Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

INGEGNERIA CIVILE, CHIMICA, AMBIENTALE E DEI MATERIALI

Ciclo XXIX

Settore Concorsuale di afferenza: 09/D3 - Impianti e Processi Industriali Chimici

Settore Scientifico disciplinare: ING-IND/25 - Impianti Chimici

Extension of Quantitative Risk Assessment to the Analysis of External Hazard Factors in the Chemical and Process Industry

Presentata da: VALERIA VILLA

Coordinatore Dottorato

PROF. LUCA VITTUARI

Relatore

PROF. ING. VALERIO COZZANI

Correlatore

PROF.SSA ING. GIGLIOLA SPADONI

Esame finale anno 2017

Alla mia famiglia,
con immenso affetto

Table of Contents

Abstract

The PhD research project is aimed at developing and applying an innovative framework toward Risk Assessment of cascading events within the chemical and process industry, addressing both domino and security-based events.

Cascading events are catastrophic accidents, triggered by external hazard factors, including safety-based (i.e., domino) and security-based events. In the chemical industry domain, barriers provide a crucial role for the prevention, control and mitigation of cascading events. Therefore, it is necessary to apply innovative techniques, aimed at the evaluation of barriers technical performance and at their optimal economic allocation, to be inserted within Quantitative Risk Assessment (i.e., QRA).

Concerning barriers technical performance, the research activity is aimed at applying Bayesian Networks to safety barriers performance assessment, regarding domino events. Starting from a conventional approach, preliminary applications have been aimed at implementing a Bayesian approach to barriers performance assessment concerning major accidents. Therefore, the approach has been extended to domino accident analysis, in purpose to evaluate the effect of barriers introduction within modelling. The case studies demonstrated that the application of a Bayesian approach provides a very accurate barriers performance assessment within QRA, with reference to external hazard factors driven accidents (i.e., domino events), offering a realistic risk picture.

Concerning barriers optimal economic allocation, the research activity is aimed at developing and applying an original economic model for the prevention of security-based cascading events. The model includes security upgrades performance and costs assessment, evaluation of benefits and definition of threat and vulnerability probabilities. The application of economic techniques, by means of cost-benefit and cost-effectiveness analyses, enables barriers optimal allocation within budgets constraints. Validation of the model is provided by application to relevant case studies. Therefore, the model enables defining rational criteria for barriers optimal selection and allocation and its outputs support the inclusion of security hazards within QRA, and related decision-making.

Extension of Quantitative Risk Assessment to the Analysis of External Hazard Factors in the Chemical and Process Industry

Section 1.
Premise

Since the past century, the worldwide population growth has caused a relentless increase of energy demand and material supply to fulfill its everyday needs. The chemical and process industry has seized the challenge by a continuous innovation in its technologies, which leads to a relevant increase of chemical production and, in turn, to process intensification, with high amounts of hazardous materials to be handled and stored, as well as severe operating conditions. Moreover, chemical and process installations tend to form huge and complex clusters, often located in proximity of densely populated areas for logistic purposes. Due to these reasons, the occurrence of cascading events, which are catastrophic escalations of accidental events, triggered by external hazard factors, and characterized by high impact and low probability, is a concerning phenomena. These accidental events may be divided based on their nature, into two classes. Safety-based events, as domino and natural events are unintentional, while security-based events, as terroristic attacks and sabotage, are the results of intentional malevolent acts. Indeed, the importance of cascading events is strictly linked to their potential consequences in terms of disruption of operations, destruction of property, environmental damages, health deterioration or loss of life, both inside and outside facility boundaries.

Nowadays, quantitative risk assessment is a widely applied tool to provide quantitative information on risk caused by conventional major accidents in the chemical and process industry. Therefore, it plays an established and fundamental role for major accidents prevention. Nevertheless, recent major catastrophic events have raised the need to go beyond the limits of conventional methods for risk assessment and related techniques to support the decision-making process, in purpose to address emerging and increasing risk issues, triggered by external hazard factors, as domino, security and natural events. This PhD research project was aimed at developing and applying a novel framework toward risk assessment of cascading events, addressing both domino and security-based events. State of the art methodologies for risk assessment and related decision-making process are presented, with a focus on recent techniques and tools for the inclusion of external hazard factors. Novel methodologies are presented and applied to case studies.

In Section 2, the state of the art of quantitative risk assessment background and recent developments within the chemical and process industry domain is provided. The

improvements of risk assessment techniques in the last thirty years, the limitations that still need to be tackled, and the possible way forward offered by dynamic risk assessment techniques, capable to deal with emerging and increasing risks, are highlighted.

In Section 3, an overview on the methods and tools to perform risk assessment and on economic techniques to support related decision-making, in the prevention of external hazard factors driven accidents, is provided. The description will focus on the role played by safety and security measures (or barriers), which are widely employed within chemical and process facilities, in purpose to prevent, control or mitigate unwanted events or accidents. Indeed, safety measures refers to unintentional (i.e., safety-based) accidents, while security-measures refers to intentional malevolent acts (i.e., security-based). Classifications and methodologies for their performance assessment are provided, highlighting parallels and differences. The analysis of research gaps is conducted to highlight possible needs to apply innovative techniques for barriers performance assessment and to develop novel economic models for their optimal selection and allocation, to be inserted within the broader risk assessment framework.

With regards to barriers performance, the research activity is aimed at developing and applying Bayesian Networks, a graphical-probabilistic technique able to dynamically revise occurrence probabilities over time, to safety barriers performance assessment in the context of major accidents and domino effects analysis. A description of the Bayesian approach is available in Section 3 and the applications thereto related are presented in Section 5. Starting from a conventional approach, preliminary applications are focused on the implementation of a Bayesian approach to safety barriers performance assessment and on the comparison of the obtained results. As the Bayesian approach proves to be able in representing accidental scenarios with enhanced flexibility in comparison with conventional methodologies and demonstrates its advantages in the revision of safety barriers performance probabilities, top event, intermediate and final events probabilities over time, it can be extended to cascading events prevention, with particular reference to domino accident analysis, to assess the effect of safety barriers application in the modelling step. Two original case studies, the first regarding a simplified tank farm and the second regarding a realistic tank farm, are carried out, in purpose to demonstrate the feasibility of the approach.

With regards to economic models for optimal barriers selection and allocation, the research activity is aimed at developing and applying an original economic model for the prevention of security-based cascading events and for related decision-making support. A description of the methodology is available in Section 4. Starting from the baseline performance of the physical security system, the model allows proposing site-specific security upgrades and accounting

both the performance improvement and the costs of their implementation. The model includes also the evaluation of benefits, considering avoided losses for several pertinent hypothetical scenarios. Moreover, it allows defining threat and vulnerability probabilities for a chemical installation, in relation with possible typologies of malicious acts. The application of economic techniques, by means of cost-benefit and cost-effectiveness analyses, enables the comparison among different security upgrades and the choice of economically feasible ones, as well as the determination of the combination with the maximum profit, with budgets constraints. The model is developed in two-fold versions, in purpose to better represent different typologies and specificities of security-based accidents within chemical and process installations. Validation of the model is provided by application to relevant case studies, presented in Section 6.

In this thesis, advanced tools and methodologies are applied, in purpose to address the inclusion of cascading events triggered by external hazards factors in quantitative risk assessment for the chemical and process industry domain.

Extension of Quantitative Risk Assessment to the Analysis of External Hazard Factors in the Chemical and Process Industry

Section 2.

State of the art on Risk Assessment background and recent developments

The objective of this section is to analyse the progress of Risk Assessment during the last decades and to offer an overview on its recent advancements and applications for chemical and process industries. Despite the general approach of Quantitative Risk Assessment (QRA) is unchanged since its origin in the early 1980s, QRA has continuously evolved in different forms and its fields of application have enlarged significantly beyond process safety, where it has always been traditionally developed and used for chemical process industries. Now risk assessment techniques play a fundamental role in process design, implementation of safety systems, inspection and maintenance planning as well as operation management. Eventually risk assessment has become an essential tool for the development, continued operation and expansion of process installations. On the other hand, QRA limitations, such as its inability to update the risk picture, led to the development of several recent dynamic risk assessment approaches, whose methodological and applicative contributions are introduced in this section. This demonstrates that risk assessment is in continuous development; nevertheless, it still shows many challenges to face: a way forward is improving its range of application, preciseness and its capability to be dynamically updated, that it will enhance its support to decision-making.

2.1 INTRODUCTION

During the last three decades, risk assessment has emerged as an essential and systematic tool that plays a relevant role in the overall management of many aspects of our life.

In particular, risk assessment has shown dramatically its importance in technical domains dealing with hazardous materials. Pasman affirms that events involving hazardous materials represent the most dreadful risk (Pasman, 2015). Such substances may range in nature and effect and a high-level definition may be provided by the CBRNE (Chemical, Biological, Radiological, Nuclear and Explosive) acronym, on which the Council of the European Union has recently focused its attention. In fact, a CBRNE agenda was defined to develop strategic and overarching approach to CBRNE policy fields involving internal and external safety and security aspects (Council of the European Union, 2012).

Loss of control of such substances has the potential to cause high consequence low probability accidents (Pasman, 2015) and specific safety measures are designed to mitigate such risk. For this reason, accurately evaluating risk of a system represents the foundation for effective prevention.

The chemical and nuclear sectors commonly store large amounts of CBRNE substances – mostly chemical and explosive the former and radiological and nuclear the latter. Presumably due to the high social impact of nuclear accidents (e.g. on the 30th anniversary of the Chernobyl disaster, access within the 30-km exclusion zone is still restricted (Fountain, 2016)), risk assessment has its roots in the nuclear sector and only later spread to the chemical process industry (Pasman, 2015).

Despite the obvious differences between the two sectors, continuous exchange of knowledge and methods from one to the other has led to huge improvements in the chemical process industry (Charvet et al., 2011) and helped to cope with increasing issues of social acceptability (Marshall, 1997).

Nuclear power risk analysts have a long tradition of quantitative approaches: the United States Nuclear Regulatory Commission developed its first nuclear power plant Probabilistic Risk Assessment in the 1970s (NUREG - US Nuclear Regulatory Commission, 2016). However, Quantitative Risk Analysis (QRA) reached the chemical process industry only at a later stage. For instance, before 2003 quantitative probability assessment was used to assess risk in the French chemical industry (Charvet et al., 2011). Similarly, the accident occurred in Buncefield (United Kingdom) in 2005 called into question the semi-qualitative risk analysis approach used for flammable substances in the British chemical industry, whereas the other hazardous substances were subject to QRA since the 1980s (Buncefield Major Investigation Board, 2008).

While the disadvantage of QRA was mainly represented by the computational effort needed to perform it, its advantage is that it deals with some of the criticisms made to qualitative analysis (Buncefield Major Investigation Board, 2008):

- vagueness in terminology, for example “a very high degree of protection”, “worthwhile (sometimes almost total) protection”, “unlikely but foreseeable”;
- arbitrariness and lack of transparency in selection of the worst-case event, and through this, potential inconsistency in treatment between installations;
- challenges at comparing the degree of protection achieved with that for other everyday risks.

With the progressive increase in computation power, QRA is nowadays a tool widely applied to provide quantitative information on risk caused by conventional accidents in chemical process plants.

Despite the obvious fact that QRA is not an exact description of reality, it may represent the best available, analytic predictive tool data to assess the risks of complex process and storage facilities. QRA consists of a set of methodologies for estimating the risk posed by a given system in terms of human loss or, in some cases, economic loss (CCPS - Center for Chemical Process Safety, 2000; Mannan, 2005). Recently, risk assessment methodologies and applications have evolved toward a dynamic direction, in order to address risk issues in a continuously evolving environment, support operations and overcome limitations of conventional techniques. Moreover, this allows for continuous integration with more accurate information and refinement of the risk picture (Paltrinieri and Khan, 2016). The Living Probabilistic Safety Analysis (LPSA), theorized for the nuclear sector in 1999 (IAEA, 1999), might have inspired such evolution.

In the past, several reviews dealt with risk assessment under different perspectives. Due to the difference in the review scopes, different techniques have been considered by these studies. However, they all address the fundamental phases of risk assessment and may provide useful insight.

Khan and Abbasi have presented a relevant state-of-art review on the techniques and methodologies available up to 1998 for risk assessment in the chemical process industry, but some steps forward have been made in the meantime (Khan and Abbasi, 1998a). Tixier et al. have listed 62 risk analysis methodologies, both qualitative and quantitative ones, for generic industrial plants (Tixier et al., 2002). Marhavilas et al. have published a review of risk analysis and assessment, but generically referred to different work sites (Marhavilas et al., 2011). More recently, Reniers and Cozzani (Reniers and Cozzani, 2013) and Necci et al. (Necci et al., 2015) presented reviews on quantitative risk assessment for the chemical process industry, specifically concerning domino accidents.

The present work aims to provide a comprehensive and up-to-date picture of risk assessment methodologies and relevant applications for the chemical process industry, which may be missing by reading the mentioned past reviews. This sector is addressed because of its high criticality in terms of safety and security. Progresses and drawbacks are identified in order to propose an overview on recent advancements and future directions. This allows understanding what is the state of the art of QRA in chemical process industry and why specific approaches are used today. Achievements and limitations suggest how risk assessment approaches may (or may not) be applied for different purposes. Moreover, limitations pave the way for future research and development of the current techniques.

The literature review proposed starts in Section 2.2 with a description of the implications of risk definition, whose concept provides sound foundation for risk assessment. Fundamentals of Quantitative Risk Assessment are reported in Section 2.3, in order to make clear what has

been nowadays accomplished as current industrial practice in risk assessment and what are eventually the criticalities. Section 2.4 intends to consider, with a novel classification approach, how risk assessment methodologies and applications have recently evolved toward a dynamic direction, in order to address risk issues in a continuously evolving environment. A review of existing dynamic risk assessment methodologies is followed by their application to different aspects inherent of the process industry: accident and consequence modelling, process design, implementation of safety systems, control systems, asset integrity and maintenance planning, inclusion of external factors. Section 2.5 presents a discussion on the advantages and limitations of dynamic approaches and, in Section 2.6, conclusions are drawn on the state of art of Risk Assessment and probable future developments for chemical process industries.

2.2 IMPLICATIONS OF RISK DEFINITION

Several efforts have been devoted to define the concept of risk in chemical process industry, as shown by related literature: Aven and Renn (Aven and Renn, 2010, 2009) proposed 9 general risk definitions, which have been later revised within risk assessment (Aven and Zio, 2011) and safety domains (Aven and Reniers, 2013) and eventually refined (Aven, 2012). Risk definitions provide a sound foundation for risk assessment and management: review of risk definitions is reported in Table 2. 1.

Table 2. 1 Review of risk definitions by Aven (Aven, 2012).

	Definition of Risk	References
1	**Expected value (Loss)**	Risk equals the expected loss. (Willis, 2007) Risk equals the expected disutility. (Campbell, 2005)
2	**Probability of an (undesirable) event**	Risk means the likelihood of a specific effect originating from a certain hazard occurring within a specified period or in specified circumstances. (Kirchsteiger, 2002)
3	**Objective Uncertainty**	Risk is measurable uncertainty, i.e. uncertainty where the distribution of the outcome in a group of instances is known (either from calculation a priori or from statistics of past experience). (Knight, 1921)
4	**Uncertainty**	Risk refers to uncertainty of outcome, of actions and events. (Cabinet Office, 2002)
5	**Potential/possibility of a loss**	Risk is the potential for realisation of unwanted, negative consequences of an event. (Rowe, 1977)
6	**Event estimated frequency (probability) × event consequences**	Risk is a measure of the probability and severity of adverse effects. (Lowrance, 1976) Risk is defined as a set of scenarios, each of which has a probability/ frequency and a consequence - set of triplets. For a given scenario, risk is the product of estimated probability/ frequency and event consequences. (Kaplan, 1997; Kaplan and Garrick, 1981)
7	**Event or consequence**	Risk is a situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain. (Rosa, 2003, 1998) Risk is an uncertain consequence of an event or an activity with respect to something that humans value. (IRGC - International Risk Governance Council, 2009)
8	**Consequences/damage/severity of these + Uncertainty**	Risk is equal to the two-dimensional combination of events/consequences and associated uncertainties (will the events occur, what will be the consequences). (Aven, 2007)
9	**Effect of uncertainty on objectives**	(ISO, 2009; ISO31000:2009, 2009)

As we can appreciate, there is a broad set of existing ways of looking at the concept of risk: expected loss (Willis, 2007), likelihood of hazard effect (Kirchsteiger, 2002), uncertainty of outcome (Cabinet Office, 2002), potential of negative consequence (Rowe, 1977) or combination of probability and consequence (Kaplan and Garrick, 1981; Lowrance, 1976).

Reading such definitions and their authors explanation, it can be derived that the terms used to express loss (Willis, 2007), disutility (Campbell, 2005), effect (ISO, 2009; ISO31000:2009, 2009; Lowrance, 1976), outcome (Knight, 1921) and (undesirable) event (Kirchsteiger, 2002) may be conceptually associated to Kaplan and Garrick's "consequence" (Kaplan and Garrick, 1981). While uncertainty (Aven, 2007; Cabinet Office, 2002; ISO, 2009; ISO31000:2009, 2009; Knight, 1921), likelihood (Kirchsteiger, 2002), potential or possibility (Rowe, 1977) may be conceptually associated to Kaplan and Garrick's "probability" (Kaplan and Garrick, 1981). In this way, the definitions of risk reported in Table 2.1 may be plotted on a "consequence/probability" diagram in order to show whether they give more importance to one or the other aspect (or both) (Figure 2. 1). This may be objected as "over-reduction" to basic terms, because each definition conveys specific (and important) shades of the risk concept, according to their authors. For this reason, the diagram gives only a high-level overview on the priorities addressed by these risk definitions. Figure 2. 1 can be read in a twofold manner to highlight the difference between risk definitions and risk itself.

1. Consequence/probability plot for risk definitions, where definition is intended as "an exact statement or description of the nature, scope, or meaning of something" (i.e. risk) (Stevenson, 2016). It shows that definition 1 (to a lower extent also definition 7 – Table 1) focuses mainly on the potential event consequence, while definition 4 focuses mainly on the probability. The other definitions address both consequence and probability, with varying degrees of accuracy – 5, 2 and 9 in a relatively less specific and detailed way than 3, 6 and 8.

2. Consequence/probability plot to categorize unbiased hypothetical risk into typologies. Risk of low-probability and low-consequence events resides in the "normal area" (green area) and it is an acceptable risk to sustain. While the probability and the event consequence raise, the associated risk is described first by the intermediate area (yellow area), for which risk mitigation measures are needed, and then by the intolerable area, for which extraordinary measures of risk prevention should be carried out.

Four priority areas are reported on the diagram, showing the typology of risk considered as worst-case scenario by the definitions from Table 2. 1. For instance, the risk definitions 1 and 7 associate risk mainly with consequence. For this reason, they may lead to identify worst-case scenarios in any point of the elongated priority area 1, without distinction on probability. Similarly, the priority area 4 shows where worst-case scenarios characterized by high

probability can be identified by following the risk description 4. The priority areas 2 and 3 rely on both consequence and probability to identify worst-case scenarios. However, while the risk definitions 5, 2 and 9 being less detailed may lead to uncalibrated assessment, following the risk definitions 3, 6 and 8 may allow defining actual high-consequence and high-probability worst-case scenarios.

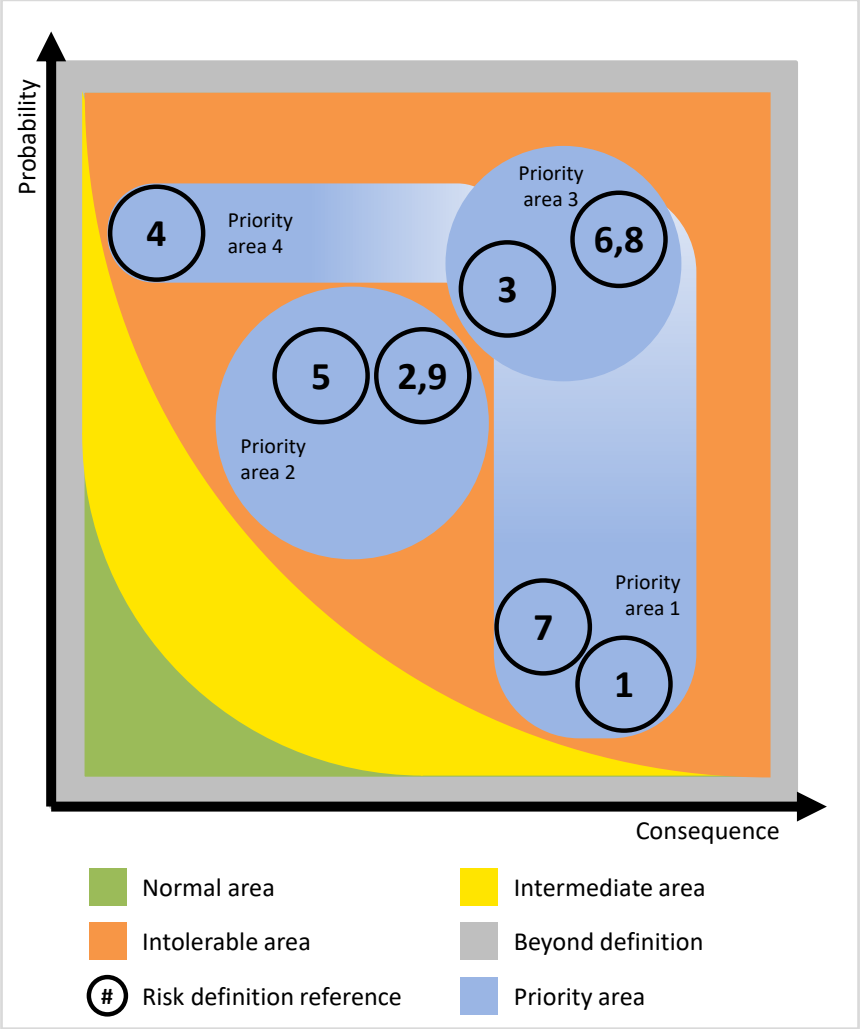


Figure 2. 1 Diagram of risk definitions and related priority areas.

Different risk definitions may lead to different ways of risk assessment and management. For instance, three out of four priority areas in Figure 2. 1 coincide with the risk classes outlined by Renn and Klinke (Renn and Klinke, 2004), for which different strategies for action were defined.

Risk priority area 1. Risk management with focus on reducing the disaster potential, improving emergency preparedness and increasing resilience – i.e. the capability to cope with the unexpected (Renn and Klinke, 2004).

Risk priority area 2. Risk management with focus on implementing precautionary principle, improving knowledge and reduction/containment (Renn and Klinke, 2004).

Risk priority area 3. Risk management with focus on consciousness building and risk communication (Renn and Klinke, 2004).

Risk priority area 4. Due to the high probability of occurrence, risk management with focus on lessons learned from past events. Not included in Renn and Klinke's classes.

This association of different perspectives on the definition of risk and related risk strategies suggests that there is not one single approach, but several paths leading to relatively different results, which may be all beneficial but intrinsically incomplete. In order to properly cover the consequence/probability diagram (Figure 2. 1), integration is needed for continuous enrichment with new and important details of the overall risk picture.

2.3 FUNDAMENTALS OF RISK ASSESSMENT

Distant events in time, such as the tragedies occurred in Bhopal (1984) and Piper Alpha (1988), as well as more recent ones, such as Buncefield (2005) and Deepwater Horizon (2010), have remarked the essential role of adequate management and control for chemical process industry. The European industrial safety regulations aiming to control major-accident hazards related to chemical substances are named after the town of Seveso, in Italy, scene of a disaster occurred in a chemical process plant in 1976.

In 2012, the third generation of these regulations (Seveso III directive) (EU, 2012) was issued and it applies to more than 10000 industrial establishments in the European Union, mainly chemical, petrochemical, logistics and metal refining sectors (European Commission - Environment Directorate, 2015). QRA is used to comply with Seveso regulations (Pasman and Reniers, 2014), evaluate the overall process safety risk in the chemical process industry and identify areas requiring risk reduction (CCPS - Center for Chemical Process Safety, 2000).

The installations to be considered in the QRA are selected following consultation between the operator of an establishment and the competent authority. The operator is responsible for the calculations needed to select installations. However, the selection of the installations to consider in the QRA is carried out by the competent authority only (TNO, 2005a).

2.3.1 Quantitative risk assessment for Chemical Process Industries

QRA is a systematic methodology for identifying and quantifying contributions to overall risk of a process facility. As defined by NORSOK Standard Z-013 (NORSOK, 2010) and by ISO/IEC standard (ISO31000:2009, 2009) Quantitative Risk Assessment includes: establishment of the context, risk identification, performance of the risk analysis, risk evaluation.

Communication, consultation, monitoring and review activities should be performed prior to, during and after the assessment, in purpose to guarantee the achievement of its goals. The Risk Assessment process defined by the NORSOK standard Z-013 (NORSOK, 2010) has been reported in Figure 2. 2.

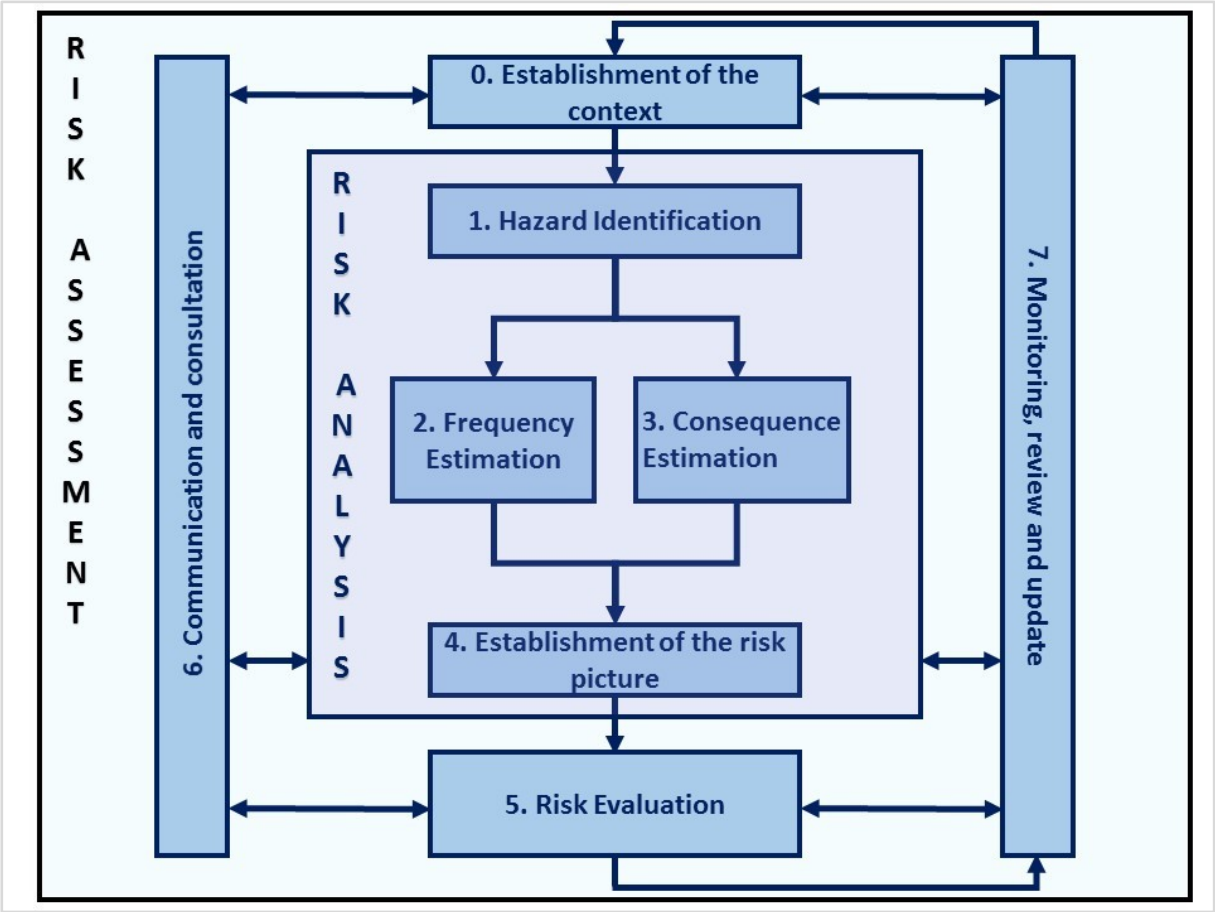


Figure 2. 2 Risk Assessment for Process Industry (CCPS - Center for Chemical Process Safety, 2000; NORSOK, 2010); figure adapted from NORSOK Standard Z-013 (NORSOK, 2010).

A QRA can provide authorities and stakeholders with a sound basis for creating awareness about existing hazards and risks. Based on the outcomes from the QRA, potential measures to control or reduce the risk can be implemented, and their effect can be assessed. A preliminary step (0 – Establishment of the context) defines objectives, responsibilities, methods, as well as risk acceptance criteria and deliveries throughout process and execution plan, in order to derive full value from the results obtained (Mannan, 2005).

The first step in the development of a chemical process QRA is the identification of hazards (1 – Hazard identification), which may have several important aims:

1. Highlighting possible malfunctions of the systems, that even without causing accident, can give raise to a loss of product quality or to the process-plant shutdown.

2. Outlining top-events that are undesired situations, often the potentials of release of hazardous substances to the environment, to be included in the QRA.
3. Describing potential scenarios associated with the top-events and their consequences. Based on the type of process upset and the performance of control and safety barriers, the scenario could involve quality loss, safety loss, or both.

As reported by the Center for Chemical Process Safety (CCPS - Center for Chemical Process Safety, 2000), several approaches to hazard identification may be employed: check lists, preliminary hazard analysis (PHA), failure modes and effects analysis (FMEA), fault tree analysis (FTA), bow-tie analysis (Figure 2. 3), hazard and operability study (HAZOP), etc. Their applicability depends on the project lifecycle, as well as the amount of information required. The maximum credible accident scenario analysis method developed by Khan and Abbasi (Khan and Abbasi, 2002) can be used as a criterion to identify credible scenarios among a large number of possibilities (Hashemi et al., 2014).

The following phases are central for the whole QRA process and lead to the estimation of potential initiating events frequencies and evaluation of event consequences (2 – Frequency estimation and 3 – Consequence estimation). As stated by Crowl and Louvar (Crowl and Louvar, 2011), risk analysis basically involves the estimation of accident consequences and frequencies using engineering and mathematical techniques.

Generic failure rates can be retrieved from databases and applied in QRA calculations; specific plant data should be applied, if available. Guidelines for Quantitative Risk Assessment "Purple Book" (TNO, 2005a) reports generic loss of containment events (LOCs) and failure frequencies for a number of standard installations like storage tanks, transport units, pipelines and loading equipment. LOCs should be included if the failure frequency is higher than 10^{-8} per year and if lethal damage (1% probability) outside the establishment boundary is possible. The failure data reported in this source are largely based on the research done in the COVO study (COVO Commission, 1981), as reported by Beerens (Beerens et al., 2006). Similarly, Health & Safety Executive (HSE) has published a set of generic failure frequency data for process installations (HSE - Health and Safety Executive, 2009) and it has recently started a comprehensive project "Storybuilder" (HSE - Health and Safety Executive, 2012), in order to update failure frequencies for process plants.

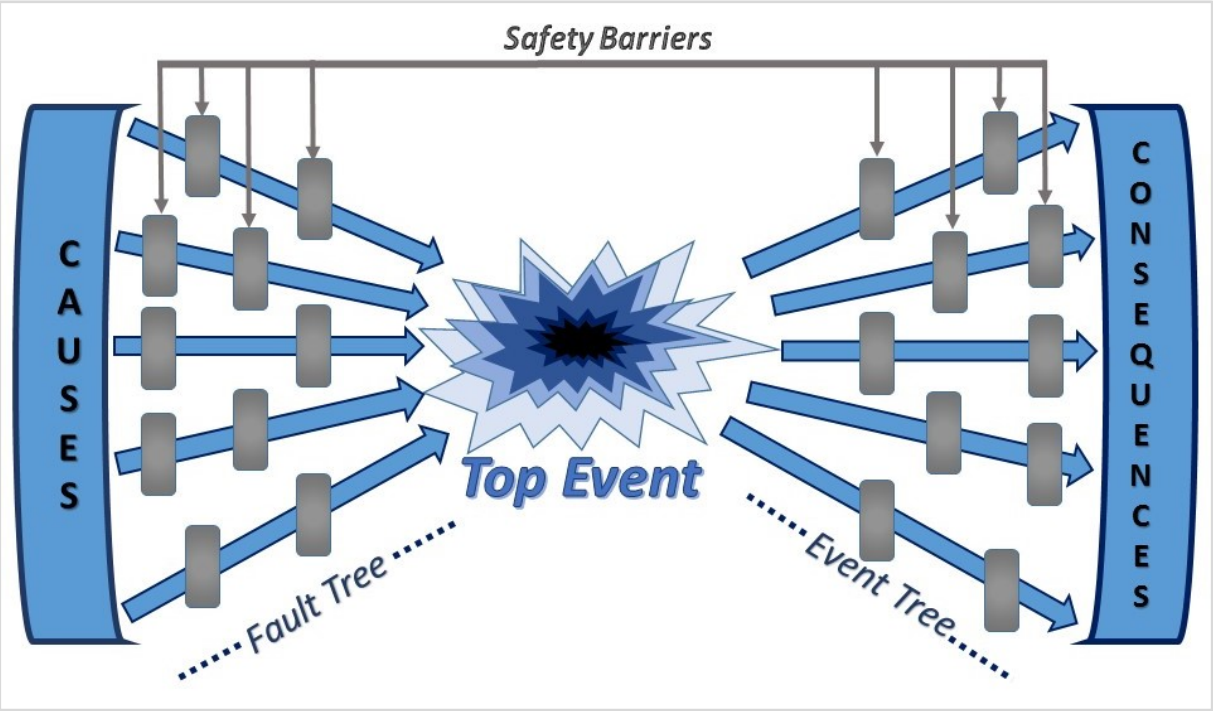


Figure 2. 3 Bow-Tie Diagram: a valuable standard tool for Risk Assessment.

Consequence estimation is used to determine the potential for damage or injury from specific unwanted events. Quantification of consequences has been usually carried out in terms of production loss, human health loss, assets loss, and environmental loss (Khan and Haddara, 2004). The assessment of consequences can be performed using a huge number of mathematical and empirical models; a description of many available approaches has been presented by Arunraj and Maiti (Arunraj and Maiti, 2009). Consequences estimation firstly includes source models, which allow assessing the loss of containment of hazardous substance (e.g., the release rate of hazardous material, the degree of flashing and the evaporation rate) and the related physical effects, such as fires, explosions and toxic dispersions (TNO, 2005b). Physical-mathematical models for the estimation of impacts, named damage models, can be applied to calculate the spatial distribution of damage, usually considered by QRA as probability of human death. For instance, a review of available models for damage estimation has been carried out by Cozzani and Salzano (Cozzani and Salzano, 2004a), which brought a significant contribution to the development of vulnerability models for storage tanks subjected to shockwaves.

The following step of QRA (4 – Establishment of the risk picture), named risk re-composition can be performed in order to estimate the risk, by summing the contribution of all scenarios to the risk in each specific position over space (CCPS - Center for Chemical Process Safety, 2000). The choice of risk metrics is critical as it directs what kind of information to obtain from the risk analysis and whether the results are considered legitimate and informative by decision-

makers and stakeholders (Johansen and Rausand, 2014). Further discussion on the choice of the risk metric is carried out later in this section.

On the basis of risk estimation results, risk is compared with acceptability criteria (5 – Risk evaluation), defined by both regulations and companies. Relevant examples of different acceptability criteria are the one developed by National Agencies (Pasman, 2011), as well as the Risk Matrix developed in the framework of European ARAMIS Project (Salvi and Debray, 2006). In case of unacceptable risk, adequate measures for its reduction are applied (Aven and Vinnem, 2005) throughout the life cycle of the plant. During the concept and engineering phase, risk reduction proposals should be focused on possible alternative process options, different layouts, equipment and location (NORSOK, 2010). During the operational phase, risk reduction proposals on operational nature and modification projects should be evaluated in order to demonstrate that the risk level during operations is the lowest, or provide a justification, if it is not (NORSOK, 2010). A summary of QRA steps from 1 to 5 is reported in Table 2. 2.

Table 2. 2 Quantitative risk assessment for Chemical Process Industries (CCPS - Center for Chemical Process Safety, 2000; NORSOK, 2010): description of the steps from 1 to 5.

Step	Description	
0	**Establishment of the context**	Definition of the context for the Risk Assessment; this implies defining the objectives, the scope, the responsibilities, the methods, models and tools to be used, the system boundaries and basis, the risk acceptance criteria, the deliveries throughout the process and the execution plan.
1	**Hazard Identification**	Definition of the potential event sequences and potential incidents. This may be based on qualitative hazard analysis for simple or screening level analysis. Complete or complex analysis is normally based on a full range of possible incidents for all sources.
2	**Frequency Estimation**	Estimation of the potential incident frequencies. Fault trees or generic databases may be used for the initial event sequences. Event trees may be used to account for mitigation and post release events.
3	**Consequence Estimation**	Evaluation of the potential incident outcomes (consequences). Some typical tools include vapour dispersion modelling and fire and explosion effect modelling. Then the estimation of incident impacts on people, environment and property is carried out.
4	**Establishment of the Risk Picture**	Estimation of the risk is done by combining the potential consequence for each event with the event frequency, and summing over all events.
5	**Risk Evaluation**	Identification of the major sources of risk and determination of cost-effective process or plant modifications, which can be implemented to reduce risk. Risk evaluation may be done against legally required risk criteria, internal corporate guidelines, comparison with other processes or more subjective criteria. If the risk is considered to be excessive, then identification and prioritization of potential risk reduction measures is required. After that, QRA should be performed iteratively, starting from step 2, up to the acceptability criteria is satisfied. If the risk is negligible, then emergency response and Land Use Planning should face residual risk.

Eventually, it must be underlined that QRA may be considered an iterative procedure that provide each time a risk picture of the process facility (CCPS - Center for Chemical Process Safety, 2000) and should be updated maximum every five years or in case of major plant changes, as stated by the Seveso directive (EU, 2012). Communications and consultation activities (6), as well as monitoring, review and update activities (7) should be performed throughout the process. (NORSOK, 2010)

Johansen and Rausand (Johansen and Rausand, 2012) provide an explanatory overview of 17 common risk metrics related to major accidents (Table 2. 3); most of the metrics express harm to humans, but environmental and material damage are also covered, even if not considered by actual standard. A specific evaluation of the choice of the risk metric should be discusses in this work, in order to introduce the applicability of QRA to different scopes.

In particular, the risk metrics addressing harm to humans (first 10 risk metrics in Table 2. 3) were analysed. A score from 1 to 5 was assigned for the following dimensions:

1. Tangible application (tangible – score 1) against hypothetical application (hypothetical – score 5) to the life cycle phases of a chemical process plant. For example, application of a risk metric to the phase of "Operation and maintenance" has relatively concrete implication and addresses known, consolidated and, somehow, routine activities (score 1). On the contrary, application of a risk metrics to the phase of "Feasibility" implies a prediction of the system behaviour, which is modelled on the basis of hypothesis (score 5). Between these two extremes, application to the other life cycle phases is ranked as it follows (from tangible to hypothetical): "Detailed Design and Engineering Installation" (score 2), "Decommissioning/ disposal" (score 3) and "Concept" (score 4). An average value is defined for risk metrics applied to more than one phase.
2. Risk metrics focusing on the harm of the single individual (individual – score 1) against risk metrics addressing the societal effect of an unwanted event (societal – score 5). Group risk metrics are in an intermediate position (score 3).
3. Specific risk metrics addressing only one life cycle phase (specific – score 1) against general risk metrics addressing all the five risk phases (general – score 5). Scoring for this dimension is straightforward and defines the level of specificity of the risk metrics.

Figure 2. 4 illustrates the results of this qualitative analysis by means of a radar chart. The three percentages reported on the diagram are calculated comparing the areas defined by the three contours and the total chart area.

Table 2. 3 Risk metrics. Characterization of risk metrics categories adapted from Johansen and Rausand (Johansen and Rausand, 2012).

Name	Type	Meaning	*Life cycle phase applicability*				
			Feasibility	Concept	Detailed Design & Engineering/ Installation	Operation/ Maintenance	Decommissioning/ disposal
IRPA - Individual Risk per annum	Loss of life; individual risk	The probability that a specific or hypothetical individual will be killed due to exposure to the hazards or activities during a period of one year. (NORSOK, 2010; Rausand, 2011)			√	√	
LIRA - Localized individual risk	Loss of life; individual risk	The probability that an average unprotected person, permanently present at a specified location, is killed during a period of one year due to a hazardous event at an installation. (Jonkman et al., 2003; Rausand, 2011)	√	√			√
IR$_{HSE}$ - Individual risk of dangerous dose	Indirect harm; individual risk	The frequency of receiving a dangerous dose of a toxic chemical, which leads to severe distress, injury or fatality, per 10^6 years. (HSE - Health and Safety Executive, 1992)			√	√	√
PLL - Potential loss of life	Loss of life; group risk	The expected number of fatalities within a specific population per year. (Jonkman et al., 2003; NORSOK, 2010)	√				
FAR - Fatal accident rate	Loss of life; group risk	The expected number of fatalities within a specific population per 100 million hours of exposure. (NORSOK, 2010; Rausand, 2011)		√	√	√	
FN - diagram	Loss of life; societal risk	Diagram displaying the relationship between severity (i.e. number of fatalities) and frequency of single accidents. (Ball and Floyd, 1998)		√		√	
RI$_{COMAH}$ - Weighted risk integral	Loss of life; societal risk	Expected number of fatalities corrected for risk aversion w.r.t. a high number of fatalities. (Hirst and Carter, 2002)	√	√			
SRI - Scaled risk integral	Loss of life; group risk	Group risk per area per year. (Ball and Floyd, 1998)		√			
TR - Total Risk	Loss of life; societal risk	Expected number of fatalities corrected for risk aversion w.r.t. extreme events. (Vrijling et al., 1995)	√				
PEF - Potential equivalent fatality	Loss of life; group risk	Expected harm per year from both fatalities and injuries, where injuries are expressed as fractions of a fatality. (EMS, 2001)				√	
PER - Potential environmental risk	Environmental damage	Frequency of a defined consequence category for a certain organism, population, habitat or ecosystem within an area. (OLF, 2007)	√		√	√	
√: yes; Blank: no							

Table 2. 3 (Continued) Risk metrics. Characterization of risk metrics categories adapted from Johansen and Rausand (Johansen and Rausand, 2012).

