CHEMICAL ENGINEERING TRANSACTIONS

VOL. 77, 2019

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Genserik Reniers, Bruno Fabiano
Copyright © 2019, AIDIC Servizi S.r.l.
ISBN 978-88-95608-74-7; **ISSN** 2283-9216

DOI: 10.3303/CET1977139

A Dynamic Approach to Fault Tree Analysis based on Bayesian Beliefs Networks

Tomaso Vairo[a]*, Maria Francesca Milazzo[b], Paolo Bragatto[c], Bruno Fabiano[d]

[a] ARPAL – Grandi Rischi, via Bombrini 8, 16149 Genoa, Italy
[b] Dip.Inge. – Department of Engineering, University of Messina, Contrada di Dio, 98166 Messina, Italy
[c] INAIL – Technological Innovation Department, Research Centre, via Fontana Candida, 1, 00078 Monteporzio, Italy
[d] DICCA – Civil, Chemical and Environmental Engineering Dept., Genoa University, via Opera Pia 15, 16145 Genoa, Italy
tomaso.vairo@arpal.gov.il

According to the Seveso Directives, the risk assessment is crucial for an effective control of major accident hazard. Nevertheless, the complexity of many Seveso sites, due to human, technical and organizational factors makes recognized common practices limited because of their intrinsic static nature. In this paper, a dynamic approach for risk assessment is proposed, which allows evaluating moment by moment the state of the system under analysis by Bayesian belief networks. A petrochemical coastal storage was selected as applicative case-study to verify the capability of the dynamic approach. Network training is performed by entering historical reliability data, near-miss and accidents data series collected on-site by periodical inspection plans on critical elements, as well as from the evidences of SMS reports. Upon proper refinement and further validation with reliable field data, the predictive approach may be used as a management decision-making tool.

1. Introduction

As many other contexts, risk analysis has been strongly affected by the big data era, that means by the ability to provide continuous acquisition, effective process and meaningful communication of such information. This amount of data is particularly interesting in managing risk and asset integrity of process plants. Research in this context is faced with the dilemma that, while there have been significant developments in understanding how accidents occur, there has been no comparable development in understanding how to adequately assess and reduce risks (Bouloiz et al., 2013), considering both process and personnel side of safety (Fabiano et al., 1995). In process safety and risk management area, a need for an integrated and holistic system approach has been explicitly described and advanced research trends include knowledge-based methods combined with process models, such as Petri nets, signed digraphs, and dynamic simulation (Jain et al., 2018). The application of BN in the field of risk and reliability was explored by many researchers, e.g. Abbasi et al., 2016. A system is safe if it is impervious and resilient to perturbations, thus the identification and assessment of relevant hazards is an essential prerequisite for system safety. Nevertheless, traditional methods for risk assessment do not take into account interactions between system components and do not adequately address human and organizational factors, thus being not appropriate for complex systems (Leveson, 2004). Some efforts have been made to include human and organizational factors (Milazzo et al., 2010), while few works attempt to integrate organizational and human factors in a dynamic approach. As examples based on Bayesian theory, Kalantarnia et al. (2009), proposed a method for dynamic safety management and Meel & Seider (2006) estimated the dynamic probabilities of accident sequences having different severity levels by using statistical analyses of near-miss and incidents. In this work, a dynamic approach for risk assessment, based on the evaluation of the state of the system under analysis, is outlined to be applied for those cases when a static assessment method is not trustable. The Bayesian networks are constructed from Fault Trees Analyses (FTA) and failure rates represents a priori probabilities. The modelling provides a set of independent nodes (root elements of FTA, i.e. critical items) and intermediate events for the top event. The network training is performed by using historical reliability data, near-miss and accidents data collected on-site by periodical

Paper Received: 14 November 2018; Revised: 17 May 2019; Accepted: 12 July 2019

Please cite this article as: Vairo T., Milazzo M., Bragatto P., Fabiano B., 2019, A Dynamic Approach to Fault Tree Analysis based on Bayesian Beliefs Networks, Chemical Engineering Transactions, 77, 829-834 DOI:10.3303/CET1977139

inspection plans on critical elements. The remainder of this paper is as follows: Section 2, outlines the background and covers the methodology; Section 3 describes the Seveso upper tier costal storage, selected for its complexity and the environmental sensitivity of the site, with main hazards connected to possible spill and fire scenarios following HC/chemicals major LOCs (Palazzi et al., 2012). Results obtained by the framework, including sensitivity analysis, are discussed in Section 4, followed by concluding remarks in Section 5.

