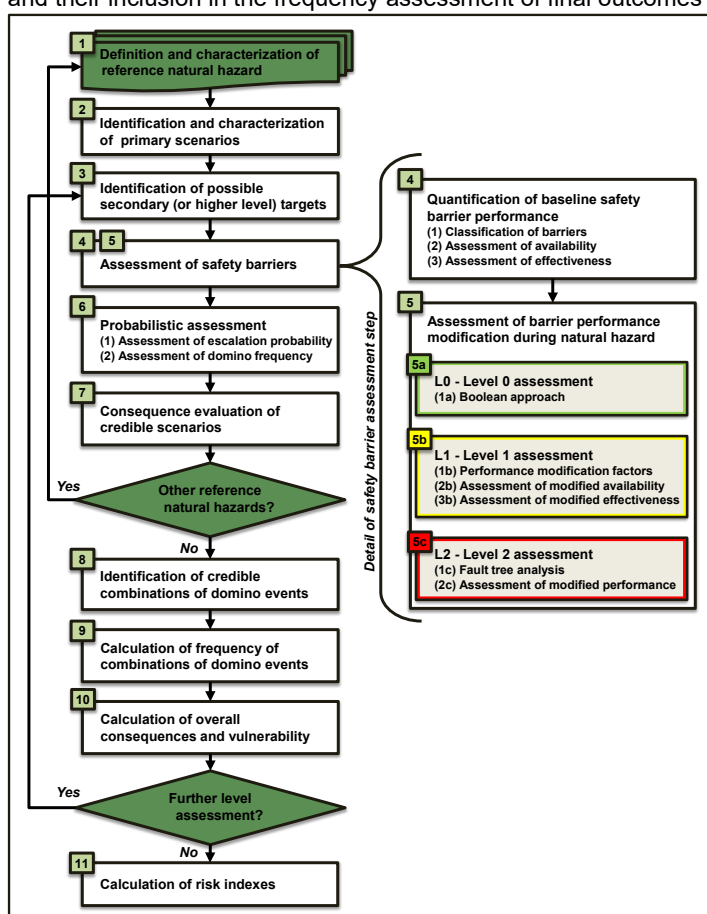


Figure 1: Methodology to perform the Natech QRA considering the role and the depletion of safety barriers on the possibility and expected frequency of accident escalation by domino effect. Adapted from (Misuri et al., 2021a).

## 3. Assessment of safety barrier performance

### 3.1 Background and classification

In the chemical and process industries the concept of safety barriers is generally used to refer to measures, either physical or non-physical, implemented to prevent unwanted outcomes and/or to mitigate their consequences (Liu, 2020). The actions that the safety barriers are designed to perform, as for instance, spill containment, heat load mitigation from fires, toxic plumes concentration reduction, are defined as safety

functions. Whereas these two definitions pertain the chemical and process industries, the conceptualization of safety barriers is used in risk management processes in a variety of sectors and can embrace a broad set of technical and non-technical measures (Liu, 2020). Various classifications are used to group together measures with shared similarities. In the context of QRA, a well-accepted classification based on working-principle might be used (CCPS, 2001). In particular, barriers are classified as (Landucci et al., 2015): i) Passive barriers: physical measures that do not require activation to perform their safety functions, as containment bunds, catch basins, or fireproofing materials; ii) Active barriers: complex instrumented systems requiring activation to perform their safety functions; most of firefighting network systems belong to this category; iii) Procedural barriers: procedures and coordinated operations performed by internal personnel or external teams, as emergency intervention of fire brigades.

### 3.2 Safety barrier performance metrics

Several metrics have been proposed in the literature dedicated to safety barrier performance evaluation. The most suitable metric to be adopted, as shown in Step 4 of Figure 1, is the one developed in the context of domino effect risk assessment (Landucci et al., 2015). The metrics is based on two parameters to describe barrier performance. The first is the probability of failure on demand (PFD), which expresses the probability that a safety barrier fails when it is required to perform its function. The second parameter is the effectiveness ( $\eta$ ), which expresses the failure in preventing accident progression upon successful activation.

This metrics has been tailored from the well-established layer of protection analysis (LOPA) approach (CCPS, 2001), although in the original approach  $\eta$  was not considered, while it is a critical parameter in risk assessment of cascading scenarios as domino and Natech events. Baseline values of PFD and  $\eta$  for common safety barriers can be found in Landucci et al. (2015) and in the cited references. Reliability techniques can be applied starting from data on component availability that can be found in technical sources.