Name	Type	Meaning	*Life cycle phase applicability*				
			Feasibility	Concept	Detailed Design & Engineering/ Installation	Operation/ Maintenance	Decommissioning/ disposal
RT - Recovery time	Environmental damage	The probability per year of having an accident that exceeds the time needed by the ecosystem to recover from damage. (OLF, 2007)		√			√
FE - diagram	Environmental damage or economic loss; societal risk	Diagram displaying the relationship between the frequency and environmental/economic loss in a single accident. (Jorissen and Stallen, 1998)		√		√	
EL - Expected economic loss	Economic loss	Expected value of economic loss per year. (Jonkman et al., 2003)		√		√	
Frequency of intermediate events	Indirect loss	Frequency of hazardous or intermediate events in an accident scenario. (NORSOK, 2010; NUREG - US Nuclear Regulatory Commission, 2003)			√		
CED - Conditional expected damage	General loss; societal risk	Conditional expected value given that the consequence severity is above a specified level. (Haimes, 2004)		√			
MCR - Monetary collective risk	Combined loss; societal/group risk	Expected total loss in terms of monetary units per year, aggregated and weighted across different damage categories (e.g. fatalities, injuries, disruption of service). (Bohnenblust and Slovic, 1998)	√				
√*: yes;* ***Blank: no***							

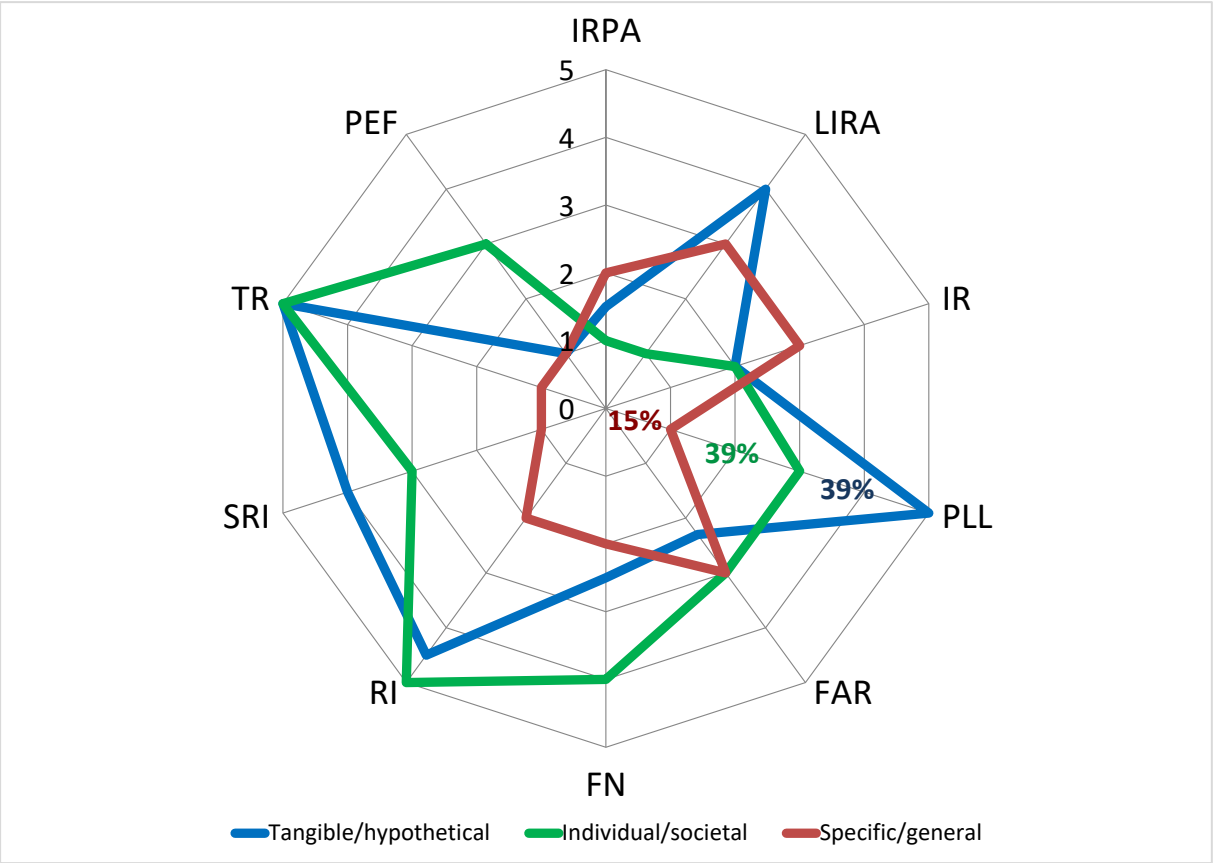


Figure 2. 4 Analysis of risk metrics expressing harm to humans.

The blue contour is defined by the tangible/hypothetical scoring of the risk metrics. Its area shows that the representative human harm risk metrics collected by Johansen and Rausand (Johansen and Rausand, 2012) tend to focus more on tangible/concrete life cycle phases of a chemical process plant (as previously defined): resulting area of 39%, where 0% represents tangible/concrete life cycle phases and 100% represents hypothetical modelling phases. This underlines the fact that there is big care also in terms of safety of the phases of "operation and maintenance" and "detailed design and engineering installation", which represent the core of the plant life cycle and are key phases in terms of productivity. However, these phases are subject to regular tests and inspections and they are supported by operational experience. Other phases that are performed only once in the life cycle of a plant and have little chance to be corrected ("Feasibility", "Concept" and "Decommissioning / disposal") might hide latent risks.

The green contour is defined by the individual/societal scoring of the risk metrics. Its area shows that the risk metrics considered tend to focus more on the individual: resulting area of 39%, where 0% represents individual risk and 100% represents societal risk. A good overlapping between the green and the blue areas shows that individual risk metrics tend to be preferred for tangible/concrete plant life cycle phases, such as "operation and maintenance"

and "detailed design and engineering installation", while group and societal risk metrics tend to be used for more hypothetical phases, such as "Feasibility" and "Concept".

The red contour is defined by the specific/general scoring of the risk metrics. Its area shows a pronounced specificity of these metrics: resulting area of 15%, where 0% represents specific metrics and 100% represents general metrics. Thus, in most of the cases, the risk metrics are defined for few life cycle phases of a chemical process plant and cannot be effectively used to describe the other phases. In the following section, more details on the applicability of QRA to these life cycle phases are discussed.

2.3.2 Application of QRA in the chemical process industry

At the beginning of its history, QRA was used primarily as a verification activity (Falck et al., 2000), while now it plays a relevant role in different aspects of process plant life cycle, as shown in the previous section. An important application of QRA is risk-based design; as pointed out by Fadier and De la Garza (Fadier and De la Garza, 2006) and Hale et al. (Hale et al., 2007), risk-based or risk-informed design plays a relevant role in risk-reduction for chemical and process installations. A valid quantitative approach to a risk-based engineering design involves acquiring and incorporating all of the possible knowledge on the design into the decision process (Demichela and Piccinini, 2004). Important QRA results are obtained at the earliest possible stage of the design process (Hendershot, 2006), such as the feasibility and the concept phases or at least as soon as the cost of plant and potential accidents can be estimated. As previously shown, specific risk metrics are applied in these phases and, with the exception of the LIRA risk metric, a particular attention is given to group and societal risk (Table 2. 3). In this framework Medina et al. have developed and applied a relevant optimization procedure, which can be applied to reduce the risk of a given plant or unit by finding an "optimum" design (Medina et al., 2009).

However, as Shariff and Zaini point out, QRA has been often applied in the detailed design and engineering installation because, at preliminary design stage, process designers normally lack of information on the risk level from process plant (Shariff and Zaini, 2013). Generally, QRA is carried out when the main equipment layout has been completed. For instance, safety system modelling is nowadays an integral part of risk assessment studies and represents a significant application of QRA. In this regard, safety systems aiming to avoid, prevent, limit or control accidents are evaluated to examine the extent to which they are effective in reducing the risk of the accident to an acceptable level. An important contribution was given by SCAP methodology (Khan et al., 2002a, 2002b, 2001), a quantitative methodology for design of safety measures based on a feedback system of fault tree and credible accident. Cozzani et al. (Cozzani et al., 2009) and Khan and Abunada (Khan and Abunada, 2010) proposed a new

methodology: a risk-based approach to measure process safety using a set of safety performance indicators.

Another relevant application of QRA is a risk-based approach to operations and maintenance, which at present time is widely recognized, after many researchers and industries have addressed this issue (Apeland and Aven, 2000; Hale et al., 1998; Vaurio, 1995). Risk-based maintenance is designed to study all the failure modes, determining the risk associated with those failure modes, and developing a maintenance strategy that minimizes the occurrence of the high-risk failure modes (Arunraj and Maiti, 2007; Okoh and Hauge, 2013). Risk-based maintenance and inspection strategies have been developed to provide a basis for not only taking the reliability of a system into consideration when making decisions regarding the type and the time for maintenance actions, but also to be able to take into consideration the risk that would result as a consequence of an unexpected failure (Khan and Haddara, 2004).

During decommissioning and disposal phases, risk assessment should be aimed at evaluating the risk to the health and safety of the personnel directly involved in the decommissioning and disposal operations and to the environment, taking into account geographical and social specificities (ISO, 2002).

However, the application of QRA is not only confined in the mentioned phases of a plant life cycle. It is applied to entire industrial areas (Egidi et al., 1995) and several subsequent developments with Land Use Planning purposes (Spadoni et al., 2003, 2000).

Moreover, in the last years, much attention has been posed on the possible extension of QRA to external hazard factors (Antonioni et al., 2009; Cozzani, 2010; Cozzani et al., 2006), as domino, security and natural hazards. A comprehensive approach was obtained to allow the inclusion of natural hazards (NaTech), such as flooding (Cozzani et al., 2010) and lightning (Necci et al., 2014), and extending its potentialities to the quantitative assessment of the contribution to industrial risk due to such scenarios. A summary of the mentioned approaches can be found in Cozzani et al. (Cozzani et al., 2014) demonstrates that the topic has almost filled its research gaps. Indeed, as stressed by several authors, the integration of QRA with domino accidents, still needs improvements in terms of methodologies to be applied and insertion of risk reducing measures in the analysis (Janssens et al., 2015; Khakzad, 2015; Khakzad et al., 2013d). Moreover, the necessity to include in QRAs security hazards, such as possible terrorist attacks and sabotages, in order to define an exhaustive risk-picture that represents in a detailed and realistic way the real situation is pointed out by several authors (Reniers, 2010; Reniers and Audenaert, 2014; Srivastava and Gupta, 2010). A detailed overview on the existing methodologies and applications for the inclusion of external hazard factors in QRA, with particular reference to domino and security hazards, is available in Section 3.

2.3.3 Accomplishments and criticisms of QRA

Greenberg et al. (Greenberg et al., 2012) describe some of the last accomplishments that generic risk analysis has had in the last years addressing health, safety, and the environment. A list of accomplishments can be also identified for QRA along the same lines of what identified by Greenberg et al. (Greenberg et al., 2012).

1. Risk perception and behaviour are increasingly affected by analytical evaluation. Risk managers may be perceived more competent by means of QRA, which leads to less concern and more benefits perceived by the public and greater acceptance of a hazard (Frewer et al., 1996; Peters et al., 1997; Siegrist, 2000; Siegrist and Cvetkovich, 2000; Slovic, 2000, 1993).
2. QRA has laid the foundation for estimating the economic impact of hazard events. Several examples show that such impact should not be disregarded and represent an important element for critical decision-making (Kyaw and Paltrinieri, 2015; Paltrinieri et al., 2014c).
3. By means of QRA, risk communication is providing reliable and useful information to all interested parties, including scientists and managers "who too often think that they already know whatever they need to know" (National Research Council, 1989).
4. Legal decisions may be now supported by the application of QRA for a more risk-informed outcome, as demonstrated by the outcome of the trials assessing the responsibilities of the explosion occurred in the Buncefield oil depot in 2005 (HSE - Health and Safety Executive, 2011).

On the other hand, there are frequent criticisms associated to QRA paving the way to follow for further improvements.

1. Creedy (Creedy, 2011) addresses the estimation of the frequencies included in the QRA by stating that “it still appears to be largely based on values from several decades ago”. He affirms that the decision-making process and management system for risk control is a field where much has been learned in the last two decades, but it is not clear how much this learning is taken into account when estimating frequencies. There is need for both realistic values of failure probability and event frequency better describing the actual conditions of the system.
2. Classical risk analysis approach is static. It decomposes a system and focuses on failure events of components. This approach is not sufficient to explain all what can go wrong, because it does not grasp the dynamics of unsafe interactions and fails to capture the variation of risks as deviations or changes in the process and plant (Kalantarnia et al., 2009; Pasman and Reniers, 2014). QRA produces a risk picture in a frozen moment of

the plant life cycle that may turn to be a partial and temporary description of the overall safety problem. For instance, analysts may tend to initially focus on changes around a reference point, such as reference value of risk assessed through a QRA, and relatively disregard extreme situations. This is explained by Greenberg et al. (Greenberg et al., 2012) with the prospect theory and may lead to the choice of an incomplete risk strategy, as introduced in Section 2.2. Moreover, as Falck et al. affirms (Falck et al., 2015), risk assessment performed for a specific life cycle phase of a plant is not always suitable for the other phases and needs to be updated. This is also demonstrated by the presence of risk metrics that are specific for some life cycle phases of the plant and not for others (Section 2.3.1). These criticisms highlight the need of a dynamic approach that can be adapted through the lifespan of a plant.

3. Apostolakis (Apostolakis, 2004) claims that probability cannot be realistically calculated, meaning that one cannot use straightforward statistical methods and divide the number of failures by the number of trials to calculate "realistic" probabilities. QRA analysts make an extensive use of expert judgment and should always look at the uncertainties associated with the results. For this reason, a project such as PDS (Reliability Prediction Method for Safety Instrumented Systems) (Hauge et al., 2013), run by SINTEF to provide an evaluation method for reliability analysis, aims to account for the major reliability influencing factors through consultation with oil companies, engineering companies, consultants, vendors and researchers.

4. Hauge et al. mentions the attempts "made to keep the PDS method and associated formulas as simple and intuitive as possible without losing accuracy" (Hauge et al., 2013). In fact, decision-makers and/or their staff may need some background in these methods in order to understand that options are clarified and not obfuscated, and someone may distrust the method because assuming that values are buried in the numbers and that these drive the decisions (Greenberg et al., 2012). The estimation of likelihood is typically treated in a cursory way and sometimes even with apparent reluctance, as if examining more deeply could call into question the validity of (or faith in) the risk assessment process (Creedy, 2011). A specific mind-set based on the trust of this quantitative method should be built by involving decision-makers in the creation and refinement of the associated tools.

5. Further methodologies to support the risk evaluation step needs to be developed, in purpose to account the economic and technical performances of risk reducing measures in the prevention, control and mitigation of major accidents triggered by external hazard factors (i.e., domino and security events) (Landucci et al., 2015a; Reniers, 2010; Villa et al., 2016).

The accomplishments show the maturity of QRA and its systematic steps – described in Section 2.3.1. QRA solidity is demonstrated by the wide application to the life cycle phases of chemical process industry – Section 2.3.2. However, despite its diffusion, the risk metrics produced by a QRA study may reveal overall rigidity, because they are suitable for only few life cycle phases of the system – as highlighted in Section 2.3.1. Rigidity is also proved by the tendency of basing QRA on outdated frequencies data and little capability of progressive improvement and update – as previously mentioned. Moreover, the necessity to further refine the extension of quantitative risk assessment to the analysis of external hazard factors was underlined. Such drawbacks pave the way to follow for further improvements.

2.4 WAY FORWARD IN RISK ASSESSMENT: DYNAMIC RISK ASSESSMENT APPROACHES

QRA drawback of intrinsic stativity precludes any possible update and integration of the overall risk figures, due to the actual real world ever-changing environment or later improvements based on new risk notions. To overcome this limit, during the last decade several efforts have been devoted to the development of novel approaches to risk assessment and management, which can consider the dynamic evolution of conditions, both internal and external to the system, affecting risk assessment (Paltrinieri and Scarponi, 2014). Herein it is reported a brief description of the most relevant methodologies and applications of dynamic approaches to risk analysis in the chemical process industry, underlining their relevant features. This specific way forward in risk assessment (Figure 2. 5), and in general, the growing interest toward the topic has been derived by:

- Over 250 references on Scopus database with inputs “dynamic risk assessment” and “process industry” in the decade 2006-2016, proving the interest of academic researchers toward this topic;
- Recent application of these techniques within consulting studies and industries (e.g., in the framework of Center for Integrated Operations in the Petroleum Industry (Norway)).

The inclusion of external hazard factors and the application of economic techniques within risk assessment for the chemical and process industry is addressed in Section 3.

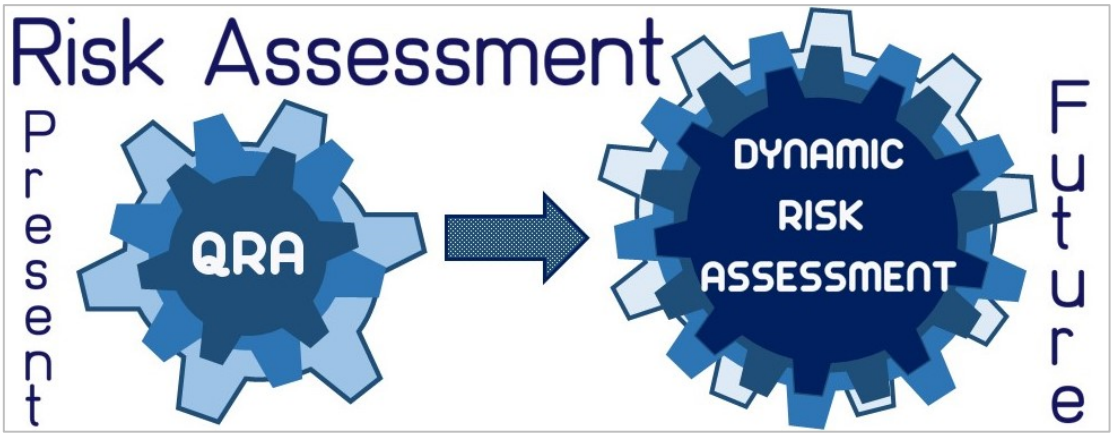


Figure 2. 5 Dynamic Risk Assessment as possible way forward for the chemical and process industry domain.

2.4.1 Dynamic Risk Assessment Methodology (DRA) with Bayesian Analysis

Some of the first attempts to simulate the dynamic nature of system behaviour were made by Swaminathan and Smidts, who proposed a methodology to extend the application of event sequence diagram (ESDs) to the modelling of dynamic situations and identification of missing accidental scenarios (Swaminathan and Smidts, 1999a, 1999b). Also, Čepin and Mavko developed an extension of the well-established fault tree to represent time requirements in safety systems (Čepin and Mavko, 2002) and similarly Bucci et al. (Bucci et al., 2008) presented a methodology to extend fault trees and event trees in a dynamic perspective. On the other hand, the attempt to deal with an ever-changing environment led to the definition and application of a new graphic formalism, named discrete-time Bayesian Network (Boudali and Dugan, 2005), which represented random variables and their dependencies by means of nodes and directed arcs. The above-mentioned methodologies, even if not completely exhaustive by themselves, may be considered as an important starting point for a comprehensive risk-updating approach.

The first complete Dynamic Risk Assessment methodology for process facilities, termed as Dynamic Failure Assessment, was developed by Meel, Seider et al. (Meel et al., 2007; Meel and Seider, 2008, 2006). This approach aims at estimating the dynamic probabilities of accident sequences, including near misses and incident data (named as Accident Sequence Precursors – ASP) as well as real-time data from processes. This method was applied to several case studies, such as CSTR reactor safety systems (Meel and Seider, 2006), Ethyl Benzene process (Meel and Seider, 2008), and alarm systems for process equipment (Pariyani et al., 2012a, 2012b).

Dynamic Risk Assessment (DRA) was further developed by Kalantarnia et al. (Abimbola et al., 2014; Kalantarnia et al., 2010, 2009; Khakzad et al., 2013a): this approach integrates Bayesian

failure mechanisms with consequence assessment. The novelty of this approach stands in the presence of two additional steps if compared with conventional risk assessment (Table 2. 4). These steps represent the key to dynamic risk assessment: accident analysis and probability updating. Accident analysis step uses the event/ fault tree along with real time process data to estimate events' probabilities. Then these probabilities can be updated using all available information and new data in the form of likelihood function, by means of Bayesian inference. Subsequently updated probabilities are applied in the re-estimation of the risk profile for a process facility following an iterative procedure, which mirrors real-time changes in the system. The Dynamic Risk Assessment process may be implemented to a selected system in five steps (Kalantarnia et al., 2010, 2009), as reported in Table 2. 4.

As a valuable alternative in revising prior failure probabilities, also a non-Bayesian updating approach, in which new data are supplied by real time monitoring of parameters, inspection of process equipment and use of physical reliability models, was proposed (Ferdous et al., 2013; Khakzad et al., 2012). Despite the slight difference in the updating process, all the other features are similar to the DRA approach above reported.

DRA was applied to a real-case represented by the BP Texas Refinery accident (Kalantarnia et al., 2010) and offshore drilling operations (Abimbola et al., 2014). The integration with established Bow-Tie technique proved to be an effective solution, as revealed by the application to a sugar refinery explosion (Khakzad et al., 2012). Starting from the foundational contribution by Kalantarnia et al. (Kalantarnia et al., 2010, 2009), several methodologies have tried to enlarge the field of application for Dynamic Risk Assessment, by introducing slight modifications. For instance, Hierarchical Bayesian Analysis (HBA) widened the field of application for DRA also to rare event, due to a two-stage Bayesian method. The feasibility of this approach was witnessed by the application to BP Deepwater Horizon accident (Yang et al., 2013) and to offshore blowouts (Khakzad et al., 2014). System hazard identification, prediction and prevention methodology (SHIPP) is another relevant approach derived from DRA and referred specifically to accident modelling, that has been developed by Rathnayaka et al. (Rathnayaka et al., 2011) and proved, in the application to a LNG facility (Rathnayaka et al., 2012), to be able to integrate technical and non-technical barriers. Another mentionable contribution, derived from DRA procedure, is Dynamic Operational Risk Assessment (DORA) methodology (Yang and Mannan, 2010a, 2010b) that included conceptual framework design, mathematical modelling and decision-making based on cost–benefit analysis.

Dynamic Risk Assessment methodology has demonstrated to be an exhaustive and versatile approach for chemical process systems, as witnessed by several recent applications. The mathematics that lies behind Dynamic Risk Assessment is explained in detail, in its application to safety barriers performance evaulation, in Section 3.4.2.2.

Table 2. 4 DRA – Dynamic Risk Assessment (Kalantarnia et al., 2009). Description of the steps.

Step	Description	
0	**Collect ASP**	Monitoring and reporting of process accidents, incidents and near misses. These data have been called Accident Sequence Precursors (*ASP*).
1	**Scenario identification**	The potential scenarios, their causes, consequences and related safety barriers are identified by means of a bow-tie analysis. A bow-tie analysis is performed at this step to provide a visual representation of consequences, causes and related safety barriers in place to mitigate or control the hazards. The "knot" of the bow-tie diagram is generally an event of loss of containment, often indicated as "critical event" *(CE)*. Consequences in left-hand part of the diagram and causes in the right-hand part of the diagram have been respectively indicated as "initiating events" *(IEs)* and "outcome events" *(OEs)*
2	**Prior function calculation**	The prior failure function of each barrier represents our understanding of it prior to the start of operation. A probability density function of type Beta can be selected to represent the failure probability of a system (Vose and Rowe, 2000) such as a safety barrier. If a bow-tie diagram approach to the calculation of prior *OE* frequencies is used, the mean value of the Beta distribution of barrier failure probability can be obtained and used as a discrete value. In fact, if the *CE* frequency (obtained by gate-by-gate fault tree calculation (Delvosalle et al., 2005)) is multiplied by the conditional probability values encountered on the branch connecting the *CE* to an *OE*, that particular *OE* frequency is obtained, as shown in the following equation: $Freq(OE) = Freq(CE) \cdot Prob(OE) \cdot Prob(SBOE)$ where *Freq(CE)* is the frequency of the *CE*, *Prob(OE)* represents the probabilities of transmission from the *CE* to the considered *OE* (e.g. probability of immediate or delayed ignition and probability of a *VCE*) and *Prob(SBOE)* the failure probability function mean values of the safety barriers encountered on the branch between the *CE* and the considered *OE*.
3	**Formation of the likelihood function**	This function is formed using real time data from the process as it operates. These data are inferred from the ASPs and are specific numbers within a discrete domain, which is best presented by a binomial distribution. Many approaches exist for selecting likelihood functions. The most convenient in the present framework is to use the conjugate pair of the prior function (Kalantarnia et al., 2010). Beta and binomial distributions are conjugate pairs and so binomial distribution is used to represent the likelihood function.
4	**Posterior function calculation**	The posterior failure function of the safety barriers has been obtained from the prior and likelihood functions using Bayesian inference. Bayesian inference is a tool, which uses data to improve an estimate of a parameter. The posterior function is the same distribution type as the prior (Beta), but the parameters are updated trough the likelihood function. Thus, the posterior function can be derived as follows: $f(x|Data) \propto g(Data|x) \cdot f(x)$ Where x is the failure probability of the barrier, $f(x)$ is the probability distribution function (prior distribution), $f(x|Data)$ is the posterior distribution and $g(Data|x)$ is the likelihood function. Posterior frequencies of the *OEs* may be obtained using the bow-tie diagram approach described previously.
5	**Consequence Analysis**	Consequence analysis is carried out on the scenario in order to estimate the potential consequences of all possible *OEs*. Consequence assessment is a straightforward approach as the consequence of an event is often constant throughout the lifetime of the process. Generally, consequences of an event in process facilities are: asset loss, human fatality, environmental loss, and confidence or reputation loss.

2.4.2 Coupling of DRA and DyPASI

The use of conventional hazard identification techniques may present some limitations related to completeness, reproducibility, inscrutability, relevance of experience and subjectivity (CCPS - Center for Chemical Process Safety, 2008a). To overcome this limit, DRA was coupled with a dynamic hazard identification technique named DyPASI (Dynamic Procedure for atypical scenario identification) (Paltrinieri et al., 2014b, 2014c, 2013a, 2013b). The DyPASI procedure allows the HAZID process to define and take into account atypical accident scenarios, which by definition are deviating from normal expectations of unwanted events or the worst-case reference scenarios. As a preliminary activity, DyPASI requires the application of a conventional bow-tie technique, followed by the retrieval from databases and search-systems of relevant information concerning undetected potential hazards and accident scenarios that may not have been previously considered (Paltrinieri et al., 2013a, 2013b). A brief description of DyPASI steps has been reported in Table 2. 5.

Table 2. 5 DyPASI (Paltrinieri et al., 2013b). Description of the steps (Paltrinieri et al., 2014c).

Step	Description	
0	**Identification of relevant accident scenarios by means of Bow-Tie analysis**	Preliminary activity in which the application of a conventional bow-tie technique is required for the identification of relevant accident scenarios and relative safety barriers. This technique provides a visual representation of the causes of unintended events, likely outcomes and the measures in place to mitigate or control the hazards. It is centred on a critical event, i.e. a loss of containment. The left part of the bow-tie, named fault tree, identifies the possible causes. The right part of the Bow-Tie, named Event-Tree, identifies the possible consequences. This step should be ignored in case of update of previous bow-tie analysis.
1	**Search for risk notions on undetected hazards**	Search for relevant information on undetected potential hazards and accident scenarios not considered by conventional bow-tie development. Information retrieval techniques are used to reduce potential information overload.
2	**Assessment of risk notion relevance**	Assessment of information to determine whether it is significant enough for further action. A register of risk notions to show relevance and impact is used as support.
3	**Scenario isolation from early warnings**	Isolation of potential scenarios from early warnings and development of cause-consequence chain to integrate into the bow-tie diagram.
4	**Definition of safety measures**	Definition of safety measures for the newly introduced scenarios. Safety barriers and related generic safety functions describe the safety measures.

DyPASI was applied to both systems where atypical scenarios occurred in the past, such as the Buncefield oil depot and the Toulouse fertilizer plant (N. Paltrinieri et al., 2012), and to emerging technologies, whose relative lack of experience may lead to atypical scenarios, such as a Carbon Capture and Sequestration plant (Paltrinieri et al., 2014d) and LNG (Liquefied Natural Gas) regasification units (Paltrinieri et al., 2015b, 2011).

The DyPASI technique, whose nature is iterative, should not be considered "stand-alone". In this case it was coupled with DRA (Paltrinieri et al., 2014c), as illustrated in Figure 2. 6. The results obtained by preliminary applications to systems where actual accidents occurred (BP Texas City Refinery (Paltrinieri et al., 2014c) and Hoeganaes Metal Dust accident (Paltrinieri et al., 2014b)) showed that the related scenarios could be identified and potentially prevented. Moreover, the application of DyPASI technique showed a strong complementarity with DRA, which is heavily dependent from the hazard identification and early warning collection systems (Paltrinieri et al., 2014c). Therefore, the coupling of two advanced methodologies established a more exhaustive dynamic risk assessment approach (Paltrinieri et al., 2014b, 2014c), as visible from Table 2. 6.

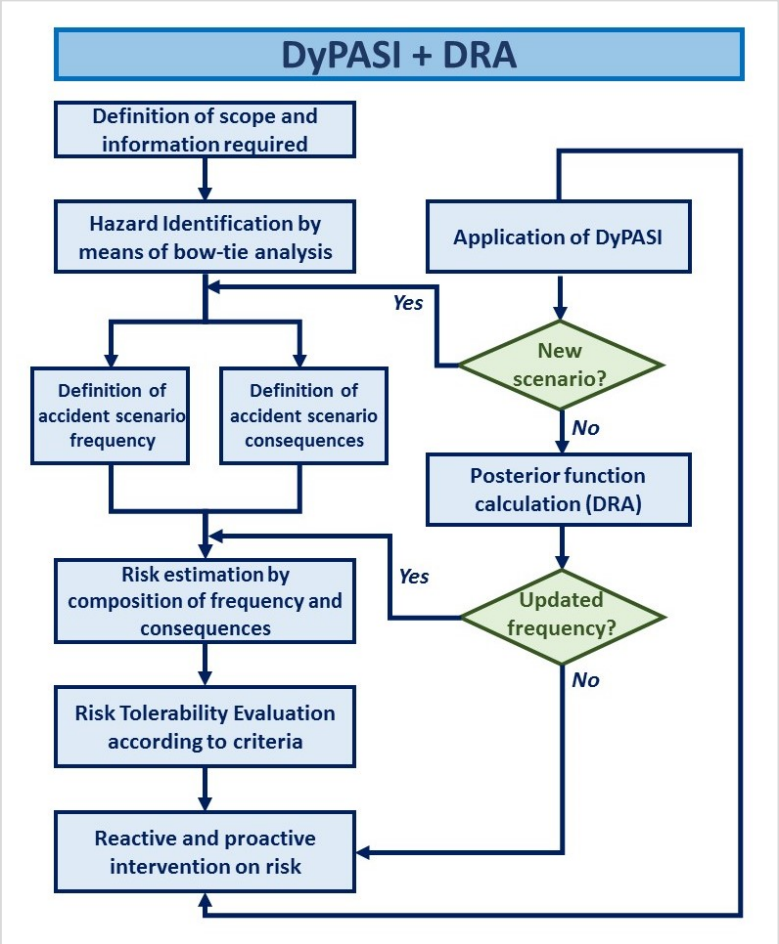


Figure 2. 6 DRA and DyPASI integrated methodology flowchart. Figure adapted from Paltrinieri et al. (Paltrinieri et al., 2014c).

Table 2. 6 Coupling of two Advanced Dynamic techniques: DRA and DyPASI. Description of the steps, adapted from Paltrinieri et al. (Paltrinieri et al., 2014c).

Step	Description	
1	**Definition of scope and information required**	The framework and the limits of the study are defined. This involves defining the scope of the risk analysis and the information that is required from it.
2	**Hazard identification by means of bow-tie analysis**	Basic hazards are identified. In this step, the HAZID methodology applied for the representation of the basic and well-recognized process hazards is the bow-tie analysis.
3	**Definition of accident scenario frequency**	Accident scenario frequency is identified. The frequency of the identified scenarios is calculated.
4	**Definition of accident scenario consequences**	Accident scenario consequences are identified. The physical extent and severity of the identified scenarios are calculated.
5	**Risk estimation by composition of frequency and consequence**	Risk is estimated. Risk is estimated by the composition of probability and consequence for the scenarios identified, as recommended by (Kaplan and Garrick, 1981).
6	**Risk tolerability evaluation according to criteria**	Risk tolerability is evaluated according to risk criteria. In case risk exceeds certain limits, appropriate actions are to be taken in the next step.
7	**Reactive and proactive intervention on risk**	Reactive and proactive intervention on risk is taken. This step is the response to the results previously obtained and, at the same time, the starting point of a new reiteration of the analysis. In fact, decision-making should address not only reactive actions in response to the calculated risk, but also proactive interventions for a more comprehensive risk assessment. In general, robustness in decision-making is of particular relevance. In a dynamic system this principle earns more importance because it is asked to cope with variations in its operating environment without alteration or loss of functionality.
8	**Application of DyPASI**	DyPASI is applied. DyPASI is used in the reiteration of the analysis in order to identify and integrate basic process hazards with new or atypical scenarios when evidence of them is demonstrated by early warnings. The latter are identified by a systematic screening process of related risk notions. Every time DyPASI identifies a new scenario, the consequence and the frequency analysis must be reiterated in order to assess its risk.
9	**Posterior function calculation (DRA)**	Posterior Probability (DRA) is calculated. By means of the DRA technique (only steps 3 and 4 should be applied) the probability of the events identified by the HAZID process is updated. The information for this step (ASPs) is provided by the screening process of related risk notions per- formed in the previous step. This reiteration represents also a way to monitor system performance.

2.4.3 Dynamic Risk Assessment with Bayesian Networks

Bayesian Networks (BNs) are a graphical representation of uncertain quantities and decisions that explicitly reveal the probabilistic dependence between the variables and the related information flow. BNs are directed acyclic graphs for reasoning under uncertainty in which random variables and their dependencies are represented by means of nodes and directed arcs. A distinct advantage of using BNs is that they provide a useful tool to deal with uncertainty and with information from different sources, such as expert judgment, observable information or experience, as well as common causes and influences of human factors (Ale et al., 2014). The mathematics that lies behind Bayesian Networks and the tools offered by a specific software for BNs application are presented in Section 3 (Section 3.4.2.2).

However, despite about 200 publications regarding Bayesian Networks are available with reference to dependability, maintenance and risk analysis areas, only 26% of them deals with risk analysis topics and few ones are related to the chemical industry domain (Weber et al., 2012).

For instance Khakzad et al. (Khakzad et al., 2013b, 2011) made clear how to map conventional techniques, as fault-tree and Bow-tie diagrams into BNs. They also discussed the enhanced flexibility of BN structure in comparison with the bow-tie diagram; the crucial point is that each conventional diagram can be mapped to its corresponding BN, while a BN is not necessarily equivalent to a Bow-Tie (or a Fault-Tree), due to multi-state variables. The mapping procedures are presented in detail in Section 3.4.2.2. As a starting point some hybrid-models were developed and successfully tested, for example in the framework of the operational safety program for offshore companies in Norwegian Sea, called Risk OMT (risk modelling - integration of organizational, human and technical factors) (Røed et al., 2009; Vinnem et al., 2012).

In the dynamic risk assessment framework, Bayesian Networks are nowadays considered to represent a promising tool, suitable to cope with complex and uncertain situations, with a graphical and easy-to-update model, which has recently gained increasing popularity in the process industry (Ale et al., 2014; Khakzad et al., 2013d; Pasman and Rogers, 2013). The potentiality of BNs approach to Dynamic Risk Assessment has been proved by several applications: Pasman and Rogers (Pasman and Rogers, 2012) applied BNs for the evaluation of process design alternatives, Khakzad et al. (Khakzad et al., 2013c) showed the role of BNs in Risk-based Design applications. The effectiveness of this approach in operational safety was demonstrated with regards to the prevention of major accidental scenarios, as off-shore blowouts (Khakzad et al., 2014, 2013a) and dust explosions (Yuan et al., 2015). Recent applications are aimed at extending the applicability of Bayesian Networks both to risk

management issues (Ale et al., 2014) and to cascading events, with particular reference to domino accident modelling (Khakzad, 2015; Khakzad et al., 2013d).

2.4.4 Risk Barometer

The Center for Integrated Operations in the Petroleum Industry has recently developed the "Risk Barometer" technique (Hauge et al., 2015; Paltrinieri et al., 2015a, 2014a; Paltrinieri and Hokstad, 2015), aiming to continuously monitor risk picture changes and support decision makers in daily operations. This proactive approach to risk is based on the contribution by Øien (Øien, 2001a) on the definition of risk indicators describing Risk Influencing Factors (RIFs), which are aspects of a system or of an activity that affect its risk level (Øien, 2001b).

The risk barometer needs to be performed on an existing QRA, in order to conduct sensitivity analysis and select the RIFs that are mostly affecting the risk picture. Indicators that assess the state of RIFs and may be evaluated on a real-time basis are then introduced. The aggregation of indicators and RIFs by means of a weighted sums approach allows the assessment of the overall risk variation. An example of Risk Barometer is available in Figure 2. 7.

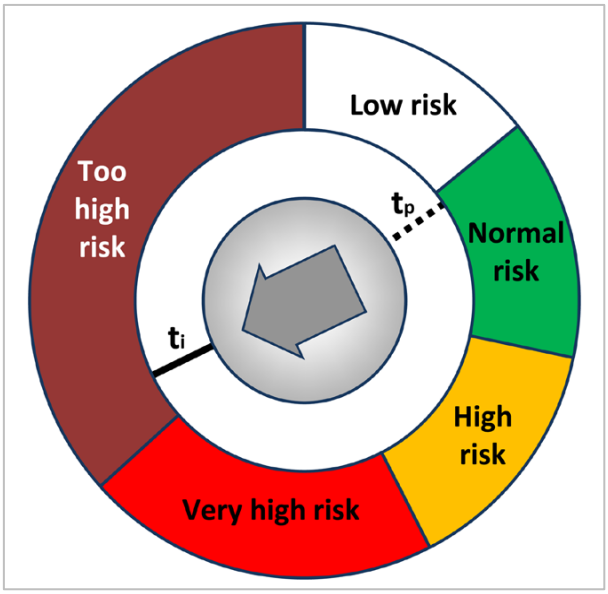


Figure 2. 7 Risk Barometer. It visualizes the average risk level measured in the last period (t_p - indicated by a dotted line) and the instantaneous risk level (t_i - indicated by a solid line and the arrow). Figure adapted from Paltrinieri et al. (Paltrinieri et al., 2014a)

This approach, whose description of steps is reported in Figure 2. 8, is based on the availability of a large amount of real-time data, whose collection is made easier by the extensive use of Information and Communication Technologies. Real-time Risk assessment can provide a basis for dynamic adjustments of inspection and maintenance plans or implementation of risk reducing measures while maintaining production (Paltrinieri et al., 2014a).

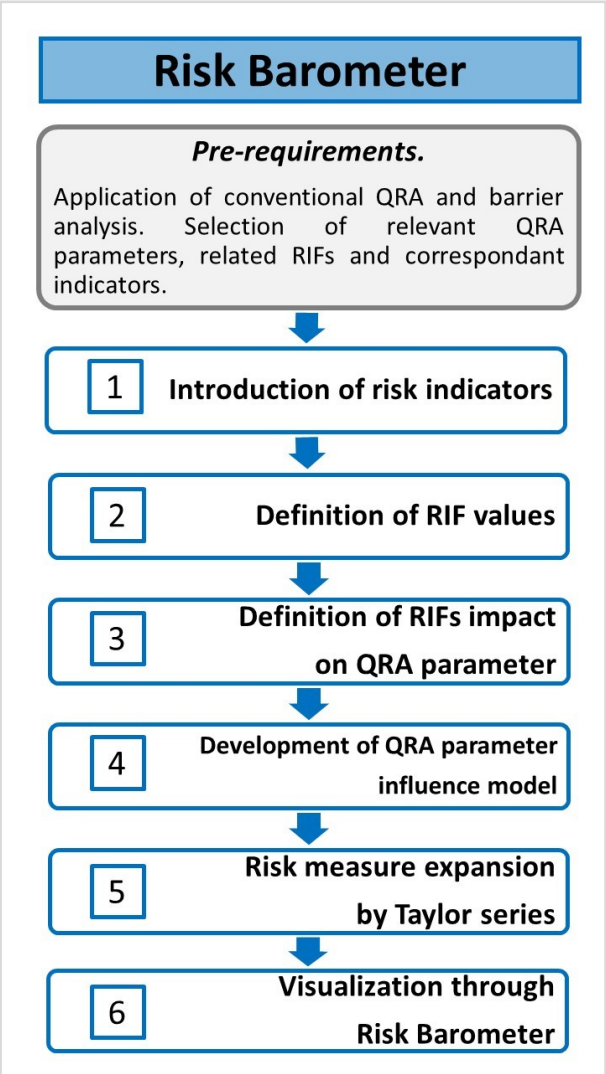


Figure 2. 8 Risk Barometer: methodology flowchart (Okstad et al., 2013).

The Risk Barometer was tested on a series of different case-studies from the Oil & Gas sector (Hauge et al., 2015):

- Process leak on an oil production platform.
- Impact between a platform and a visiting vessel.
- Loss of containment due to sand erosion/corrosion in a Floating Production Storage and Offloading unit.
- Well leak and blowout

One of the advantages of the Risk Barometer in comparison with other dynamic techniques is the fact that the model is built in collaboration with the potential users, decision-makers and key organization personnel. The application on the case-studies listed was conducted through a series of workshops in order to involve the operators and build trust in the quantitative evaluation tool (Hauge et al., 2015). A "drill-down" capability was also implemented to allow

the user to keep a track of each element of the model, for instance by checking the trend of the single indicators. The philosophy of the "transparent box" (opposite of "black box") was followed. The user should not only be able to see inputs and outputs, but also the processes occurring in the box and how the indicators (inputs) turn into overall risk variation (output).

2.5 DISCUSSION

2.5.1 Advantages and limitations of Dynamic Risk Assessment approaches

Dynamic risk assessment aims to take into account new risks notions and early warnings, and to systematically update the related risks, ensuring enhanced flexibility. This may answer the need for more realistic values of failure probability and event frequency. Generic values may be then refined by the continuous improvement of dynamic assessment (DRA and DRA with Bayesian Networks). Morover, the application of dynamic techniques (as DRA and DRA with Bayesian Networks) will allow accounting in a more detailed and effective manner risk reducing measures performance, therefore avoiding overestimation of the risk picture; this topic is developed in Section 3.4.2.2 by a description of specific methodologies.

Integration of partial initial risk assessment would be also possible if a dynamic approach ranging from hazard identification to risk evaluation is employed (coupling of DRA and DyPASI). Through the use of techniques such as DRA and the Risk Barometer, analysts may relatively increase their awareness of uncertainties associated with the results. Expert judgment may be constructively used for the creation and refinement of dynamic tools of risk assessment in order to oppose the possible scepticism such techniques may lead to (e.g., Risk Barometer). Ultimately, techniques such as the Risk Barometer would represent a support for critical decision and allow risk-informed decision-making, i.e. results obtained from Risk Assessment process would be weighted with other attributes during the decision process. The applicability of these methods within the chemical and process industry domain is enforced by many recent applications, described in Section 2. 4 and summarized in Table 2. 7.

Dynamic risk assessment may be applied not only in the design stage of a process, but also throughout its lifetime, allowing safer operations and easier maintenance, as well as supporting a more precise, risk-informed and robust decision-making process (Khakzad et al., 2014).

As reported in Table 2. 8, Dynamic Approaches may show advantages in design and operation on processing facilities, while the main limitations are shared between design and operation phases. Dynamic methods may improve design and comparison between different alternatives of safety systems, by integrating standard processes of hazard identification with notions on

emerging risks or external experience on relevant events. Accounting for human and organizational factors since the beginning of the design process would also allow for proactive prevention of potential underlying issues. The operation phase of a plant would be the main phase to benefit from dynamic risk assessment. In fact, frequent reiteration of risk assessment may allow continuous evaluation of safety measures, refinement of their management and enhanced management of safety-critical operations and improved maintenance planning. Moreover, constant monitoring of human and organizational factors would allow for feedback on the organization safety culture and support training sessions focusing on key organizational issues.

In particular, next challenges will be devoted to solving the issues of formalization, standardization and creation of completely automated software able to perform Dynamic Risk Assessment. Eventually, despite several steps forward have been made from the pioneering studies, every dynamic approach showed to be effective only if associated with a proper safety culture, which continuously search for learning opportunities by monitoring and recording process performance and incidents (Paltrinieri et al., 2014b). Moreover, research on Risk Assessment may be further developed in order to futher include by means of innovative methods/tools cascading events (e.g. domino events) and management issues.

Table 2. 7 Dynamic Risk Assessment applications in the Chemical and Process industry domain.

Name	***Main tasks***	***Applicative contributions – Main Topics***					***Theoretical/ Methodologic Contributions***
		Accident/ Consequence Modelling	***Design***	***Safety***	***Asset integrity***	***Other***	
Dynamic Risk Assessment (DRA)	• First applications termed as Dynamic Failure Assessment • Two more steps in comparison with conventional QRA: accident analysis and probability updating (often Bayesian) • Use of real time data, near-misses, ASP to update probabilities • Possible integration with Bow-Tie diagrams • Application also to rare events (HBA - Hierarchical Bayesian Approach modification) • Application to Process accident model with predictive capability (SHIPP - *System hazard identification, prediction and prevention methodology*) • Application to operational Risk Assessment (DORA – *Dynamic Operational Risk Assessment*).	√	√	√	√	√	√
DRA + DyPASI	• Coupling of two advanced dynamic techniques: DyPASI (Dynamic Procedure for Atypical Scenarios Identification) and DRA (Dynamic Risk Assessment) • Improved Hazard Identification (first step of Risk Assessment) in comparison with DRA by itself.	√	***X***	√	***X***	***X***	√
Dynamic Risk Assessment with Bayesian Networks	• Direct acyclic graphs representation of variables and probabilities, with flexible and time-dependent structure • Possible conversion from Bow-Tie to BNs • Easy integration of technical and non-technical factors (e.g. human and organizational ones). • Transparency and intuitiveness, due to graphical appearance, may be suitable in purpose to involve non-expert people in important decisions (e.g. stakeholders). • Complex events description, with the ability to incorporate multistate variables and common cause failure.	√	√	√	√	√	√
Risk Barometer	• Proactive method based on Risk Indicators • Requires a QRA to be performed • Capture real-time information of critical safety barrier, allowing to incorporate human barrier performance indicators • Easy visualization of results • Still limitations in aggregation of data	√	√	√	***X***	***X***	√

√: Contributions available ***X****: No contributions currently available, but application is possible. Blank: application is not possible.*

Table 2. 8 Possibilities and limitations of dynamic approaches application to Risk Assessment in design and operation of chemical and process facilities.