2. Bayesian belief networks

When implementing a critical safety application, it is essential to be able to present the argument that it meets, i.e. the system requirements, in terms of availability and reliability, and how often it returns a response and how often such a response is correct. Typically, this argument is supported by a combination of (i) hard and soft evidence and (ii) a priori and a posteriori evidence. BBNs provide a tool for incorporating these types of evidence and providing quantitative results, e.g. to model alarm management (Wang et al., 2018). Fault Tree Analyses (FTA) encapsulate the concept that the failure of a (sub)system can be caused by the failure of lower-level (sub)systems, so that the minimal cut sets can be identified. Given a FTA, failure rates and failure distributions can be associated with each leaf in a BBN and then consolidated into a failure rate and failure distribution for an entire system. In practice, quantifying leaf failures for an entire system is difficult or, in many cases, impossible. Bayesian networks allow the quantification by accepting evidence for the failure rate of any node and, then, using Bayes' theorem to calculate the a posteriori probabilities of the failure rates of the sub-elements. API recommended practice (API 581, 2016) uses Bayes' theorem to update the prior knowledge of the failure rate λ with the information gained during an inspection. λ is not considered as a single value variable, but as a random variable expressed in the form of a probability density function (pdf). Then a posterior pdf given E is determined, which is the newly observed evidence. This posterior distribution can be derived from the product of a prior distribution of failure rate values, $f(\lambda)$, and the new information as a likelihood function, $L(E|\lambda)$:

$$f\ (\lambda|E) = \frac{f(\lambda)L(E|\lambda)}{\int_0^\infty f(\lambda)L(E|\lambda)d\lambda} \tag{1}$$

The likelihood function represents the probability that E is observed given a value of λ. With little information to start with as a prior distribution, a uniform distribution can be assumed, while for a likelihood function, in case of a constant failure rate, a Poisson distribution is suited.

3. The coastal storage facility

Seveso II Directive produced a growth of interest in the field of environmental risk assessment from a legislative point of view, with a specific classification of dangerous substances (Sikorova et al.,2017). As demonstrated by recent statistical analysis on process accidents hazardous releases still represent a serious concern in the petrochemical industries notwithstanding the available accurate modelling techniques and the achievement of acceptable preventive risk limits (Fabiano et al., 2018). Storage siting in coastal areas implying possible sea environment contamination in case of accidental oil spill (Palazzi et al., 2004) evidences the need for reliable accident forecasting, accurate consequence assessment and effective emergency management plans. The coastal storage facility is a Seveso upper tier terminal consisting of a quay (the Western Dock) and four piers (Alfa, Beta, Gamma and Delta), where loading/unloading operations of hazardous products take place according to typology, berths availability and tanker characteristics, as follows. For oil products:

- load arms installed on the Beta, Gamma and Delta berths, which connect the ship with the pipes that run on the pier (dock line); the arms are equipped with two safety systems: (i) automatic closing of the "double valve" devices, to segregate the flow of product moved on the ship and on the ground side in case of emergency; (ii) sectioning of the "double valve" in the event of abandonment of the ship's mooring, which prevents the product from escaping. Therefore, if a ship has to move away in an emergency, the system automatically closes the "double valve" and disconnects the arm preventing avoiding releases;
- the pier lines that engage in a complex system of pipes and allow different interchanges based on the dock, the product to be moved and the product’s destination;
- the collector pit lines that actually connect the pontoon lines with the booster stations of the user companies and with the manifold area of another company;
- booster stations that send products to factories or warehouses located inland through relaunch pumps and oil pipelines.

For chemical products:

- the hoses installed on the Western Dock, which connect the ship with the pipes that run on the quay;
- the lines of the quay that are grafted, from each approach, in the relative line that runs in *collector pit*;
- collector pit lines directly connected to deposits located outside the terminal.

The industrial activity involves only handling and storage without any processing. Handling takes place at room temperature (with the exception of the fuel oil that can be heated up to a maximum temperature of 60°C) and at the pressure supplied by the on-board pumps and by the the pumps of the coastal storage deposit.