### 3.3 Safety barrier performance during natural hazards

As shown in Step 5 of Figure 1, to tailor barrier performance to the case of Natech accidents, three different levels can be adopted according to barrier complexity and impact uncertainty. The simplest level is the Level 0 (L0), which is suitable for situations when there is low uncertainty on the impact of the reference natural event on the barrier. The L0 is based on a Boolean approach leveraging rules-of-thumbs, that enable to assess with confidence whether the barrier should be considered affected or not (e.g., the position). Thus, according to L0, if the  $k$ -th barrier is considered unaffected, it will have the baseline performances  $PFD_{0,k}$  and  $\eta_{0,k}$  during the natural event. On the contrary, in case the basic evaluations indicate the barrier would be clearly impaired, the  $k$ -th barrier should be considered unavailable. Thus,  $PFD_{j,k} = 1$  is assumed for active systems, and  $\eta_{j,k} = 0$  is assumed for passive barriers (Misuri et al., 2021).

The Level 1 (L1) is used when there is some uncertainty concerning barrier performance during the reference natural event. According to L1, modified barrier performance is described by means of a covariate, defined as a performance modification factor  $\phi$ , which expresses the likelihood that similar reference barriers would fail directly due to the natural event, as proposed by Misuri et al. (2020).

Considering the lessons learnt from past accident analysis,  $\phi$  is applied to modify the PFD of active barriers to model their possible lack of activation when required to perform their safety function, while for the case of passive barriers  $\phi$  is applied to modify the  $\eta$  to model the possible structural damages they might undergo during natural hazards. Thus, the performance of the  $k$ -th active barrier during the  $j$ -th reference natural event can be evaluated applying Eqs.(1)-(2):

$$PFD_{j,k} = 1 + (\phi_{j,k} - 1)(1 - PFD_{0,k}) \quad (1)$$

$$\eta_{j,k} = \eta_{0,k} \quad (2)$$

where  $\phi_{j,k}$  is a performance modification factor for the  $j$ -th reference natural event, while  $PFD_{0,k}$  and  $\eta_{0,k}$  are the baseline parameters assessed for the  $k$ -th active safety barrier determined in Step 4 of Figure 1.

The performance of the  $k$ -th passive barrier during the  $j$ -th reference natural event is evaluated by Eq.(3):

$$\eta_{j,k} = (1 - \phi_{j,k}) \eta_{0,k} \quad (3)$$

where  $\phi_{j,k}$  is a performance modification factor for the  $j$ -th reference natural event, and  $\eta_{0,k}$  is the baseline effectiveness for the  $k$ -th passive safety barrier.

The Level 2 (L2) for barrier assessment is suggested in case complex systems are considered (e.g., firefighting systems), where the actual consequences of the impact of the reference natural event are affected by a high uncertainty. It is also advised for situations when safety barrier architecture features some specificities and cannot be assessed by means of performance modification factors valid for reference configurations. The L2

level is based on a fault tree analysis (FTA) focused on possible subsystem failures during the reference natural event. The minimal cut sets (MCSs) are identified in the fault tree, and among the basic events, the ones that might be influenced by the impact of the reference natural event are identified based on specific information on barrier subsystems, including their position, interdependencies, or possible redundancies. Then, the probabilities of the basic events involving vulnerable barrier subsystems are updated to unitary values, to indicate their expected failure during the reference natural event. In formulas,  $Q_j(MCS_{m,k})$ , the updated probability of the  $m$ -th MCS of the  $k$ -th barrier during the  $j$ -th reference natural event is assessed by Eq. (4):

$$Q_j(MCS_{m,k}) = \sum_p (q_{p,0} + \delta_{p,j}(1 - q_{p,0})) \quad (4)$$

where  $q_{p,0}$  is the probability of the  $p$ -th event comprised in the  $m$ -th MCS, and  $\delta_{p,j}$  is 1 if the  $p$ -th event involves at least one of the identified vulnerable subsystems, and 0 if not. The tailored PFD for the  $k$ -th barrier  $PF_{D_{j,k}}$  is finally obtained by Eq. (5):

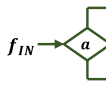
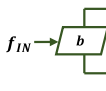
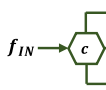
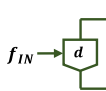
$$PF_{D_{j,k}} = 1 - \prod_m (1 - Q_j(MCS_{m,k})) \quad (5)$$

For what concerns procedural barriers, a methodology of general validity for their assessment during natural hazards was not developed. Indeed, due to the high site-specificity of measures as emergency response actions, a case-specific assessment considering the possible impact of natural hazards on each required task is advised. Nevertheless, simplified approaches are available in the literature and might be used for preliminary estimates of delays or even failures of emergency teams during accident progression (Landucci et al., 2015).