Plant life cycle phase	Possibilities	Limitations
Design	Improved development of scenario generation and description, due to application of early-warnings and specific data from the process (Al-Shanini et al., 2014). → Dynamic Methods for Hazard Identification can tackle Atypical Scenarios, whose detection influences the design process and safety systems implementation.	▪ No regulations currently available on Dynamic Risk Assessment Methodologies and Applications (Paltrinieri et al., 2014b). ▪ Effectiveness of the methods relies on continuous monitoring activity and real-time data capturing. It implies the necessity to collect early-warnings, near misses, incidents and accident data (Khakzad et al., 2014). ▪ Most of the methodologies presented herein are part of on-going studies. There are still some issues to be addressed in each methods (e.g. for DRA the use of free-distribution data (Paltrinieri et al., 2014c), for Bayesian Networks the Net development (Pasman and Rogers, 2013), for Risk Barometer the Indicators aggregation processes (Paltrinieri and Hokstad, 2015)). ▪ Lack of knowledge on these methods: no completely automated software existing, very limited experience in industry (Pasman and Rogers, 2013). ▪ Need of conventional models as pre-requirements (e.g. Bow-Tie for DyPASI, conventional QRA for Risk Barometer) (Paltrinieri and Scarponi, 2014). ▪ Necessity to further develop and apply these methods, in particular to the inclusion of external factors (e.g. domino effect, natural hazards) (Pasman and Rogers, 2013).
	Transparent comparison between different design alternatives, determining (dis-)utility on the basis of risk costs and benefits (Pasman and Rogers, 2012).	
	Uncertainties introduced in the analysis are clearer (Pasman and Rogers, 2013). → Increased QRA transparency.	
	Effective visualization of results (e.g. Risk Barometer, Bayesian Nets, Graphs of Risk vs Time) → Improved decision-making process and stakeholders' involvement during the design phase and throughout the plant lifetime (Weber et al., 2012).	
	Integration among technical, human and organizational factors from the beginning of the design process (Ale et al., 2014). → Improved frequency and consequence calculations, that takes into account common causes and human influences.	
Operation	Evaluation of additional safety measures during the operational phase based on updated consequences in order to fulfil risk minimization (Yuan et al., 2013).	
	Managing operation effectively, determining whether to continue it or stopping it, in order to review the existing operating condition to avoid accidents (Abimbola et al., 2014).	
	Possibility to reiterate Risk Assessment more frequently in comparison with static methods (Paltrinieri et al., 2014c). → Real-time Risk Picture.	
	Effective detection of lacking/defective maintenance (Paltrinieri et al., 2014c). → Improved inspection and maintenance time intervals.	
	Effective detection of organizational issues during operation phase. → Improved training, planning for personnel and safety communication (Paltrinieri et al., 2014b).	

2.5.2 Towards the development of a Dynamic Risk Management Framework

Paltrinieri et al. (Paltrinieri et al., 2014b, 2014c) have recently proposed a dynamic approach to Risk Management - Dynamic Risk Management Framework (DRMF), developed from a set of well-known risk management and governance frameworks (IRGC - International Risk Governance Council, 2009; ISO31000:2009, 2009). The DRMF aims at implementing the need of continuous improvement and updating in the risk management process, by applying Dynamic Techniques for Hazard Identification and Risk Assessment. The framework, whose schematization has been reported in Figure 2. 9 a, is composed by two general stages, four sequential phases and two continuous activities involving all the process. The first stage is a process of learning and understanding that refers to the process of knowledge and information management, and includes the phases of Horizon Screening and Hazard Identification. The second stage is the Decision process, which refers to process of elaboration and judgement of information subsequent intervention, and includes an assessment phase and a decision and action phase. Along with the risk assessment phases, there are two “continuous” activities that should be constantly performed: “monitoring, review and continuous improvement” and “communication and consultation”; this framework results to be open to external constraints and continuously reiterated in order to effectively take into account real-time changes in the process.

The effectiveness in the application of a Dynamic Risk Management framework in collecting and considering evidence of emerging risks relies on the continuous development of Dynamic Techniques for Hazard Identification and Risk Assessment, joined with a proper safety culture. This is also illustrated by the 3D elaboration of the DRMF in Figure 2. 9 b. In fact, initially there may be events that are defined by the QRA analysists as "Unknown Unknowns" (analysts are not aware they do not know them). Information about these events is gradually collected through the continuous activity of "monitoring, review and continuous improvement" once a reasonable doubt is raised. This information is represented by early warnings, past events, accident precursors, test results or related studies. Due to an increased awareness of the potential disregarded related risk, these events turn to be "Known Unknowns" (analysts are aware they do not know them). The risk evidence is then integrated in the analysis through the dynamic techniques mentioned in this work, the knowledge about these potential accident events increases and vice versa, the uncertainties decrease, as shown by Figure 2. 9 b. Once the potential scenarios are assessed and metabolized in the process, analysts can define them as "Known Knowns" (analysts are aware they know them). The dynamic process of risk assessment can be described not only as a circular process (Figure 2.9 a), but as a 3D spiral,

where the radial centripetal movement represents the increase of awareness and the vertical movement from the top to the bottom represents the decrease of related uncertainties.

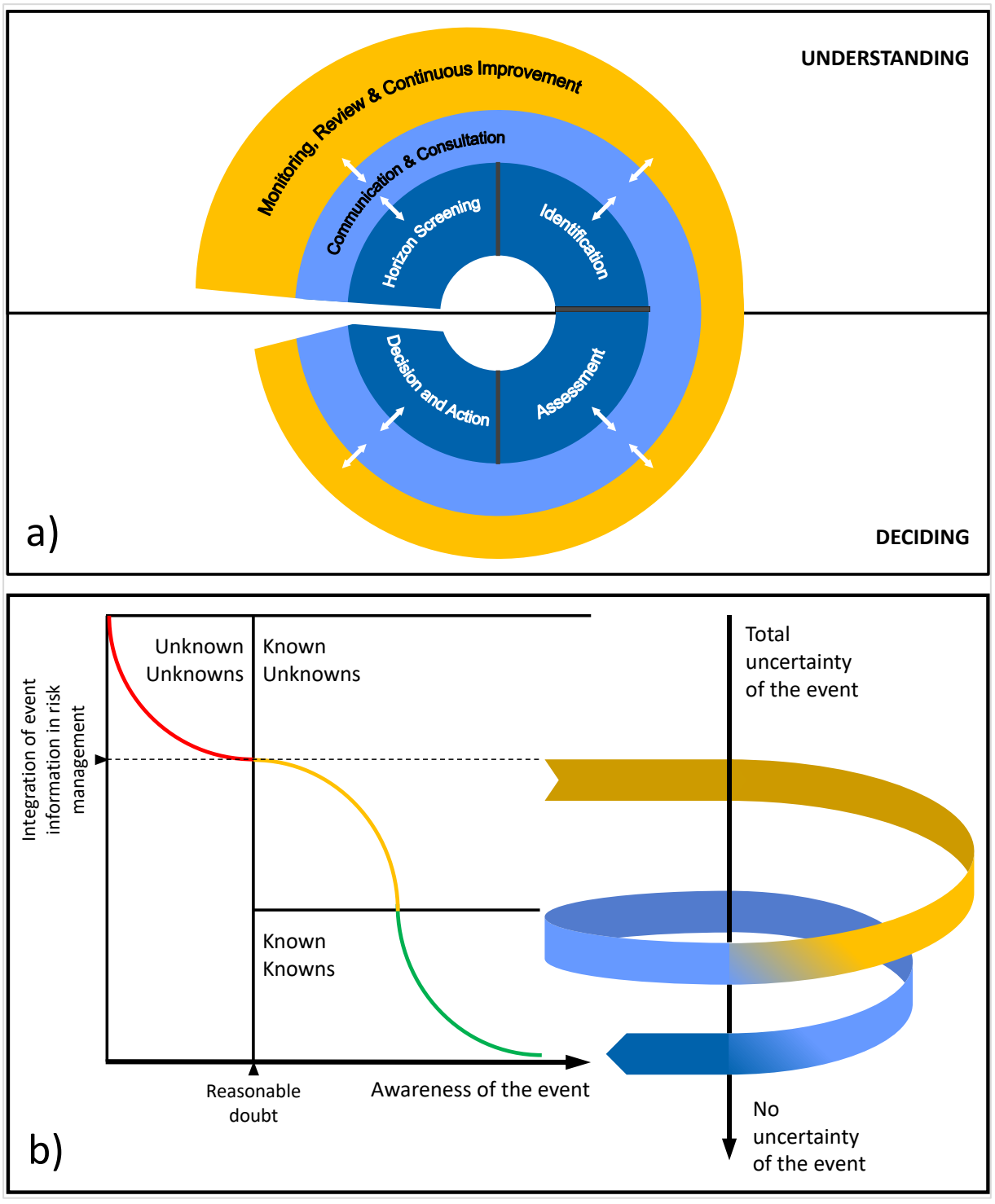


Figure 2. 9 Dynamic Risk Management Framework (a) and its 3D perspective (b).

2.6 CONCLUSIONS

In the present section, relevant approaches to risk assessment for chemical and process facilities have been analysed and classified, applying novel criteria. The classification highlighted how the application of Risk Assessment has supported process safety in the last thirty years, and showed its usefulness to support the process industry business by enabling risk management. Despite the obvious fact that it is not an exact description of reality, QRA proved to be the best available, analytic, predictive tool to assess the risks of complex chemical process systems. However, the present overview pointed out that more refinements of Risk Assessment tools are required to exploit its full potential. Most of the research is oriented to improve basic aspects, such as data frequencies. A possible development pathway is given by the application of dynamic approaches, as a direct consequence of the nowadays-feasible possibility of real-time monitoring for process facilities. In particular dynamic risk assessment approach, either coupled with a dynamic procedure for hazard identification, seems to be a promising step forward. For instance, a novel method based on indicators, the Risk Barometer, has demonstrated valuable features in its first applications. On the other hand, the incorporation of Bayesian networks into Risk Assessment may be another interesting focus, for both research and industrial purposes, because it allows a systemic approach considering human error and management influences. The application of a dynamic approach within cascading events (e.g., domino accidents) modelling is outlined as possible research field. In a broader perspective, the insertion of dynamic risk assessment approaches within a Dynamic Risk Management framework allows effectively taking into account real-time changes in the process, which results into increased awareness of the analysts toward potentially disregarded risks.

To conclude, despite the fact that risk assessment application has deeply increased the safety of chemical process plants, major accident scenarios are still occurring and in order to guarantee a certain level of safety, risk assessment techniques should be constantly improved and evolve in parallel with the increasing complexity of the systems where they are applied.

Section 3.

State of the art on external hazard factors and economic evaluations within Risk Assessment

3.1 INTRODUCTION

During the past years, several accidental events raised the attention toward the possible escalation of major accidental scenarios into cascading events within chemical and process facilities. Cascading events are catastrophic accidents triggered by external hazard factors, as domino effects (i.e., triggered by safety-based accidents, as primary fire/explosions), security threats (i.e., sabotages or terroristic attacks) and natural events (i.e., lightnings, floodings, earthquakes).

External hazards factors are widely recognized causes of major accidents and cascading events, which determined about 30.7% of all these accidental events worldwide (Darbra et al., 2010). Therefore, they should be accounted within Quantitative Risk Assessment in the chemical and process industry domain.

Considering risk as the effect of uncertainties on objectives (ISO31000:2009, 2009), the key different element between safety and security domains is the risk source that in the safety domain can be considered unintentional, while in the security domain it is the result of a specific intent. Therefore, many authors (Aven, 2007; Reniers, 2014; Reniers and Audenaert, 2014) suggested a unified framework the inclusion of external hazard factors within safety and security risk assessment.

Despite their different causes, all these accidents share low probabilities of occurrence and very high impacts in terms of human, environmental and assets losses, both inside and outside facilities boundaries (Reniers and Cozzani, 2013). These catastrophic accidents tend to affect particularly chemical and process installations, due to the high inventory of hazardous chemicals and possibly severe operating conditions.

In Section 3. 2, a description of different typologies of cascading events is carried out, together with available techniques to model and include external hazard factors driven accidents within risk assessment.

Indeed the analysis of risk assessment techniques made clear the role of safety and security measures within cascading events prevention. Safety barriers (or measures) are widely applied, concerning domino accidents, as well as security barriers (or measures), concerning security-based accidents, in purpose to prevent, control or mitigate their occurrence. Therefore, quantitative assessment of barriers performances, from both technical and economic point of view, takes on a major role in the risk evaluation step of risk assessment, and in a broader context, in accidents modelling and prevention (Janssens et al., 2015).

Therefore, different typologies of risk reducing measures applied within chemical and process installations are described in Section 3. 3, together with methodologies to evaluate their performances.

For what concerns safety barriers, conventional methodology for performance evaluations is based on Bow-Tie diagram and/or on its constituents (i.e., Fault-Tree and Event-Tree). Dynamic risk assessment techniques have recently emerged within the process industry domain, due to their flexibility in mirroring systems changes over time and to their enhanced intuitiveness in the presentation of results, as described in Section 2. Among these techniques, Bayesian Networks, a graphical probabilistic method, is nowadays a promising and increasingly popular tool, suitable to cope with complex and uncertain situations (Ale et al., 2014), and therefore to model safety barriers behaviour within a chemical installation; the mathematics behind Bayesian Networks and a software to construct them will be presented. Therefore, the conversion processes from conventional techniques into Bayesian Networks will be presented, together with methodologies for safety barriers performance assessment by means of Bayesian techniques and Bayesian Networks. A methodology, which combines existing ones, to assess safety barriers performance assessment, by means of Bayesian Networks, with an eventual extension to domino accident analysis, is outlined.

For what concerns security barriers, existing methodologies for performance evaluations are site-specific and accident-specific; an overview on the most applied techniques is presented.

Due to the increased attention for safety and security issues, an optimal selection and allocation of risk reducing measures, including related cost issues, is becoming progressively more important for decision-makers. A description of economic models for supporting risk assessment and related decision-making process is presented in Section 3. 4. Indeed, economic analyses, such as cost-benefit and cost-effectiveness analyses, may offer rational criteria for the selection and allocation of safety and security measures. An overview of recent contributions regarding theoretical, methodological and applicative aspects of economic analyses within the safety and security domain, referred to chemical and process industry installations, is presented. The analysis of research gaps highlighted that, despite the potential

of economic analyses in establishing competitive business advantage, previous contributions and ongoing research within the chemical industry address economic assessment with respect to unintentional major and occupational accidents (i.e., safety-based accidents). No specific complete economic models and applications are yet available addressing the selection and allocation of preventive security measures (e.g., counter terrorism related measures), within the chemical and process industry domain.

3.2 CASCADING EVENTS TRIGGERED BY EXTERNAL HAZARD FACTORS

3.2.1 Safety-based accidents: domino accidents

3.2.1.1 Definition of domino effect

A domino effect indicates a catastrophic escalation of accidental events, characterized by very low frequency and high consequences that can affect both workers and population in the nearby, as well as assets and environment. In a domino effect, a chain of accidents in which a primary accident escalates and triggers other secondary or higher-order accidents, occurs. As explained in Section 2, many significant progresses have been made in the context of Quantitative Risk Assessment for the Chemical and Process industry domain in the last thirty years, but the topic of cascading events modelling and inclusion within QRA still needs to be further investigated. Nevertheless, in the past decades cascading events, and among them, domino accidents, were often neglected by risk analysts because of their very low probability and high complexity, but, unfortunately, defining an accidental event a “Black Swan” (Murphy and Conner, 2012) does not mean it would be impossible.

For instance, two surveys on domino effect accidents (Darbra et al., 2010; Planas et al., 2014) emphasized an increasing trend of domino events occurrence, between 1961 and 1980-1990, within the chemical domain, followed by a more recent decreasing trend, as visible from Table 3. 1, which may be justified by increasing safety culture and improved risk management. According to Darbra et al. (Darbra et al., 2010), domino accidents are nowadays significantly more severe in underdeveloped countries, due to safety culture deficits and lack of proper risk planning. However, domino events, as demonstrated by BP Texas city refinery accident in 2005 (CSB, 2007a), where a primary Vapor Cloud Explosion was followed by several fires and explosions and Buncefield depot accident (Buncefield Major Investigation Board, 2008) may still occur everywhere.

The awareness of hazards posed by domino events requires efforts to prevent these catastrophic accidental scenarios. In the European Union, the legislation on the control of major accident hazard (i.e., “Seveso-III” Directive, 2012/18/EU (EU, 2012)) includes measures

to assess, control and prevent domino accidents (Bagster and Pitblado, 1991; Khan and Abbasi, 1999).

Since there is disagreement on what people define as domino effect, the natural consequence is that the most of studies on domino effect are carried out independently and focuses either on very particular aspects of accident escalation process like vulnerability models or on the definition of methodologies for risk assessment. An overview on available domino events definitions is presented in Table 3. 2; among these the most recent is the one by Reniers and Cozzani (Reniers and Cozzani, 2013).

Domino effects modelling requires at its basis the definition of three concepts: primary accident, accident propagation and escalation probability (Darbra et al., 2010).

A primary event is an accidental scenario that occurs in a certain unit (i.e., either a fire or an explosion). According, to Landucci et al. (Landucci et al., 2015a), domino accident scenarios triggered by the escalation of fires were responsible of severe accidents that affected the chemical and process industry. Past accident data analysis review carried out by Necci et al. (Necci et al., 2015) confirmed that in more than half of the industrial accidents involving a domino effect, occurred in the past fifty years, escalation was triggered by a primary fire. Indeed, fires act a severe heat load to every structure, both irradiative and convective, capable and destroy hazardous substance containers. There are many different kind of fire accidents due to hazardous substances, but in the framework of risk assessment four typologies of fires are relevant: pool fire, flash fire, fireball and jet fire.

A description of accident propagation and escalation probabilities concepts is reported in the following sections (see Section 3.2.1.2, Section 3.2.1.3 and Section 3.2.1.4).

Table 3. 1 Historical analysis of domino events occurrence within the chemical industry domain, adapted from Darbra et al. (Darbra et al., 2010).

Period	Number of accidents	% of domino accident events
1961-1970	49	22
1971-1980	70	31
1981-1990	63	28
1991-2000	24	11
2001-2007	19	8

Table 3. 2 Domino effects definitions according to the literature, adapted from Necci et al. (Necci et al., 2015).

Source/authors	Definition
Third Report of the Advisory Committee on Major Hazards (HSE - Health and Safety Commission, 1984)	The effects of major accidents on other plants on the site or nearby sites.
(Bagster and Pitblado, 1991)	A loss of containment of a plant item that results from a major incident on a nearby plant unit. An event at one unit that causes a further event at another unit.
Lees' Loss Prevention in the Process Industry (Mannan, 2005)	An event at one unit that causes a further event at another unit. A factor to take account of the hazard that can occur if leakage of a hazardous material can lead to the escalation of the incident, e.g. a small leak which catches fire and damages by flame impingement a larger pipe or vessel with subsequent spillage of a large inventory of hazardous material.
(Khan and Abbasi, 1998b)	A chain of accidents or situations when a fire/explosion/missile/toxic load generated by an accident in one unit in an industry causes secondary and higher order accidents in other units.
(Darbra et al., 2010; Delvosalle, 1998)	A cascade of events in which the consequences of a previous accident are increased both spatially and temporally by the following ones, thus leading to a major accident.
(TNO, 2005a)	The effect that loss of containment of one installation leads to loss of containment of other installations. An accident that starts in one item and may affect nearby items by thermal, blast or fragment impact.
(CCPS - Center for Chemical Process Safety, 1995)	An accident that starts in one item and may affect nearby items by thermal, blast or fragment impact.
(Vallee et al., 2002)	An accidental phenomenon affecting one or more installations in an establishment that can cause an accidental phenomenon in an adjacent establishment, leading to a general increase in consequences.
(EU, 2012)	A loss of containment in a Seveso installation that is the result (directly and indirectly) from a loss of containment at a nearby Seveso installation. The two events should happen simultaneously or in very fast subsequent order, and the domino hazards should be larger than those of the initial event.
(Post et al., 2003)	A major accident in a so-called 'exposed company' as a result of a major accident in a so-called 'causing company'. A domino effect is a subsequent event happening as a consequence of a domino accident.
(Cozzani et al., 2006)	Accidental sequences having at least three common features: ▪ A primary accidental scenario, which initiates the domino accidental sequence; ▪ The propagation of the primary event, due to "an escalation vector" generated by the physical effects of the primary scenario, that results in the damage of at least one secondary equipment item; ▪ One or more secondary events (i.e., fire, explosion and toxic dispersion), involving the damaged equipment items (the number of secondary events is usually the same of the damaged plant items).
(Gorrens et al., 2009)	A major accident in a so-called secondary installation that is caused by failure of a so-called external hazards source.
(Antonioni et al., 2009)	The propagation of a primary accidental event to nearby units, causing their damages and further "secondary" accidental events resulting in an overall scenario more severe than the primary event that triggered the escalation.
(Reniers and Cozzani, 2013)	An accident in which a primary unwanted event propagates within an equipment ('temporally'), or/and to nearby equipment ('spatially'), sequentially or simultaneously, triggering one or more secondary unwanted events, in turn possibly triggering further (i.e., higher order) unwanted events, resulting in overall consequences more severe than those of the primary event.

3.2.1.2 Accident propagation

Domino effect takes place when an accident in a unit, known as a "primary event," triggers other accidents in adjacent units by means of escalation vectors (Khakzad et al., 2013d). Therefore, the study of domino accidents requires the analysis of the physical effects that trigger the escalation chain, named escalation vectors. The typologies of escalation vectors depend on several factors including the primary event and the distance between the accident

epicenter and nearby units. Destructive physical effects that may be accounted as escalation vectors are fire impingement, fire engulfment, heat radiation, overpressure, or explosion caused by the projection of fragments (Reniers and Cozzani, 2013). Several models are available in literature regarding the calculation of escalation vectors (i.e., often named vulnerability models, which may be divided into three main classes: analytical model, integral model and averaged model (CCPS - Center for Chemical Process Safety, 2000; TNO, 2005b). In purpose to determine which nearby units are impacted, a comparison between the escalation vectors derived from the primary event on the nearby units and predefined threshold values is carried out; for instance several contributions proposed typical values for heat radiation and overpressure (Cozzani et al., 2009; Cozzani and Salzano, 2004b, 2004c); a summary is available in Table 3. 3.

Table 3. 3 Reference values for domino accident analysis (Cozzani et al., 2009). From the left to the right, in column order: primary events, escalation vector, secondary unit, threshold value, safety distance. (*) R indicates Sachs energy-scaled, calculated as $R = \frac{x}{(E/P_{atm})^{1/3}}$, where x is the distance from explosion center (m); E is released energy of explosion (J), P_{atm} is atmospheric pressure (Pa).

Primary event	Escalation Vector	Secondary unit	Threshold value	Safety distance
Fireball	Heat radiation	Atmospheric	15 kW/m^2	Fireball radius
	Fire engulfment	Pressurized	50 kW/m^2	N/A
Jet fire	Heat radiation	Atmospheric	15 kW/m^2	Flame length + 50 m
	Fire impingement	Pressurized	50 kW/m^2	Flame length + 25 m
Pool fire	Heat radiation	Atmospheric	15 kW/m^2	Flame length + 50 m
	Fire engulfment	Pressurized	50 kW/m^2	Flame length + 15 m
Explosion	Overpressure	Atmospheric	22 kPa	$R^a = 1.8$ (*)
		Pressurized	16 kPa	$R^a = 2.0$ (*)

The escalation vectors whose values is above the relevant thresholds may cause credible damage to the nearby units, resulting in loss of containment or loss of physical integrity. Thus, based on a comparison between escalation vectors and threshold values, a preliminary screening of the nearby units is performed, leading to the specification of potential secondary targets. The potential secondary units are the units adjacent to primary unit that may give a potential contribution to domino effect. Moreover, the escalation vectors that are generated from secondary units, may in turn trigger other accidents in further units (i.e., tertiary units),

either by themselves or by means of synergistic effects. By means of synergistic effects, the escalation vectors of a unit of order i collaborates with those of already engaged units (i.e., order $i-1$) to impact the units of order $i+1$ that had not passed the threshold criteria in previous levels (Reniers and Cozzani, 2013). Further information on accident propagation concept is presented in Section 3.3.2.1.3, together with the advanced methodology that will be applied in case studies. Indeed, it should be remarked that the concept of accident propagation is particularly significant, because it does not only results in a more realistic and accurate calculation, but it avoids possible underestimation of the potential risk. Moreover, it offers a sound support to safety analysts in purpose to choose safety barriers, and consequently to hinder domino effect in the early stages.

3.2.1.3 Calculation of escalation probabilities

The calculation of escalation probabilities (P_d), named also damage probabilities, is generally carried out by means of Probit methods (Antonioni et al., 2009; Cozzani et al., 2005; Cozzani and Salzano, 2004b). Probit methods may consider both the type of equipment (e.g., atmospheric or pressurized) and the type of escalation vector that affects the equipment (e.g., heat radiation or overpressure); for instance, the Probit variable (Y) can be calculated as follows, in its generic formula (Reniers and Cozzani, 2013):

$$Y = a + b \cdot \ln(V) \tag{3.1}$$

Where:

- a and b are Probit coefficients determined using experimental data or regression methods;
- V is either the escalation vector (e.g., static overpressure (ΔP) in case of explosions) or an escalation related parameter (e.g., time to failure (ttf) in case of heat radiation).

Therefore, in case of domino accident triggered by heat radiation, Probit values can be calculated according to the following version of equation (3.1):

$$Y = a + b \cdot \ln ttf \tag{3.2}$$

Where $[ttf] = [s]$ is the time lapse between the fire start and the thermally induced failure.
In case of domino accident triggered by overpressure, Probit values can be calculated according to the following version of equation (3.1):

$$Y = a + b \cdot \ln(\Delta P) \tag{3.3}$$

Where $[\Delta P] = [kPa]$ is the peak static overpressure.
In turn, escalation vectors, expressing the physical effects that trigger the escalation chain, can be estimated according to specific vulnerability models, as mentioned in Section 3.2.1.2.

The values of Probit coefficients to be applied are reported in Section 5, in correspondence of each case study. Then, the normalized Probit variable $(Y-5)$ is calculated and the cumulative density function of normal standard distribution (Φ) is applied to get P_d values, according to the following expression:

$$P_d = \Phi(Y-5) \tag{3.4}$$

3.2.1.4 Conventional approach to risk assessment of domino accidents

The inclusion of domino accidents within QRA requires as crucial point the estimation of events likelihood and consequences. Several past contributions that are analysed in a recent comprehensive review by Necci et al. (Necci et al., 2015), led to the creation of a conventional approach. According to the conventional methodology (Antonioni et al., 2009; Cozzani et al., 2005; Necci et al., 2015) the use of escalation probabilities, domino accident frequencies can be calculated as follows (Reniers and Cozzani, 2013):

$$f_{DOMINO} = f_{PE} \cdot P_d = f_{PE} \cdot P(E|PE) \tag{3.5}$$

Where f_{DOMINO} is the domino event frequency, f_{PE} is the primary event frequency, P_d is the escalation probability of the impacted unit and $P(E|PE)$ is the probability of escalation (E), conditioned to the happening of the primary event (PE).
In addition, a probabilistic version of equation (3.5) can be retrieved from technical literature (Khakzad et al., 2013d):

$$P_{DOMINO} = P_{PE} \cdot P_d \tag{3.6}$$

Where P_{DOMINO} is the domino event probability and P_{PE} is the primary event probability.
Once the domino accident propagation and frequencies are identified, and physical effects are evaluated, a proper risk profile can be defined. The application of a GIS (i.e., Geographical Interface Software) tool (Cozzani et al., 2006) may allow the calculation of individual and societal risk contours due to domino accidents, even to entire industrial areas (Antonioni et al., 2009). However, it should be remarked that the inclusion of domino accidents within QRA deeply influences also many other safety-related aspects (e.g., safety management, plant design, emergency planning) requiring new solutions to be found (Janssens et al., 2015).

3.2.2 Security-based accidents

3.2.2.1 Definitions and characteristics of security-based accidents

Several recent events raised the attention toward possible major accidents triggered by external acts of interference in industrial facilities, named for instance security-based accidents. Many categories of critical infrastructures (Moteff, 2005) can be attractive targets for deliberate attacks, such as airports, power plants, roads and maritime means of transportation. Chemical (and process) fixed installations were recognized several years ago

by CCPS (CCPS - Center for Chemical Process Safety, 2008b, 2003) (amongst others) as attractive targets for potential intentional malevolent acts, such as terroristic attacks and sabotage. Due to the high inventory of hazardous chemicals and possibly severe operating conditions, the potential consequences of these events, in terms of disruption of operations, destruction of property, health deterioration or loss of life (Bajpai and Gupta, 2007), are severe and include the possibility of cascading effects (Landucci et al., 2015b; Nolan, 2008).

In particular, among possible typologies of security-based accident, a growing concern is present with respect to the intentional release of dangerous substances resulting in environmental and eco-terroristic attacks. Two environmental security-related phenomena, named enviro-terrorism and eco-terrorism, emerged among security threats to tackle in chemical and process facilities worldwide. Enviro-terrorism and eco-terrorism are aimed at respectively triggering severe environmental damages and demonstrating radical environmentalism by means of unlawful set of actions within chemical facilities (Alpas et al., 2011). Comparison between the two has been reported in Table 3. 4.

For instance, in 2015, two security-related accidents, possibly terroristic attacks, took place in France: an attack to a warehouse of explosive chemicals in a gas production factory on June 26th, 2015 (BBC News, 2015a) and the sabotage, with consequent explosions, of two storage tanks in an oil refinery on July 14th, 2015 (Le Guernigou and Revilla, 2015). Investigations, which are still underway, consider the intentional nature of both events and two suspects have been arrested, one for each of them; crime and terrorism are thus deemed as possible motivations (Associated Press, 2015; BBC News, 2015a; Pardini, 2016).

These two security-based accidents are just the latest ones of a long series; as reported by the ARIA governmental agency, only in France, 850 malicious acts have been perpetrated within industrial facilities, mainly chemical industrial sites, in the period 1992-2015 (ARIA, 2015). Indeed, the importance of environmental losses in the context of security-related accidents has been highlighted by the results of them mentioned ARIA survey (ARIA, 2015). Security-based accidents may be classified according to four main possible typologies of consequences: environmental, economic, social and human. For instance, the survey results highlight that 46% of security-based accidents resulted in severe environmental consequences (Figure 3. 1 A), leading also to economic consequences. For instance, economic consequences include internal damages necessitating repair expenses and production losses, as well as damages to third parties operations and properties. Environmental damages include soil, air, surface and ground water pollution. Moreover, release of hazardous or polluting substances occurred in almost half of security-based accidents (Figure 3. 1 B).

Table 3. 4 Definitions and comparison of enviro-terrorism and eco-terrorism in industrial facilities, adapted from Alpas et al. (Alpas et al., 2011).

	ENVIRO-TERRORISM	**ECO-TERRORISM**
DEFINITION	Unlawful action or set of actions, committed by individuals or groups, leading to short or long term disruption of environmental resources and properties to deprive others of its use.	Severe damage/disruption to property, rare threat and/or harm against people, and/or nonviolent activism caused by individuals or groups protesting because of perceived harm/destruction to the environment and/or nature.
EXAMPLES	Sabotage or terroristic action w.r.t. industrial facilities containing large inventories of hazardous substances (e.g., chemical and process plants, nuclear installation, infrastructures involved in energy production) with the aim to trigger a major accident, with the worst environmental damages possible.	Arson actions against housing/industrial developments, targeting companies using animals for tests, theft and trespassing; demonstrative actions (e.g., machinery and vehicles sabotage) in industrial facilities perceived as pollutant.
MOTIVATION	Political, religious, personal, economic, etc.	Ideological (i.e., "very radical environmentalism")
TARGETS	Environment	Assets (e.g., equipment), rarely people (e.g., managers)
SCALE OF THE ACCIDENT/ CONSEQUENCES	Relevant environmental, health and assets losses, sometimes not confined within facility boundaries. The accident may cause the partial/complete interruption of operations for several hours/days and may contribute to the facility closedown. Severe environmental damages take place, generally requiring massive emergency intervention, causing health consequences to workers and, less often to the resident population (including injuries and/or casualties). Remediation costs and assets losses are relevant.	Generally, the consequences consist on minor assets losses, confined within facility boundaries that might cause a short and/or partial interruption of operations.

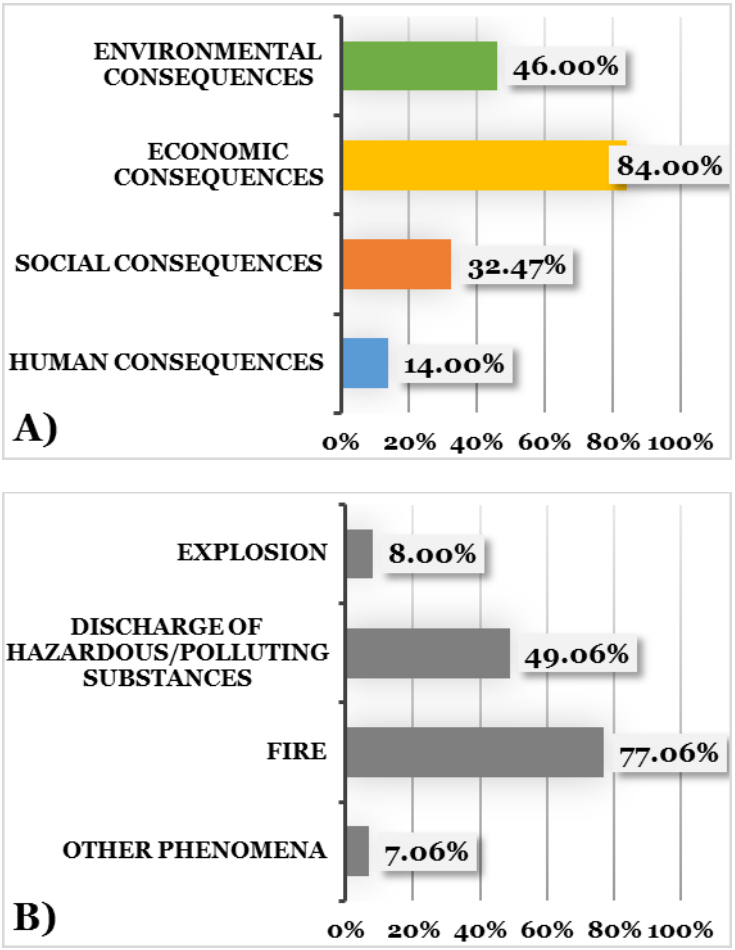


Figure 3. 1 Overview on security accidents consequences in industrial facilities, based on ARIA survey regarding 850 accidents in the period 1992-2015 (ARIA, 2015). (A) General overview on consequences percentage composition according to four main consequence categories: environmental, economic, social and human. (B) General overview on security-based scenarios according to four main scenario categories: explosion, discharge of hazardous/polluting substances, fire and other phenomena. The consequences percentages in (A) and (B) are obtained with respect to the total number of accidents considered in the mentioned survey (i.e., 850). Consequences and scenario category percentages do not sum into 100% as a security-based accident may determine consequences and scenario belonging to more than one of the listed categories.

However, as demonstrated by Figure 3. 1, security-based accidents are complex phenomena, not limited only to environmental and economic damages, wherein social consequences (e.g., installation of safety perimeters and personnel redundancies) and human consequences (e.g., casualties and morbidities) should be considered too. Therefore, an accurate monetary quantification of environmental damages within security-based accident losses, including intervention and remediation costs, may lead to a more realistic description of all the other accidents consequences. Consequently, the monetary quantification should be tailored on the typology of security-based accident to be studied (i.e., enviro-terrorism or generic security-based accident).

Despite the growing attention towards counter-terrorism issues in the chemical and process industry, at a European Union level only a general Directive on how to prevent, prepare and

respond to terrorist attacks related to critical infrastructures (Council Directive, 2008) was issued. No detailed guidelines for security management of chemical enterprises currently exist. Instead, in the United States, following the 9/11 attack, a specific regulation named CFATS (i.e., Chemical Facility Anti-Terrorism Standards) has become effective since 2007, and applied to all the facilities classified by US Department of Homeland Security as "high-risk" (DHS - US Department of Homeland Security, 2007).

3.2.2.2 Risk assessment of security-based accidents

According to Reniers and Audenaert (Reniers and Audenaert, 2014), security can be defined as the state of being protected against potential danger or loss that can result from the deliberate, malicious, and unlawful acts of others. Security risks assume threats, vulnerabilities and consequences as main components. Security risk sources can be several: individuals, business competitors, intelligence organization, terrorists, and criminals. All may behave according to different motivations, varying from personal to political, religious, economic and business advantage. Security risk assessment within chemical plants is a systematic approach to collect and organize information regarding (Bajpai and Gupta, 2007; CCPS - Center for Chemical Process Safety, 2003; Reniers et al., 2015):

- Site-specific assets (i.e., people, properties, infrastructures, reputation and information) that need to be protected;
- Threats that may be posed against those assets;
- Probabilities and consequences of malevolent attacks against them.

The result of a security risk assessment is a number of consequent actions planning and tracking on the threats tackled by the analysis.

Reniers et al. (Reniers et al., 2015) have recently proposed a methodology for security risk assessment within chemical facilities (Figure 3. 2) that mirrors exactly in its constituents the steps of conventional QRA (Figure 2. 2).

The process start with the facility characterization step that consists on undertaking a geographical overview of the company, including the identification of neighboring industrial activities (e.g., hazardous chemicals storages) and facility access. The security hazard and risk identification process should identify all company security risks, by means of historical data analysis and other methods. The process should be performed by including relevant stakeholders (e.g., company, government officials, intelligence representatives, etc.). Then, the security risk picture is established and the outcomes are compared with acceptability criteria, generally defined by security management and including both technical and economic criteria, to define possible security risk-reducing measures to be adopted. As in conventional QRA, the procedure is iterative and every step in the process has to be rigorous and transparent.

However, for security-based events, as terroristic attacks, only qualitative probabilities of occurrence may be available (e.g., low, medium, high) (Broder and Tucker, 2012; Garcia, 2005), while quantitative probabilities and frequencies of safety related events are generally available on databases (TNO, 2005a).

Moreover, for security-based events, also consequences are generally not calculated by means of specific damage model, but only a severity ranking is presented. Therefore, qualitative (or semi-quantitative) security risk analysis methodologies are largely applied within the chemical industry domain, instead of QRA (Garcia, 2005). Nevertheless, qualitative approaches do not allow obtaining an accurate risk picture, which is of paramount importance whenever HILP (i.e., high impact, low probability) events may occur, as in the chemical and process industry domain.

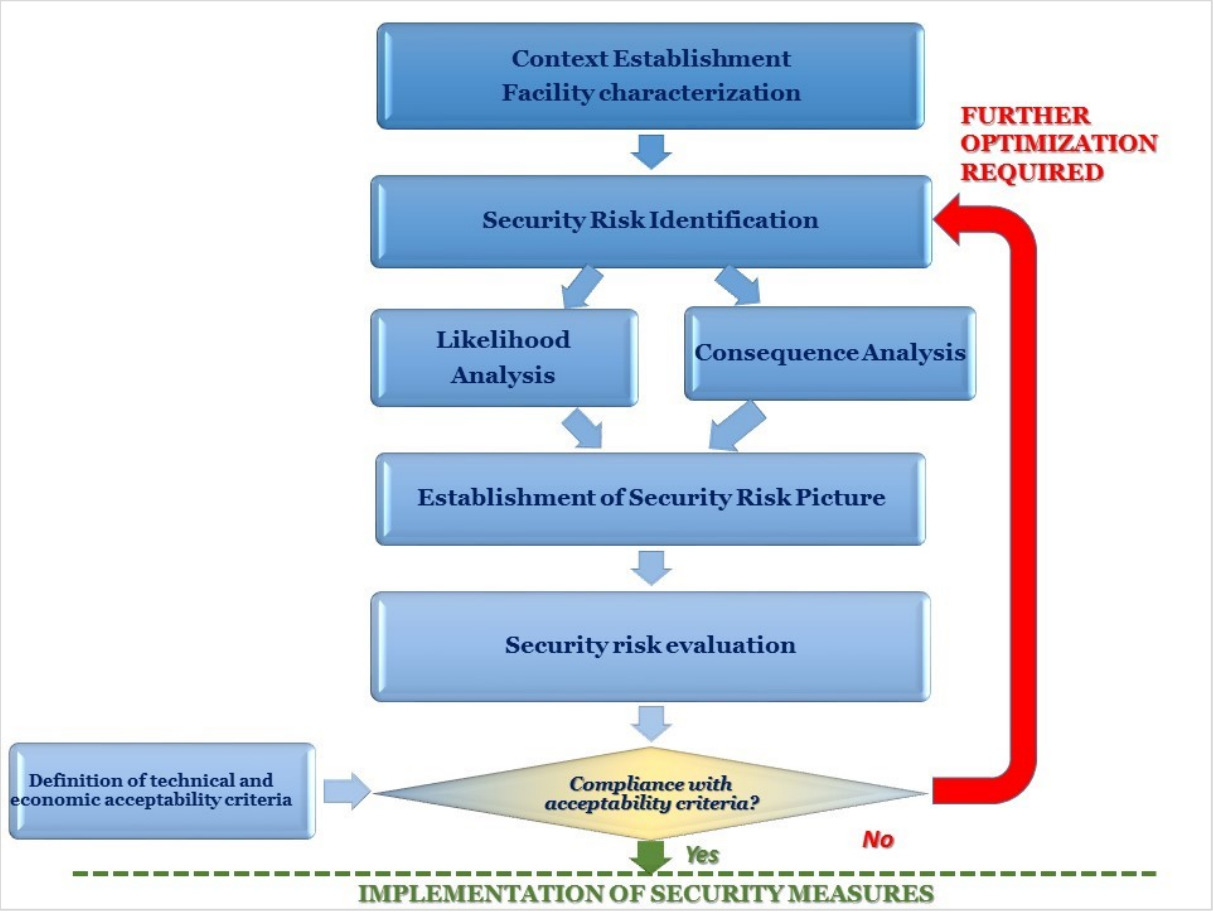


Figure 3. 2 Methodology for Security Risk Assessment, adapted from Reniers et al. (Reniers et al., 2015).

3.2.3 A common framework for the inclusion of external hazard factors within risk assessment

Many authors (Aven, 2007; Reniers, 2014; Reniers and Audenaert, 2014) suggested a unified generic framework for safety and security risk assessment. Considering risk as the effect of uncertainties on objectives (ISO31000:2009, 2009), the key different element between the two domains is the risk source, that in the safety domain can be considered unintentional, while in the security domain it is the result of a specific intent.

The common framework, reported in Figure 3. 3, applies the standard QRA methodological steps (see Section 2.3.1 for further details). External hazard factors (e.g., domino, security and natural events) are included in the Hazard Identification step. The framework emphasizes the importance of the risk evaluation step, which requires the identification, by means of a technical performance assessment, and the evaluation of possible risk reducing measures, by means of economic analyses techniques. The technical and economic performance criteria derived from the risk evaluation step are needed to select the eventual additional risk reducing measures to be implemented and to eventually comply with the acceptability criteria.

3.3 THE ROLE OF RISK REDUCING MEASURES IN EXTERNAL HAZARD FACTORS - DRIVEN ACCIDENTS

3.3.1 Description of risk reducing measures

3.3.1.1 The concept of risk reducing measure

The implementation of risk reducing measures (i.e., safety and security measures) may prevent, control or mitigate unwanted events or accidents within chemical installations. Risk reducing measures may either prevent the occurrence of a chain of events or limiting its consequences (Mannan, 2005). Before going into details regarding risk reducing measures classification and performance evaluation, it is necessary to briefly explain the definition of risk reducing measure. Several synonyms (i.e., barrier, defence, protection layer, safety/security critical elements, safety/security function, etc.) are used in the literature to describe risk reducing measures (Sevcik and Gudmestad, 2014). From a general point of view, the concept of barrier refers to an obstruction towards and emerging threat or accident. According to Janssens et al. (Janssens et al., 2015), the most complete definition of barrier is provided by Norwegian Petroleum Safety Authority: *"…technical, operational and organizational elements on an offshore or onshore facility, that, individually or collectively, reduce the possibility of concrete failures, hazard and accident situations occurring, or that limit or prevent harm/inconveniences"*.