4. FTA development and risk assessment

4.1 Conventional approach

The top events presented in this work are the following:

1. *Leakage of petroleum products or crude oil into collectors* during the loading/unloading ship can be connected to the following immediate causes: significant loss or catastrophic breakage of the pipes used for handling petroleum products and crude oil (pipe sections passing through the collector pit); leakage from valves/flanges.
2. *Leaking from the vapor recovery system* and losses from components can occur both under random conditions and due to overpressures due to maneuvering errors on board (e.g. failure to open the valve of a tank during loading). However, it should be emphasized that the lines used for handling crude oil and diesel oil are protected by overpressure with safety valves set at 14 bar in the form of an underground tank located near the DISCOIL.
3. *Product losses along the piers* can be connected to one of the following immediate causes: significant loss of containment, or catastrophic breakage of the pipes used for handling oil and crude products (sections of pipes passing along the piers); loss from valves/flanges; leakage from the vapor recovery unit (VRU); loss from the loading arms.

Table 1 summarizes the basic failure rates adopted for this study (Cremer & Warner, 1982; TNO, 1999).

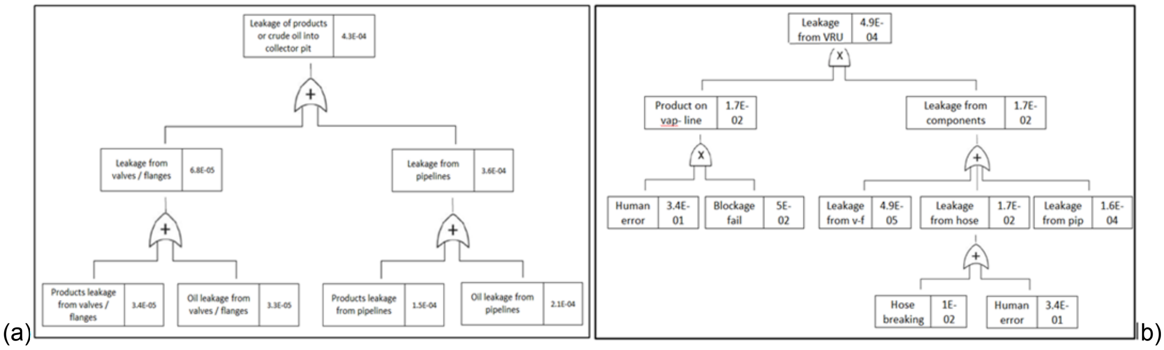

Figure 1: FTA (a) Oil/chemicals leak into collector pits; (b) Leak from vapour recovery system (VRU)

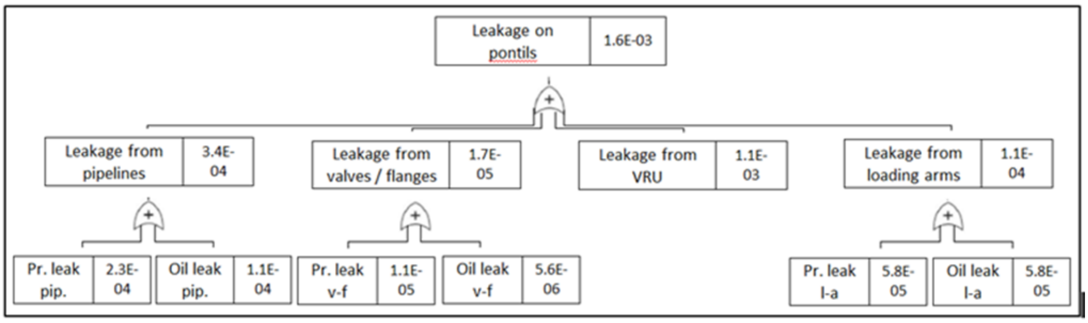

Figure 2: FTA Oil/chemical leak on piers

Results of FTA for the considered loss of containment scenarios are summarized in Figures 1 and 2.

Table 1: Basic events probability of failures (leak in the collector pits or leak on piers and VRU)

Basic event	Failure rate	Failure probability
Collector pit		
Valve full rupture, (chemicals)	8E-06	0.0034
Valve full rupture, (oil)	8E-06	0.0033
Significant pipeline LOC (chemicals)	3E-05	0.015
Significant pipeline LOC (oil)	3E-05	0.02
Piers and VRU		
Significant pipeline LOC (chemicals)	3E-05	0.023
Significant pipeline LOC (oil)	3E-05	0.011
Valve full rupture, (chemicals)	8E-06	0.0011
Valve full rupture, (oil)	8E-06	0.00056
Loading arms catastrophic rupture (chemicals)	3E-06	0.0058
Loading arms catastrophic rupture (oil)	3E-06	0.0055
Operative error or omission	5E-01	34
Incorrect hose connection	4E-04	0.65