#### 4. Risk assessment

Once the performance of safety barrier is characterized, it can be embedded into the frequency assessment of scenarios through an event tree analysis (ETA) originally proposed for the analysis of escalation via domino effects (Landucci et al., 2016), and successfully applied also to the case of Natech events (Misuri et al., 2021b).

*Table 1: Logical rules associated with the gates to include safety barrier performance into the ETA.*

Gate	Representation & quantification rules	Description
a	 $Out_1 = f_{IN} * [PF_{D_{j,k}} + (1 - \eta) * (1 - PF_{D_{j,k}})]$ $Out_2 = f_{IN} * (1 - PF_{D_{j,k}}) * \eta$	Simple composite probability: unavailability, expressed as PFD, is combined with a single probability value for $\eta$ .
b	 $Out_1 = f_{IN} * [PF_{D_{j,k}} + (1 - \eta) * (1 - PF_{D_{j,k}})]$ $Out_2 = f_{IN} * (1 - PF_{D_{j,k}}) * \eta$	Composite probability distribution: unavailability, expressed as PFD, is combined with a probability distribution expressing $\eta$ . An integrated PFD can be used, obtaining the rule reported.
c	 $Out_1 = f_{IN} * PF_{D_{j,k}}$ $Out_2 = f_{IN} * (1 - PF_{D_{j,k}}) * (1 - \eta)$ $Out_3 = f_{IN} * (1 - PF_{D_{j,k}}) * \eta$	Discrete probability distribution: depending on barrier $\eta$ , three events may arise. Used for emergency intervention modelling (Landucci et al., 2015).
d	 $Out_1 = f_{IN} * P_D$ $Out_2 = f_{IN} * (1 - P_D)$	Equipment fragility gate: is used to model the escalation of the accident through domino effect, thus $P_D$ is the item failure probability due to an escalation vector (e.g., received heat load).

The ETA leverages a set of specific logical gates to include the performance of each barrier into the quantification of event frequencies (Landucci et al., 2015), summarized in Table 1. According to the ETA, at most three outcomes are expected from each target equipment (Landucci et al., 2016): i) unmitigated domino scenarios (State "2"), in case all the barriers fail; ii) mitigated domino scenarios (State "1"), intermediate situations when only a part of safety barrier fails; and iii) no domino scenarios (State "0"), when escalation is interrupted. A detailed characterization of the consequences of mitigated domino scenarios proposed in a previous study is suggested (Landucci et al., 2017). When the complete set of the secondary escalation scenarios is characterized, the frequency assessment and consequence analysis of overall domino scenarios are performed. Considering the escalation logic with at most three possible states for each of the  $n$  domino targets, the maximum number of different secondary domino scenarios from a primary Natech scenario ( $N_c$ ) can be determined as  $N_c = 3^n$ . Each overall final scenario  $\mathbf{C}^n$  is a vector of  $n$  elements representing the combination of the events involving the  $n$  domino targets. If  $P(C_i^n)$  is probability of  $C_i^n$  (i.e., the  $i$ -th element of  $\mathbf{C}^n$ ) indicating the outcome of the generic  $i$ -th target, the joint probability of a generic overall final scenario  $P(\mathbf{C}^n)$  and the related frequency  $f(\mathbf{C}^n)$  are assessed by Eqs. (5)-(6):

$$P(C^n) = \prod_{i=1}^n P(C_i^n) \tag{5}$$

$$f(C^n) = f_p \times P(C^n) \tag{6}$$

where  $f_p$  is the frequency of the primary Natech scenario generating the escalation. Overall consequence assessment is done by standardized procedures applied in the context of Natech and domino QRA (Antonioni et al., 2015). The calculation of risk indices is performed in agreement with previous works (Misuri et al., 2021a).

### 5. Case study

The methodology was applied to a case study. A primary Natech scenario involving an atmospheric tank T01 storing gasoline (5000 m<sup>3</sup>) is assumed. Two targets are considered, one atmospheric tank T02 storing gasoline (5000 m<sup>3</sup>) and one pressurized vessel P01 storing ammonia (160 m<sup>3</sup>) are assumed. A set of conventional scenarios involving T01 is assumed to have baseline risk figures in analogy with (Misuri et al., 2021a). A severe flooding ( $f=2.0 \times 10^{-3} \text{y}^{-1}$ ,  $h_w=2\text{m}$ ,  $v_w=1\text{m/s}$ ) is chosen as reference natural event, and applying the model of Landucci et al. (2012) and considering 0.9 ignition probability, a primary pool fire with  $f_p = 7.395 \times 10^{-4} \text{y}^{-1}$  is obtained. The set of safety barriers is reported in Table 2, together with the barrier analysis level selected from Figure 1 and the updated performance.