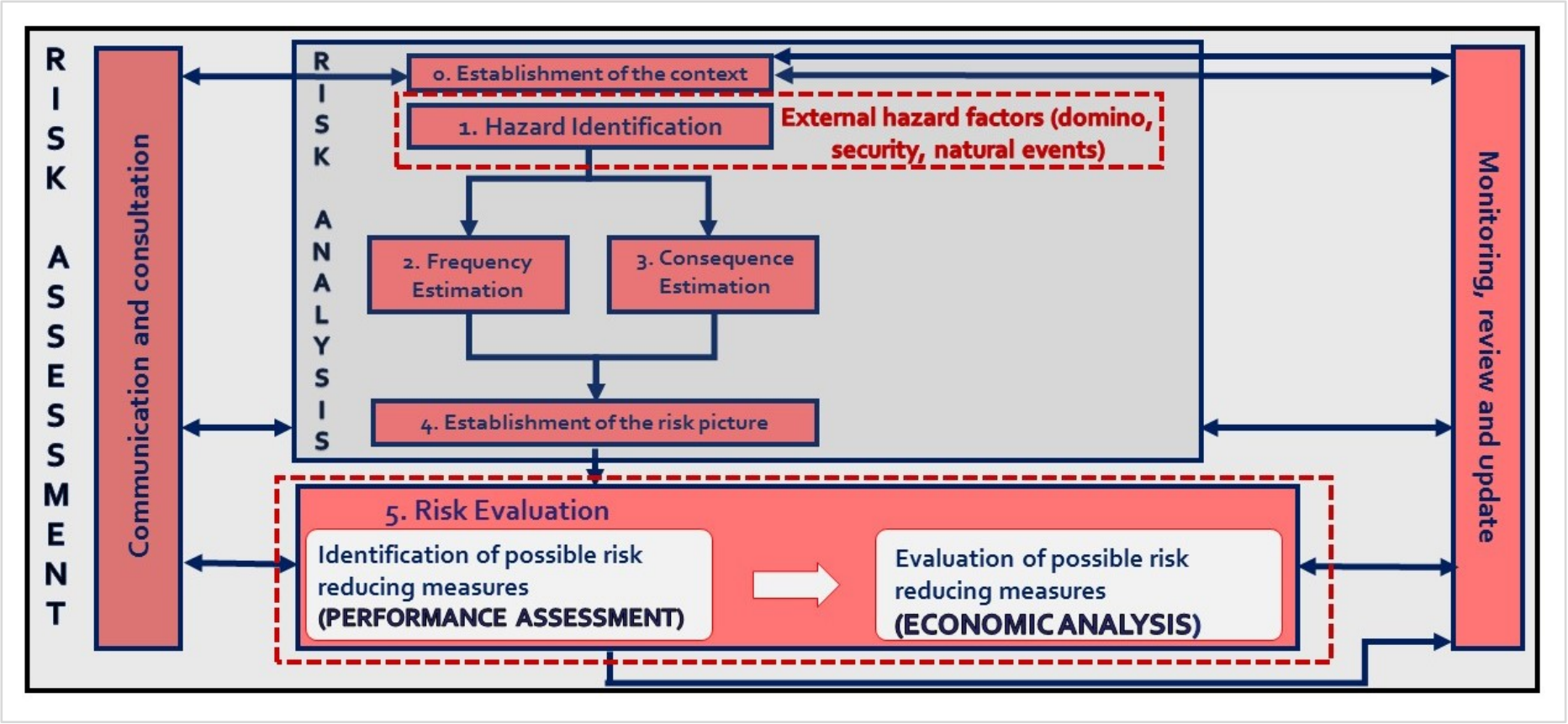


Figure 3. 3 A unified framework for the inclusion of external hazard factors within QRA.

3.3.1.2 Safety measures

Safety measures (or barriers) need to be categorized, before evaluating their performances in the prevention of major accidents and cascading events. Three different categories of barriers were identified, adapting the classification of protection layers proposed by AIChE (CCPS - Center for Chemical Process Safety, 2000) and in the Aramis project (Gowland, 2006):

- active barriers;
- passive barriers;
- procedural and emergency barriers;

A combination of all categories of safety barriers is generally required to assure the safety of humans, environment and assets (Mannan, 2005).

Active or mitigative safety barriers are activated by a detection system. The mitigation action is carried out using hardware, software, and/or human actions. Despite their wired application, active protection systems are critically dependent on the availability and correct design of the detection system and the software activation loop. The high number of components that requires to be activated on demand may limit the overall system performance.

On the other hand, a generic passive protection device is a system or a barrier, which does not require either power or external activation to trigger the protection action. Thus, the performance is not significantly influenced by physical or psychological conditions of operators or by the performance and position of other equipment. However, in the case of passive safety barriers such as firewalls, blast walls, dikes, and catch basins, the main limitations are given by cost and design constraints, maintenance, and possibility of inspection.

Procedural and emergency safety measures rely on management methods such as training, evacuation, and emergency response. These safety measures depend strongly on human factors such as safety training effectiveness and human response time. However, in the case of instantaneous accidental events procedural safety measures become ineffective (Khakzad et al., 2013e).

The use of protective systems or barriers in the context of domino effects may restrict the propagation of domino effects, mitigate its consequences and reduce the vulnerability of possible targets (e.g., by increasing the time to failure).

Nevertheless, it should be remarked that the application of safety barriers, often termed as “add-on safety” is not the solely answer possible to escalation prevention. According to Janssens et al. (Janssens et al., 2015), a significant portion of current research is concerned

with design-based safety with respect to domino effects, which means applying the concept of inherent safety. Inherent safety focuses on material characteristics, process design, and plant layout to eliminate the possibility of an escalation scenario, rather than on physical barriers to be implemented (Cozzani et al., 2009, 2007). However, the implementation of inherent safety principles requires major plants changes that in most of existing installations are not so easy to be made, so it becomes very important to optimize safety barriers within an existing industrial installation, according to technical and economic performance criteria (Janssens et al., 2015).

The typologies of safety barriers to be implemented may depend also on the typology of critical event, possibly triggering escalation. For instance, particular attention is posed to fire protection safety barriers, as fire is identified as the most common hazard factor triggering domino events; a summary of fire protection safety barriers typologies is adapted from Landucci et al. (Landucci et al., 2015a).

Active fire protection systems more relevant in escalation prevention can be divided into two different categories:

- Systems for the delivery of fire-fighting agents (such as water or water-based foam) which can be further classified into fixed, semi-fixed, mobile and portable systems;
- Emergency Shutdown Systems (i.e., ESD) and Emergency Depressurization Systems (i.e., EDP).

Active fire protection systems are aimed and designed to:

- Mitigate fire exposure protection of the target, keeping a water film on exposed surfaces to absorb radiant heat and to cool the steelwork, thus preventing loss of strength (water delivery systems);
- Isolate and empty the target vessel, reducing the potential loss and consequent damage connected to the large inventory (ESD and EDP systems);
- Provide effective control of the primary fire and prevention of fire spread in nearby units (fire-fighting agents delivery systems).

In the framework of escalation prevention, the application of passive fire protection measures consists on the use of fireproofing material (cementitious or vermiculite sprays, intumescent, mineral or ceramic fibers, etc.). Pressure Safety Valves (PSVs) are a further widely applied passive safety barrier. Fireproofing and PSVs are aimed at combining two possible effects of mitigation:

- Reduction of the vessel wall temperature (heat resistant coating/shielding effect);

- Limitation of the vessel internal pressure by the control of the vapor pressure increase due to the raise of the liquid temperature (PSV effect).

Procedural measures include the company operating procedures, which are relevant with respect to escalation prevention. Emergency measures represent the coordinated response to a major accident scenario, in which different roles and functions are to be performed by different actors. They typically involve the mobilization of resources and follow specific procedures since all actions are to be carried out in agreement with local authorities, fire brigade, emergency teams, etc.

The selection and allocation of safety barriers, with respect to possible accidental events and escalation, should be supported by appropriate methodologies for technical and economic performance assessment, which are described in details in the following sections.

3.3.1.3 Security measures

Physical Protection Systems (PPS) have a crucial role in providing adequate security protection. A physical protection system is an integration of protection components and elements that can include people, procedures and equipment for the protection of assets or facilities against security threats, as theft, sabotage or other malevolent human attacks (Garcia, 2007, 2005).

The selection, design and upgrade of PPS, often indicated as security barriers or security measures, require a methodological approach in which the objectives of the PPS are weighted against available resources and it eventually turns into a proposed design, that may be evaluated and subsequently further optimized in order to improve its performance (Garcia, 2007).

Generally, the PPS design and implementation should address the systematic and integrated protection of assets in anticipation of adversary attacks rather than in reaction of attack occurrence. It should also achieve the protection objectives with respect to operational, safety, legal and economic constraints of the facility (CCPS - Center for Chemical Process Safety, 2003). However, the occurrence of an attack may offer the occasion to tackle the weakness of PPS and consequently upgrade the security measures present in the facility.

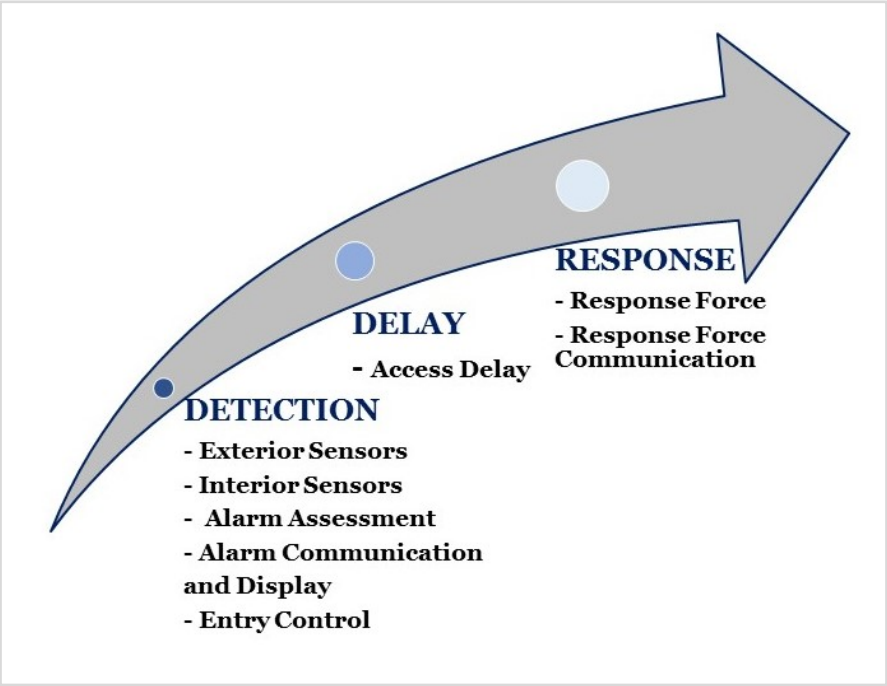


Figure 3. 4 Security measures classification.

The classification of PPS is generally carried out in three main categories accordingly to the function they serve and the elements that compose a security system (Garcia, 2007, 2005): detection of an adversary, delay of that adversary and response by security personnel.

Indeed, for the system to be effective in protecting critical assets from theft or sabotage by a malevolent adversary, there must be notification of an attack (i.e., detection), then adversary progress must be slowed (i.e., delay), which will allow the response force time to interrupt or stop the adversary (i.e., response). The response force time indicates the time it takes for the response personnel, including proprietary guards, contractors and/or members of local law enforcement, to arrive at a location and establish interruption of the adversaries from progressing in their attack.

A flowchart representing the three main security functions and the most common typologies of security measures belonging to each of them is reported in Figure 3. 4. A detailed description of each typology of security measures to be applied in chemical facilities is presented from Table 3. 5 to Table 3. 11.

Table 3. 5 Exterior intrusion sensors as part of detection function.

DETECTION	**NAME OF SECURITY MEASURE**	***Exterior Intrusion Sensors***	
	GENERAL DESCRIPTION	Sensors posed in outdoor environment for detection of a person or of a vehicle attempting to gain unauthorized entry into an area that is being protected by someone who is able to authorize or initiate an appropriate response.	
	PERFORMANCE CHARACTERISTICS	▪ Probability of assessed detection (P_{AD}); the likelihood of detecting an adversary within the zone covered by an intrusion detection sensor. For an ideal sensor, $P_{AD} = 1$. For real sensors $P_{AD} \cong 0.9$. ▪ False Alarm Rate; the expected rate of alarms from an intrusion detection sensor that can be attributed to known causes unrelated to intrusion attempts. For an ideal sensor, false alarm rate is 0. ▪ Vulnerability to defeat; exploitable capability of the sensor to be defeated though bypass or spoof by taking advantage of the sensor physics, signal processing, installation, degradation and site conditions. Also: communication system for sending and assessing alarms, lightning and assessment systems, balanced system for adequate protection though the perimeter.	
	AVAILABLE CLASSIFICATION CRITERIA	▪ Passive/Active; detector of some type of energy emitted by the target of interest/ transmitter of some type of energy and detector of a variation in the received energy. ▪ Covert/Visible: hidden from view/ in plain view of the intruder. ▪ Line-of-Sight/Terrain-Following: requiring a flat ground surface or a clean Line-of Sight/ capable of detecting on flat and irregular terrain. ▪ Volumetric/Line Detection; detection in a certain volume not identified by the intruder/ detection along a line often easy to identify. ▪ Application mode: buried line/ fence-associated/freestanding.	
	SENSOR TECHNOLOGY (Classification according to application mode)		
	Buried-Line Sensors	Pressure or seismic sensors	Ported coaxial cables
		Magnetic field sensors	Fiber-optic cables
	Fence-Associated Sensors	Fence-disturbance sensors	Electric field or capacitance
		Sensor fences	
	Freestanding Sensors	Active infrared	Bistatic microwave
		Passive infrared	Monostatic microwave
		Dual-technology sensors	
	Emerging Technology	Video motion detection	Ground-based radar
		Passive scanning thermal Imagers	Wireless sensor network
		Active scanning thermal imagers	Red/blue force tracking

Table 3. 6 Interior intrusion sensors as part of the detection function.

DETECTION	**NAME OF SECURITY MEASURE**	***Interior Intrusion Sensors***	
	GENERAL DESCRIPTION	Sensors posed in indoor environment for the detection of unauthorized acts or unauthorized presence of insiders, as well as outsiders, into an area that is being protected by someone who is able to authorize or initiate an appropriate response. The main difference with external detection sensors is that internal ones are vulnerable to both insiders and outsiders.	
	PERFORMANCE CHARACTERISTICS	▪ Probability of detection (P_{AD}); the likelihood of detecting an adversary within the zone covered by an intrusion detection sensor. For an ideal sensor $P_{AD} = 1$. For real sensors $P_{AD} \cong 0.9$. ▪ False Alarm Rate: the expected rate of alarms from an intrusion detection sensor that can be attributed to known causes unrelated to intrusion attempts. For an ideal sensor false alarm rate is 0. ▪ Vulnerability to defeat; exploitable capability of the sensor to be defeated though bypass or spoof by taking advantage of the sensor physics, signal processing, installation, degradation and site conditions. Also: choice of sensor placement in relation with its physical operation and with other sensors present (i.e., sensor detection areas should overlap). Consideration of the interaction among equipment, environment (e.g., electromagnetic, nuclear radiation, acoustic, thermal environment) and potential intruders in the selection of sensor technology.	
	AVAILABLE CLASSIFICATION CRITERIA	▪ Passive/Active; detector of some type of energy emitted by the target of interest/ transmitter of some type of energy and detector of a variation in the received energy. ▪ Covert/Visible: hidden from view (e.g., in walls, under floor)/ in plain view of the intruder (e.g., attached to a door). ▪ Volumetric/Line Detection: detection in a certain volume not identified by the intruder, regardless of the point of entry into the zone/ detection along a line often easy to identify. ▪ Application mode: boundary penetration sensors/Interior motion sensors/ Proximity sensors; detection of penetration of the boundary to an interior area/ detection of motion of an intruder within a confined interior area/ detection of the intruder in the area adjacent to the object or when the intruder touch the object.	
	SENSOR TECHNOLOGY (Classification according to application mode)		
	Boundary-Penetration Sensors	Vibration sensors	Electromechanical sensors
		Capacitance sensors	Infrasonic and passive sonic sensors
		Active infrared sensors	Fiber-optic cable sensors
	Interior Motion Sensors	Microwave sensors	Ultrasonic sensors
		Active sonic sensors	Passive infrared sensors
		Dual-technology sensors	Video motion detection
	Proximity Sensors	Capacitance proximity sensors	Pressure sensors
	Others	Wireless sensors	Miscellaneous (e.g., light and electric field)

Table 3. 7 Alarm assessment as part of the detection function.

DETECTION	**NAME OF SECURITY MEASURE**	***Alarm Assessment***
	GENERAL DESCRIPTION	Process of determining an alarm condition status (i.e., whether the event is an attack or a false alarm). Alarm is defined as a warning from a sensor or sensor system that a sensor has been triggered or activated, usually signaled by light or sound; alarm may indicate a nuisance or a false alarm, or a valid alarm. Alarm assessment includes appraisal of the credibility, reliability pertinence, pertinence, accuracy, or usefulness of an indicated alarm. Alarm assessment may be carried out by installing closed-circuit television (CCTV) cameras. Rarely it has been carried out by dispatching guards to an alarm location.
	PERFORMANCE CHARACTERISTICS	Alarm assessment performance must support system objectives: ▪ An immediate on-site response (short time between alarm and response) is needed to protect high-consequence targets, the system resolution and timing must be sufficient to enable a timely response. ▪ A delayed response may be sufficient to protect low-consequences targets. ▪ Choice of adequate level of resolution depending on the expected threats, their tactics, the target asset to protect, the way the video information are used. It includes also: conscientious approach toward installation and maintenance with equipment burn-in tests before final installation and preventive maintenance for the light. Minimization of camera vulnerabilities though correct placement. Realizing integration between alarm assessment system and intrusion detection system, considering interactions between the video system, intrusion sensors and display systems. Use of different cameras for safety and security monitoring.
	AVAILABLE CLASSIFICATION CRITERIA	▪ Primary/secondary assessment: determining whether the alarm is due to an adversary or a nuisance alarm/ providing additional information about an intrusion that can be relayed to the response force. ▪ Resolution of the camera (3 levels): detection/classification/ identification; ability to detect the presence of an object in the area of interest/ ability to determine what is present by class (e.g., animal, blowing debris, person)/ ability to uniquely identify an object based on details of appearance (e.g., Marco, not Luca).
	COMPONENTS OF A VIDEO ALARM ASSESSMENT SYSTEM	
	Camera and lens	Converting an optical image of the physical scene into an electric signal.
	Lighting system	Illuminating the alarm location evenly with enough intensity for camera and lens.
	Transmission system	Connecting the remote cameras to the local video monitors.
	Video switching equipment	Connecting video signals from multiple cameras to monitors and video recorders.
	Video recording system	Producing record of an event.
	Video monitors	Converting electric signal to a visual scene.
	Video controller	Interfacing between alarm sensor system and alarm assessment system.

Table 3. 8 Alarm communication and display as part of the detection function.

DETECTION	**NAME OF SECURITY MEASURE**	***Alarm Communication and Display (AC & D)***
	GENERAL DESCRIPTION	Alarm communication and display plays a fundamental role in the successful and timely response to a threat by controlling the flow of information from sensors to the operator and displaying it quickly and clearly. The alarm communication and display system collects alarm data, presents information to a security operator and enables the operator to enter commands to control the system. The system may be a simple alarm panel display or a complex multicomputer control and communication system, depending on specific needs and resources.
	PERFORMANCE CHARACTERISTICS	An AC & D should promote the rapid evaluation of alarms, by means of: ▪ Fast reporting time (AC & D system speed is often a measure of effectiveness); quick information for the operator. ▪ Communication of the following information: where an alarm has occurred/ what or who caused the alarm/ when the alarm happened. ▪ Line supervision of all cables. ▪ Easy and quick discovery of single point failure that should be repaired (or at least isolated) without affecting the whole system. ▪ Isolation and control of sensors by means of a path to check and isolate individual sensors. ▪ Expansion flexibility by capability to accommodate easily new sensors in a computer system. It includes also: adequate design for the environment (e.g., wide temperature variations), robustness, reliability by availability of individual components, redundancy or backup for critical components.
	AVAILABLE CLASSIFICATION CRITERIA	▪ Classification into two main subsystems: alarm communication subsystem/ alarm control & display subsystem; alarm communication subsystem moves data from the collection point (sensors) to a central repository (display) and often throughout the repository / alarm control and display subsystem presents information to a security operator and enables the operator to enter commands affecting the operation of AC&D system. ▪ Classification based on Open Source Interconnection (OSI) Reference Model: Physical Layer/Link Layer/ Network Layer.
	MODEL LAYERS FOR AC & D (Classification according to OSI Model Layers)	
	Physical Layer	The physical layer provides mechanical, electrical, functional, and procedural methods used to transmit information from one place to another. It deals with the media (wire, fiber, etc.) and network architecture (star, bus, point - to – point), low - level protocols or direct current line supervision that are characteristics of a communication channel.
	Link Layer	The data link layer provides protocol delimiters and framing information. This layer also performs basic error - checking, notifying higher layers by means of specific protocols.
	Network Layer	The network layer provides addressing, sequencing, flow-control, receipt/acknowledgement, and error - handling services. The network layer takes higher - level data and packages it for transmission. It provides the overall redundancy and reliability of the communication system.

Table 3. 9 Entry control as part of the detection function.

DETECTION	**NAME OF SECURITY MEASURE**	***Entry Control***		
	GENERAL DESCRIPTION	Entry control indicates the technology used to verify access (entry/exit) authorization to a facility and to detect contraband. Access control includes the databases, procedures and rules for access that complement technology. The main objectives of an entry control system are: ▪ Permitting only authorized personnel to enter and exit. ▪ Detecting and preventing the entry or exit of contraband material (weapons, explosives, authorized tools and goods, and critical assets). ▪ Providing information to security personnel to facilitate assessment and response.		
	PERFORMANCE CHARACTERISTICS	▪ Throughput: measure of the time it takes for an authorized person or material to successfully pass an entry or an exit point (e.g., avoiding use of long throughput components for entry gates at shift changes in an industrial facility) ▪ Error rates in personnel identity verification (biometric technologies): Type I error (False reject) is the improper rejection of a valid user / Type II error (false accept) is the improper acceptance of an unauthorized person. Choice of Acceptance precision should take into account these two opposite trends of Error Rate VS Acceptance precision. Also: eventual presence of CCTV surveillance, eventual integration with AC & D system, testing of the system under different (i.e., normal, abnormal and malevolent) conditions, entry control system impact on fire codes.		
	AVAILABLE CLASSIFICATION CRITERIA	▪ Based on classes: something you know/ something you possess/ something you are. ▪ Based on components' subsystems: personnel control entry/ contraband detection/ Locks/ Procedure/ Administrative Procedures.		
	COMPONENTS OF AN ENTRY CONTROL SYSTEM			
	Personnel Entry Control	Portion of an entry control system used to authorize entry and to verify the authorization of personnel for entrance in a controlled area.	Personal Identification Number – PIN	
			Credentials (Photo-identification badge, exchange badge, stored image badge, coded credentials)	
			Personnel Identity Verification – Biometrics (Hand/finger geometry, handwriting, fingerprints, eye pattern, voice, face, other techniques)	
			Personnel entry control bypass	
	Contraband Detection	Contraband screening is aimed at detecting unauthorized weapon, explosives and tools.	Manual search	Metal detectors
			Package search (bulk and trace explosives detection), chemical and biological agent detection	
	Locks	Locks secure the moveable portions of barriers in conjunction with other protection measures.	Fastening device	Strike
			Hasps and Shackles	Coded Mechanism (Keyless/ key coded)
	Procedures	Procedural and administrative tasks	Employees' training courses	Development of back-up procedures

Table 3. 10 Access delay as part of delay function.

DELAY	**NAME OF SECURITY MEASURE**	***Access Delay***		
	GENERAL DESCRIPTION	Access delay follows detection in effective PPS. Delay element prevent completion of the malevolent act, provide delay until an adequate response force can arrive, or until additional remotely activated delay and response system can be activated. The aim of access delay barriers (e.g., reinforced concrete walls, fences, gates, guards) is to complicate the adversary's progress by introducing impediments along any possible path the adversary may choose.		
	PERFORMANCE CHARACTERISTICS	Time is the key performance measure for access delay barriers; it depends on the barrier to be breached and the tools/skills that are necessary for it. Barrier penetration time is a function of the attack mode, which is in turn determined by the equipment needed. Presence of multiple barriers of different types along possible adversary paths. Barriers' location next to detection alarm to aid accurate assessment. If possible, incorporation of barriers into the design of the facility (e.g., facility underground or aboveground with massive overburden). Use of compensatory measures, as additional guards, during critical operations (e.g., fire drills, maintenance by contractors employees). Also: assets consolidation into a single room (reduced response time, reduced cost of delay upgrades), use of design basis threat to make forecasts about adversary's level of technical skills and appropriate equipment, barriers' upgrading over time.		
	AVAILABLE CLASSIFICATION CRITERIA	Based on barrier types and principles: Passive barriers/ guards/ dispensable barriers;		
	ACCESS DELAY BARRIERS CLASSIFICATION			
	Passive Barriers	Barriers that do not require any activation, they are always in place and fail secure. They are commercially available, with reduced costs and high accessibility, but they are weak against explosive attacks and they often impose operational and esthetic constraints on a facility.	Perimeter barriers	▪ Fences ▪ Gates ▪ Vehicle barriers
			Structural barriers	▪ Walls ▪ Doors ▪ Windows and utility ports ▪ Roofs and floors
	Guards	Presence of guards can provide flexible and continuous delay to adversaries using stealth or cover tactics to gain entry. Guards may only provide minimal delay to adversaries using force, unless in fixed and protected positions. Nevertheless, it is an operational expense and guards can be subjected to compromise with adversaries.		
	Dispensable Barriers	Barriers that are deployed only during adversary attack: active barriers can, on command (e.g., guard force and/or sensor), stop or delay an adversary, passive barriers do not require any command and control and they are activated by the penetration attempt.	Rigid polyurethane foam	Stabilized aqueous foam
			Smoke or fog	Sticky thermoplastic foam

Table 3. 11 Response force and response force communication as part of the response function.

RESPONSE	**NAME OF SECURITY MEASURE**	***Response Force & Response Force Communications***
	GENERAL DESCRIPTION	It indicates the element of a PPS designed to counteract adversary activities and interrupt the threat. Response force includes corporate policies and procedures, training, determination of response force tactics, use of force and normal operating procedures. The response force includes the proprietary guards and external (contractor and/or members of local law enforcement) personnel who may be involved in the immediate response to counter the threat of an adversary at a particular facility (both on-site and off-site).
	PERFORMANCE CHARACTERISTICS	Two main measures of an immediate response: ▪ Time for arrival: time it takes for the response personnel (one or more, depending on the threat) to arrive at a location and establish interruption that is preventing the adversary from progressing in their attack. Interruption is a measure of the detection, delay, communication and response function of the PPS and is represented by the probability of interruption (P_I). Interruption depends on reliable, accurate, and fast alarm reporting and assessment, as well as on dependable communication and effective deployment to the proper location. ▪ Neutralization effectiveness: neutralization measures response force numbers, training, tactics, and use of any weapons or equipment and is represented by the probability of neutralization (P_N). Neutralization refers to any confrontation between the adversary and responders and is defined as defeat of the adversary; neutralization effectiveness depends on training and capability, the techniques used depend on the threat.
	AVAILABLE CLASSIFICATION CRITERIA	According on different aspects of response function: contingency planning/ communication/ interruption/ neutralization/ procedures. According to time: immediate/ after-the-fact recovery.
	RESPONSE ASPECTS CLASSIFICATION	
	Contingency Planning	▪ Development of tactical plans to address various threats on relevant targets; ▪ Interaction with outside agencies for joint training exercises; ▪ Definition of the facility use of force policy; ▪ Development of additional procedures describing guard force daily operations and assistance during abnormal events (e.g., safety events, bad weather).
	Communication	Communication network resistant to eavesdropping, deception and jamming: ▪ Implementation of voice-private radios make the network more resistant to eaves dropping and deception, but more susceptible to jamming; ▪ Implementation of digitally encrypted radio transmission can be more secure, but often is too expensive; ▪ Spread-spectrum radios can provide resistance to jamming.
	Interruption & Neutralization	Careful planning, training and testing of response force capabilities. Periodical evaluation of the response force through limited scope performance drills and written examination.

3.3.2 Performance assessment for risk reducing measures

In the context of major accidents and cascading events prevention, control and mitigation, risk reducing measures (i.e., safety and security barriers) are widely employed. Therefore, quantitative assessment of barriers performances takes on a major role. In the current section, a selection of available methods, including most advanced ones (i.e., dynamic techniques, mostly based on Bayesian Networks), for safety and security barriers technical performance assessment are illustrated and compared, with particular mention to cascading events prevention within the chemical industry domain.

3.3.2.1 Performance assessment for safety measures

3.3.2.1.1 Conventional methodology for safety measures performance assessment

At the present time, conventional quantitative assessment of safety barriers performance with respect to major accident prevention is largely based on Event-Tree Analysis, representing the right side of Bow-Tie diagram. Event-Tree is a probabilistic model that correlates a top event with its outcomes, or consequences. It illustrates, from a qualitative and quantitative perspective, the logical relationships present in the system and indeed, it helps understanding which safety barriers failures would escalate the top event to a certain consequence (De Dianous and Fiévez, 2006).

The construction of an Event-Tree starts from the identification of credible scenarios, by means of past-accident data review (Delvosalle et al., 2006). Then, the identification and detailed description of pertinent safety barriers with respect to the specific operational context should be carried out. In this phase, the relations among the elements present in the system should be investigated both qualitatively and quantitatively. In particular, the latter aspect aims at determining the performance of safety barriers.

Generally, only the availability is accounted as a measure of safety barriers performance (i.e., expressed by the probability of failure on demand – PFD). The values of PDF can be either retrieved by technical literature or calculated by means of conventional techniques, as Fault-Tree analysis (Khakzad et al., 2013b). Eventually, the potential accident sequences and safety barriers contributions are outlined by the calculation of final events frequencies (or probabilities), according to the following equation:

$$f_{FE\_i} = f_{Top\_Event} \cdot \prod_{i=1}^{n} PFD_i = f_{Top\_Event} \cdot P_{Cons,i} \quad (3.7)$$

Where f_{FE_i} is the frequency (or probability) of a final state i, obtained by multiplying the top event frequency (or probability) (i.e., f_{Top_Event}) with the n failure probabilities of the safety barriers (i.e., PFD_i) leading to that consequence, whose probability is $P_{Cons,i}$.

3.3.2.1.2 A recent methodology for quantitative safety measures performance assessment in the prevention of domino escalations

Recent applications stressed the importance of quantitative safety barriers performance assessment, by means of Event-Tree based analysis, in the context of cascading effects prevention, for instance regarding domino accidents (Janssens et al., 2015; Landucci et al., 2015a). Recently, the contribution by Landucci et al. (Landucci et al., 2015a) proposed a novel approach to quantitative safety barriers performance assessment in the prevention of domino escalations triggered by fires. The approach is based on the conventional Event-Tree tool, but it includes specific gates to quantitative evaluate all categories of barriers performance (i.e., active, passive and procedural ones), in reducing escalation probability. Therefore, the procedure allows defining final events probabilities and eventually domino scenario frequency. A flowchart of the methodology is reported in Figure 3. 5.

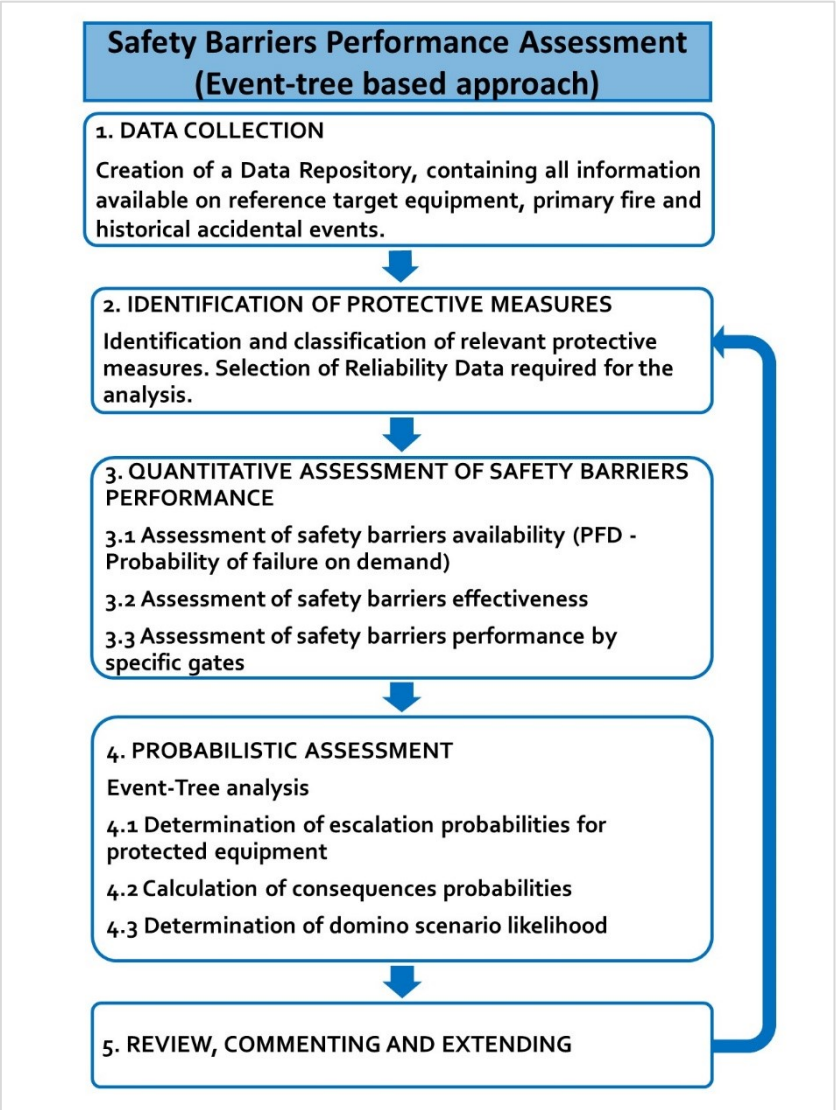


Figure 3. 5 Methodology for quantitative assessment of safety barriers performance in the prevention of domino accidents, triggered by fire. Figure adapted from Landucci et al. (Landucci et al., 2015a).

After the creation of a specific data repository (i.e., according to step 1), the procedure requires the identification and classification of safety measures in place (i.e., step 2). Therefore, three main categories of Reference installations are identified:

- Refinery tank farms (RI. 1)
- LPG storage facilities (RI. 2)];
- Offshore Oil&Gas (O&G) rigs for hydrocarbon extraction (RI. 3)

For each RI identified, possible target equipment (i.e., RTE) for domino escalation and safety measures in place are identified and summarized in Table 3. 12.

Table 3. 12 Summary of safety barriers considered for each Reference Installation, according to Landucci et al. (Landucci et al., 2015a). Symbols: *PSV*= Pressure safety valve; *ESD* = Emergency Shut Down system; *EDP* = Emergency Depressurization System; *PFP* = Passive Fire Protection with fireproofing material. * not considered in the quantitative assessment.

RI	RTE description	RTE	Active Protection Systems		Passive Protection Systems		Procedural/ Emergency measures
RI.1	Floating roof diameter > 60 m	T.1	*Foam-water sprinkler system* *Semi-fixed Foam System * + Fixed Water Spray**	*Rim seal by foam flooding**	*PSV*	-	*Emergency team*
	Floating roof diameter > 30 m Fixed roof Diameter > 20 m	T.2	*Foam-water sprinkler system or* *Semi-fixed Foam System* + Fixed Water Spray**	-	*PSV*	-	*Emergency team*
	Floating roof diam. <30 m Fixed roof diam. < 20 m	T.3	*Semi-fixed foam injection system**	-	*PSV*	-	*Emergency team*
RI.2	Abovegroud pressurized vessel	V.1	*Water Spray system*	-	*PSV*	*PFP (2h rating)*	*Emergency team*
	Mounded pressurized vessel	V.2	-	-	*PSV*	*PFP (2h rating)*	*Emergency team*
RI.3	Horizontal separator	S.1	*Object specific deluge*	*ESD&EDP system*	*PSV*	*PFP (2h rating)*	-
	Condensate treaters	S.2	*Area deluge*	*ESD&EDP system*	*PSV*	*PFP (2h rating)*	-

Then, the third step of the methodology requires performing quantitative safety barriers performance assessment. According to the mentioned approach, the performance of a safety barrier is represented by a combination of availability and effectiveness:

- *Availability* is defined as the probability of failure on demand (i.e., PFD) of the safety barriers;
- *Effectiveness* is defined as the probability that the safety barrier, even if successfully activated, will be able to prevent the escalation.

The performance of a safety barrier can be described by the following specific gates, reported in Figure 3. 6 (Landucci et al., 2015a); the upper branch of each gate (i.e., OUT 1) indicates the failure state. Its probability is the failure probability of the barrier, by combining its availability, expressed as probability of failure on demand (i.e., PFD_i), and its effectiveness (i.e., η). All possible outputs from the same gate are mutually exclusive. The three possible typologies of gates are:

- A simple composite probability (gate type A): availability, expressed as the probability of failure on demand, is multiplied by a single probability value expressing the probability of barrier success in the prevention of the escalation. OUT 1 indicates the failure (i.e., unavailability) of the barrier, OUT 2 indicates the success of the barrier (i.e., available and with $\eta = 1$);
- A composite probability distribution (gate type B): availability, expressed as the probability of failure on demand, 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 indicates the failure (i.e., unavailability) of the barrier, OUT 2 indicates the success of the barrier (i.e., available, with $\eta \neq 1$);
- A discrete probability distribution (gate type C): depending on barrier effectiveness, three or more events may originate from the gate describing barrier performance: barrier success (e.g., OUT 3, no escalation), barrier failure (e.g., OUT 1, unmitigated escalation), and one or more partially mitigated scenarios (e.g., OUT 2, partial or delayed escalation).

From a general point of view, gate type A is applied for passive safety measures, gate type B for active safety measures and gate type C for procedural safety measures, but there are exceptions. For instance, gate type A is applied for Water Deluge System (i.e., *WDS*), Pressure Safety Valve (i.e., *PSV*), Fireproofing coating (i.e., *PFP*) and Emergency shutdown system (i.e., *EDS*). Gate

type B is applied for Foam-Water sprinkler system (i.e., *Sprinkler*), gate type C is applied for Emergency intervention (i.e., *Em_Team*).

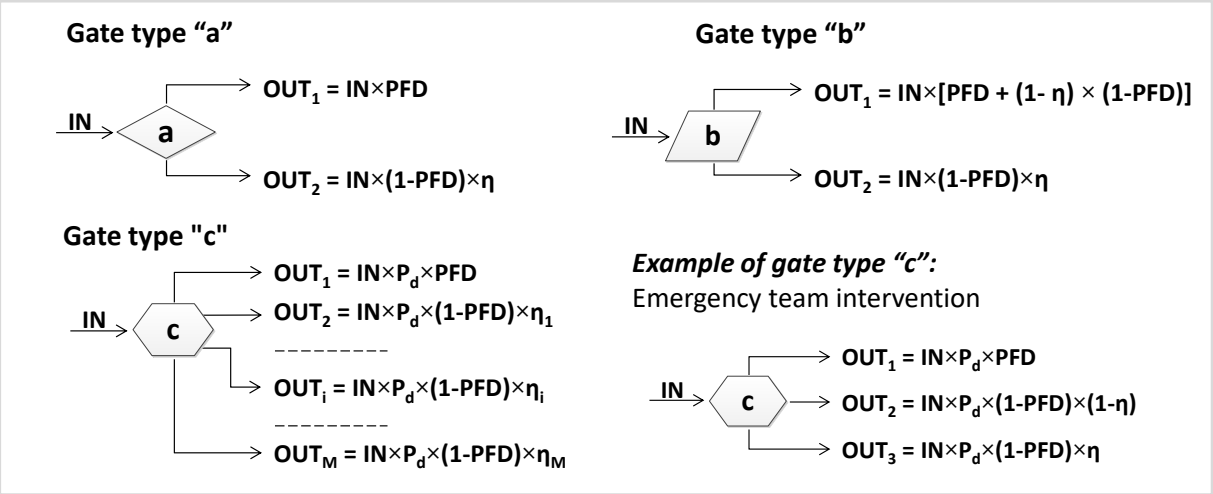


Figure 3. 6 Gates for safety barriers performance, accounting both availability and effectiveness (Landucci et al., 2015a).

Then, according to step 4, the Event-Tree based approach is applied. Escalation probability values (P_d), are calculated depending on safety barriers states, defined by Event-Tree branches. Three different procedures are outlined for active, passive and procedural measures respectively.

For active measures, two specific approaches are available for sprinkler and WDS. For a sprinkler, a gate type B is applied, with $\eta = 0.954$. A WDS is represented by a gate type A; in case of available WDS system, a reduced heat load (Q_{WDS}) should be obtained as follows:

$$Q_{WDS} = Q_{HL} \cdot \varphi \tag{3.8}$$

Where Q_{HL} is the full heat load value $[Q_{HL}] = \left[\frac{kW}{m^2}\right]$ which can be reduced, according to an adimensional intensity reduction factor φ of 0.5 when the safety barrier is available; else way φ is equal to 1. In case of WDS availability, η is unitary.

Passive safety measures are generally represented by a gate type A. Concerning availability, passive fire protections (PFP) can be considered as single components, with PFD values can be derived from literature. Concerning fireproofing effectiveness, this parameter identifies the degree by which the target resistance is enhanced due to PFP presence: the higher the *ttf* (i.e., time to failure) of the target is, the more effective the PFP. In case of failure of PFP system (e.g. upper output branch of the gate – OUT 1), the *ttf* value can be estimated as a function of the heat load by the following formula:

$$ttf = 0.0167 \cdot e^{\left(cV^d + \ln Q_{HL} + f\right)} \tag{3.9}$$

In which *ttf* is expressed in minutes, Q_{HL} is the heat load, which may be substituted by Q_{WDS} in presence of effective activation of WDS system, V is the vessel volume (m^3) and the coefficients (c, d, f) depend on types of process and storage equipment.
In case of availability of PFP barrier (e.g., lower output branch of the gate – OUT 2) an effectiveness value equal to 1 is considered, adding a further term (namely ttf_c) to the *ttf* estimated for the unprotected vessel as follows:

$$ttf_P = ttf + ttf_C \tag{3.10}$$

Where ttf_p is the time to failure in presence of thermal protection. A simplified assessment of ttf_c is proposed herein; a ttf_c value of 70 minutes is considered if PFP is available and effective.

For what concerns procedural measures, emergency response can be provided by internal and/or external emergency teams. These teams can be composed of experts or fire-fighters as well as of volunteers or workers who receive a specific training. Three reference times were defined and associated to the emergency operations for a given industrial facility:

- *tta* (*time to alert)*: maximum time required to start the emergency operations, defined as the time needed for the fire to be detected and the alarm to be given;
- *tsm* (*time to on-site mitigation)*: maximum time required to start the pre-planned response actions to be put in place by personnel and with resources available on site, defined as the time needed to start the pre-planned operations to contain the fire hazard or mitigate its impact (e.g. start of the emergency water deluges, gathering and deployment in the fire area of mobile firefighting equipment, start of water cooling and/or fire control operations by using fire-fighting water reservoir or tap water network);
- *tfm (time for final mitigation)*: characteristic time of an effective intervention of external emergency teams, defined as the maximum time required by the external emergency team to provide and keep constant, by means of suitable equipment and vehicles, the amount of water which is required for primary fire suppression or effective cooling action on the target.

In order to establish the value of barrier effectiveness and to quantify the escalation Event-Tree, the *tfm* value (i.e., time for final mitigation) is compared to the *ttf* of each target. The *tfm* is calculated as the sum of different contributions, according to procedure specific for the Reference Installation, provided by Landucci et al. (Landucci et al., 2015a). The gate type C is used in the escalation event tree for procedural barriers involving emergency team intervention. The following three alternative outputs were identified:

- OUT_1: if the emergency response is not activated or not available, the escalation will occur;

- OUT_2: if the emergency response is activated but *tfm* results higher than *ttf*, emergency team is not effective since required actions will come too late to prevent escalation (η=0), a mitigated escalation scenario will occur;
- OUT_3: if the emergency response is activated and *tfm* is lower than *ttf*, the mitigation action is successful and the fire escalation will be prevented (η=1).