4.2 The Bayesian approach

BBN can be seen as a natural extension of FTA, which allows incorporating local dependence between events and enabling both predictive and inference analysis. BBN approaches require specifying exact prior probabilities for each elementary event and conditional probabilities for every dependency. Under the working hypothesis of elementary event independency, it is mandatory to elicit a prior distribution for each elementary event, then to use simulations for the derivation of the prior distributions for intermediate events and the Top Event, and finally to find posterior distributions using priority sampling. Starting from the above-mentioned fault trees, the following Bayesian networks have been constructed, in which the failure rates of the trees represent the a priori probabilities. The basic networks are shown in Figure 3 a-b-c.

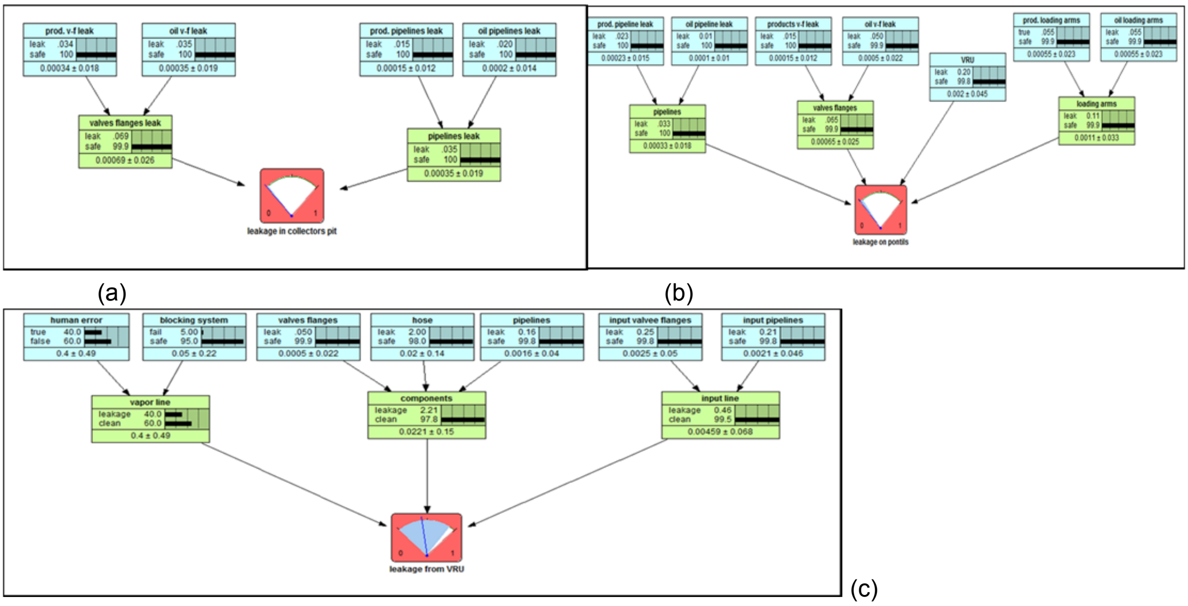

Figure 3: BNs (a) Oil/chemicals leak into collector pits; (b) Leak from VRU; (c) Oil/chemicals leak on piers

Sensitivity analysis can be empirically performed by altering each of the parameters of the query nodes and observing the consequent variation in the posterior probabilities of the query node (such as the endpoint). Tables 2-3 show the results of networks analysis performed by MCMC (Markov Chain Monte Carlo) sampling, evidencing the sensitivity of the Top Event nodes to findings in the other nodes and suggesting the possibility of setting up key management priorities, upon further validation with significant field data information.

Table 2: Sensitivity of “Leak in the collector pits”' to a finding at another node

Node	Variance reduction	Percent	Mutual info	Percent	Beliefs variance
Collector pit	0.001039	100	0.01180	100	0.0010385
Valves / flanges	0.0006889	66.3	0.00728	61.7	0.0006889
Oil valves / flanges	0.0003494	33.6	0.00356	30.2	0.0003494
Pipelines	0.0003494	33.6	0.00356	30.2	0.0003494
Chemicals valves / flanges	0.0003394	32.7	0.00346	29.3	0.0003394
Oil pipelines	0.0001996	19.2	0.00201	17	0.0001996
Chemicals pipelines	0.0001497	14.4	0.00150	12.7	0.0001497