Table 2: Equipment considered in the case study. In italics the item involved in the primary Natech scenario.

Barrier	T02	P01	$PFD_0$	$\eta_0$	Level	$PFD_f$	$\eta_f$
Foam-water system (FWS)	X		$5.42 \times 10^{-3}$	$9.54 \times 10^{-1}$	L2	1.00	$9.54 \times 10^{-1}$
Passive fire protection (PFP)		X	0	$9.99 \times 10^{-1}$	L1	0	$8.49 \times 10^{-1}$
Water deluge system (WDS)		X	$4.33 \times 10^{-2}$	1.00	L2	1.00	1.00
Emergency intervention (EEI)	X	X	$1.00 \times 10^{-1}$	0;1	n.a.	$1.00 \times 10^{-1}$	0;1

In particular, the PFP is assessed by L1 applying the  $\phi = 0.15$  retrieved from Misuri et al. (2020), while the L2 was applied both to the FWS and the WDS, demonstrating their expected unavailability during the reference natural event due to actuation failure, as shown in the FTAs reported in Figure 2.

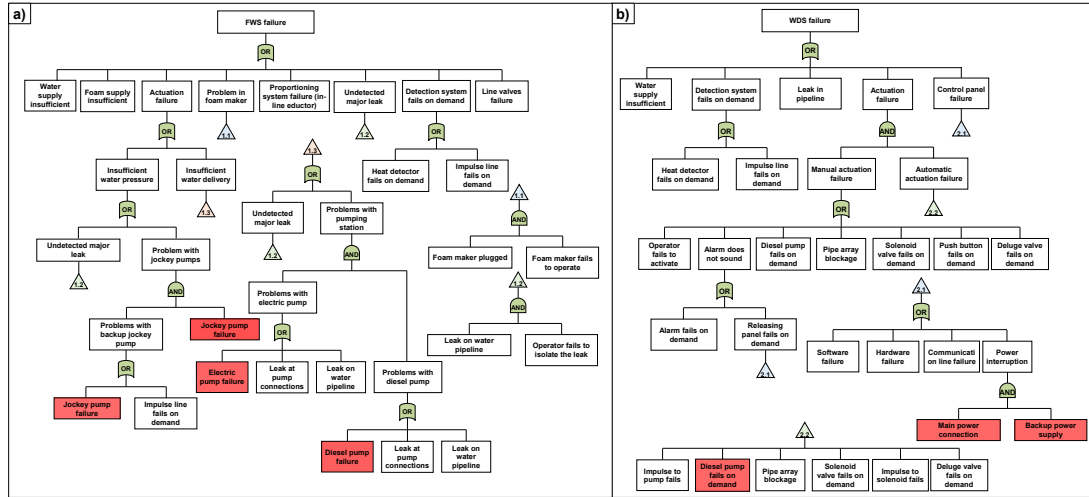


Figure 2: FTAs used for L2 analysis of the FWS (panel a) and the WDS (panel b). In red the nodes affected by the flood. Adapted from (Misuri et al., 2021a).

The logical rules of Table 1 have been used in the ETA to assess secondary domino scenarios involving T02 and P01. As benchmarks, also the best-case of barriers with baseline performance and the worst-case of absence of safety barriers have been considered, obtaining the results of Figure 3. As it can be seen comparing Figure 3-a and Figure 3-b, the LSIR obtained applying the approach of Section 3.3 for barrier assessment enabled a more realistic risk quantification. This is confirmed by the F/N curves of Figure 3-c, indicating that considering baseline barrier performance (best-case) would have led to an underestimation of risk, while assuming the absence of barriers (worst-case) would have led to possibly overconservative estimates.