It should be noted that availability values can be either retrieved from technical literature, or calculated (only in case of active safety barriers) by means of Fault-Tree Analysis.

At this stage, the values of associated escalation probability $(P_{d,i})$, corresponding to each final state of the Event-Tree can be calculated according to equation (3.2) and equation (3.4). The probability of each consequence $(P_{Cons,i})$ can be defined by multiplying the performance probabilities of all safety barriers leading to that specific consequence, according to Section 3.3.2.1.1. Final event probability $(P_{FE,i})$ for each final state *i* can be calculated as follows:

$$P_{FE,i} = P_{d,i} \cdot P_{Cons,i} \tag{3.11}$$

Then, final events frequencies can be calculated $(f_{FE,i})$ as follows:

$$f_{FE,i} = f_{PE} \cdot P_{FE,i} \tag{3.12}$$

Where f_{PE} is the frequency of the primary event.

However, it should be noted that this procedure has been applied only to a first level domino and to a simplified case study; moreover, it is based on a conventional static methodology (i.e., Event-Tree).

3.3.2.1.3 Dynamic safety measures performance assessment and domino accident analysis methodologies

Despite the popularity of Event-Tree based approach within the process industry, the methodology shows several limitations. For instance, Event-Tree cannot include multi-state variables, cannot represent conditional dependencies and cannot apply real-time information from a facility to update prior "beliefs", which are prior probabilities of top events, intermediate events and safety barriers (Khakzad et al., 2013b). These limitations hinder from obtaining a real-time picture of safety barriers performances and final consequences probabilities, therefore offering just a static risk picture, which is not able to account systems modifications and information derived from operational experience. Therefore, dynamic risk assessment techniques are increasingly developed within the chemical and process industry domain; as described in Section 2, Bayesian Networks are promising techniques to be applied within major accidents and cascading events prevention.

3.3.2.1.3.1 Fundamentals of Bayesian Analysis technique

As discussed in Section 2.4.1, Bayesian Analysis technique is the first complete dynamic risk assessment procedure, developed by Kalantarnia et al. (Kalantarnia et al., 2010, 2009), which is widely applied and established. Therefore, a summary of its 5 key steps is available in Section 2.4.1. Indeed, the mathematics fundamentals, necessary to apply the procedure to case studies in Section 5, are described in the current subsection. The procedure starts in Step 0 from the retrieval of existing accident precursors data (i.e., ASP), either from the same installation, the same reference sector, or to contiguous ones.

Then, in Step 1, the potential scenarios, their causes, consequences and related safety barriers are identified by means of a conventional Risk Assessment tool (e.g., Bow-Tie analysis or Event-Tree analysis). This step provides a visual representation of consequences, causes and related safety barriers in place to mitigate or control the hazards.

Step 2 is aimed at calculating the prior failure probability function for each barrier. The prior failure function of each barrier represents our understanding of it prior to the start of operation. Different typologies of probability density function can be selected to represent the failure probability of a safety barrier (e.g., Beta, Gamma) (Vose and Rowe, 2000), termed as $f(x)$, where x is the failure probability of the safety barrier. Each function is characterized by two parameters (i.e., α and β) and can be expressed by the following formula:

$$f(x) \propto x^{\alpha-1}(1-x)^{\beta-1} \tag{3.13}$$

Then, the prior probabilities or frequencies of occurrence of each final state of the Event-Tree are calculated according to equation (3.7). Two approaches are available, for instance, deterministic and probabilistic one. According to the deterministic approach, the value of each end state can simply multiply the probabilities of each branch related to the state, according to the second member from the left of equation (3.7). According to the probabilistic approach, the median value of the selected probability distribution is accounted as failure probability of the safety barrier for the calculation of prior final states probabilities, according to the latter member of equation (3.7).

In step 3, the likelihood function is created $\left(g(Data|x)\right)$. This function is formed using real time data from the process as it operates, according to the following equation:

$$g(Data|x) \propto x^{\gamma}(1-x)^{\delta} \tag{3.14}$$

Where γ and δ are the revised parameter of the likelihood function. These data are inferred from the ASPs and are specific numbers within a discrete domain, which is best presented by a binomial distribution. Many approaches exist for selecting likelihood functions. The most

convenient in the present framework is to use the conjugate pair of the prior function (Kalantarnia et al., 2010).

In step 4, the posterior function ($f(x|Data)$) is calculated; this probability revising technique is often termed as Bayesian adapting. The posterior failure function of the safety barrier has been obtained from the prior and likelihood functions using Bayesian inference. Bayesian inference is a tool which uses data to improve an estimate of a parameter. The posterior function is the same distribution type as the prior (Beta), but the parameters are updated trough the likelihood function. Thus, the posterior function can be derived as follows:

$$f(x|Data) \propto g(Data|x) \cdot f(x) \propto x^{\alpha-1}(1-x)^{\beta-1}x^{\gamma}(1-x)^{\delta} \propto x^{\alpha+\gamma-1}(1-x)^{\beta+\delta-1} \quad (3.15)$$

Where x is the failure probability of the barrier, $f(x)$ is the probability distribution function (prior distribution), $f(x|Data)$ is the posterior distribution and $g(Data|x)$ is the likelihood function; $(\alpha+\gamma)$ and $(\beta+\delta)$ are the two parameters of the posterior distribution.

The last step of the methodology is the consequence analysis, carried out on the scenario in order to estimate the revised frequencies (or probabilities) of occurrence of final states, according to the equation (3.7), by inserting the posterior failure function in the equation, to describe each safety barrier performance.

In Section 5.2.2, some relevant existing applications of the methodology are proposed in purpose to show how it can be put into practice. However, it should be noted that Dynamic Risk assessment methodology, especially in case of complex systems, is particularly laborious.

3.3.2.1.3.2 Fundamentals of Bayesian Networks and Limited Memory Influence Diagrams

Among several existing approaches, Bayesian Networks (BNs) have emerged. The most relevant advantage of BNs is that they provide a useful tool to deal with uncertainties and information from different sources, such as expert judgment and observable experience, being able to take into account common causes and influences of human factors as well (Ale et al., 2014). Bayesian Networks are also known as Bayesian Belief Networks (BBNs), Causal Probabilistic Networks, Causal Nets, Graphical Probability Networks, Probabilistic Cause-Effect Models, Directed Acyclic Graphs and Probabilistic Influence Diagrams (Haugom and Friis-Hansen, 2011).

Bayesian Networks (BNs) are a graphical representation of uncertain quantities and decisions that explicitly reveal the probabilistic dependence between the variables and the related information flow. In BNs, variables and their relations are represented by means of nodes and directed arcs; conditional probability tables (CPTs), assigned to the nodes, represent conditional dependencies.

The arcs denote direct dependencies or cause-effect relationships between linked nodes, whereas conditional probabilities assigned to the nodes determine the type and strength of such dependencies. In other words, a BN is defined by a qualitative part and a quantitative part. The qualitative part consists of a set of nodes which represents the system variables, and a set of directed arcs between variables, representing the dependencies or the case-effect relations between variables. The quantitative part consists of conditional probability distributions for each node, given the states of the influencing nodes, called also parent nodes.

Together, the quantitative and qualitative parts encode all the relevant information about the system variables and their interrelations, which, mathematically, means the joint distribution of these variables.

Therefore, according to Jensen and Nielsen (Jensen and Nielsen, 2007), under the assumption of conditional independence, a BN represents the joint probability distribution *P(U)* of variables $U = \{A_1, \dots, A_n\}$, as described by the following equation:

$$P(U) = \prod_{i=1}^{n} P\left(A_i | Pa(A_i)\right) \tag{3.16}$$

Where $Pa(A_i)$ is the parent set of A_i. Indeed, a BN expands the joint probability distribution of a set of linked nodes. Considering local dependencies, BN factorizes the joint probability distribution of a set of random variables as the multiplication of the conditional probabilities of the effect nodes given their direct cause nodes.

To better understand the reasoning, let's consider the joint probability distribution of the random variables *A*, *B*, *C*, and *D* in the BN of Figure 3. 7, which is exclusively expanded as (Khakzad et al., 2013d):

$$P(A, B, C, D) = P(A) \cdot P(B \mid A) \cdot P(CA) \cdot P(D \mid B, C) \tag{3.17}$$

In this way, instead of working with a large joint probability distribution, one can work with smaller pieces of it, but preserving the overall component interaction within the system.

Accordingly, the marginal probability of each random variable, for example *C*, can be calculated via marginalization as:

$$P(C) = \sum_{A,B,D} P(A, B, C, D) \tag{3.18}$$

The main application of BN the use of probability revising techniques. BN applies Bayes theorem to revise the prior probabilities of random variables given new information (i.e., called evidence) to render posterior or updated probabilities. For example, knowing that the random variable *D* is in state *d* (i.e., evidence), the revised probability of *A* being in state *a* can be calculated as (Khakzad et al., 2013e):

$$P(A = a \mid D = d) = \frac{P(A=a, D=d)}{P(D=d)} = \frac{\sum_{B,C} P(a,B,C,d)}{\sum_{A,B,C} P(A,B,C,d)} \tag{3.19}$$

Indeed, Bayesian Networks allows taking into account new evidences and consequently modifying probability distributions, by means of two different probability-revising techniques, which are Bayesian Analysis techniques. In fact, Bayesian analysis can be performed through probability updating and probability adapting techniques.

Probability updating consists in the calculation of the Most Probable Explanation (i.e., MPE), which is the most probable state of all the variables (i.e., most probable configuration), given the accident occurrence (i.e., evidence), according to the following formula (Bobbio et al., 2001; Khakzad et al., 2011):

$$P(most\ likely\ configuration) = \frac{P(most\ likely\ configuration, evidence)}{P(evidence)} \tag{3.20}$$

Therefore, probability updating calculates the posterior probability of event x_i given a certain state of event Q, i.e. $P(x_i|Q)$. Probability adapting consists in the calculation of posterior probability for a generic event x_i, given another event Q has occurred n times, which can be expressed in statistical terms as $P(x_i|Q = n)$. Therefore, probability adapting means applying prior experience, in the form of additional information collected during a certain time span, named Accident Sequence Precursors (i.e., ASP), to adapt conditional probabilities distributions, and therefore, to revise final events probabilities and safety barriers performance over time.

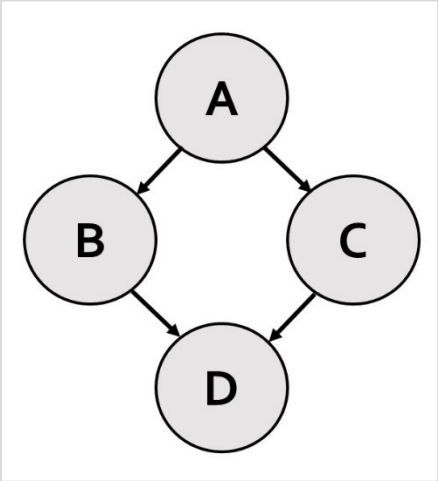


Figure 3. 7 Example of Bayesian Network; this modelling technique includes both qualitative and quantitative features. A, B, C, D are random variables.

From a general point of view, the principal steps in application of Bayesian theory include (Weber et al., 2012):

1) Specifying a probability model for unknown parameter values that includes prior knowledge about the parameters, if available;

2) Updating knowledge about the unknown parameters by conditioning this probability model using observed data;
3) Evaluating the goodness of the conditioned model with respect to the data and the sensitivity of the conclusions to the assumptions in the probability model.

Up to now, three different versions of BBNs have been applied successfully to the description of complex real systems, which need to be represented by non-linear non-deterministic models. These versions are Discrete Bayesian Belief Nets, Gaussian Bayesian Belief Nets and Non-parametric BBNs (NPBBNs); the main differences consist of the mathematical functions and input-data; the most applied typology that will be applied in the following case studies, is Discrete Bayesian Belief Net (Weber et al., 2012).

Eventually, the main advantages of Bayesian methods and applications with respect to major accident and cascading events prevention have been summarized in the attached list (Khakzad et al., 2013e):

- Probability updating, using real-time information.
- Flexible structure, with possibility to develop specific sub-models.
- Transparency and intuitiveness, due to graphical appearance, may be suitable in purpose to involve non-expert people in important decisions (e.g. stakeholders).
- Quantitative technique, by applying conditional probabilities, with the benefits of a qualitative one.
- Complex events description, with the ability to incorporate multistate variables and common cause failure.

Bayesian Techniques offer the advantage of evaluating various decision alternatives and the utilities associated with these.

To some extent it is possible to construct a model for decision making with a pure BN (as the one just described), but the concepts of utility and decisions are not explicitly covered.

A limited memory influence diagram (LIMID) is simply a Bayesian Network, extended with utility nodes and decision nodes, which makes a suitable tool for operational safety decision-making (e.g., suitable to define selection criteria for a safety barrier). The other nodes are renamed in influence diagrams as “chance nodes”.

Therefore, utilities are associated with the state configurations of the network. These utilities are represented by utility nodes. Each utility node can be either represented by direct values or by utility values. In the latter case, a utility function that associates to each configuration of

states its parents is applied; an example of utility function can be following one (Reniers and Van Erp, 2016):

$$U_i = 1 - \frac{x_i - x_{max}}{x_{max}} \tag{3.21}$$

Where U_i is the utility value, obtained from the direct value (x_i), with respect to the constraint present (i.e., x_{max}, expressing for instance the maximum budget/cost).

By making decisions, the analyst influences the probabilities of the configurations of the network. Therefore, it is possible to compute the expected utility of each decision alternative and the global utility function is the sum of all the local utility functions. The choice will be on the alternative with the highest expected utility; this is known as the maximum expected utility principle.

The "Limited Memory" prefix indicates that this kind of diagrams relaxes two fundamental assumptions of the traditional influence diagram: the non-forgetting assumption and the total order on decisions. Relaxing the non-forgetting assumption and the total order on decisions implies a significant change in the semantics of a LIMID compared to a traditional influence diagram. In a LIMID it is necessary to specify for each decision the information available to the decision maker at that decision. There are no implicit informational links in a LIMID. A link into a decision node specify that the value of the parent node is known at the decision. Each decision in the LIMID has an initial policy which can be defined by the user either manually or using expressions. The initial policy is a table specifying a mapping from configurations of the parents of the decision to states of the decision. This initial policy is updated in the process of solving the LIMID.

Therefore, Bayesian Network and Bayesian analysis share the same fundamental mathematics concepts, as they both derive from Bayes theorem. The main difference is that dynamic risk assessment can be either performed manually, by means of Bayesian Analysis, or with more ease, by means of Bayesian Networks, applying specific software, as Hugin Expert software version 8.1, which offers dedicated tools (Hugin, 2016). Hugin software has been applied in several case studies, regarding Bayesian Networks and LIMID presented in Section 5.

Hugin software version 8.1 can be run in two modes: the "Edit" mode allows building manually the BNs/LIMID, by creating nodes and connecting them with arcs. It is necessary in this step to fill the Conditional Probability Tables/Utility Tables manually. Then, according to the "Run" mode, the net can be compiled and the results of probability propagation are summarized in a probability output panel. Probability revising techniques can be applied by means of specific tools.

With reference to probability updating, an evidence can be inserted of a node being in a specific state from the probability panel and the net can be recompiled by means a "max propagate

tool", in purpose to identify the weak links leading to that specific final state. With reference to probability adapting, information are inserted manually in a specific adaptation panel and then, the net is run according to the "sum propagation tool".

For instance, the tutorials available in Section 5.2.2 for BNs and LIMID explain the tools of the software that are useful with reference to safety barriers performance assessment.

3.3.2.1.3.3 Methodologies for conversion of conventional methodologies into Bayesian Networks

3.3.2.1.3.3.1 Mapping a Fault-Tree into a Bayesian Network

Nowadays Fault-Tree Analysis (FTA) is a widely applied methodology in the field of risk assessment for process systems and fault diagnosis. FTA aims at determining the potential causes of an undesired event (top-event); a downward approach allows linking the top event (placed at the top of the tree) to primary events. FTA can be applied also to determine the probability of failure on demand of a safety barrier. However, FTA suffers of some relevant limitations:

- Primary events are considered binary (with two states – work/fail) and statistically independent.
- Relations between events are generally represented AND-gates and OR-gates.
- Redundant failures and common cause failures cannot be accounted.
- Necessity to determine minimal cut-sets of events.

Khakzad et al. (Khakzad et al., 2011) proposed a mapping algorithm from Fault–Tree to Bayesian Network, originally developed by Bobbio et al. (Bobbio et al., 2001), that includes graphical and numerical steps, represented in Figure 3. 8.

In graphical mapping, primary events, intermediate events, and the top event of the FT are represented as root nodes, intermediate nodes, and the leaf node in the corresponding BN, respectively. The nodes of a BN are connected in the same way as corresponding components in the FT.

In numerical mapping, the occurrence probabilities of the primary events are assigned to the corresponding root nodes as prior probabilities. For each intermediate node as well as leaf node, a conditional probability table (CPT) needs to be developed (Martins et al., 2014). The CPTs should be developed according to the type of gate, as reported in Figure 3. 9. Eventually in a BN the equivalent versions of OR and AND - Gates differ only for CPT, while the graphical aspect is exactly the same one.

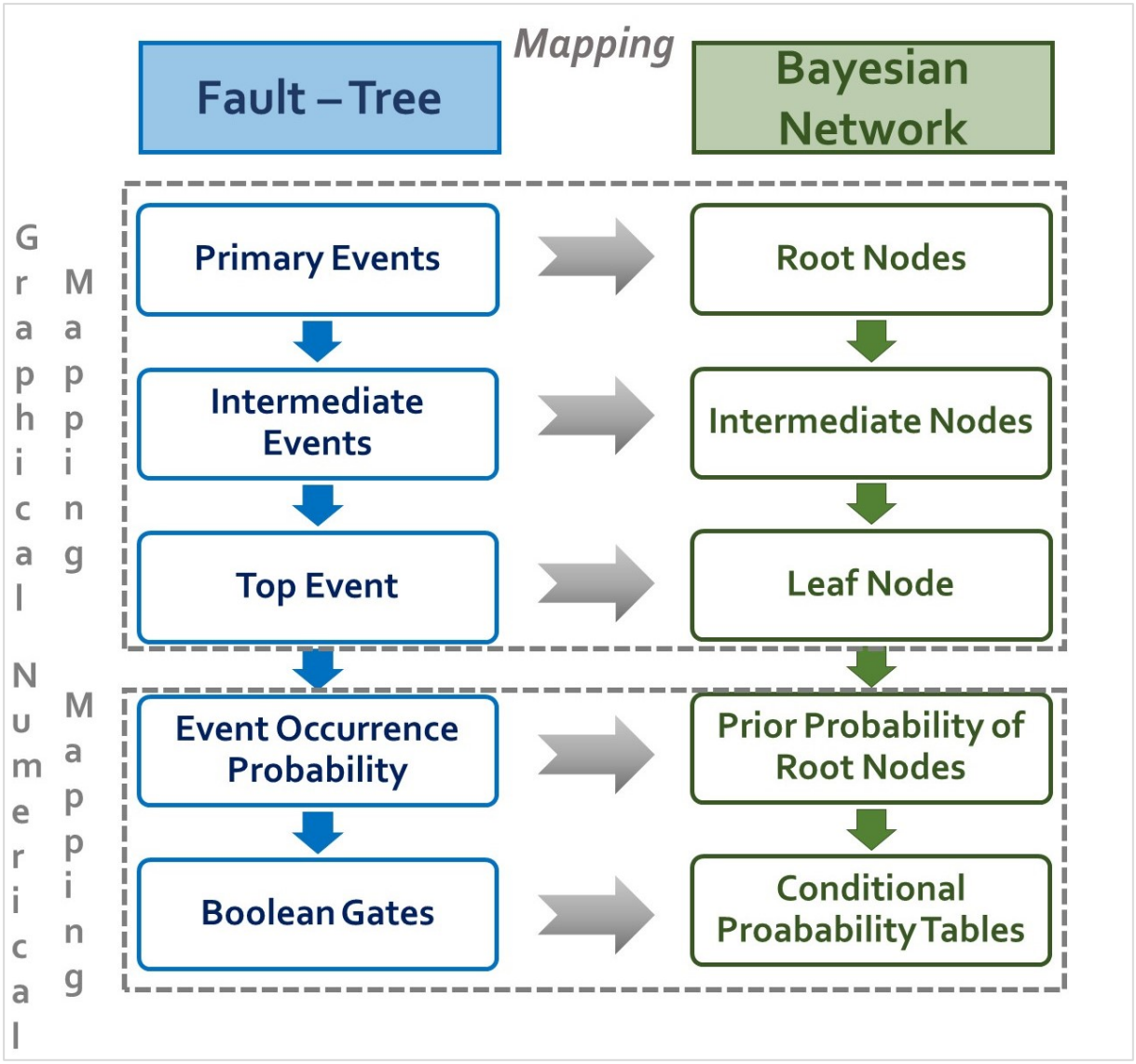


Figure 3. 8 Mapping algorithm of Fault-Tree into Bayesian Network, as developed by Khakzad et al (Khakzad et al., 2011).

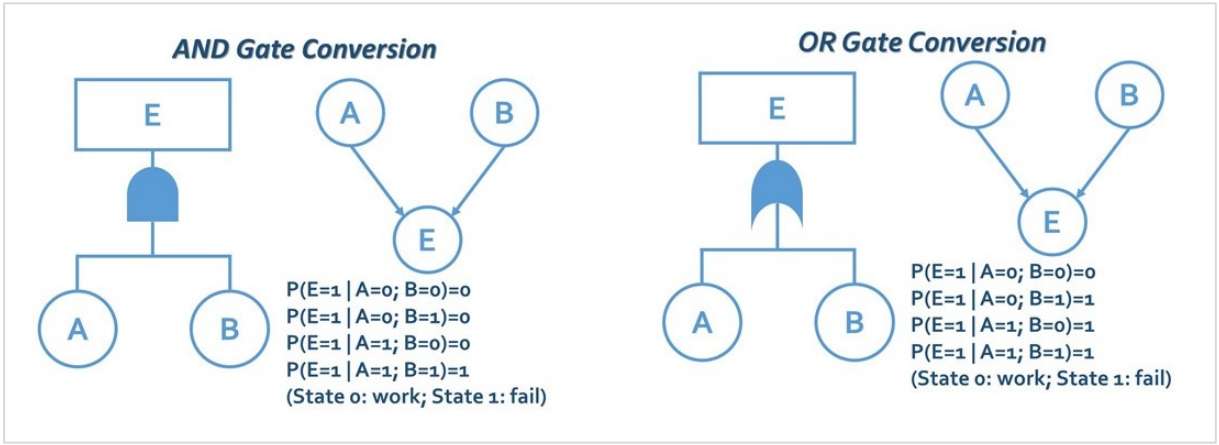


Figure 3. 9 Conversion of AND-Gate and OR-Gate into Bayesian Network.

3.3.2.1.3.3.2 Mapping a Bow-Tie into a Bayesian Network

Bow-Tie (i.e., BT) is a probabilistic cause-consequences model that contains on the left side a fault tree, and on the right side an event tree. It correlates critical events with outcomes, or consequences in general. BT represents a complete accident scenario because, from a qualitative and quantitative perspective, clearly illustrates the logical relationships here-in present and it helps understanding which possible combination of primary events would lead to the top event and which safety barriers failure would escalate the top event to a particular consequence. Nowadays Bow-Tie diagram is a popular tool in Risk Analysis for many chemical companies; however, it suffers limitations that are typical of its constituents (i.e. Fault Tree and Event Tree). To mention the most relevant ones, BT cannot include multi-state variables, cannot represent conditional dependencies and cannot apply real-time information from a facility to update prior "beliefs", that are prior failure probability of primary events and safety barriers. (Khakzad et al., 2013b, 2012) Some studies referred to the chemical process industry domain have recently compared and/or integrated Bow-Tie and Bayesian network methods, or, at least, Bayesian Updating (Ferdous et al., 2013, 2012, Khakzad et al., 2013b, 2012), pointing out the advantages of Bayesian Networks.

Fault-Tree mapping procedure has already been described in the previous subsection. Event-Tree mapping procedure is mainly based on the work of Bearfield and Marsh (Bearfield et al., 2005), a graphical algorithm is presented in Figure 3. 10.

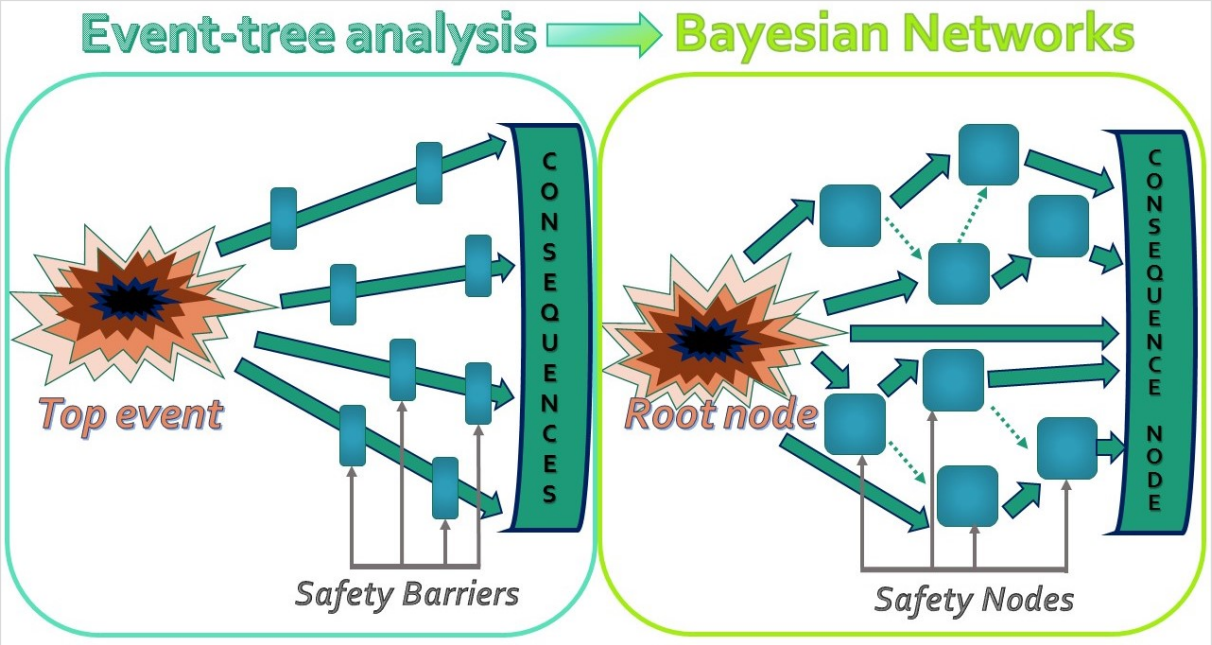


Figure 3. 10 Graphical visualization of the conversion from an Event-Tree into a Bayesian Network (Villa and Cozzani, 2016).

Khakzad et al. (Khakzad et al., 2013b) proposed a complete mapping algorithm from Bow-Tie to Bayesian Network that includes Fault Tree mapping and Event Tree mapping, as represented in Figure 3. 11. Each safety barrier of the Event-Tree is represented by a safety node having two states, one for the failure and the other for the success of the safety barrier; anyway it is possible to consider multi-state variables. Also, a consequence node having as many states as the number of the event tree consequences (i.e.,C_i) should be added to the network. When mapping Event-Tree into BN, a safety node SB_i should be connected to the previous safety node, SB_{i-1}, only if the failure probability of SB_i depends on whether SB_{i-1} has worked or failed. In probabilistic terms, SB_i must be connected to SB_{i-1} only if $P(SB_i|\, SB_{i-1}) \neq P(SB_i|\, \overline{SB}_{i-1})$; in the same way SB_{i+1} must be connected to SB_{i-1} only if $P(SB_{i+1}|\, SB_i, SB_{i-1}) \neq P(SB_i|\, \overline{SB}_{i-1})$. In addition, there must be a connection between each safety node and the consequence node only if the probabilities of the states of the consequence node are influenced by the failure or the success of that safety node. After the BN is constructed, the probabilities of safety barriers are considered as the prior probabilities of safety nodes, and a CPT is assigned to the consequence node, following a AND – Gate logical model. CPTs for intermediate safety nodes are assigned too, as simple causal relations. After the equivalent BNs of the Fault-Tree and the Event-Tree are developed, they are connected to each other via the Top Event as a pivot node. The Top Event node should be connected also to the consequence node, this implies the definition of another state (e.g., "Safe") to the consequence node; this additional state accounts the effect of the non-occurrence of the top event on the consequence node.

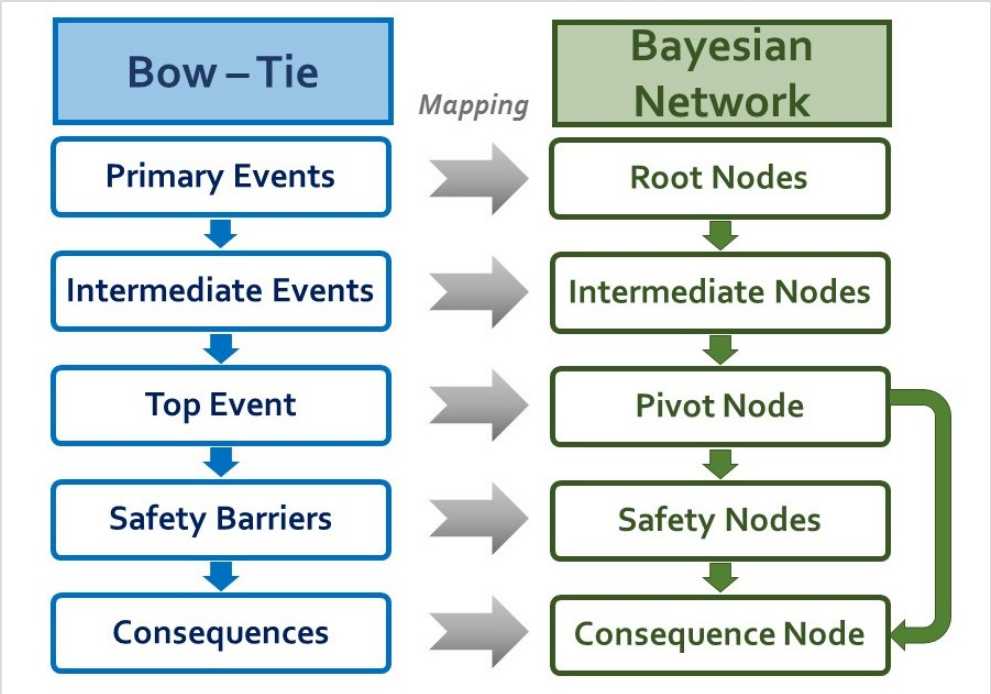


Figure 3. 11 Flowchart representing mapping process from Bow-Tie Diagram to Bayesian Network, adapted from Khakzad et al. (Khakzad et al., 2013b).

Two issues raise from the mapping process:

1) Each BT can be mapped to its corresponding BN, while a BN does not necessarily have an equivalent BT, due to multi-state variables, different causal relationships rather than simple Boolean functions such as OR-gate and AND-gate, and sequentially dependent failures.

2) Although able to consider the dependency of sequential safety barriers, BT cannot capture the conditional dependency of safety barriers on the top event. In other words, in a BT the top event is simply an initiating event for the event tree, and cannot influence the failure or success probability of safety barriers. On the other hand, BN accommodates such dependence by means of causal arcs drawn from the top event to those safety barriers whose failure probabilities depend on the occurrence and non-occurrence of the top event.

3.3.2.1.3.4 Application of Bayesian Networks to domino accident analysis

Khakzad et al. (Khakzad et al., 2013d) applied Bayesian Networks to domino accident modelling and prevention, by developing a specific methodology for the propagation pattern, whose flowchart is reported in Figure 3. 12; the methodology is described in the current section. To model the likely propagation path of domino effect, expressing the core of the BN, the following steps are taken:

1. According to the layout of the plant, a node is assigned to each unit (e.g., storage tank). Each unit is either susceptible to the accident or capable of escalating the accident. The example of a plant layout with six units (*Xi*, with i ranging from 1 to 6), reported in Figure 3. 13, is taken to explain the procedure.
2. The primary unit where the domino accident is likely to start is determined (e.g., *X1* in Figure 3. 13), by considering reasonable occurrence probabilities and enough inventory of hazardous materials to produce credible escalation vectors should be taken into account when choosing the primary unit.
3. According to the type of possible accident scenarios in the primary unit, the escalation vectors transmitted by the primary unit to nearby units are specified and calculated.
4. 4.1: Based on a comparison between predefined threshold values and escalation vectors, those nearby units for which the received escalation vectors exceed the threshold values are defined as potential secondary units (e.g., *X2, X3*, and *X4* in Figure 3. 13).
   4.2: In the case of fire or explosion, the probit values (*Y*) are calculated for the potential secondary units, according to equation (3. 1).
   4.3: Using the Probit values, the escalation probability of potential secondary units given the primary event, i.e., $P(X2|X1)$, $P(X3|X1)$, and $P(X4|X1)$.

4.4: Among the potential secondary units, the one(s) with the highest escalation probability is chosen as the secondary unit (for example, *X3* in Figure 3. 13). Because the secondary events are caused by the primary event, a causal arc must be directed from *X1* to *X3*, showing that the occurrence of *X3* is conditional on the occurrence of *X1*.

5. Given damaged secondary units, potential accident scenarios and their occurrence probabilities for the secondary units are specified.
6. Substituting the secondary units for the primary unit, steps 3 to 5 are repeated to determine potential tertiary units (e.g., *X2* and *X4*), potential quaternary units (e.g., *X5* and *X6*), and so forth. In this case, it has been assumed because *X2* and *X4* (*X5* and *X6*) have the same escalation probabilities, they both are selected as tertiary units.

By repeating the same procedure, synergistic effects should be considered. For example, in Figure 3. 13, *X2* and *X3* coooperate with each other (i.e., their escalation vectors are superimposed) to trigger an accident in *X5*. So, causal arcs have to be directed from *X2* and *X3* to *X5*, showing the conditional dependency of the latter on the former units. Accordingly, when assigning the CPT of *X5*, the escalation probability of *X5* is *P(X5|X2, X3)*, calculated by implementing a noisy OR-gate.

At that point, the propagation pattern is defined. According to the layout in Figure 3. 13, three levels of domino, indicated respectively by $DL1$, $DL2$ and $DL3$ should be added, as three nodes to the BN. The probability of first level domino can be expressed by the following:

$$P(DL1) = P(X1) \cdot P(X3|X1) \tag{3.22}$$

So, *DL1* is connected to *X1* and *X3* by AND-gate causal arcs and *P(DL1)* will be equal to the probability of the first-level domino effect. This implies that for the first-level domino effect to occur, not only the primary event *X1*, but also the secondary event *X3* is needed.

Similarly, the domino effect could proceed to the second level only if at least one of the tertiary units *X2* and *X4* is impacted by the first-level domino accident. Therefore, the probability of the second-level domino effect can be computed as follows:

$$P(DL2) = P(X1) \cdot P(X3|X1) \cdot P(X2 \cup X4|X1, X3) \tag{3.23}$$

An auxiliary node, named $L1$, is added to the net, such that $L1 = X2 \cup X4$; so *X2* and *X4* are connected to $L1$ and the CPT is filled with an OR gate. Then, causal arcs are drawn from $L1$ and $DL1$ to $DL2$; the CPT of $DL2$ is filled with an AND gate to obtain $P(DL2)$.

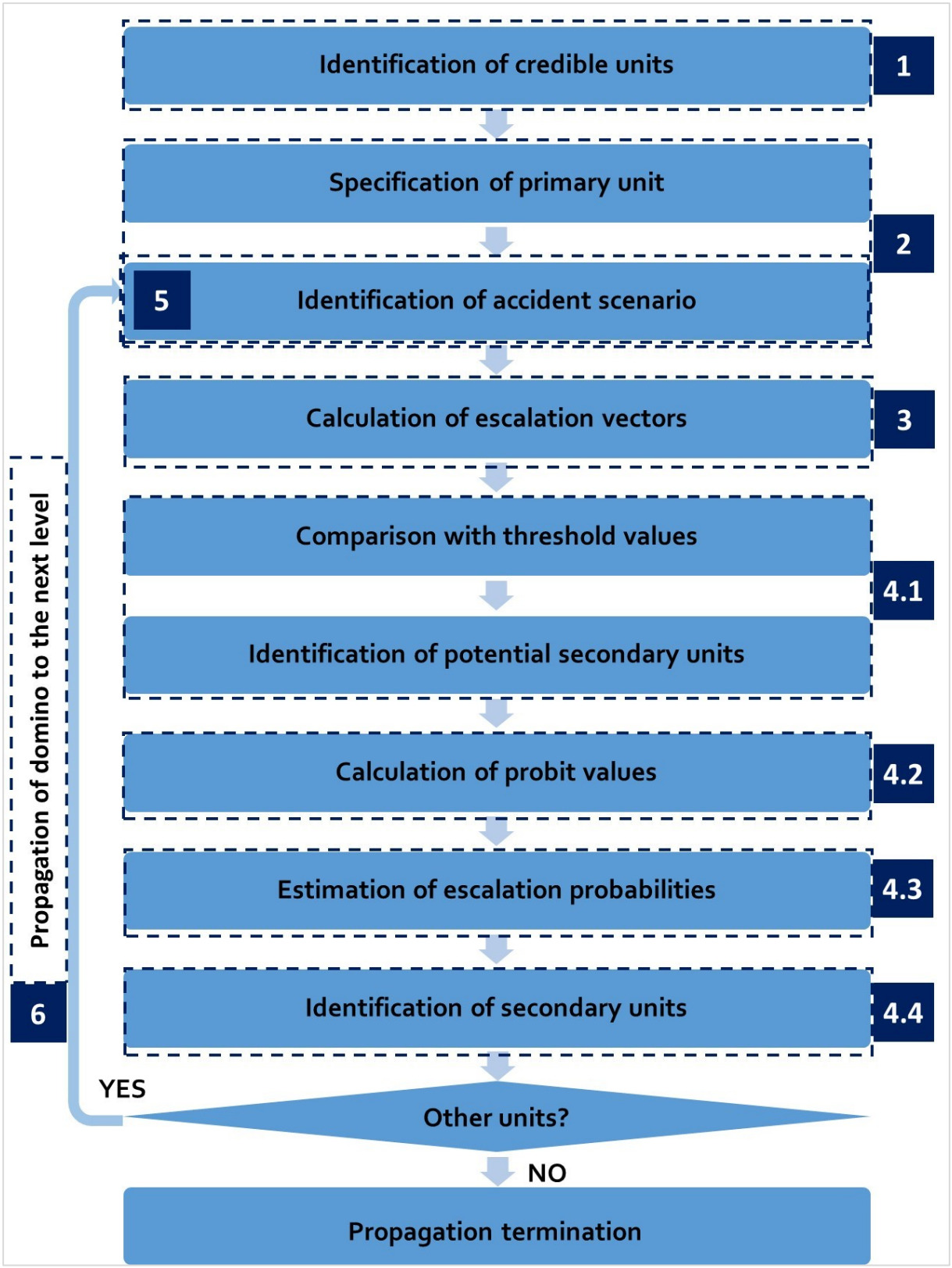


Figure 3. 12 Procedure to develop the propagation pattern to domino effect, adapted from Khakzad et al. (Khakzad et al., 2013d)**.**

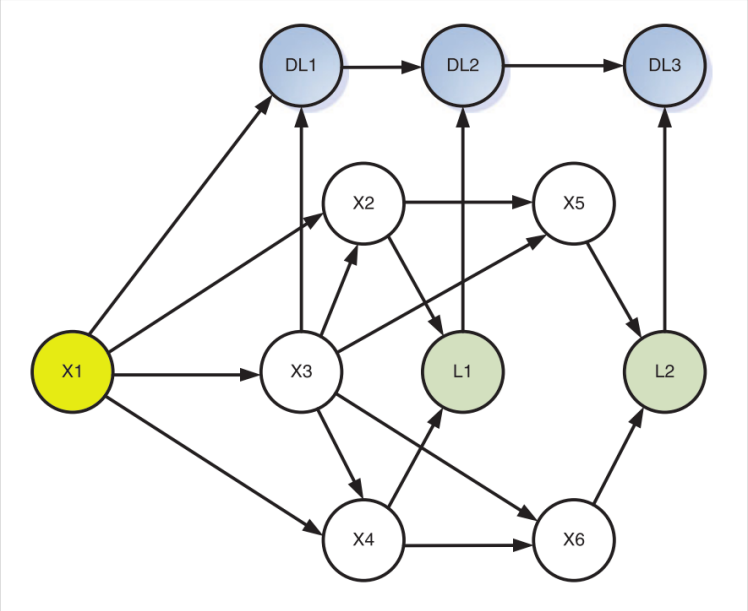


Figure 3. 13 BN to explain the propagation pattern and occurrence probability estimation for domino effect, according to Khakzad et al. (Khakzad et al., 2013d).

Then, the domino effect can proceed to the third level. According to the layout considered, either $X5$ or $X6$ has to be impacted by the second-level domino effect to have a third-level domino effect. In this way, the probability of the third-level domino effect is:

$$P(DL3) = P(X1) \cdot P(X3|X1) \cdot P(X2 \cup X4|X1, X3) \cdot P(X5 \cup X6|X2, X3, X4) \quad (3.24)$$

An auxiliary node, named $L2$, is added to the net, such that $L2 = X5 \cup X6$; so $X5$ and $X6$ are connected to $L2$ and the CPT is filled with an OR gate. Then, causal arcs are drawn from $L2$ and $DL2$ to $DL3$; the CPT of $DL3$ is filled with an AND gate to obtain $P(DL3)$.

The same reasoning can be extended to additional domino levels. The described procedure allows a detailed domino accident modelling with the powerful tool of BNs. However, domino probabilities might be overestimated, as safety barriers are not included in the methodology proposed by Khakzad et al. (Khakzad et al., 2013d).

3.3.2.2 Performance assessment for security measures

3.3.2.2.1 Preliminary assumptions regarding security measures performance assessment

The performance of a Physical Protection System (i.e., PPS) is generally expressed by its effectiveness (i.e., η_{PPS}), which expresses the probability of an attacker's path of actions being foiled, deterred or disrupted.

Effectiveness assessment should take into account the complex configuration of detection, delay and response function that compose the PPS; for high-security systems (i.e., as the ones

considered for counter-terrorism) the response is generally assumed to be immediate on-site, so the response force time is part of the PPS effectiveness. The effectiveness of a PPS can be evaluated according to a qualitative or quantitative form. Quantitative analysis is required for protections of assets with unacceptably high consequences of loss, regardless a low probability of adversary attack (Garcia, 2007); Chemical and Process facilities and transportation systems should be counted among these ones due to the high consequences of an attack – loss of lives, damage to valuable assets and to the environment (Nolan, 2008). This approach is "performance-based" in the sense that it evaluates how the elements of the PPS (i.e., detection, delay and response) contributes to the system effectiveness (Garcia, 2005).

On the other hand, a qualitative approach can be applied for either lower threats and lower consequences loss assets or whenever the lack of information on the PPS does not allow carrying out a quantitative approach.

Effectiveness assessment should take into account the complex configuration of detection, delay and response function that compose the PPS system; for high-security systems (i.e., as the ones here in considered) the response is generally assumed to be immediate on-site, so the response force time is part of the system PPS effectiveness.

Effectiveness assessment results are important for two main reasons:

- They provide a sound basis for the risk evaluation phase within Quantitative Risk Assessment, together with economic analysis for security measures selection and allocation;
- They helps to reevaluate and update the design of protection systems over time, in order to keep it in the state of art and to accommodate the introduction of new processes, functions or assets within the facility.

The analysis of a protection system requires applying the concept of adversary paths. An adversary path is an ordered series of actions against a facility, which if completed, results in successful theft, sabotage, or other malevolent outcome, such as a terroristic attack (Garcia, 2007). The selection of an adversary action sequence should be based on Adversary Sequence Diagrams and site-specific data. An Adversary Sequence Diagram is a graphic representation of the plant layout that should consider possible adversary starting points, distances up to the target(s), locations and typologies of security measures in place, and availability of security guards on site. Reasonable assumptions regarding the adversary mode of action (e.g., by foot or by car), tactic and attack scope (e.g., triggering an explosion or stealing an asset) should be taken.