Table 3: Sensitivity of “Leak on piers” to a finding at another node

Node	Variance reduction	Percent	Mutual info	Percent	Beliefs variance
Piers	0.004058	100	0.03821	100	0.0040576
VRU	0.001988	49	0.01674	43.8	0.0019877
Loading arms	0.001092	26.9	0.00897	23.5	0.0010920
Valves / flanges	0.0006451	15.9	0.00524	13.7	0.0006451
Chemicals loading arms	0.0005458	13.5	0.00442	11.6	0.0005458
Oil loading arms	0.0005458	13.5	0.00442	11.6	0.0005458
Oil valves / flanges	0.0004962	12.2	0.00402	10.5	0.0004962
Pipelines	0.0003274	8.07	0.00264	6.91	0.0003274
Chemicals pipelines	0.0002282	5.62	0.00184	4.8	0.0002282
Chemicals valves / flanges	0.0001488	3.67	0.00119	3.13	0.0001488
Oil pipelines	9.92e-05	2.44	0.00080	2.08	0.0000992

4.3 Introducing evidences

The networks are then updated, on one hand, with the reliability parameters (results of the inspections or failures on demand - hard evidences) and, on the other one, with the evidences of the ongoing activities, which represent the likelihood coefficients (soft evidences). By considering a product transfer lasting nearly ten hours, soft evidence included, among others, the absence/presence of failures or losses in the early hours of the operation, which are the most critical. These evidences increase the likelihood coefficient related to the absence/presence of failures during the operation. Other evidences are, for instance, the absence/presence of failures, or malfunctions, at the start of VRU, or the absence of human error during the operations.
From this, the trend of the probability of occurrence of the top events can be obtained, in relation to what is happening in the plant when introducing “good” evidences (Figure 4), “bad” evidences (Figure 5), or “bad” evidences taking into account designed preventive actions (Figure 6).

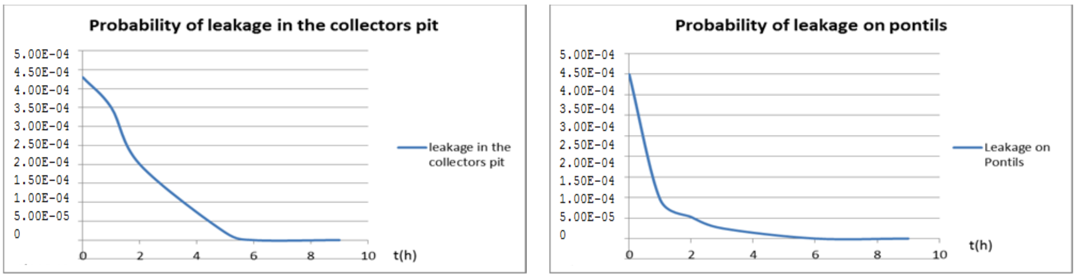

Figure 4: "Good" evidences: trend of the posterior probability of leakage in the collectors pit and on piers

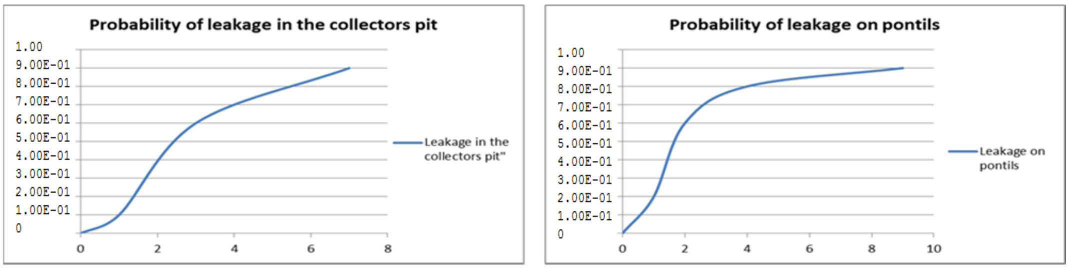

Figure 5: "Bad" evidences: trend of the posterior probability of leakage in the collectors pit and on piers