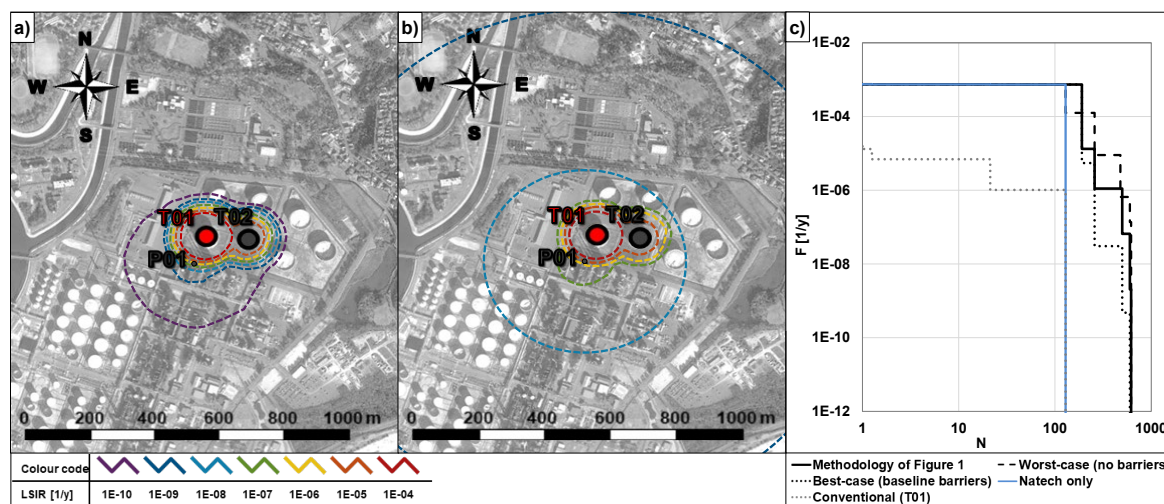


Figure 3: Results obtained for the case study. LSIR contours obtained for: (panel a) the best-case (barriers with baseline performance) and (panel b) approach of Figure 1. F/N curves obtained for the case study (panel c).

## 6. Conclusions

A comprehensive framework to address the quantification of Natech risk considering safety barrier depletion is presented. A novel multi-level approach to update safety barrier performance during natural events is conceived. The methodology enables a more realistic quantification of Natech risk and is crucial to define strategies to enhance the capabilities of these systems also in light of possible effects of climate change.

## References

- Antonioni G., Landucci G., Necci A., Gheorghiu D., Cozzani V., 2015 Quantitative assessment of risk due to NaTech scenarios caused by floods, *Reliability Engineering and System Safety*, 142, 334-345.
- CCPS, 2001, Layer of protection analysis: simplified process risk assessment, AIChE Centre of Chemical Process Safety, New York, NY.
- CSB, 2018, Organic peroxide decomposition, release and fire at Arkema Crosby following Hurricane Harvey flooding, US Chemical Safety and Hazard Investigation Board, Washington DC.
- Girgin S., 2011, The Natech events during the 17 August 1999 Koaceli earthquake: aftermath and lessons learned, *Natural Hazards and Earth System Sciences*, 11, 1129-1140.
- Krausmann E., Cruz A.M., Salzano E., 2017, Natech Risk Assessment and Management, Reducing the Risk of Natural-Hazard Impact on Hazardous Installations, Elsevier, Amsterdam, NL.
- Landucci G., Antonioni G., Tugnoli A., Cozzani V., 2012, Release of hazardous substances in flood events: Damage model for atmospheric storage tanks, *Reliability Engineering and System Safety*, 106, 200-216.
- Landucci G., Argenti F., Spadoni G., Cozzani V., 2016, Domino effect frequency assessment: The role of safety barriers, *Journal of Loss Prevention in the Process Industries*, 44, 706-717.
- Landucci G., Argenti F., Tugnoli A., Cozzani V., 2015, Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire, *Reliability Engineering and System Safety*, 143, 30-43.
- Landucci G., Necci A., Antonioni G., Argenti F., Cozzani V., 2017, Risk assessment of mitigated domino scenarios in process facilities, *Reliability Engineering and System Safety*, 160, 37-53.
- Liu Y., 2020, Safety barriers: Research advances and new thoughts on theory, engineering and management, *Journal of Loss Prevention in the Process Industries*, 67, 104260.
- Mesa-Gómez A., Casal J., Sánchez-Silva M., Muñoz F., 2020, Advances and gaps in Natech quantitative risk analysis, *Processes*, 9, 40.
- Misuri A., Landucci G., Cozzani V., 2020, Assessment of safety barrier performance in Natech scenarios, *Reliability Engineering and Systems Safety*, 193, 106597.
- Misuri A., Landucci G., Cozzani V., 2021a, Assessment of risk modification due to safety barrier performance degradation in Natech events, *Reliability Engineering and System Safety*, 212, 107634.
- Misuri A., Landucci G., Cozzani V., 2021b, Assessment of safety barrier performance in the mitigation of domino scenarios caused by Natech events, *Reliability Engineering and System Safety*, 205, 107278.
- Misuri A., Cozzani V., 2021, A paradigm shift in the assessment of Natech scenarios in chemical and process facilities, *Process Safety and Environmental Protection*, 152, 338-351.