In order to achieve his goal the adversary may adopt two opposite tactics: force attack and stealth attack. A force attack strategy is based on the minimization of the time required to

complete the path, with almost no regard of the probability of being detected; the adversary is successful if the path is completed before guard response. A stealth attack is based on the minimization of the probability of detection, with little regard to the time required; the adversary is successful if the path is completed with no detection. Often the adversary tactics may be intermediate between these two extremes. Adversary path depends also on adversary objectives: if theft, it implies that the adversary must get in and out the facility to succeed, if sabotage, it requires only the adversary to get to the asset and complete the sabotage action. Different adversary objectives turn into different times for the response force to interrupt the adversary and consequently in different PPS effectiveness.

Quantitative analysis of PPS effectiveness can be carried out according to either a single measure or a systematic model. Three possible measures of PPS effectiveness can be applied in chemical and process industries, according to the approach proposed by Garcia (Garcia, 2007), referred to industrial facilities:

- Minimum delay time;
- Cumulative probability of detection;
- Timely detection.

Alternatively, a more structured approach (i.e., EASI model) can be applied.

3.3.2.2.2 Minimum delay time

Minimum delay time (Figure 3. 14) is the comparison of the minimum cumulative time along the path (t_{MIN}) and the guard response time (t_G). The condition of an effective system is $t_G < t_{MIN}$; a system improvement can be achieved either by reducing the guard response time, which decreases t_G, or by adding a protection element with higher delay, increasing t_{MIN}. However, this effectiveness measure does not take into account the detection function but only the delay, even if a delay without prior detection is not meaningful since the response force must be alerted in order to respond and interrupt the adversary.

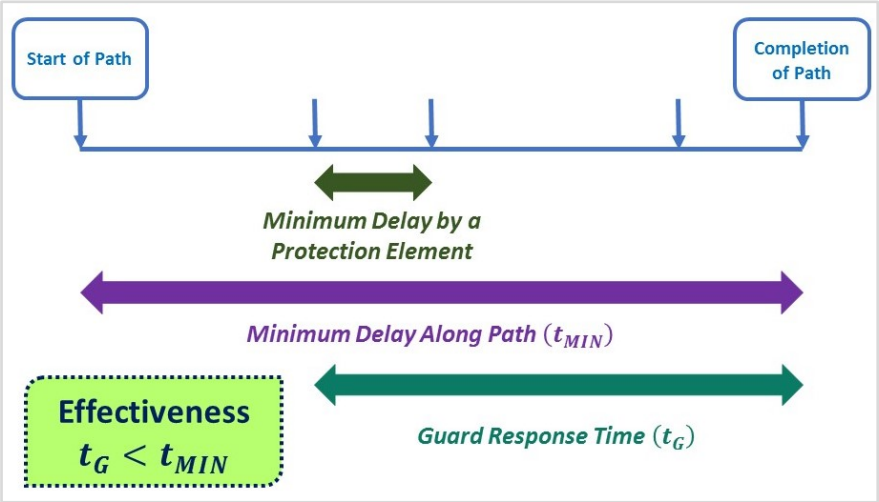


Figure 3. 14 Minimum Delay Time as a Measure of PPS Effectiveness.

3.3.2.2.3 Cumulative probability of detection

Cumulative probability of detection (Figure 3. 15) is the cumulative probability of detecting the adversary before the goal is achieved (P_{MIN}). The condition of an effective system is $P_{MIN} < P_{MIN,ACC}$, where $P_{MIN,ACC}$ represents the acceptability threshold. It should be noted that no consideration on the delay is conveyed by this definition of PPS effectiveness, even if detection without sufficient subsequent delay is not effective because the response force may not have enough time to interrupt the adversary.

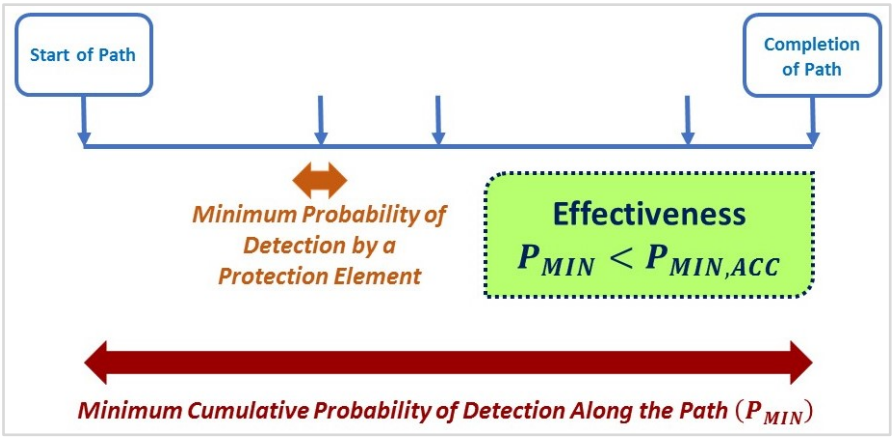


Figure 3. 15 Cumulative Probability of Detection as an Effectiveness Measure.

3.3.2.2.4 Timely detection

Timely detection measures a system effectiveness by the cumulative probability of detection at the point where there is still enough time remaining for the response force to interrupt the adversary (Figure 3. 16). It includes P_{MIN}, t_{MIN} and t_G; the delay elements along the path determine the point in which the adversary must be detected. That point has been named "Critical Detection Point" (CDP) and it corresponds to the point where the minimum delay

along the remaining path (t_R) just exceeds the guard response time (t_G); in other words CDP is determined by the first point for which the condition $t_R > t_G$ is valid.

Then the probability of interruption (P_I) can be computed as the cumulative probability of detection from the start of the path up to the CDP; P_I is the measure of the system effectiveness.

Quantitative analysis of PPS effectiveness by applying the timely detection measure requires to determine the probability of detection, delay times and on-site response time and eventually to compute the probability of interruption (P_I). It should be noted that P_I is different from the total cumulative probability of detection because it considers detection up to the CDP. Timely detection measures however do not account "force engagement" between response force and adversaries.

After having chosen a specific path, under specific conditions of threat and system operation, P_I can be quantified by the following equations (Garcia, 2007):

$$t_R = \sum_{i=k}^{m} t_i > t_G \tag{3.25}$$

$$P_I = 1 - \prod_{i=k}^{k-1} P_{ND,i} \tag{3.26}$$

Where t_R is the minimum time delay remaining along the path, t_G is the guard response time, m is the number of protection elements along the path, k is the first point at which $t_R > t_G$, i is a generic protection element, t_i is the minimum time delay provided by element i and $P_{ND,i}$ is the non-detection probability provided by element i.

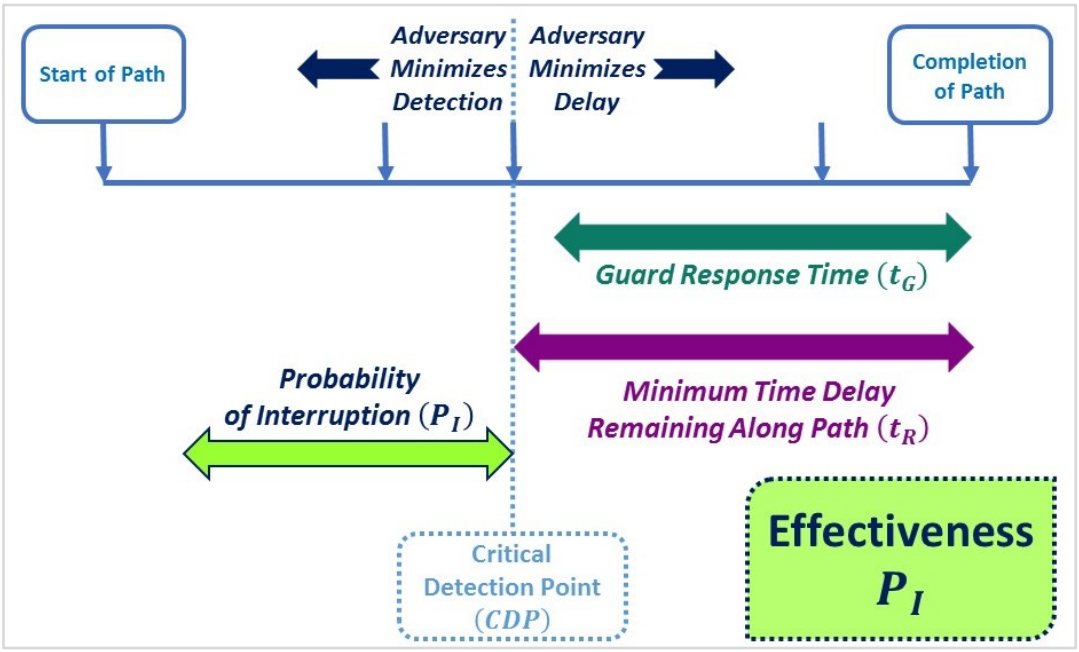


Figure 3. 16 Timely Detection as the Usual Measure of System Effectiveness.

The assumptions at the basis of the model are independency of each security element and the presence of an adaptive adversary tactic. The latter assumption indicates that the adversary

will try to minimize detection before the CDP (i.e., by applying a stealth or deceit tactic) and he will try to minimize delay after the CDP (i.e., by applying a force tactic, moving very fast and with almost no concern for detection). This assumption is conservative because the adversary may also choose to adopt the same tactic along the whole path; it implies also that the most skillful adversary is supposed to defeat or bypass detection along the path up to CDP and to know the response force time. If adversary tactics does not follow this assumption, it will turn into an increase of PPS effectiveness.

However, it should be highlighted that PPS effectiveness is dependent also on adversary tactics and a well-defined design basis threat is important for system effectiveness.

Clearly, the adversary may follow different paths into a facility, depending on his objective (e.g., steal or sabotage), but the one with the lowest P_I (i.e., $P_I{}^*$) characterizes the effectiveness of the overall protection systems and it has been named critical path. A tutorial on timely detection model is available in Section 6.2.2.

3.3.2.2.5 EASI model

Among the three main measures of PPS effectiveness, timely detection is generally the preferred one because it includes detection, delay and guard response time.

However, in case of a complex system, with many possible adversary paths, with several scenarios to consider and several targets as well, the system's complexity led to the necessity of a computer-aided tool that is able to repeat the calculation of PPS effectiveness along each possible adversary path, under specific conditions of threat and system operation.

As reported by Garcia (Garcia, 2007), quantitative computer aided models for the evaluation of PPS effectiveness, based on the concept of timely detection, are continually being developed. Among these, the EASI model (i.e., Estimate of Adversary Sequence Interruption), developed by Sandia Laboratories (Garcia, 2007) stands for the good combination between easiness to use and accuracy in the results.

This EASI model determines the PPS performance as the probability of interruption (P_I), referred to a sequence of adversary actions aimed at theft or sabotages. Due to the fact that the EASI model will be inserted in the original methodology presented in Section 4 for the calculation of security measures performances, a detailed description of EASI is provided.

EASI is a path-level model, meaning that it can analyze PPS performance along one adversary path per time; consequently, the preliminary step for its application is the selection of an adversary action sequence, based on site-specific data and reasonable assumptions about the adversary. An adversary sequence includes a starting point, one or more detection sensors, transit and barrier delays and an ending point. This systematic representation of the assets

within the facility that allow the analyst to review possible adversary paths, has been named Adversary Sequence Diagram (ASD): ASD are site-specific graphical representation of the physical layers around a facility, the protection elements between layers and paths to the asset. The creation of ASD includes (Garcia, 2005): modeling the facility by separating it into adjacent physical areas, defining protection layers and path elements between the adjacent areas, recording detection and delay value for each element. In case of multiple paths possible, effectiveness analysis should be repeated for each of them.

EASI model requires as input parameters: detection and communication probabilities (i.e., indicated respectively with $P_{AD,i}$ and $P_{C,i}$), delay and response mean times and standard deviations for each protection element i (i.e., indicated respectively with t_i and t_G). EASI model (Garcia, 2007, 2005) estimates the cumulative probability of sequence interruption, as follows:

$$P_I = P_{D1} \cdot P_{C1} \cdot P_{R\,|\,A1} + \sum_{i=2}^{n} P_{R\,|\,Ai} \cdot P_{C,i} \cdot P_{AD,i} \cdot \prod_{i=1}^{n-1}(1 - P_{AD,i}) \tag{3.27}$$

Where: $P_{R\,|\,Ai}$ is the probability of response force to arrive prior to the end of adversary actions, given an alarm for each element i present along the path; P_{Ci} is the probability of communication to the response force for each element i present along the path; $P_{AD,i}$ is the probability of assessed detection for a generic element i.

In case of single detection sensor, equation (3.27) becomes:

$$P_I = P_{R\,|\,A} \cdot P_A \tag{3.28}$$

Where $P_A = P_D \cdot P_C$ is the probability of notification of the response force, named probability of an alarm.

In order to have adversary interruption, it is necessary that the remaining time for the adversary to reach the ending point (t_R) exceeds the response force time (t_G):

$$t_R - t_G > 0 \tag{3.29}$$

Assuming the random variables t_R and t_G as independent and normally distributed, then the random variable x:

$$x = t_R - t_G \tag{3.30}$$

The variable x is normally distributed with mean:

$$\mu_x = E(x) = E(t_R) - E(t_G) \tag{3.31}$$

and variance:

$$\sigma_x^2 = Var(x) = Var(t_R) + Var(t_G) \tag{3.32}$$

Then $P_{R\,|\,A}$ should be computed as:

$$P_{R\,|\,A} = P(x > 0) = \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] \mathrm{dx} \tag{3.33}$$

The method requires the evaluation of $E(t_R)$ and $E(t_G)$ at a point j along the path of interest, with respect to the terminal point n, assuming the penetration time through each barriers and the transit time between barriers as random variables:

$$E(t_R)\ at\ point\ j = E(time\ after\ detection\ at\ point\ j) + \sum_{i=j+1}^{n} E(t_i) \tag{3.34}$$

Where:

- $E(t_i)$ is the expected time to perform task i
- $E(time\ after\ detection\ at\ point\ j) = \begin{cases} E(t_i)\,, & detection\ at\ B \\ \frac{E(t_i)}{2}\,, & detection\ at\ M \\ 0\,, & detection\ at\ E \end{cases}$,

  with B beginning, M mid and E end point.

Under the hypothesis of independency among each task, the variance of the path time remaining between point j and the terminal point n can be expressed:

$$Var(time\ after\ detection\ at\ point\ j) = \begin{cases} Var(t_i)\,, & detection\ at\ B \\ \frac{Var(t_i)}{4}\,, & detection\ at\ M \\ 0\,, & detection\ at\ E \end{cases}$$

with B beginning, M mid and E end.

Clearly, the adversary may follow different paths into a facility, depending on his objective (e.g., steal or sabotage), but the one with the lowest P_I (i.e., $P_I{}^*$) characterizes the effectiveness of the overall protection systems and it has been named critical path:

$$P_I{}^* = \min\left(P_{I,p}\right) \qquad with\ p = \{1, \dots, q\}, q \in Z \tag{3.35}$$

Where p is a generic adversary path, among q possible ones. An attempt of security managers is to balancing protection among different paths by allocating security upgrades in order to have approximately the same P_I in all the paths leading to critical assets.

In quantitative analysis for most of industrial facilities, the probability of interruption for the critical path is the measure of PPS effectiveness (Garcia, 2007), which varies from 0 to 1:

$$\eta_{PPS} = P_I{}^* \tag{3.36}$$

Nevertheless, equation (3.36) does not account the neutralization in PPS effectiveness, because, as stated by Garcia (Garcia, 2007), it is unlikely that any industrial facility will engage

in use of lethal force against an adversary. In case a force-on-force engagement (from verbal commands to deadly force) is expected additional modelling is necessary to predict the outcome of the conflict, measured by the probability of neutralization (P_N). In this case, mostly inherent to very high-security applications, PPS effectiveness for the most critical path is expressed as follows:

$$\eta_{PPS} = P_I^* \cdot P_N \tag{3.37}$$

EASI model has been summarized into a single equation (i.e., equation (4.1)) within original model application presented in Section 4; EASI can be implemented in an Excel version 2013 datasheet. A tutorial on EASI model application is provided in Section 6.2.3.

3.4 ECONOMIC EVALUATIONS FOR RISK ASSESSMENT SUPPORT

Due to the increased attention for external hazard factors, an optimal allocation of risk reducing measures, including related cost issues, becomes progressively more important. Today there are several approaches available to support the decision-making process; among these, Cost-Benefit Analysis and Cost-Effectiveness Analysis stands as the most common ones. Cost-Benefit Analysis (CBA) compares, through the assignment of monetary value, the investment benefits (often seen as the averted costs) with the costs, in order to provide an objective evaluation concerning the investment. On the other hand, cost-effectiveness analysis is aimed at determining the most profitable investments with reference to a specific scenario, under the constraint of the budget (Campbell and Brown, 2003).

3.4.1 Existing applications of economic evaluations within Safety and Security domains

Table 3. 13 and Table 3. 14 summarize recent contributions regarding theoretical, methodological and applicative aspects of economic analyses within the safety and security domain, referred to chemical and process industry installations. The analysis of research gaps highlighted that, despite the potential of economic analyses in establishing competitive business advantage within chemical process safety and security (Reniers, 2014), previous contributions are referred mostly to the selection and allocation of safety measures with respect to unintentional major and occupational accidents (i.e., safety-based accidents). Indeed, the past decades, cost-benefit analyses and the specific features of its application to the safety domain were explored (Gavious et al., 2009; Martinez and Lambert, 2012; Nicola Paltrinieri et al., 2012). Ongoing research within the chemical industry addresses economic assessment for safety decision-making (Janssens et al., 2015; Khakzad and Reniers, 2015; Reniers and Brijs, 2014a, 2014b). However, no specific complete economic models and

applications are yet available addressing the selection and allocation of preventive security measures, within the chemical and process industry domain.

3.4.2 Cost-Benefit and Cost-Effectiveness analysis for risk reducing measures selection

Reniers and Brijs (Reniers and Brijs, 2014b) have developed a tool, named CESMA, for the selection of safety measures within the chemical industry domain, with respect to major accident scenarios. Following the approach developed by these authors, the general expression for the Net Benefit of a single safety countermeasure with reference to a single scenario can be computed as (Reniers and Brijs, 2014b):

$$Net\ Benefit = \left(\left(f_{without} \cdot C_{Loss,without}\right) - \left(f_{with} \cdot C_{Loss,with}\right)\right) \cdot Pr_S - C_S \quad (3.38)$$

Where:

- $f_{without}$: frequency of an initiating event if the safety measure is not implemented;
- $C_{Loss,without}$: Loss or consequences, expressed in monetary values, without the additional safety measure;
- $f_{without}$: frequency of an initiating event if the additional safety measure is implemented;
- $C_{Loss,without}$: Loss or consequences, expressed in monetary values, with the additional safety measure;
- Pr_S: performance of the additional safety measure (e.g., expressed by PFD – probability of failure on demand);
- C_S: cost of the safety measure.

Cost modelling indicates the costs of providing the risk-reducing measure that are required to attain the benefit (C_S). The cost evaluations (e.g., the CESMA tool (Reniers and Brijs, 2014b)) included several classes (Table 3. 15): Initial Costs, Installation Costs, Operating Costs, Maintenance Costs, Other Running Costs, Specific Costs.

Hypothetical benefits modelling consists on the definition of the costs of averted accident that are indeed the losses sustained in a successful attack, either with $\left(C_{Loss,with}\right)$ or without $\left(C_{Loss,without}\right)$, the additional safety measure. The losses sustained in a successful attack include the fatalities and other damages, both direct and indirect, which will accrue because of a major accident, taking into account the value and vulnerability of people and infrastructure. Benefit categories for safety measures available in a study referred to safety measures for Chemical and Process Industry (e.g., the CESMA tool (Reniers and Brijs, 2014b)) are reported in Table 3. 16.

CBA can be applied either to each safety device separately or to a combination of several ones.

It should be noted that in order to compare total benefits and total costs occurring at different point in time it is necessary to introduce a discount rate to convert all cash flows to present values of annuities (Campbell and Brown, 2003). So the $Net\ Benefit$, accounting the conversion of all cash flows to present value of annuities, can be named also $Net\ Present\ Value\ (NPV)$. An investment is acceptable if $Net\ Present\ Value\ (NPV) \geq 0$, else it should be rejected.

Often, safety investments should be compared with budget limitations; in this situation, the economic evaluation method turns into a Cost-Effectiveness Analysis. Cost-Effectiveness Analysis (CEA) determines the optimal combination of investments that leads to the maximum net benefit, respecting budget constraints. As suggested by Reniers and Sörensen (Reniers and Brijs, 2014b; Reniers and Sörensen, 2013a), the optimization problem to be solved, known as "Knapsack problem", has been applied previously in the safety framework:

$$\begin{cases} \max Net\ Benefit_i\ x_i \\ C_{S,i}x_i \leq C_{Budget} \\ x_i \epsilon \{0,1\} \end{cases} \tag{3.39}$$

The first equation expresses the total benefit from the selected investments portfolio, which should be maximized, that means obtaining the maximum Net Benefit. The second equation expresses the fact that the total cost of the selected measures $(C_{S,i}x_i)$ should not exceed the budget (C_{Budget}). The third constraint implies that a measure/combination of measures (x_i) is either fully taken or not taken at all.

A number of assumptions are implicitly taken in this formulation:

- The safety investments under consideration are either fully taken or not (i.e., they cannot be partially taken);
- The total hypothetical benefit of all measures taken is the sum of the individual benefits of the chosen safety countermeasures;
- The total cost of all safety countermeasures taken is the sum of the costs of the individual measures;
- Safety countermeasures can be implemented independently, without consequences for the other investments.

Therefore, the state of art highlighted that economic analyses methodologies and applications have been defined firmly within the chemical and process industry domain and provide rational criteria for the risk evaluation phase within QRA, with respect to safety-based accidents.

Table 3. 13 Previous contributions on economic analysis, regarding safety and security aspects, within the chemical and process industry domain.

Keyword / Contribution	Reference accident/ measure typology	Elements of economic analysis				
		Measure performance/ risk reduction assessment	**Cost assessment**	**Losses/consequences assessment**	**Probability of attack/accident occurrence**	**Economic analysis**
(Ale et al., 2015)	Unintentional (safety-based) accidents/ safety measures	Not considered.	Discussion on hidden costs; no classification provided	Discussion on ethical issues; no classification provided	Not considered	Cost-benefit analysis, budget limitations
(Garcia, 2007, 2005)	Intentional (security-based) major accidents/ Physical security measures	EASI model; other models proposed	No classification provided	No classification provided	Deterministic approach	Qualitative discussion on cost-benefit analysis
(Gavious et al., 2009)	Unintentional (safety-based) accidents/ safety measures	Not considered	Not considered	Specific classification including categories, subcategories and formula	Not considered	Qualitative discussion on cost-benefit analysis
(HSE - Health and Safety Executive, 2016)	Unintentional (safety-based) accidents/ safety measures	Not considered	Discussion on costs; generic classification provided (no formula)	Discussion on benefit; generic classification provided (no formula)	Not considered	Cost-benefit analysis
(Janssens et al., 2015)	Unintentional (safety-based) major accidents (domino)/ safety measures.	Overall values; no classification provided	Overall values; no classification provided	Overall values; no methodology provided	Calculation of domino probabilities	Cost-effectiveness analysis
(Kyaw and Paltrinieri, 2015)	Unintentional (safety-based) major accidents/ safety measures	Not considered	Not considered	Calculation of reputational losses for notorious major accidents	Not considered	Qualitative discussion on the possible use within cost-benefit analysis
(Martinez and Lambert, 2012)	Unintentional (safety-based) major accidents/ safety measures	Layer of Protection Analysis	Overall values; no classification provided	Overall values; no classification provided	Deterministic approach	Cost-benefit analysis
(Nicola Paltrinieri et al., 2012)	Unintentional (safety-based) major accidents/ safety measures	Specific methodology for passive safety measures	Overall values; no classification provided	Overall values; no classification provided. Only human benefits considered	Deterministic approach	Cost-benefit analysis
(Reniers, 2014)	Intentional (security-based) and unintentional (safety-based) major accidents	Theoretical discussion on performance parameters	Theoretical discussion; no classification provided	Theoretical discussion; no classification provided	Not considered	Theoretical discussion on interactions between economic analyses and risk management

Table 3. 14 Previous contributions on economic analysis, regarding safety and security aspects, within the chemical and process industry domain.

Keyword / Contribution	Reference accident/ measure typology	Elements of economic analysis				
		Measure performance/Risk reduction assessment	**Cost assessment**	**Losses/consequences assessment**	**Probability of attack/accident occurrence**	**Economic analysis**
(Reniers and Brijs, 2014b; Reniers and Van Erp, 2016)	Unintentional (safety-based) major accidents/ safety measures	Overall values; no methodology provided	Detailed classification specific for safety measures including categories, subcategories and formula	Classification for major accidents, including categories, subcategories and formula	Deterministic approach	Cost-benefit analysis, cost-effectiveness analysis
(Reniers and Brijs, 2014a)	Occupational accidents/ safety measures	Not considered	Not considered	Not considered	Not considered	Presentation of available cost-benefit analysis software/ methodologies
(Reniers and Sörensen, 2013b)	Occupational accidents/ safety measures	Overall values	Overall values; no classification provided	Severity classes; no classification provided	Occurrence classes	Cost-effectiveness analysis
(Tappura et al., 2014)	Occupational accidents/ safety measures	Presentation of available models	Discussion on costs; no classification provided	Discussion on benefits; no classification provided	Not considered	Presentation of available cost-benefit analysis methodologies

Table 3. 15 Cost categories and subcategories for a generic safety measure (Reniers and Brijs, 2014b).

Cost Classification for Safety measures	
Cost category	**Cost subcategory**
INITIAL COSTS	▪ Investigation costs ▪ Selection and design costs ▪ Material costs ▪ Training costs ▪ Changing of guidelines and informing costs
INSTALLATION COSTS	▪ Production Loss cost ▪ Start-up costs ▪ Equipment costs ▪ Installing costs
OPERATING COSTS	▪ Utilities costs
MAINTENANCE COSTS	▪ Material costs ▪ Maintenance team costs ▪ Production loss costs ▪ Start-up costs
INSPECTION COSTS	▪ Inspection team costs

Economic analyses, such as cost-benefit and cost-effectiveness analyses, may offer rational criteria for the selection and allocation of security measures within the decision-making process, as demonstrated by the application to other domains, as aviation (Stewart and Mueller, 2013, 2011, 2008) and navy facilities (Cox, 2009; Dillon et al., 2009). However, no economic model for the allocation security measures to be used within the chemical industry has yet been developed.

Few existing contributions proposed a rather simplified cost-benefit analysis methodology for the selection of security measure within another domain (i.e., aviation) (Stewart and Mueller, 2013, 2012, 2011, 2008). The calculation of the Net Benefit, or Net Present Value, for a security countermeasure can be implemented as follows:

$$Net\ Benefit = E(C_b) + \sum_T \sum_H \sum_L P(T) \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss} \cdot \Delta\eta - C_{Security} \qquad (3.40)$$

Where $E(C_b)$ indicates the expected benefit from the security countermeasure not directly related to mitigating security threats (e.g., increased personnel confidence, reduction in crime, etc.). Often the assumption of $E(C_b) \cong 0$ is introduced in order to obtain conservative results. $P(T)$ represents the threat probability (e.g., the probability of attack) referred to a critical infrastructure. $P(H \mid T)$ and $P(L \mid H)$ are the vulnerability probabilities. C_{Loss} indicates the overall losses or consequences, expressed in monetary values, and indicated also as "overall benefits". $\Delta\eta$ represents the effectiveness improvement achieved by implementing the Security

measure (or Physical Protection System, i.e. PPS). $C_{Security}$ indicates the overall costs of the specific security measures (or systems) required to attain the benefits. The summation refers to the number of possible Threats (T) scenarios, Hazard (H) levels and Losses (L). With the assumptions of $E(C_b) = 0$, equation (3.40) can be rewritten for a single scenario j as:

$$Net\ Benefit_j = P(T) \cdot P(H|\ T) \cdot P(L|\ H) \cdot C_{Loss,j} \cdot \Delta\eta - C_{Security} \quad (3.41)$$

The product of threat and vulnerability probability is sometimes indicated as a single term (i.e., P_A) (Stewart and Mueller, 2012, 2011, 2008), expressing the probability of a "successful" attack. Equation (3.41) can be the starting point for the development of an original economic model, aimed at the selection and allocation of security measures within the chemical industry domain.

Table 3. 16 Benefit categories and subcategories for a major accidental scenario (Reniers and Brijs, 2014b).

Benefit Classification	
Benefit category	**Benefit subcategory**
SUPPLY CHAIN BENEFITS	▪ Production loss benefits ▪ Start-up benefits ▪ Schedule benefits
DAMAGE BENEFITS	▪ Damage to own material/property ▪ Damage to other companies' material/properties ▪ Damage to surrounding living areas ▪ Damage to public material property
LEGAL BENEFITS	▪ Fines-related benefits ▪ Interim lawyers benefits ▪ Specialized lawyer benefits ▪ Internal research team benefits ▪ Expert at hearings benefits ▪ Legislation benefits ▪ Permit and license benefits
INSURANCE BENEFITS	▪ Insurance premium benefits
HUMAN AND ENVIRONMENTAL BENEFITS	▪ Compensation victims benefits ▪ Injured employees benefits ▪ Recruit benefits ▪ Environmental damage benefits
INTERVENTION BENEFITS	▪ Intervention benefits
REPUTATION BENEFITS	▪ Share price benefits
OTHER BENEFITS	▪ Manager work-time benefits ▪ Cleaning benefits

It should be noted that the existing model by Stewart and Mueller (Stewart and Mueller, 2012, 2011, 2008) has some relevant limitations, paving the way to follow for further improvements:

- It does not address the specificities of operational security within the chemical industry domain;
- Cost assessment and loss assessment need to be improved, by introducing categories, subcategories and expressions allowing quantitative assessment instead of applying empirical flat rates for overall costs and benefits.
- Uncertainties regarding threat and vulnerabilities probabilities need to be addressed by specific approaches;
- An approach to cost-effectiveness analysis needs to be introduced. The application of cost-effectiveness analysis is particularly important since it allows the allocation of the security budget on the most profitable combination of security measures. An original scoring system needs to be developed to provide overall economic indicators.

3.5 CONCLUSIONS

In this section, an overview on the state of the art regarding the inclusion of external hazard factors and economic evaluations within risk assessment for the Chemical industry domain is presented. A description of two typologies of accidental events triggered by external hazard factors (i.e., domino effects and security-based accidents) is carried out, together with available techniques to include external hazard factors within risk assessment. Research contributions highlighted the necessity to implement unified generic framework for safety and security risk assessment.

Indeed the analysis of risk assessment techniques made clear the paramount important role of safety and security measures within cascading events prevention, control and mitigation. For instance, safety measures are applied with respect to unintentional accidents (i.e., domino effects), while security measures refer to intentional accidents (i.e., security-based accidents). Indeed, the identification and evaluation of possible risk reducing measure is a fundamental step of QRA, referred to external hazard factors.

Therefore, different typologies of risk reducing measures applied within chemical and process installations were described, together with methodologies to evaluate their performances, from economic and technical point of views. A parallelism among the three classes of safety and security measures (i.e., active-detection measures; passive-delay measures; procedural-response measures) has been highlighted, but methodologies needed to address performance assessment have demonstrate to be very different between safety and security measures.

With regards to the inclusion of safety and security measures performance within risk assessment of external hazard factors, two main research gaps have been found and are described in the following paragraphs.

3.5.1 Application of dynamic safety barriers performance assessment by means of Bayesian Networks with respect to major accidents and cascading events prevention

The analysis of existing techniques and methodologies for safety measures performance assessment pointed out that the applications of advanced techniques (i.e., Bayesian Networks) to safety barriers performance assessment with respect to major accidents are still scarce and need to be widened and improved. Moreover, with regards to domino effect modelling and prevention, no applications of advanced techniques which take into account safety barriers are available. Therefore, the original research will be aimed at filling this gaps (see Section 5), according to the concepts expounded in the following subsections.

3.5.1.1 Comparison between quantitative safety barriers performance assessment by means of Bayesian Networks and Event-Tree analysis

The conventional methodology for safety barriers performance assessment is based on Event-tree Analysis, a probabilistic model that correlates a top event with its consequences. A recent Event-Tree based methodology, provided by Landucci et al. (Landucci et al., 2015a) and presented in Section 3.3.2.1.3, allows an accurate evaluation of safety barriers performance by means of novel gates and can be applied both to major accident and to domino events.

Nevertheless, the limitations of Event-tree analysis hinder from obtaining a real-time picture of safety barriers performances and consequences probabilities, offering just a static risk picture, which is not able to account systems modifications and additional information. These drawbacks promise to be solved by Bayesian Networks.

Therefore, according to the mapping procedure from Event-Tree to Bayesian Network, provided by Khakzad et al. (Khakzad et al., 2013b), the procedure for safety barriers performance assessment provided by Landucci et al. (Landucci et al., 2015a) can be converted into Bayesian Networks, keeping the same main steps ad constituents.

Safety barriers performance assessment by means of Bayesian Networks, presented in Figure 3. 17, takes advantage over the Event-Tree based approach, as it allows performing Bayesian Analysis by means of the discussed probability revising techniques (i.e., probability updating and probability adapting). Indeed, the Bayesian networks based approach is capable to revise safety barriers performance and final events probabilities over time, providing a more-updated risk picture. Moreover, the conversion of specific gates (type A, B, C) into BNs represent an

additional element of novelty, as they have never been implemented before within BNs. The procedure can be applied both to major accident prevention, in particular fire prevention, and to the prevention of fire escalation into domino effect. In the latter case, escalation probabilities corresponding to each final state are calculated exacting the same way, both in the Bayesian approach and in the conventional one.

The comparison between the procedure by Landucci et al. (Landucci et al., 2015a) and safety barriers performance assessment by means of Bayesian Network will be developed in several case studies in Section 5. 3, in purpose to validate the application of Bayesian Networks within this specific context.

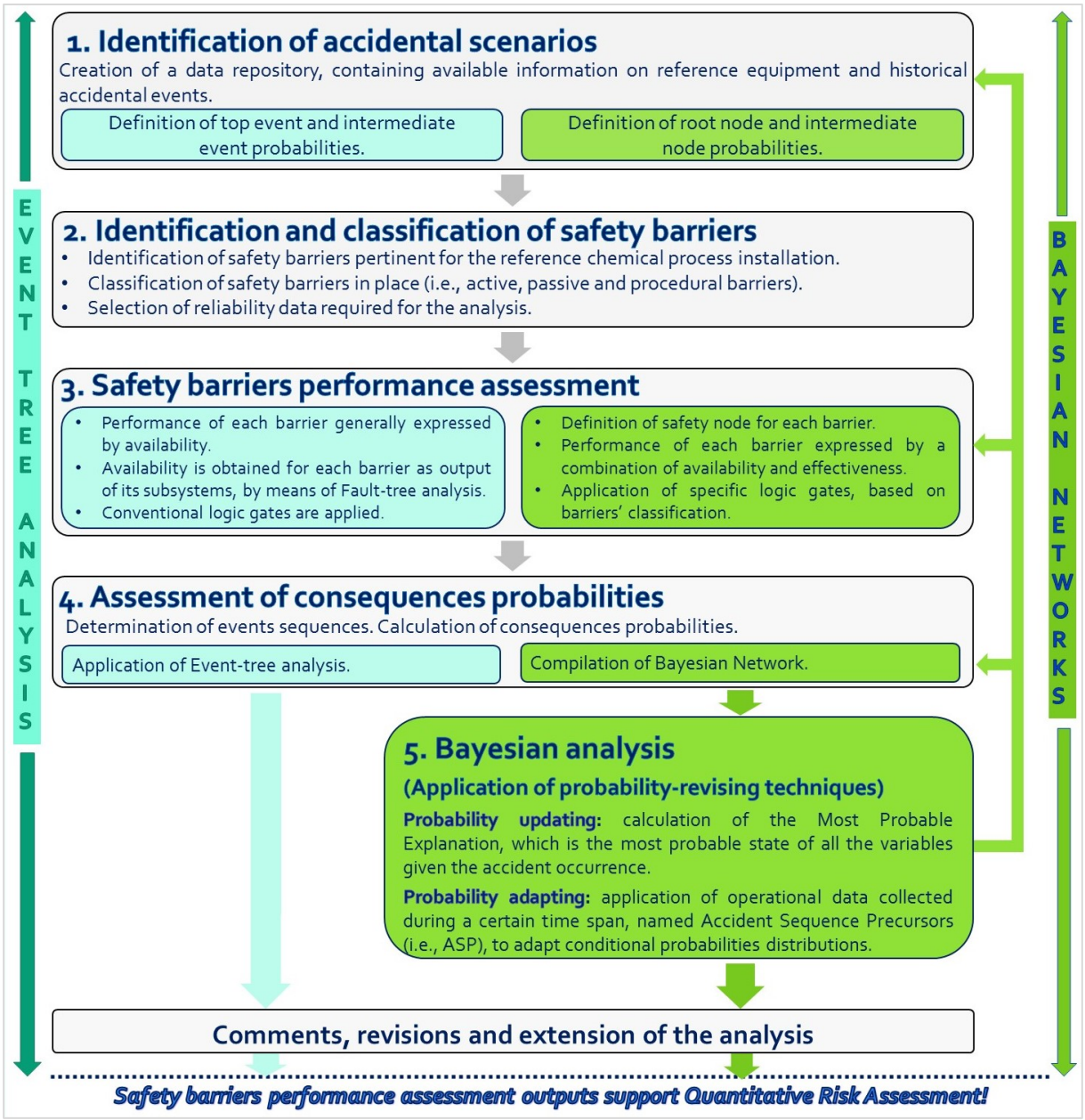


Figure 3. 17 Comparison between quantitative safety barriers performance assessment by means of Event-Tree analysis and Bayesian Networks.

3.5.1.2 Inclusion of safety barriers performance assessment by means of Bayesian Networks within domino accident modelling and prevention

With respect to domino accident modelling and prevention, Khakzad et al. (Khakzad et al., 2013d) have recently developed an advanced methodology to be implemented by means of Bayesian Networks, which allows considering synergistic effects and several domino levels. However, in the methodology, safety barriers are not included, resulting in an unrealistic representation of the system. Therefore, original contributions that compare the introduction of safety barriers within domino accident modelling and prevention are required, in a Bayesian Network environment. A flowchart representing this reasoning is reported below (Figure 3. 18).

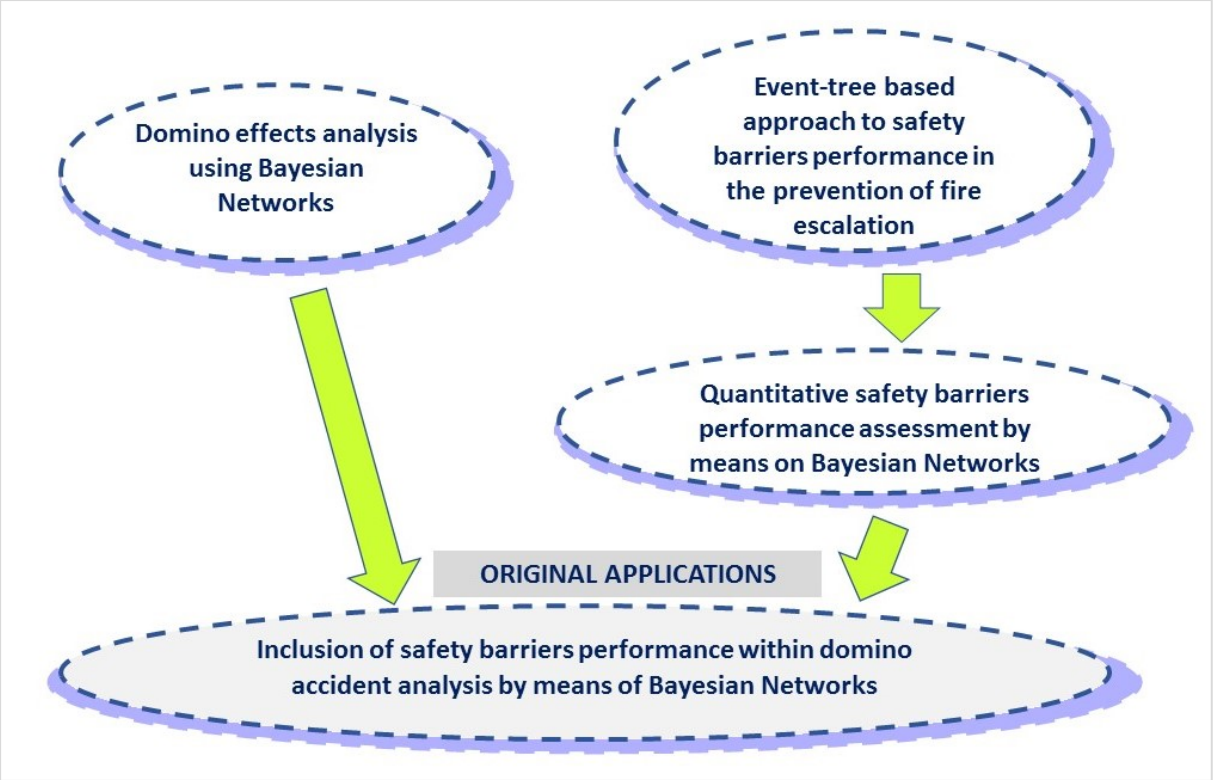


Figure 3. 18 Flowchart representing the need to include safety barriers performance within domino accident analysis by means of Bayesian Networks.

3.5.2 Development and application of an economic model for the allocation of preventive security measures against terroristic attacks in chemical facilities

The state of the art highlighted that, despite the existence of economic models for supporting decision-making processes in general, for instance cost-benefit and cost-effectiveness analyses, no specific economic models (and applications) are available in the domain of operational security (including counter-terrorism decision-making) to be applied within the

chemical and process industry. As suggested by Stewart and Muller (Stewart and Mueller, 2013, 2012) that have recently developed and applied Cost-Benefit Analysis for aviation security, the task is particularly challenging because it involves defining the threat probability, the losses sustained in the successful attack, the performance and the costs determined by the implementation of a security countermeasure (accordingly to its specific features).

Therefore, an original model for economic analysis and selection of physical security measures, with respect to different typologies of terroristic attacks in chemical facilities needs to be developed and validated by application to several case studies. The model, described in Section 4 and applied in Section 6, allows performing site-specific analysis of the baseline physical security system performance and comparing the costs of different security upgrades with the benefits related to either prospective or retrospective losses, meanwhile accounting the uncertainties related to the threat probability. Selection of the most profitable security measures within budget constraints and definition of economic indicators will be the main outputs of the model, in order to support decision-making processes for allocation of security barriers within the chemical industry domain; a graphical abstract addressing this research topic is reported in Figure 3. 19.

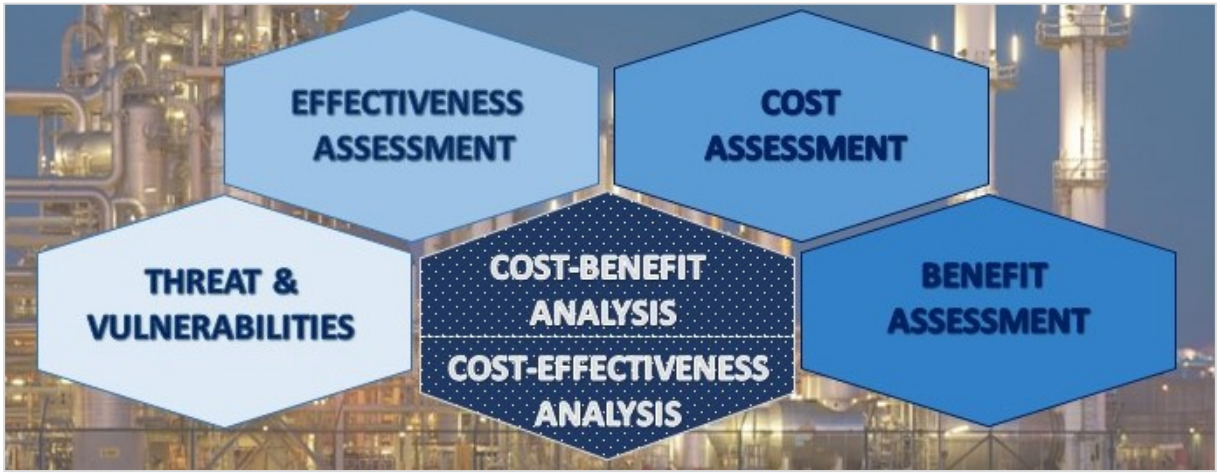


Figure 3. 19 Graphical representation of the possible constituents of an original model for the selection and allocation of security measures within the chemical industry domain.