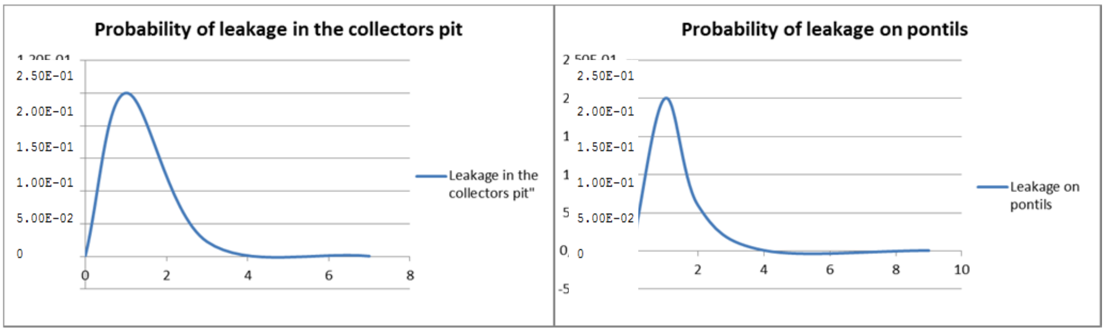

Figure 6: "Bad" evidences with corrective measures: trend of the posterior probability of given leakages

5. Conclusions

BBNs are a robust and flexible method for modeling complex systems that allows incorporating quantitatively into the safety analysis both hard and soft evidence. The prediction of variable influences and the analysis of variables dependence strength permits identifying which, among the basic failures, are the most influencing on the probability of the top events. The true probability of failure on demand of a component is of paramount importance for reliance on safeguards and addresses maintenance priorities. Additionally, the relationship between the risk trend represented as a probability function and the evidences during the operation in progress is analyzed. The framework may represent a tool allowing to manage in a real-time mode the operations with a focus on safety and combined with proper advanced analytics applications allows anticipating what should be done to avoid upcoming incidents.

References

Abbassi R., Bhandari J., Khan F., Garaniya V., Chai S., 2016, Developing a quantitative risk-based methodology for maintenance scheduling using bayesian network, Chem Engineering Trans, 48, 235-240.

API 581, 2016, Risk-Based Inspection Technology RP581, American Petroleum Institute, Washington, USA

Bouloiz H., Garbolino E., Tkiouat M., Guarnieri F., 2013, A system dynamics model for behavioral analysis of safety conditions in a chemical storage unit, Safety Science, 58, 32–40.

Cremer and Warner Ltd, 1982, Risk analysis of six potentially hazardous industrial objects in the Rijnmond area, London (known as COVO Study).

Fabiano B., Parentini I., Ferraiolo A., Pastorino R., 1995, A century of accidents in the Italian industry - Relationship with the production cycle, Safety Science, 21, 65-74.

Fabiano B., Currò F., Reverberi A., Palazzi E., 2018, Generalized mathematical modelling of spray barriers, Chemical Engineering Journal, https://doi.org/10.1016/j.cej.2018.10.045

Jain P., Rogers W.J., Pasman H.J., Mannan M.S., 2018, A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer, Proc Saf Env 118, 115-124.

Kalantarnia M., Khan F., Hawboldt K., 2009, Dynamic risk assessment using failure assessment and Bayesian theory, Journal of Loss Prevention in the Process Industries, 22, 600–606.

Leveson N., 2004, A new accident model for engineering safer systems, Safety Science, 42, 237-270.

Meel A., Seider W., 2006, Plant-specific dynamic failure assessment using Bayesian theory, Chemical Engineering Science, 61(21), 7036-7056.

Milazzo M.F., Maschio G., Uguccioni G., 2010, The influence of risk prevention measures on the frequency of failure of piping, International Journal of Performability Engineering, 6, 19-33.

Palazzi E., Currò F., Fabiano B., 2004, Simplified modelling for risk assessment of hydrocarbon spills in port area, Process Safety and Environmental Protection, 82, 412-420.

Palazzi E., Fabiano B., 2012, Analytical modelling of hydrocarbon pool fires: conservative evaluation of flame temperature and thermal power. Process Safety and Environmental Protection, 90, 121-128.

Sikorova K., Bernatik A., Lunghi E., Fabiano B., 2017, Lessons learned from environmental risk assessment within the framework of Seveso Directive in Czech Republic and Italy, Journal of Loss Prevention in the Process Industries, 49, 47-60.

TNO, 1999, Guidelines for Quantitative Risk Assessment CPR 18E (Purple Book). Committee for the Prevention of Disasters, The Hague, The Netherlands.

Wang H., Khan F., Abimbola M., 2018, A new method to study the performance of safety alarm system in process operations, Journal of Loss Prevention in the Process Industries, 56, 104-118.