Section 4.
Development of an economic model for the allocation of preventive security measures against terroristic attacks in chemical facilities

4.1 INTRODUCTION

Several recent events raised the attention toward possible major accidents triggered by external acts of interference in industrial facilities. In particular, among possible security-based accidents, a growing concern is present with respect to the intentional release of dangerous substances resulting in environmental and eco-terroristic attacks. Therefore, optimal selection and allocation of preventive security measures is becoming more important for decision-makers. Despite the existence of economic models for supporting decision-making processes in general, for instance cost-benefit and cost-effectiveness analyses, no specific economic models are available in the context of operational security (including counter-terrorism decision-making) to be applied within the chemical and process industry domain, as pointed out in Section 3. 6. This section describes a novel model for economic analysis and allocation of preventive physical security measures (or barriers) specifically for use in the chemically and process industry domain. The model, starting from the analysis of the baseline physical security system, allows proposing security upgrades and accounting both the performance improvement and the costs derived from their implementation. The model also includes the evaluation of benefits related to either prospective or retrospective losses, meanwhile accounting threat and vulnerability probabilities for a chemical installation, in relation with possible malicious acts.

The model, presented in Section 4. 2, can be depicted in a two-fold version, referred to different typologies of applications. The first version, EM-PICTURES (i.e., Economic Model for Process-Industry related Counter Terrorism measURES) allows performing cost-benefit and cost-effectiveness analysis of preventive security measures, against generic security-based accidents and terroristic attacks in chemical facilities. The evaluation of uncertainties related to the definition of threat and vulnerability probabilities is provided by the analysis. Thus, EM-PICTURES enables the comparison among different security upgrades and the choice of

economically feasible ones, as well as the determination of the combination with the maximum profit, within budget constraints.

The latter version, ECO-SECURE (i.e., ECOnomic model for the selection of SECurity measURES) is specifically aimed at preventing potential environmental terroristic attacks in chemical facilities by means of a rational allocation of security resources. Indeed, a specific classification for environmental losses is elaborated. A coupled approach toward the estimation of the threat probability (i.e., deterministic and break-even) allows defining a broad set of economic indicators, made clearer by the development of a specific scoring system. Indeed, the coupled approach allows including the sensitivity analysis within ECO-SECURE application. Selection of the most profitable security measures within budget constraints and definition of economic indicators are the main outputs of ECO-SECURE.

The ultimate aim of the model is allowing a more rational allocation of preventive security measures and supporting risk assessment and related decision-making process, within the context of chemical and process industries. The model is specifically tailored for security measures aimed at the prevention of security-related events, even if also the adoption of safety measures may offer sound support in the prevention, control and mitigation of security-based accidents (Aven, 2007; Reniers, 2010).

4.2 MODEL DESCRIPTION: EM-PICTURES AND ECO-SECURE VERSIONS

4.2.1 General layout of the model

The model layout is shown in Figure 4.1. Definition of the site-specific adversary sequence of actions and assessment of baseline physical protection system (PPS) performance need to be carried out before the model application. This preliminary step was defined as module 0. Six steps are then required to complete the assessment:

- In Module 1, the effectiveness improvement ($\overline{\Delta\eta_i}$) achieved by implementing an additional security measure i to the baseline Physical Protection System (i.e., PPS) is evaluated. It provides the degree to which the security measure foils, deters, disrupts or protects against a threat. Guidance on the equations and data necessary to apply this methodology step and on the possible security upgrades to adopt is provided to users.
- In Module 2, the overall costs of a specific security measure, $C_{Security,i}$, are assessed, by means of 22 cost subcategories and formula to calculate each cost category. This includes direct and indirect economic costs derived from the application and use of a security device.

- Module 3 defines the overall losses or consequences of either perspective or retrospective accidental scenarios (i.e., $C_{Loss,j}$), expressed in monetary values, and indicated in the following section also as "overall benefits". Guidance on the scenarios to adopt in case of prospective/retrospective accidents is provided to users.
- Module 4 is aimed at defining the threat probability (i.e., the likelihood of the attack) within a chemical facility. In this module also the vulnerability probabilities, expressing the conditional hazard and loss probabilities, are defined.
- Module 5 allows defining the single security measures that are economically justified (by means of a cost-benefit analysis, indicated with the acronym CBA throughout the manuscript) with reference to a set of scenarios.
- Module 6 provides the most profitable combination of security measures (by means of a cost-effectiveness analysis, indicated with acronym CEA throughout the manuscript) with reference to a set of scenarios.

The outputs of the model are cost-benefit and cost-effectiveness indicators aimed at supporting the security decision-making process from an economic perspective. The two-fold versions of the model (i.e., EM-PICTURES and ECO-SECURE) share the mentioned six methodological steps. However, they present a relevant number of differences, in particular:

- Concerning effectiveness assessment, EM-PICTURES allows considering in the calculations different adversary mode of actions (e.g., sequential, simultaneous actions) in case of multi-targets terroristic attacks within a chemical facility.
- Concerning losses assessment, the categories are different depending on the focus of the analysis. In EM-PICTURES, the damages derived from a generic security-based major accident are accounted, while ECO-SECURE focuses on environmental consequences.
- Concerning the definition of the threat probability, as wella as cost-benefit and cost-effectiveness analyses, a coupled approach (i.e., deterministic and break-even) is provided in ECO-SECURE, instead of the solely deterministic approach presented in EM-PICTURES. The coupled approach allows including the sensitivity analysis on the threat probability within model application. An original scoring system is developed in ECO-SECURE to provide overall economic indicators.

The model can be implemented in Excel® version 2013 modelling environment. The authors suggest using 7 different datasheets, defined according to the modules (i.e., from Module 0 up to Module 6). The content and procedures applied in the single modules are explained in detail in the following.

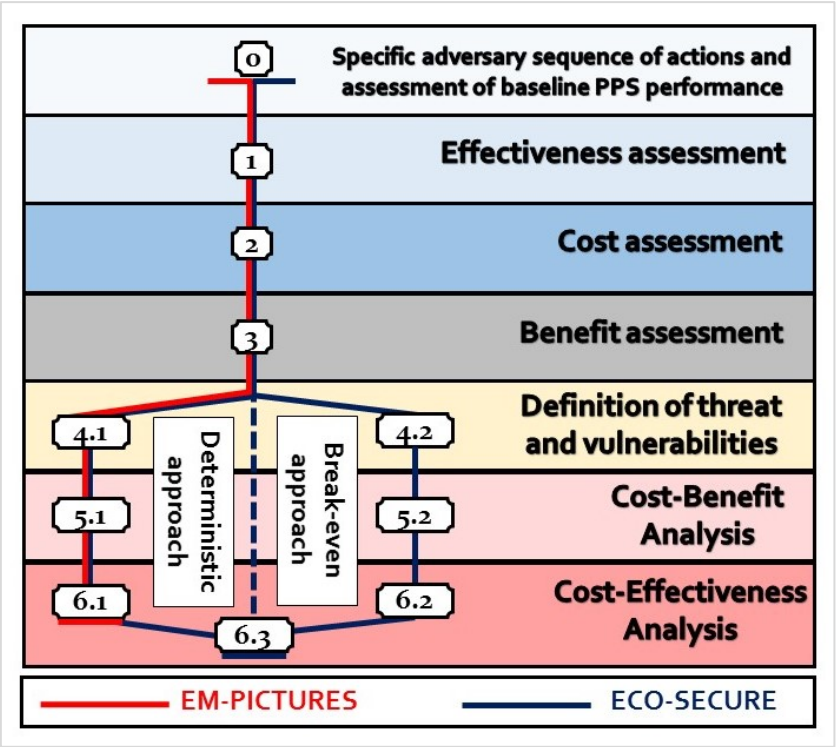


Figure 4. 1 General layout of the model, with a two-fold version, named EM-PICTURES and ECO-SECURE.

4.2.2 Module 0: data gathering and assessment of baseline physical security system performance

Module 0 is the preliminary step for the application of the model: it provides the definition of the site-specific adversary sequence of actions and the assessment of baseline physical protection system performance. The selection of an adversary action sequence should be based on Adversary Sequence Diagrams and site-specific data. An Adversary Sequence Diagram is a graphic representation of the plant layout that should consider possible adversary starting points, distances up to the target(s), locations and typologies of security measures in place, and availability of security guards on site. Reasonable assumptions regarding the adversary mode of action (e.g., by foot or by car), tactic (e.g., stealth or deceit) and attack scope (e.g., triggering an explosion or stealing an asset) should be taken.

Several models may be used to determine the baseline physical protection system performance, whose principal indicator is its effectiveness (η_{PPS}) (Hester et al., 2010). A description of available methodologies for the evaluation of physical security measures performance is available in Section 3.4.3. Estimate of Adversary Sequence Interruption (i.e., EASI) model, developed by Sandia Laboratories (Garcia, 2007, 2005), was applied to determine physical protection system performance. Estimate of Adversary Sequence Interruption (i.e., EASI) model, calculates the probability of interruption $(P_{I,p})$, referred to a single sequence of adversary actions aimed at theft or sabotage. The probability of interruption expresses the

conditional probability of an attacker's path of actions (i.e., indicated with p) being foiled, deterred or disrupted. EASI model requires the following input parameters: assessed detection and communication probabilities (i.e., indicated respectively with $P_{AD,i}$ and P_C), delay mean times of each protection element i (i.e., indicated with $t_{D,i}$ and expressing the mean duration time of a task), response force mean time (t_G) and standard deviations for the mentioned parameters (i.e., indicated respectively with $\sigma_{D,i}$ and σ_G). Standard deviation input values are required because the EASI model, applied for the calculation of the effectiveness, takes into account uncertainties regarding each task (e.g., presence of a lag time) by applying probability distribution. According to the conservative assumption on data dispersion of the model (Garcia, 2007), standard deviation values referred to the delay parameter for each security element and to the response parameter have been assumed as $3/10$ of the mean value.

According to EASI model, $P_{I,p}$ can be computed as follows, with reference to a path p with l tasks:

$$\begin{cases} P_{I,p} = \left(1 - \prod_{i=1}^{j}(1 - P_{AD,i})\right) \cdot P_C \cdot \left(\int_0^T \left(1/\sqrt{2\pi(\sigma_D^2 + \sigma_G^2)}\right) \exp(-T^2/(\sigma_D^2 + \sigma_G^2))dT\right) \\ T = t_D - t_G \\ t_D = \sum_{i=j+1}^{l} t_{D,i} \\ \sigma_D = \sum_{i=j+1}^{l} \sigma_{D,i} \end{cases} \quad (4.1)$$

Details on the EASI model can be found elsewhere (Garcia, 2007, 2005) and in Section 3.4.3; the suggested modeling environment is an Excel® datasheet. A sample Excel® datasheet of EASI model can be retrieved from the mentioned source (Garcia, 2007). In the evaluation of effectiveness, the neutralization probability is not accounted for, following the stated assumption that in industrial facilities the use of lethal force against an adversary is unlikely (Garcia, 2007).

Module 0 differs between EM-PICTURES and ECO-SECURE in the calculation of the baseline PPS effectiveness regarding multi-targets sequence of actions, as visible from Figure 4.2.

According to EM-PICTURES, in case of multiple targets, the path should be divided into k segments, with t number of the targets, and effectiveness calculations should be repeated for each of them. In case of multiple paths possible between contiguous targets, effectiveness analysis should be repeated for each of them. Therefore, the baseline system effectiveness for a segment k $(\eta_{PPS,old\,k})$ can be assessed, as follows:

$$\eta_{PPS,old\,k} = P_{I,p^*} = \min(P_{I,p}) \qquad with\ p = \{1, \dots, q\} \quad (4.2)$$

$$\forall k \in \{1, \dots, t\}, t \in Z$$

Where the path p^* with the lowest P_I (i.e., P_{I,p^*}) among q possible ones, characterizes the baseline effectiveness of the protection system along the segment k. k indicates a generic segments that connects either the starting point to the first target or two contiguous targets; k is multiple of the number of possible targets (t). The calculation should be repeated for each of the t segments. The calculation of baseline PPS effectiveness for each path segment provided by EM-PICTURES may allow a detailed site-specific description of adversary mode of action in case of multi-target attacks.

According to ECO-SECURE, the baseline PPS effectiveness (i.e., $\eta_{PPS,old}$) can be assessed as follows, according to:

$$\eta_{PPS,old} = P_{I,p^*} = \min(P_{I,p}) \qquad with\ p = \{1, \dots, q\} \tag{4.3}$$

Where the path p^*, with the lowest $P_{I,p}$ (i.e., P_{I,p^*}) among q possible ones has been named critical path. P_{I,p^*} characterizes the baseline effectiveness of the physical protection system, according to the principles of EASI model (Garcia, 2007). Therefore, ECO-SECURE provides an overall value of baseline PPS effectiveness, regardless the number of targets involved.

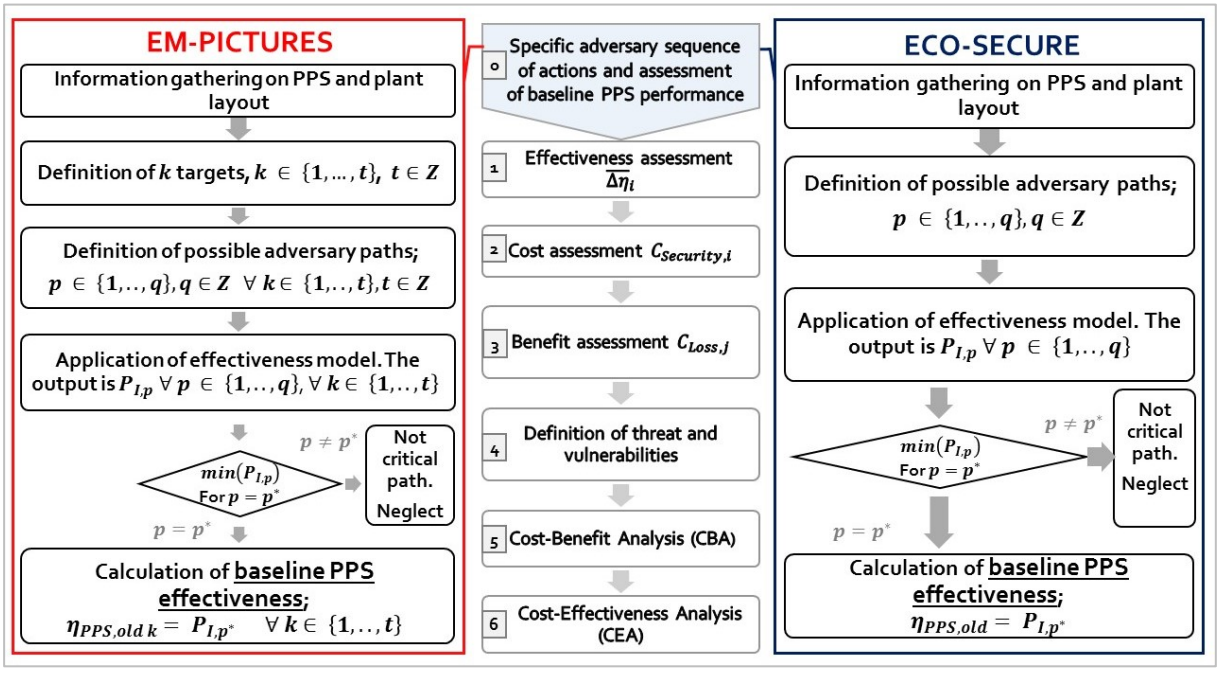


Figure 4. 2 Main contents of Module 0, according to EM-PICTURES and ECO-SECURE versions.

4.2.3 Module 1: preventive security measures performance assessment

This module is aimed at proposing security upgrades and determining the overall effectiveness improvement $\overline{\Delta\eta_i}$ due to each security measure i. Module 1 differs between EM-PICTURES and ECO-SECURE in the calculation of the upgraded PPS effectiveness regarding multi-targets sequence of actions, as visible from Figure 4.3.

According to EM-PICTURES, following the assumption of adding one security device at time, effectiveness improvement due to the introduction of a generic security measure i in the existing Physical Protection System along a generic segment k can be computed as:

$$\Delta\eta_{ik} = \eta_{PPS,new\ ik} - \eta_{PPS,old\ k}$$

$$\forall i \in \{1, \dots, n\}, n \in Z \qquad (4.4)$$

$$\forall k \in \{1, \dots, t\}, t \in Z$$

Where $\eta_{PPS,new\ ik}$ expresses the probability of attacker's path of actions being foiled, deterred or disrupted in presence of each additional (i.e., "new") security measure i among the possible n security measures. It expresses the upgraded PPS effectiveness. In order to determine the upgraded effectiveness, the EASI model was reapplied to the critical path p^* for each of the security upgrades i, obtaining $\eta_{PPS,new\ ik}, \forall i \in \{1, .., n\}, n \in Z$, and therefore the correspondent effectiveness improvement ($\Delta\eta_{ik}$), referred to each segment k.

On the other hand, $\eta_{PPS,old\ k}$ represents the probability of attacker's path of actions being foiled, deterred or disrupted before the addition of a security measure along a segment k; it has been indicated as baseline PPS effectiveness and it is the output of module 0. Therefore, the determination of the effectiveness improvement along a segment k ($\Delta\eta_{ik}$) requires the evaluation of PPS effectiveness before and after the addition of a security measure i. $\Delta\eta_{ik}$ is sometimes named "risk reduction" (Stewart and Mueller, 2013, 2011, 2008); an explanation regarding the nomenclature is available in Section 4.2.7. The calculation should be reapplied to each of the k segments, in purpose to obtain the overall effectiveness improvement ($\overline{\Delta\eta_i}$), as follows:

$$\overline{\Delta\eta_i} = f\left(\sum_{k=1}^{t} \Delta\eta_{ik}\right) \qquad (4.5)$$

$$\forall i \in \{1, \dots, n\}, n \in Z$$

Where f is a function of adversary's mode of action.

In case of a sequential action (e.g., one attacker that sabotage a target and just after a second one), the overall effectiveness improvement for each security upgrade i can be expressed according to a "series model":

$$\overline{\Delta\eta_i} = \sum_{k=1}^{t} \Delta\eta_{ik} \qquad (4.6)$$

$$\forall i \in \{1, \dots, n\}, n \in Z$$

In case of a simultaneous action (e.g., two or more attackers that sabotage one target each in the same time), the overall effectiveness improvement for each security upgrade i can be expressed according to a "parallel model":

$$\overline{\Delta\eta_i} = 1/(\sum_{k=1}^{t} 1/\Delta\eta_{ik}) \quad (4.7)$$

$\forall i \in \{1, \dots, n\}, n \in Z$

The application of the described EM-PICTURES approach toward effectiveness assessment allows taking into account different adversary's mode of action in case of multi-target attacks; nevertheless, it requires a relevant amount of inputs.

On the other hand, ECO-SECURE provides a global approach toward effectiveness assessment, also in case of multi-target attacks. Within model application, in case of no information available regarding adversary's mode of action, it is suggested to apply the generic approach toward effectiveness assessment presented in ECO-SECURE version of the model. According to ECO-SECURE, following the assumption of adding one security device at a time, overall effectiveness improvement due to the introduction of a generic security measure i in the existing Physical Protection System can be computed as:

$$\overline{\Delta\eta_i} = \eta_{PPS,new\,i} - \eta_{PPS,old} \quad (4.8)$$

$\forall i \in \{1, \dots, n\}, n \in Z$

Where $\eta_{PPS,new\,i}$ expresses the probability of attacker's path of actions being foiled, deterred or disrupted in presence of each additional (i.e., "new") security measure i among the possible n security measures. It expresses the upgraded PPS effectiveness. On the other hand, $\eta_{PPS,old}$ represents the probability of attacker's path of actions being foiled, deterred or disrupted before the addition of a security measure, calculated in module 0, according to ECO-SECURE version of the model. In order to define the effectiveness of upgrades, the EASI model is applied to the critical path for each of the security upgrades i, obtaining $\eta_{PPS,new\,i}$, $\forall i \in \{1, .., n\}, n \in Z$. Further details on effectiveness assessment by means of EASI model are provided by Garcia (Garcia, 2007, 2005); a description of EASI model is available in Section 3.4.3.

It should be noted that EASI model, applied in both EM-PICTURES and ECO-SECURE for the calculation of the baseline and upgraded system effectiveness, specifically refers to physical security measures and cannot be generalized (i.e., it cannot be applied for safety measures performance evaluations). The choice of an appropriate pool of security upgrade should be based on the Organizational-Physical-Electronics-Reporting principle (i.e., OPER) (Reniers et al., 2015), which considers a complete PPS as a combination of the three security functions of detection, delay and response. Therefore, the range of choices should include at least one security measure belonging to each security function. Further details on security measures

classification (CCPS - Center for Chemical Process Safety, 2003; Garcia, 2007), based on security functions, are available in Section 3.4.1.2. A detailed guideline on the possible security upgrades to be adopted is presented in Section 3.4.1.2; therefore, it is not necessary to use a specific software for the selection of appropriate security upgrades within EM-PICTURES and ECO-SECURE versions.

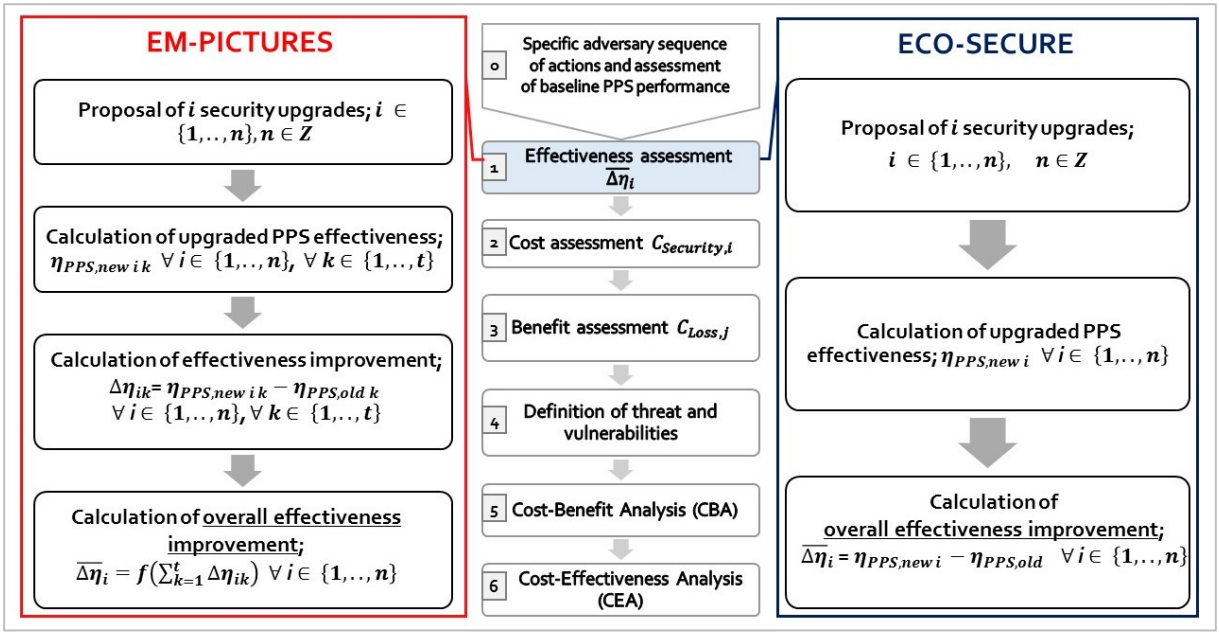


Figure 4. 3 Main contents of Module 1, according to EM-PICTURES and ECO-SECURE versions.

4.2.4 Module 2: cost assessment

This module, which is completely analogous for EM-PICTURES and ECO-SECURE versions, as visible from Figure 4.4, provides the evaluation of costs for each preventive security measure $(C_{Security,i})$. The cost assessment for a security device includes the direct economic costs of applying the device and the indirect costs associated with its use. Therefore, it may include general terms as purchase costs, personnel costs and running costs. On the other hand, also cost terms either specific for each category of PPS or site-specific might be determined. Six main cost categories have been considered. Among these, five are in close analogy with a cost evaluation referred to safety measures for the chemical and process industry (Reniers and Brijs, 2014b), described in Section 3.5: i) initial costs; ii) installation costs; iii) operating costs; iv) maintenance, inspection and sustainability cost; v) other running costs; vi) specific costs. Despite the similarities with the cost classification applied to safety measures (Reniers and Brijs, 2014b), Module 2 contains cost items specifically tailored for physical security measures, as described below.

Initial costs are the costs incurred during the investigation, selection and design phases of the project, involving furthermore the costs of materials, training and eventual guidelines changes (Campbell and Brown, 2003). Installation costs refer to the expenses sustained to put the

security measure in place and ready for use (Campbell and Brown, 2003). The main difference with similar cost evaluations referred to safety measures (e.g. see (Reniers and Brijs, 2014b)) is the absence of a "Production loss cost" term and the different composition of the linked "Start-up cost". Installation of security measures usually does not interfere with the production rate of chemical plants, determining the necessity to neglect this term from the analysis. However, in some situations an integration of safety and security measures has been realized, allowing to extend the term "production loss cost" also to security measures.

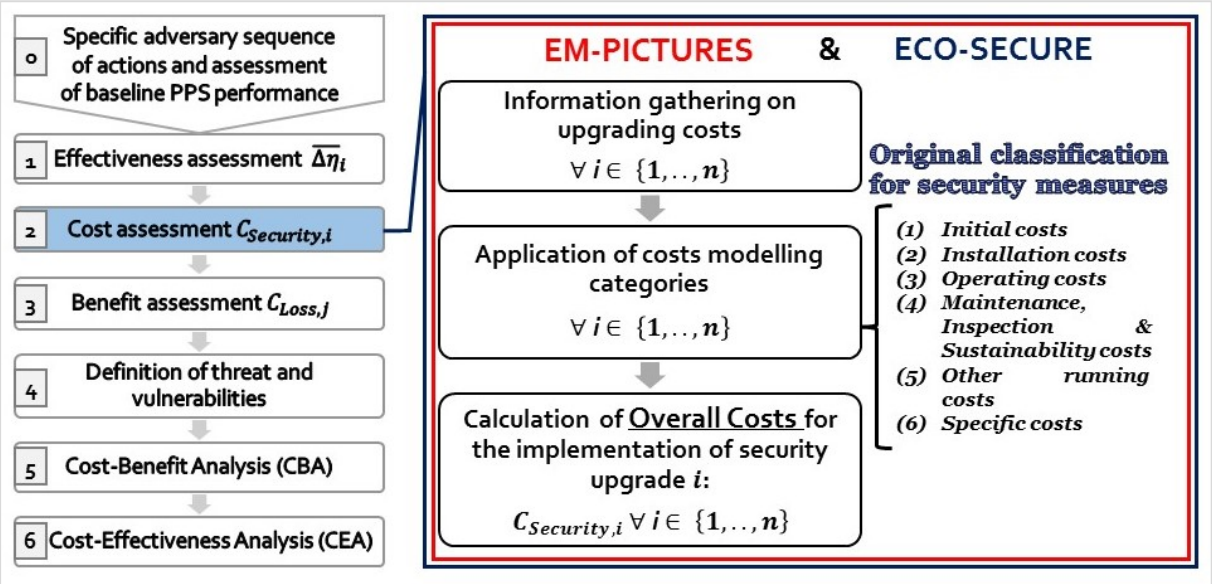


Figure 4. 4 Main contents of Module 2, according to EM-PICTURES and ECO-SECURE versions.

Operating costs are the expenses derived from the operation of the security measure, in terms of utilities consumption and labor (Campbell and Brown, 2003). The maintenance costs should incorporate also inspection and sustainability costs (e.g., renewing license and rental costs). Also, "other running costs" (e.g., cost of providing office furniture, transport, insurance, and stationery items) should be added as a separate category, due to its limited influence on the Overall costs (Campbell and Brown, 2003). The last category ("specific costs") includes all the cost features that are peculiar of a specific category of security measure or a site.

The Overall annual costs due to the implementation of one generic security measure $(C_{Security,i})$ can be calculated as the sum of the six mentioned contributions for each security measure i considered in the analysis:

$$C_{Security,i} = \left(C_{INITIAL,OV} + C_{INSTALL,OV} + C_{OPERATION,OV} + C_{MIS,OV} + C_{OR,OV} + C_{SPEC,OV}\right)_i$$

$$\forall\, i \in \{1,\ldots,n\}, n \in Z \qquad (4.9)$$

Where: $C_{INITIAL,OV}$ is Overall initial costs, $C_{INSTALL,OV}$ is Overall installation costs, $C_{OPERATION,OV}$ is Overall operating costs, $C_{MIS,OV}$ is Maintenance, inspection and sustainability costs, $C_{OR,OV}$ is Other running costs and $C_{SPEC,OV}$ is Overall specific costs.

The expressions applicable to the calculation of each cost category in equation (4.9) were developed according to the fundamentals of CBA (Campbell and Brown, 2003) and reported in Table 4. 1.

In order to calculate each cost category, the costs pertaining to each subcategory identified in Table 4. 1 need to be added:

$$C_C = \sum_{i=1}^{n} C_{SC,i} \tag{4.10}$$

Where C_C is the cost category of interest, and $C_{SC,i}$ is the i-th cost subcategory identified in Table 4. 1.

The expressions reported in Table 4. 1 allow the calculation of the single cost terms for a generic security device. Grouping them into the six mentioned cost categories, the total annual cost due to the implementation a security measure can be computed. The cost estimation can be extended to more than one security device. All the cost terms should be expressed in coherent monetary value.

For the determination of Overall specific costs $(C_{SPEC,OV})$, specific cost subcategories were outlined for each class of security measures, according to their functions and features. As stated by Lee et al. (Lee et al., 2002) cost metrics are often site-specific because each organization has its own security policies and risk factors. Despite the fact that this cost category is open to eventual additional contributions, Overall specific costs were determined as:

$$C_{SPEC,OV} = C_{FP} + C_{SITE\_SP} \tag{4.11}$$

Where C_{FP} indicates Overall cost of a false-positive case and C_{SITE_SP} site-specific costs. The false-positive rate refers to a situation in which the detection device identifies an object (person or thing) as a potential hazard, when it is not (Lin and Van Gulijk, 2015). This error turns into additional security procedures that cause inconvenience to employees, but it may also delay systems operation (i.e., due to re-inspection) and it may eventually turn into a money and person-hours waste and reduced employees confidence toward security systems. The formula proposed by Lin and Van Gulijk (Lin and Van Gulijk, 2015, 2014) was applied to calculate the cost of such events:

$$C_{FP} = C_{FA} \cdot P(FA) = C_{FA} \cdot P(alarm \mid no\ attack) \cdot \left(1 - P(T)_{ij}\right) \tag{4.12}$$

Where: C_{FP} is the Overall cost of a false-positive case, C_{FA} is the cost of a single false-positive case, $P(FA)$ is the false-positive probability or false-alarm probability, $P(T)_{ij}$ is the likelihood

of the attack. $P(FA)$ is a function of the security device and it expresses the probability of having the alarm without an actual threat ($P(FA) = P(alarm, no\ attack)$).

Table 4. 1 Overview on Overall annual cost estimation for a generic security measure. Symbols are listed in the key according to appearance order.

Cost modelling for a generic security measure				
Cost category	**Symbol**	**Cost subcategory**	**Symbol**	**Formula**
INITIAL COSTS	$C_{INITIAL,OV}$	**Investigation costs**	C_{INV}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Selection and design costs	$C_{S\&D}$	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Material costs	$C_{MAT,I}$	$\sum_{i=1}^{s} C_{M,i} \cdot N_{M,i}$
		Training costs (start-up/in service)	C_T	$\left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_{start-up} + \left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_{service}$
		Changing of guidelines and informing costs	$C_{G\&I}$	$\sum_{i=1}^{s} C_{G\&I,i} \cdot n_i$
INSTALLATION COSTS	$C_{INSTALL,OV}$	**Start-up costs**	C_{START}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Equipment costs (including P - purchase & R - rental costs, space requirement costs)	C_E	$\left(\sum_{i=1}^{s} C_{E,i} \cdot N_{E,i}\right)_P + \left(\sum_{i=1}^{s} C_{E,i} \cdot N_{E,i}\right)_R + \sum_{i=1}^{s} C_{Space,i} \cdot V_{E,i} \cdot N_{E,i}$
		Installing costs	$C_{INSTALL}$	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
OPERATING COSTS	$C_{OPERATION,OV}$	**Utilities costs**	$C_{U,OP}$	$\sum_{i=1}^{s} C_{M,i} \cdot N_{M,i}$
		Human resources operating costs	C_{HRO}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
MAINTENANCE, INSPECTION & SUSTAINABILITY COSTS	$C_{MIS,OV}$	**Material costs**	$C_{MAT,M}$	$\sum_{i=1}^{s} C_{M,i} \cdot N_{M,i}$
		Maintenance team costs (A- scheduled m. /B- unscheduled m.)	C_{MNT}	$\left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_A + \left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_B$
		Inspection team costs	C_{INSP}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		License and rental renewal	C_{LIC}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
OTHER RUNNING COSTS	$C_{OR,OV}$	**Office furniture costs**	C_{OF}	$C_{U,OF} \cdot A_{office}$
		Transport costs	C_T	-
		Additional communication costs	C_{COMM}	-
		Insurance costs	C_I	-
		Office utilities costs	C_{OU}	$C_{U,OU} \cdot A_{office}$
		Office supplies costs	C_{OS}	-
SPECIFIC COSTS	$C_{SPEC,OV}$	**False-positive case costs**	C_{FP}	$C_{FA} \cdot P(FA)$
		Site-specific costs	C_{SITE_SP}	-

Table 4. 1 (continued) Overview on Overall annual cost estimation for a generic security measure. Symbols are listed in the key according to appearance order.

Key			
Symbol	**Definition**	**Symbol**	**Definition**
w_i	*Hourly wage of category i* $\left(\frac{€}{h \cdot person}\right)$	n_i	*Number of employees of category i (n° people)*
h_i	*Number of hours of category i* (h)	t	*Number of employee categories*
$C_{M,i}$	*Price for unit of material i* $\left(\frac{€}{unit}\right)$	$N_{M,i}$	*Amount of units for material i (n° units)*
s	*Number of different materials (or equipment)*	$C_{G\&I,i}$	*Unit cost for changing of guidelines and informing* $\left(\frac{€}{unit}\right)$
$C_{E,i}$	*Price for unit of equipment i* $\left(\frac{€}{unit}\right)$	$N_{E,i}$	*Amount of units for equipment i (n° units)*
$C_{Space,i}$	*Space requirement cost for unit of equipment i* $\left(\frac{€}{unit \cdot m^3}\right)$	$V_{E,i}$	*Volume of equipment i* (m^3)
$C_{U,OF}$	*Cost of office furniture per unit area* $\left(\frac{€}{m^2}\right)$	A_{office}	*Total office area* (m^2)
C_T	*Cost of transport* (€)	C_{COMM}	*Cost of communication (e.g., post, phones, mails, etc.)* (€)
C_I	*Cost of insurance* (€)	$C_{U,OU}$	*Cost of office utilities per unit area* $\left(\frac{€}{m^2}\right)$
C_{OS}	*Cost of office supplies* (€)	C_{FA}	*Cost of a single false-positive case* (€)
$P(FA)$	*False-alarm probability (adimensional)*		

The right member of equation (4.12) has been determined by applying the probability chain rule to $P(FA)$, with $P(FA) = P(alarm \mid no\ attack) \cdot \left(1 - P(T)_{ij}\right)$. Further details on the formula might be retrieved from a deliverable of SURVEILLE European Project on surveillance devices (Lin and Van Gulijk, 2014). Therefore, false-positive costs depend on the assumption regarding the likelihood of the attack. Assuming the likelihood of the attack equal to 1 (i.e., a possible value according to the deterministic approach) turns false-positive costs to zero. Indeed, it leads to the minimum specific costs value, and consequently to the minimum Overall costs for a generic security measure. Setting $P(T)_{ij} = 0$ leads to the maximum value of specific costs and consequently to the maximum value of Overall costs for a generic security measure. Therefore, the overall costs for a generic security measure, corresponding to intermediate values of $P(T)_{ij}$, fall within these extremes. Further information on the definition of the likelihood of the attack is reported in Section 4.2.6.

Site-specific costs $\left(C_{SITE\_SP}\right)$ can be eventually added when available. An example of typical site-specific costs might be the cost related to modification of safety measures/procedures necessary to accomplish the company safety standards after the implementation of the security measure. Therefore, specific costs are represented by a range of values (i.e., solely for detection elements), determining consequently a range of values for Overall costs of a generic security measure. Nevertheless, in case of a narrow range of values for overall costs, meaning very low values of specific costs with respect to overall costs, this dependence may be neglected.

4.2.5 Module 3: benefit assessment

Benefit assessment consists on the definition of the costs of an either prospective or retrospective accident scenario j among m possible ones.

Therefore, benefit assessment requires the quantification of the losses (i.e., named also damages) derived from a successful terroristic attack or, generally, from a security-based accident $(C_{Loss,j})$. Benefit modelling was indicated as module 3 in the general model layout (Figure 4. 1). As reported by CCPS (CCPS - Center for Chemical Process Safety, 2003), a security risk assessment, as well as the related selection and implementation of security measures, requires a definition either of reference assets or of reference scenarios, leading respectively to an "asset-based approach" and to a "scenario-based approach". Despite the accidental or intentional nature of the event, a scenario-based approach is aimed at quantifying the probability of occurrence of a given outcome, as well as its causal chain and its consequences in terms of production loss, human health loss, assets loss, and environmental loss (CCPS - Center for Chemical Process Safety, 2003).

As stated by Reniers (Reniers, 2010), in the case of security risk assessment within the chemical and process industry, a scenario-based approach might be more familiar to experts of safety risk assessment, wherein scenario-thinking is widely applied to picture possible unwanted situations. Considering that the effects of accidental or intentional events are often comparable (Nolan, 2008), in the tentative selection of security scenarios those considered for safety thinking can be considered. Le Sage (Le Sage, 2013) stressed the importance of considering in the security field a wide range of fictional scenarios to identify to which extent the proposed security measures can mitigate the identified risks (or threats) and fit within their operational context.

If available, information should be gathered on previous accidents triggered by terroristic attacks on similar reference installations. In case of a retrospective analysis (i.e., posterior application based on a real security-based accident), the actual losses sustained in the attack, named realistic benefits, may be accounted. In case of a prospective analysis, if available, information should be gathered on previous accidents triggered by terroristic attacks on similar reference installations. An expected scenario, which considers the average hypothetical benefits, weighted by probabilities of occurrence, of different possible outcomes, can be indeed considered in the scenario selection phase with reference to prospective analysis (US Department of Defense, 2000). In this model, a rating for consequence severity composed by four categories; for instance T1 (i.e., catastrophic accident), T2 (i.e., critical accident), T3 (i.e., marginal accident) and T4 (i.e., negligible accident), has been adapted from a previous study (US Department of Defense, 2000). The mentioned approach has been already applied to the

economic analysis of safety prevention investments within the chemical industry (Reniers and Sörensen, 2013b).

Otherwise, in case of no information available regarding scenario selection and prospective analysis, a "worst-case scenario" should be taken into account. In fact, adversaries (e.g., in case of environmental-terrorism, eco-terrorism or generic malicious acts) deliberately search for the best manner to execute their plans. This means that they are aiming to cause as much damage as possible, and therefore, certain scenarios that would be labelled as extremely unlikely in case of safety thinking, might actually be considered in case of security thinking (Reniers and Audenaert, 2014). Therefore, also a "worst-case scenario", should be taken into account in the security domain. For instance, the application of both expected and worst-case scenarios is considered common practice within economic analyses for safety purposes in the chemical industry domain (Reniers and Van Erp, 2016). For what concerns the definition of probability for each scenario, the model framework allows considering different values of $P(T)_{ij}$ for different scenarios, if the security analyst deems it necessary.

The losses derived from a successful attack include the damages, both direct and indirect, which will accrue because of a successful attack, taking into account the value and vulnerability of people, environment and infrastructure.

Generally, in CBA approach, a monetary quantification of both direct and indirect losses is carried out, but also non-quantifiable damages (i.e., psychological and political effects) should be at least mentioned (Stewart and Mueller, 2011), as described in Section 3. 5. Quantification of direct tangible costs (e.g., replacement costs due to property damage) is quite straightforward. The quantification of indirect losses has been carried out within the model, provided that they are often comparable or even superior to direct losses (Reniers and Brijs, 2014b). The indirect losses derived from a major accident include reputational losses, legal expenses, costs due to accident investigation, involving both internal and external personnel, costs related to supply-chain delays and bottlenecks at the start-up phase (Gavious et al., 2009). On the other hand monetizing intangible terms related to a terroristic attack (e.g., value of human lives loss after an attack, long-term environmental consequences, fear or social issues emerging after the attack, sufferance and victimization costs) is a very difficult task that has always arisen ethical dilemma since its introduction (Hansson, 2007; Kelman, 1981). Among these terms, the most controversial issue is the assignment of a monetary figure on a person's life (Ackerman and Heinzerling, 2002; Ale et al., 2015). Although the monetization of the value of human lives loss after an attack is a common practice in CBA (Cropper and Sahin, 2009; Viscusi and Aldy, 2003), it has arisen ethical concerns since its introduction (Kelman, 1981). Indeed, the definition of the "Value of a Statistical Life" (VSL) has been defined a "complicated situation" (Tappura et al., 2014) and a "philosophical problem" (Hansson, 2007)

within the cost-benefit analysis domain. As reported by Viscusi and Aldy (Viscusi and Aldy, 2003), the variability of VSL all over the world may give raise to ethical issue and criticism. Despite detailed descriptions, which can be found elsewhere (Nicola Paltrinieri et al., 2012; Viscusi and Aldy, 2003), it should be clear that the monetary value is referred to as "Value of a Statistical Life" (i.e., VSL), avoiding any personal involvement. Indeed, also the monetary estimation of environmental damages may raise ethical bias, as it reflects the subjective environmental attitude of the analyst (Spash, 1997). Furthermore, environmental and health consequences of a hazardous substance release, as demonstrated by the notorious Seveso accident in Italy (1976), may last over 40 years. Indeed, as stressed by Lin and Van Gulijk (Lin and Van Gulijk, 2015) the alternative of not recognizing these damages is probably even more arguable. For instance, an alternative approach to economic analysis with respect to the model here-in presented, may require different studies for tangible assets and intangible damages (i.e., human losses) to solve the mentioned issue (Hansson, 2007).

The main steps of module 3 are analogous between EM-PICTURES and ECO-SECURE, as visible from Figure 4. 5. The aim of the module is the calculation of the Overall benefits that indicates, within risk assessment domain (Reniers, 2010), the damages derived from an accidental scenario $(C_{Loss,j})$. However, benefit classification is different, depending of the focus of the application, even if benefit categories within the security domain, for both EM-PICTURES and ECO-SECURE, have been developed in analogy with a similar study referred to the safety domain for the chemical and process industry (e.g., the CESMA tool described in Section 3.5 (Reniers and Brijs, 2014b)). The details concerning the loss categories of the present study, according to EM-PICTURES and ECO-SECURE versions, have been reported below.

Regarding EM-PICTURES version, the Overall annual benefits (i.e., avoided losses) derived from a generic accidental scenario $(C_{Loss,j})$ can be computed as the sum of nine benefit categories, for each scenario j considered in the analysis:

$$C_{Loss,j} = \left(B_{SUPC,OV} + B_{DAMAGE,OV} + B_{LEGAL,OV} + B_{INS,OV} + B_{H\&E,OV} + B_{INTV,OV} + B_{REPT,OV} + B_{OTH,OV} + B_{SPEC,OV}\right)_j$$

$$\forall j \in \{1,\dots,m\}, m \in Z \qquad (4.13)$$

Where: $B_{SUPC,OV}$ is Overall supply chain benefits, $B_{DAMAGE,OV}$ is Overall damage benefits, $B_{LEGAL,OV}$ is Overall legal benefits, $B_{INS,OV}$ is Overall insurance benefits, $B_{H\&E,OV}$ is Overall human and environmental benefits, $B_{INTV,OV}$ is Overall intervention benefits, $B_{REPT,OV}$ is Overall reputation benefits, $B_{OTH,OV}$ is Overall other benefits and $B_{SPEC,OV}$ is Overall specific benefits.

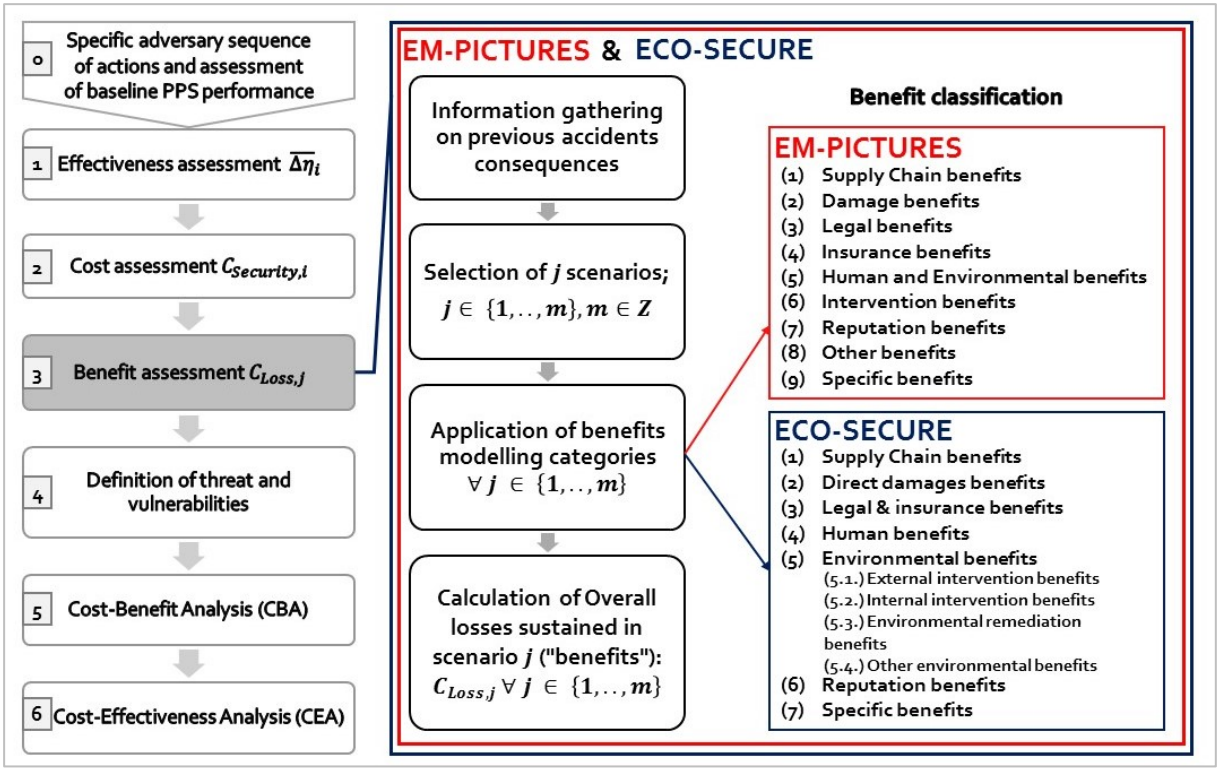


Figure 4. 5 Main contents of Module 3, according to EM-PICTURES and ECO-SECURE versions.

Regarding ECO-SECURE version, the categories and subcategories referred to the costs of each scenario were adapted to enhance the focus on short-term and long-term environmental damages. Within ECO-SECURE, Overall benefits can be computed as the sum of seven contributions, for each scenario j considered in the analysis:

$$C_{Loss,j} = \left(B_{SUPC,OV} + B_{DMG,OV} + B_{LGL\&INS,OV} + B_{H,OV} + B_{ENV,OV} + B_{REPT,OV} + B_{SPEC,OV}\right)_j$$

$$\forall j \in \{1,\ldots,m\}, m \in Z \qquad (4.14)$$

Where: $B_{SUPC,OV}$ is Overall supply chain benefits, $B_{DMG,OV}$ is Overall damage benefits, $B_{LGL\&INS,OV}$ is Overall legal and insurance benefits, $B_{H,OV}$ is Overall human benefits, $B_{ENV,OV}$ is Overall environmental benefits, $B_{REPT,OV}$ is Overall reputation benefits and $B_{SPEC,OV}$ is Overall specific benefits.

The expressions applicable to the calculation of each benefit category were developed accordingly to the fundamentals of CBA (Campbell and Brown, 2003) and are reported in Table 4. 2 and Table 4. 3, for EM-PICTURES and ECO-SECURE versions respectively.

In order to calculate each benefit category, for both EM-PICTURES and ECO-SECURE versions, the benefits pertaining to each subcategory identified in the mentioned table need to be added:

$$C_B = \sum_{i=1}^{n} C_{SB,i} \qquad (4.15)$$

Where C_B is the benefit category of interest, and $C_{SB,i}$ is the i-th benefit subcategory identified in Table 4. 2 for EM-PICTURES and in Table 4. 3 for ECO-SECURE respectively.

The expressions reported in Table 4. 2 and Table 4. 3 allow the calculation of the single benefit terms for either a prospective or a retrospective accidental scenario, according to EM-PICTURES and ECO-SECURE. Grouping them in the pertinent benefits categories (i.e., nine in EM-PICTURES, seven in ECO-SECURE), the total losses due to a generic accidental scenario can be computed. All the benefits terms should be expressed in coherent monetary value (e.g., all of them should be expressed in €/2016). Although this category is open to eventual additional contributions, Overall specific benefits have been determined, both in EM-PICTURES and in ECO-SECURE as:

$$B_{SPEC,OV} = B_{SITE\_SP} + B_{IMM} \tag{4.16}$$

Specific benefits are mostly site-specific (B_{SITE_SP}) and should be considered in case of additional information available. If additional information is available, also other immaterial terms (B_{IMM}), such as the "cost of fear", psychological damages, social and political tensions might be added to the analysis.

Table 4. 2 Overview on Overall annual benefits estimation for a generic accidental scenario, according to EM-PICTURES version. The table key is available in Table 4. 4.

Benefit modelling for a generic scenario				
Benefit category	**Symbol**	**Benefit subcategory**	**Symbol**	**Expression**
SUPPLY CHAIN BENEFITS	$B_{SUPC,OV}$	**Production loss benefits**	B_{PL}	$Q \cdot t_{PS} \cdot Pr_U$
		Start-up benefits	B_{START}	$(Q - Q^*) \cdot t_D \cdot Pr_U$
		Schedule benefits	B_{SCH}	$(F_{canc} \cdot n_{canc}) + (F_d \cdot n_d \cdot d) + \left(n_{con} \cdot (C_{con} - C_{in\_h})\right)$
DAMAGE BENEFITS	$B_{DAMAGE,OV}$	**Damage to own material/property**	$B_{D,OM\&P}$	$A + B + C$
		Damage to other companies' material/property	$B_{D,OCM\&P}$	$D + E + F$
		Damage to surrounding living area	$B_{D,SA}$	G
		Damage to public material property	$B_{D,PM\&P}$	$H + I + J$
LEGAL BENEFITS	$B_{LEGAL,OV}$	**Fines-related benefits**	B_{FINES}	$K + L + M$
		Interim lawyers benefits	B_{ILAW}	$w_{SL} \cdot n_{SL} \cdot d_{SL} + w_{JL} \cdot n_{JL} \cdot d_{JL}$
		Specialized lawyer benefits	B_{SLAW}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Internal research team benefits	B_{IREST}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Expert at hearings benefits	B_{EH}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Legislation benefits	B_{LEG}	$S_B \cdot I_{SB}$
		Permit and license benefits	$B_{P\&LIC}$	$C_{CD} \cdot L_P$
INSURANCE BENEFITS	$B_{INS,OV}$	**Insurance premium benefits**	$B_{P,INS}$	$P_F \cdot I_{PF}$
HUMAN AND ENVIRONMENTAL BENEFITS	$B_{H\&E,OV}$	**Compensation victims benefits**	$B_{H,CF}$	$VSL \cdot n_F$
		Injured employees benefits	$B_{H,IE}$	$C_{LI} \cdot n_{LI} + C_{SI} \cdot n_{SI}$
		Recruit benefits	$B_{H,RECR}$	$\sum_{i=1}^{t} (C_{H,i} + C_{T,i}) \cdot n_i$
		Environmental damage benefits	B_E	$\left(\sum_{i=1}^{y} m_{SP,i} \cdot C_{SP,i}\right)$
INTERVENTION BENEFITS	$B_{INTV,OV}$	**Intervention benefits**	-	$F_{INT} + P_{INT} + A_{INT} + S_{INT}$
REPUTATION BENEFITS	$B_{REPT,OV}$	**Share price benefits**	B_{SP}	$M_{REP} \cdot D_{REP}$
OTHER BENEFITS	$B_{OTH,OV}$	**Manager work-time benefits**	B_{MWT}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Cleaning benefits	B_{CLN}	$w_c \cdot h_c \cdot n_c$
SPECIFIC BENEFITS	$B_{SPEC,OV}$	**Site-specific benefits**	B_{SITE_SP}	-
		Immaterial benefits	B_{IMM}	-

Table 4. 3 Overview on Overall annual benefits estimation for an accidental scenario, with focus on environmental benefits, according to ECO-SECURE version. The table key is available in Table 4. 4.

Benefit modelling for an environmental scenario				
Benefit category	**Symbol**	**Benefit subcategory**	**Symbol**	**Expression**
SUPPLY CHAIN BENEFITS	$B_{SUPC,OV}$	**Production loss benefits**	B_{PL}	$Q \cdot t_{PS} \cdot Pr_U$
		Start-up benefits	B_{START}	$(Q - Q^*) \cdot t_D \cdot Pr_U$
		Schedule benefits	B_{SCH}	$(F_{canc} \cdot n_{canc}) + (F_d \cdot n_d \cdot d) + \left(n_{con} \cdot (C_{con} - C_{in\_h})\right)$
DAMAGE BENEFITS	$B_{DMG,OV}$	**Damage to own material/property**	$B_{D,OM\&P}$	$A + B + C$
		Damage to other companies material/property	$B_{D,OCM\&P}$	$D + E + F$
		Damage to surrounding living area	$B_{D,SA}$	G
		Damage to public material/property	$B_{D,PM\&P}$	$H + I + J$
LEGAL & INSURANCE BENEFITS	$B_{LGL\&INS,OV}$	**Fines-related benefits**	B_{FINES}	$K + L + M$
		Interim lawyers benefits	B_{ILAW}	$w_{SL} \cdot n_{SL} \cdot d_{SL} + w_{JL} \cdot n_{JL} \cdot d_{JL}$
		Specialized lawyer benefits	B_{SLAW}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Internal research team benefits	B_{IREST}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Expert at hearings benefits	B_{EH}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Legislation benefits	B_{LEG}	$S_B \cdot I_{SB}$
		Permit and license benefits	$B_{P\&LIC}$	$C_{CD} \cdot L_P$
		Insurance premium benefits	B_{INS}	$P_F \cdot I_{PF}$
HUMAN BENEFITS	$B_{H,OV}$	**Compensation victims benefits**	$B_{H,CF}$	$VSL \cdot n_F$
		Injured employees benefits	$B_{H,IE}$	$C_{LI} \cdot n_{LI} + C_{SI} \cdot n_{SI}$
		Recruit benefits	$B_{H,RECR}$	$\sum_{i=1}^{t} (C_{H,i} + C_{T,i}) \cdot n_i$
ENVIRONMENTAL BENEFITS	$B_{ENV,OV}$	**External intervention benefits (salaries related to emergency interventions / materials / post-accident monitoring / others)**	$B_{E,INTV}$	$\sum_{i=1}^{z} C_{S,i} + \sum_{i=1}^{s} C_{ME,i} \cdot N_{ME,i} + \sum_{i=1}^{v} C_{MONIT,i} \cdot N_{MONIT,i} + C_{OTH,INTV}$
		Internal intervention benefits (manager work-time benefits/ cleaning benefits)	$B_{I,INTV}$	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i + (w_c \cdot h_c \cdot n_c)$
		Environmental remediation benefits (short-term / long-term)	B_{REM}	$\left(\sum_{i=1}^{y} m_{SP,i} \cdot C_{SP,i}\right) + C_{REM,LT}$
		Other environmental benefits	$B_{OTH,ENV}$	-
REPUTATION BENEFITS	$B_{REPT,OV}$	**Share price benefits**	B_{SP}	$M_{REP} \cdot D_{REP}$
SPECIFIC BENEFITS	$B_{SPEC,OV}$	**Site-specific benefits**	B_{SITE_SP}	-
		Immaterial benefits	B_{IMM}	-

Table 4. 4 Table key referred to Overall annual benefits estimation for an accidental scenario, according to both EM-PICTURES and ECO-SECURE versions of the model. Symbols are listed according to the order of appearance in Table 4. 2 and Table 4. 3.

Key			
Symbol	**Definition**	**Symbol**	**Definition**
Q	*Production rate of the factory* $\left(\frac{n°units}{h}\right)$	t_{PS}	*Duration of the stop in production* (h)
Pr_U	*Profit per unit sold* $\left(\frac{€}{unit}\right)$	Q^*	*Production rate of the factory at the start of line reactivation* $\left(\frac{n°units}{h}\right)$
t_D	*Duration of reduced production during reactivation* (h)	F_{canc}	*Fine for a cancelled order/contract* $\left(\frac{€}{contract}\right)$
n_{canc}	*N° of orders/contracts cancelled* $(n°contracts)$	F_d	*Fine for delays in deliveries per day* $\left(\frac{€}{delay \cdot day}\right)$
n_d	*N° of orders with a delay* $(n°delay)$	d	*N° days of tardiness in the orders* $(n°days)$
n_{con}	*N° of units given by the contractor* $(n°units)$	C_{con}	*Cost per unit asked by the contractor* $\left(\frac{€}{unit}\right)$
C_{in_h}	*In-house cost per unit* $\left(\frac{€}{unit}\right)$	A	*Damage to the company equipment and machines* (€)
B	*Damage to the company buildings and other infrastructures* (€)	C	*Damage to the company raw materials and finished goods* (€)
D	*Damage to other companies equipment and machines* (€)	E	*Damage to other companies buildings and other infrastructures* (€)
F	*Damage to other companies raw materials and finished goods* (€)	G	*Damage to surrounding living area* (€)
H	*Damage to public equipment and public machines* (€)	I	*Damage to public buildings and other public infrastructure* (€)
J	*Damage to public materials and public goods* (€)	K	*Civil liability fines* (€)
L	*Criminal liability fines* (€)	M	*Administrative liability fines* (€)
w_{JL}	*Hourly wage of junior lawyers* $\left(\frac{€}{day \cdot lawyer}\right)$	w_{SL}	*Hourly wage of senior lawyers* $\left(\frac{€}{day \cdot lawyer}\right)$
n_{SL}	*Number of senior lawyers* $(n° lawyers)$	n_{JL}	*Number of junior lawyers* $(n° lawyers)$
d_{SL}	*Number of work days per senior lawyers* $(n° days)$	d_{JL}	*Number of work days per junior lawyers* $(n° days)$
w_i	*Hourly wage of category i* $\left(\frac{€}{h \cdot person}\right)$	h_i	*Number of hours of category i* (h)
n_i	*Number of employees of category i (n° people)*	t	*Number of employees categories*
S_B	*Total security budget of the facility* (€)	I_{SB}	*Increase of the security budget for the facility after major accident occurrence* (%)
C_{CD}	*Cost due to facility close-down* (€)	L_P	*Likelihood of losing operating permit* (%)
P_F	*Current total premium cost of the facility* (€)	I_{PF}	*Expected increase of the premium* (%)
VSL	*Value of a statistical life* $\left(\frac{€}{person}\right)$	n_F	*Number of fatalities* $(n° people)$
C_{SI}	*Cost of one serious injured worker* $\left(\frac{€}{person}\right)$	n_{SI}	*Number of serious injured workers* $(n° people)$
C_{LI}	*Cost of one light injured worker* $\left(\frac{€}{person}\right)$	n_{LI}	*Number of light injured workers* $(n° people)$
$C_{H,i}$	*Hiring cost per employee of category i* $\left(\frac{€}{person}\right)$	$C_{T,i}$	*Training cost per employee of category i* $\left(\frac{€}{person}\right)$
F_{INT}	*Fire department costs charged to the company* (€)	P_{INT}	*Police department costs charged to the company* (€)
A_{INT}	*Ambulance service costs charged to the company* (€)	S_{INT}	*Special units costs charged to the company* (€)
$C_{ME,i}$	*Unit cost for material i applied during emergency intervention* $\left(\frac{€}{unit}\right)$	$N_{ME,i}$	*Amount of units of material i applied during emergency intervention (n° units)*
s	*Number of emergency materials applied during emergency intervention*	$C_{MONIT,i}$	*Unit cost of monitoring action type i* $\left(\frac{€}{unit}\right)$
$N_{MONIT,i}$	*Number of monitoring actions type i (n° units)*	v	*Number of monitoring actions categories*
$C_{OTH,INTV}$	*Other environmental costs* (€)	w_c	*Hourly wage of a cleaning employee* $\left(\frac{€}{h \cdot person}\right)$
n_c	*Number of cleaning employees (n° cleaning employees)*	h_c	*Number of hours worked by a cleaning employee* (h)
$m_{SP,i}$	*Amount of product i spilled* (kg) *or* (m^3)	$C_{SP,i}$	*Cost per unit of product i spilled* $\left(\frac{€}{kg}\right)$ *or* $\left(\frac{€}{m^3}\right)$
y	*Number of products spilled*	$C_{REM,LT}$	*Long-term remediation costs* (€)
M_{REP}	*Current total market value of the company* (€)	D_{REP}	*Expected drop in the share price* (%)

4.2.6 Module 4: definition of threat and vulnerabilities

In module 4, the threat likelihood and the vulnerability probabilities to be considered in the economic analysis are determined, according to the steps reported in Figure 4. 6. The threat likelihood ($P(T)_{ij}$), named also "likelihood of the attack" and "probability of the attack", expresses the probability of an individual or a group with adequate motivation and capability to attack a chemical and process facility, committing theft, sabotage or other malevolent acts that would result in loss of assets.

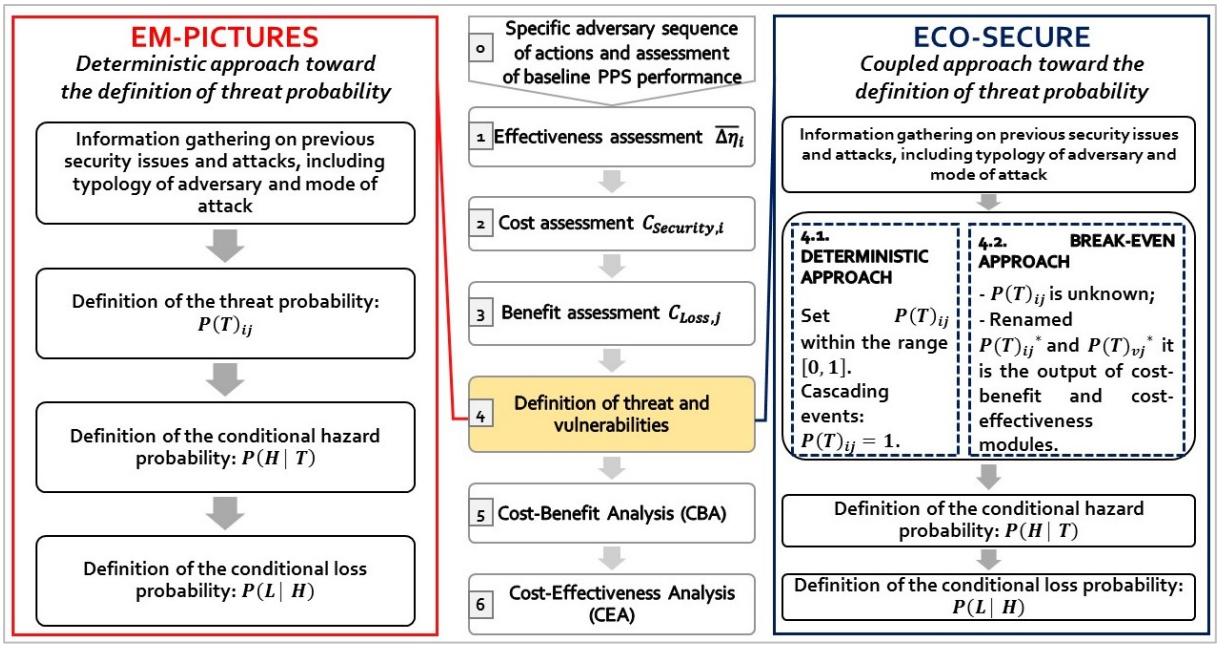


Figure 4. 6 Main contents of Module 4, according to EM-PICTURES and ECO-SECURE versions.

Threat assessment is aimed at quantifying the actual or potential threat on a facility by means of statistical data treatment, based on expert elicitation, as well as on available intelligence, law enforcement and open source information.

However, the probability of terroristic attacks on chemical installation is context-sensitive and therefore it may vary significantly over time, depending on social and political phenomena (European Commission, 2008). As stated by Stewart and Mueller (Stewart and Mueller, 2013), assessing the probability of terrorist acts is a challenging task, because terrorism is a phenomenon of multi-causal factors and terrorists deliberate effort to defy prediction. The complexity of terrorism combined with the unique attributes of individual groups makes it nearly impossible to capture the explanatory characteristics of the phenomenon in a single variable (i.e., the probability of the attack) (European Commission, 2008). Indeed, several authors (Garcia, 2007; Stewart and Mueller, 2013; Villa et al., 2016) stressed the difficulty to get a significant estimate of this term.

Therefore, in the presence of uncertainties and lack of information on this term, two approaches can be applied:

Module 4.1 Deterministic approach. In this case, a defined value of $P(T)_{ij}$ within the range [0,1] is assumed, and is considered an input of the economic analysis. A possible guidance in the choice of the threat probability, adapted from Stewart and Mueller (Stewart and Mueller, 2012) has been reported in Table 4. 5. As suggested by Garcia (Garcia, 2005), in case of unacceptably high consequences (i.e., major accidents with possibility of cascading effects, national security at stake), for both prospective and retrospective accidents, a conditional threat approach may be applied: it implies to consider $P(T)_{ij} = 1$. This assumption means that the consequences of a possible attack are so severe that the estimation of the threat probability is not required; therefore, it allows focusing on the role of security measures management.

Module 4.2 Break-even approach. According to this approach $P(T)_{ij}$, renamed ${P(T)_{ij}}^*$ and ${P(T)_{vj}}^*$, respectively for cost-benefit and cost-effectiveness analyses, is the output of the economic analyses and it represents the minimum threat probability required for the benefits of a specific scenario j to equal the costs of a security measure i (or a combination of security measures v); the threat probability is calculated in modules 5 and 6.

According to EM-PICTURES version, just a deterministic approach to the threat probability is carried out (i.e., Module 4.1); this requires performing an additional sensitivity analysis. According to ECO-SECURE version, a coupled approach toward the threat likelihood, including deterministic (i.e., Module 4.1) and break-even (i.e., Module 4.2) approaches is applied. The application of a break-even approach offers a sensitivity analysis on the likelihood of the attack, directly included in the model.

For both EM-PICTURES and ECO-SECURE typologies of applications, module 4 is aimed at defining also the vulnerability probabilities, which are $P(H|\,T)$ and $P(L|\,H)$. $P(H|\,T)$ is the conditional probability of a hazard that indicates an initiating event leading to damage and loss of life, which can be expressed as follows (Stewart and Mueller, 2012):

$$P(H|\,T) = PSF \cdot R_{IED} \tag{4.17}$$

Where R_{IED} expresses the reliability of the device, which is often an improvised explosive device (i.e., IED) (Landucci et al., 2015b); the Performance Shaping Factors (i.e., PSF) represents the performance of adversaries in the use of the device, depending on its complexity, on adversary skills and location. $P(L|\,H)$ guidance global data referred to terroristic organizations and other typologies of adversaries (e.g., insurgent organization, criminals) have been reported in Table 4. 5; more detailed information regarding specific geographical areas can be found elsewhere (Stewart and Mueller, 2012).

$P(L|H)$ is the conditional probability of loss or consequences (e.g., having at least asset damages), given the occurrence of a hazard; guidance values have been reported in Table 4. 5.

The product of threat and vulnerability probability is sometimes indicated as a single term (i.e., P_A) (Stewart and Mueller, 2012, 2011, 2008), expressing the probability of a "successful" attack:

$$P_A = P(T) \cdot P(H|T) \cdot P(L|H) \quad (4.18)$$

However, in the present model, it was preferred to maintain threat and vulnerabilities as separate terms, in purpose to evaluate clearly their contributions to the final results.

Table 4. 5 Guidance values for the estimation of threat and vulnerability probabilities, retrieved from (Garcia, 2005; Stewart and Mueller, 2012).

Threat severity	**Example of adversaries and malicious act**	$P(T)_{ij}$	$P(L\|H)$
Low	Individual stealing asset/ vandals	0.6	0.25
Medium	Organized criminals/ terrorists stealing assets/ weak sabotage action	0.3	0.80
High	Terrorists aimed at causing a major accident	0.1	1
Conditional threat	Terrorists aimed at causing cascading effects	1	1
$P(H\|T)$			
Reliability of Improvised Explosives Devices			
Device complexity	**Representative IED design**		R_{IED}
Simple	Pipe bomb		0.931
Medium	Mobile phone initiated VBIED (Vehicle Borne Improvised Explosive Device)		0.920
Complex	Improvised mortar		0.910
Conservative assumption	No information available		1
Global Performance Shaping Factors			
Device complexity	***PSF* for organizational culture**		
	Terrorist organization	**Individual**	**Criminal**	**Insurgent organization**
Simple	0.981	0.588	1	1
Medium	0.980	0.695	0.972	1
Complex	0.905	-	0.550	1
No information available	1	1	1	1

4.2.7 Module 5: Cost-Benefit analysis for preventive security measures selection

In module 5, the single security measures i that are economically feasible with reference to all the m scenarios are identified. According to EM-PICTURES version, only a deterministic approach is applied, according to the description provided in subsection 4.2.7.1. According to ECO-SECURE version, deterministic and break-even approaches, indicated as module 5.1 and 5.2 in the model flowchart (Figure 4. 1), are coupled, following the procedure explained in

subsections 4.2.7.1 and 4.2.7.2. The content of module 5 is summarized in Figure 4. 7, for both EM-PICTURES and ECO-SECURE typologies of applications.

Before starting an economic analysis, it should be noted that the total benefits and the total costs occur at different points in time. Therefore, it is necessary to introduce a discount rate to convert all cash flows in the future to present values of annuities. This conversion process, named "actualization", is shown by the following formula (Campbell and Brown, 2003):

$$\begin{cases} \bar{C} = C \cdot \frac{((1+r)^z - 1)}{((1+r)^z \cdot r)}, r \neq 0 \\ \bar{C} = C, \ r = 0 \end{cases} \quad (4.19)$$

Where $\bar{C}$ is the actualized value of overall cost or benefit, C is the yearly overall cost or benefit, z is the number of years the security measure will be operating and r represents the discount rate, intended here as the real rate of interest.

4.2.7.1 Module 5.1: Cost-Benefit analysis with deterministic approach

When deterministic approach is applied, the Net Benefit for every security measure i and each scenario j is determined according to the following equation:

$$\begin{cases} Net\ Benefit_{ij} = P(T)_{ij} \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \overline{\Delta\eta}_i - C_{Security,i} \\ \forall i \in \{1, \dots, n\}, n \in Z \\ \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \quad (4.20)$$

Where $Net\ Benefit_{ij}$ indicates the Net benefit obtained by applying a security measure i, among n possibilities, with reference to a specific scenario j, among m scenarios considered in the analysis.

Following the standard CBA terminology, the term $P(T)_{ij} \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \overline{\Delta\eta}_i$ indicates the overall risk variation obtained by the application of security measure i for scenario j, while $C_{Security,i}$ indicates the costs of providing the risk-reducing security measure i that is necessary to obtain the benefits. Equation (4.20) allows considering different values of the threat and vulnerability probabilities for different scenarios, if the security analyst deems it necessary.

According to a deterministic approach, the implementation of a single security measure i is acceptable, with reference to all the m scenarios if:

$$\begin{cases} Net\ Benefit_{ij} \geq 0 \\ \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \quad (4.21)$$

Else, it should be rejected. The calculation of $Net\ Benefit_{ij}$ represents the output of cost-benefit analysis submodule 5.1. The analysis should be repeated for each security measure i and for each scenario j, obtaining therefore $n \times m$ values of Net benefits. A single security measure should be accepted or rejected over all the m scenarios.

Since the purpose of cost-benefit analysis is to support the security risk management and decision-making, often the security risk is made explicit:

$$R = P(T)_{ij} \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \eta_{PPS} \tag{4.22}$$

According to equation (4.21), the risk variation (ΔR_i) achieved by implementing an additional security measure i with reference to the same scenario, depends only on the effectiveness improvement (i.e., $\overline{\Delta\eta_i}$), as follows:

$$\Delta R_i = P(T)_{ij} \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \overline{\Delta\eta_i} \tag{4.23}$$

Indeed, it explains how sometimes the nomenclature for the two terms overlaps (Stewart and Mueller, 2013, 2011, 2008; Villa et al., 2016).

Therefore, Cost-benefit analysis results, according to the deterministic approach, can be presented also in a column graph reporting ΔR_i versus $C_{Security,i}$. According to this alternative presentation the acceptability threshold for the implementation of a single security measure i, with reference to all the m scenarios can be expressed as follows:

$$\begin{cases} \Delta R_i \geq C_{Security,i} \\ \forall j \in \{1,\dots,m\}, m \in Z \end{cases} \tag{4.24}$$

4.2.7.2 Module 5.2: Cost-Benefit analysis with break-even approach

This submodule, which belong to ECO-SECURE version, calculates the break-even point, which is the probability of the attack $P(T)_{ij}{}^{*}$, corresponding to $Net\ Benefit_{ij} = 0$ for every security measure i and each scenario j, according to the following equation:

$$\begin{cases} P(T)_{ij}{}^{*} = \frac{C_{Security,i}}{C_{Loss,j} \cdot \Delta\eta_i} \\ \forall i \in \{1,\dots,n\}, n \in Z \\ \forall j \in \{1,\dots,m\}, m \in Z \end{cases} \tag{4.25}$$

According to a break-even approach, the implementation of a single security measure i is acceptable, with reference to all the m scenarios, if:

$$\begin{cases} P(T)_{ij}{}^{*} \leq P(T)_{ij}{}' \\ \forall j \in \{1,\dots,m\}, m \in Z \end{cases} \tag{4.26}$$

Where $P(T)_{ij}{}'$ is a threshold value for the likelihood of the attack, which can be derived from different sources, as intelligence data or generic accident data gathering, as well as expert elicitation. Else, the security measure should be rejected. The calculation of $P(T)_{ij}{}^{*}$ represents the output of cost-benefit analysis submodule 5.2. The analysis should be repeated for each security measure i and for each scenario j, obtaining therefore n x m values of $P(T)_{ij}{}^{*}$. A single security measure should be accepted or rejected over all the m scenarios. The application of a

break-even approach offers a sensitivity analysis on the likelihood of the attack, directly included in the model.

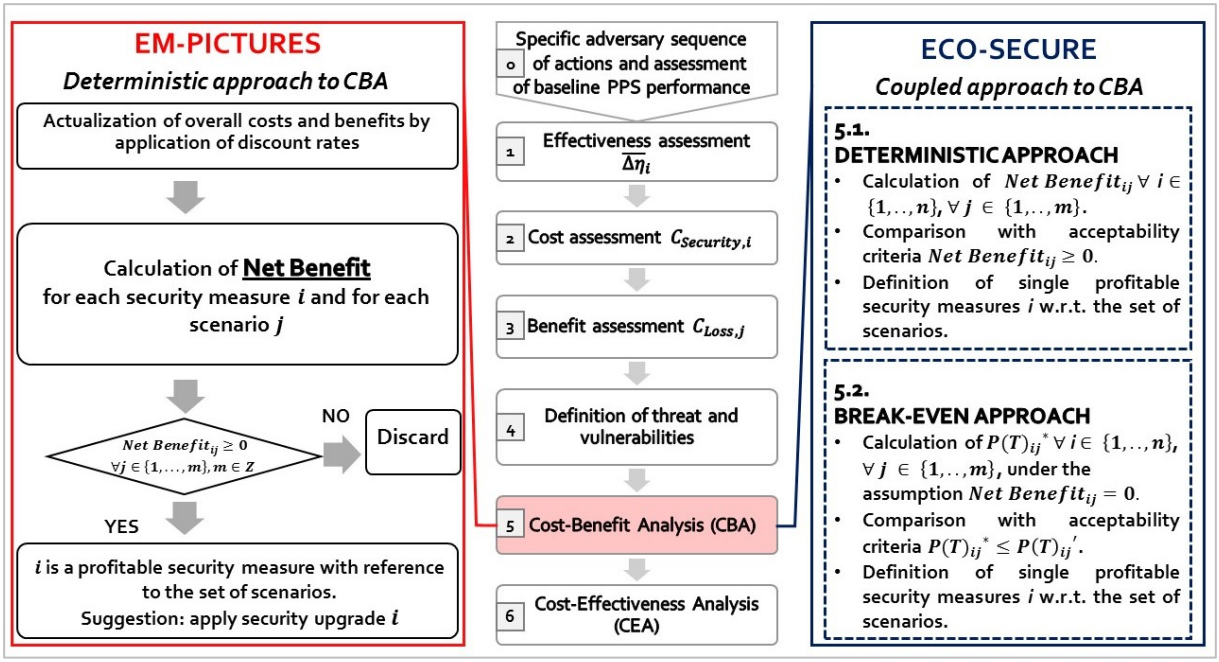


Figure 4. 7 Main contents of Module 5, according to EM-PICTURES and ECO-SECURE versions.

4.2.8 Module 6: Cost-Effectiveness analysis for preventive security measures allocation

This module calculates the most profitable combination of security measures with reference to the scenarios. Often, security investments should be compared with budget limitations. In this situation, the economic evaluation method turns into a cost-effectiveness analysis.

Within EM-PICTURES version, cost-effectiveness analysis is performed according to the deterministic approach described in subsection 4.2.8.1. Within ECO-SECURE version, cost-effectiveness analysis is performed according to both deterministic and break-even approaches, described in subsections 4.2.8.1 and 4.2.8.2 respectively. Then, ECO-SECURE results derived from the two approaches are coupled by means of a specific scoring system, described in subsection 4.2.8.3. The content of module 6 is summarized in Figure 4. 8, for both EM-PICTURES and ECO-SECURE typologies of applications.

4.2.8.1 Module 6.1: Cost-Effectiveness analysis with deterministic approach

According to the deterministic approach, the optimization problem to be solved, known as the "Knapsack problem" in the field of Operations Research, consists on finding the solution of the following system:

$$\begin{cases} \max\left(Net\ Benefit_{vj} \cdot x_v\right) \\ C_v \cdot x_v \leq C_{Budget,j}\ \forall j \in \{1,\dots,m\}, m \in Z \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1,\dots,w\}, w \in Z \end{cases} \quad (4.27)$$

The formulation of the problem is analogous for security measures to the one already applied in the safety domain.

The first equation of the system expresses the total Net benefit from the selected investments portfolio, which should be maximized, hence obtaining the $\max\left(Net\ Benefit_{vj} \cdot x_v\right)$, among all the possible w combinations of security measures, indicated by $v \in \{1,\dots,w\}, w \in Z$. The values of $Net\ Benefit_{vj}$ can be calculated according to equation (4.20), by replacing a single measure i with a combination v. Therefore the calculation should be applied for each combination of security measures v and for each scenario j, obtaining w x m values of Net benefits.

The second equation expresses the fact that the total cost of the selected measures, composing combination v, $(C_v \cdot x_v)$ should not exceed the security budget $\left(C_{Budget,j}\right)$. The same constraint allows discarding directly also single security measures not respecting the budget. The security budget $\left(C_{Budget,j}\right)$ is the total annual monetary amount defined by security managers that can be allocated on a combination of measures. The security budget is often scenario-dependent, as it can vary based on scenario severity. However, in case of unacceptably high losses (e.g., cascading events, national security at stake) security budget might have a lower threshold fixed value, which cannot be reduced. The third constraint $(x_v \in \{0,1\})$ implies that a measures combination is either fully taken or not taken at all.

A number of assumptions are implicitly embedded in this formulation:

- Security investments cannot be partial: a measure is either adopted or not;
- The overall hypothetical benefits of all measures considered is the sum of the individual benefits;
- The overall cost of all security measures adopted (C_v) is the sum of the costs of the individual measures, composing a combination v, as expressed by the second equation;
- Each security measure can be implemented independently, without consequences for the other investments. This simplifying assumption was kept in the present

formulation. However, it might be overcome in future studies by considering reduction cost factors due to the combined implementation of security measures.

The output of submodule 6.1 is the most profitable combination of security measures (v^*), within the constraint of the security budget, for each scenario j, according to deterministic approach. A ranking of all the combinations, in order of decreasing profitability, is provided. However, the top-three most profitable combinations are identified, as they might be the probable final security investments. Therefore, the combinations that are outlined are the most profitable ones, under the deterministic assumption of $P(T)_{ij}$ as a defined value within the range [0,1]. According to EM-PICTURES version, the output of submodule 6.1, which is a set of indicators derived from economic analyses that can support the security decision-making process within the chemical and process industry domain, overlaps with the entire model output.

Therefore, within EM-PICTURES version an additional sensitivity analysis, at least regarding the threat probability, needs to be performed.

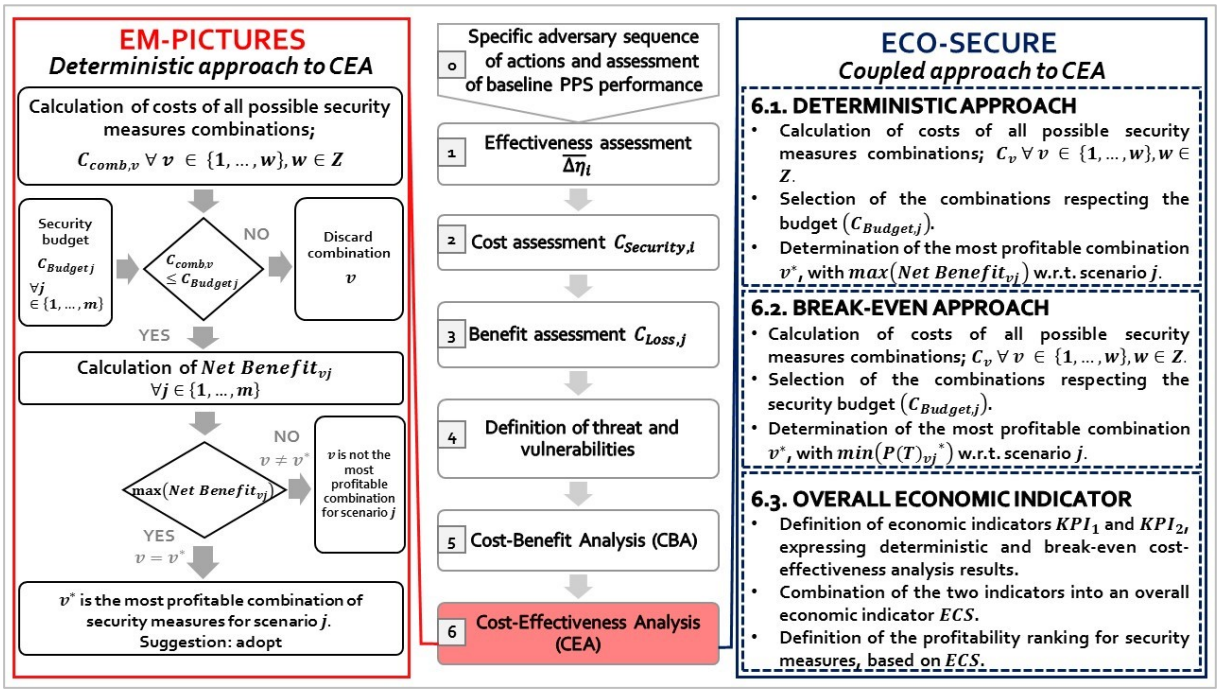


Figure 4. 8 Main contents of module 6, according to EM-PICTURES and ECO-SECURE versions.

It should be noted that the results of cost-effectiveness analysis, according to the deterministic approach, might differ significantly among scenarios. According to ECO-SECURE, the outputs of submodule 6.1 flow into the application of an original scoring system, described in subsection 4.2.8.3, that allows defining an economic indicator expressing overall cost-effectiveness analysis results, derived from multiple scenarios, according to the deterministic approach.

4.2.8.2 Module 6.2: Cost-Effectiveness analysis with break-even approach

ECO-SECURE version of the model include submodule 6.2, which allows performing cost-effectiveness following a break-even approach. In this situation, the optimization problem consists on finding the solution of the following system:

$$\begin{cases} \min\left(P(T)_{vj}{}^{*} \cdot x_v\right) \\ C_v \cdot x_v \leq C_{Budget,j}\ \forall j \in \{1,\dots,m\}, m \in Z \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1,\dots,w\}, w \in Z \end{cases} \quad (4.28)$$

The first equation of the system (4.28) expresses the probability of the attack with the application of a selected investments portfolio, which should be minimized, hence obtaining $\min\left(P(T)_{vj}{}^{*} \cdot x_v\right)$, among all the possible w combinations of security measures, indicated by $v \in \{1,\dots,w\}, w \in Z$. Therefore, the calculation should be applied for each combination of security measures v and for each scenario j, obtaining w x m values of $P(T)_{vj}{}^{*}$. The values of $P(T)_{vj}{}^{*}$ can be calculated according to equation (4.25), by replacing a single measure i with a combination v. The constraint expressed by equation (4.25), regarding $Net\ Benefit_{vj} = 0$ is embedded in the formulation of system (4.28).

The second equation expresses the fact that the total cost of the selected measures $(C_v \cdot x_v)$, composing combination v, should not exceed the security budget $\left(C_{Budget,j}\right)$, which in turn is often scenario-dependent. The third constraint $(x_v \in \{0,1\})$ implies that a measure is either fully taken or not taken at all. The assumptions embedded in the formulation, the constraints and the notations are the same ones as those expressed with a deterministic cost-effectiveness analysis.

The output of submodule 6.2 is the combination of security measures, v^{*}, with the lowest probability of the attack, within the constraint of the security budget, for each scenario j, according to a break-even approach. A ranking of all the combinations, in order of increasing break-even probability (i.e., decreasing profitability), is provided. However, the top-three most profitable combinations are identified, as they might be the probable final security investments. The combinations that are outlined are the most profitable ones with the assumption of $Net\ Benefit_{vj} = 0$.

The application of a break-even approach to cost-effectiveness analysis offers a sensitivity evaluation on the likelihood of the attack, directly included in the model, according to ECO-SECURE version. The results of cost-effectiveness analysis, according to the break-even approach, may differ significantly among scenarios. The application of an original scoring system, described in submodule 6.3, allows defining an economic indicator expressing overall

cost-effectiveness analysis results, derived from multiple scenarios according to the break-even approach.

4.2.8.3 Module 6.3: Overall Economic indicator

The outputs of submodule 6.1 and submodule 6.2 may offer significant support to security decision-making. However, the indications provided by deterministic and break-even cost-effectiveness analyses, within ECO-SECURE version, might be different and sometimes conflicting with respect to the same scenario (e.g., a combination might have a high $P(T)_{vj}{}^{*}$ and a high $Net\ Benefit_{vj}$), as visible from Figure 4. 9. For this reason, it is not possible to compare directly cost-effectiveness analyses results obtained from the two approaches, because Net Benefits are monetary values, within the range $(-\infty, +\infty)$ whereas $P(T)_{vj}{}^{*}$ are adimensional values, ranging within [0,1]. Moreover, within the same approach to cost-effectiveness analysis, results might be very different among scenarios, as discussed in Sections 4.2.8.1 and 4.2.8.2 and visible from Figure 4. 9. Consequently, security investments that are not profitable with respect to a marginal scenario, might become economically feasible with respect to a catastrophic scenario.

The introduction of specific scoring systems is a common approach to provide more understandable information to stakeholders (Argenti et al., 2015; Srivastava and Gupta, 2010).

As visible from Figure 4. 9, $Net\ Benefit_{vj} = f(P(T)_{vj})$ is a linear function increasing monotonically in the range [0,1] (i.e., under the assumptions expressed in the two economic analyses modules) for each combination of security measures and each scenario, considering the same assumptions regarding vulnerabilities.

Therefore, it is possible to define, within ECO-SECURE version, two original economic indicators, named KPI_1 and KPI_2, expressing respectively the results of deterministic and break-even cost-effectiveness analysis, and eventually to combine them linearly. The combined application of the two approaches, and then of the two indicators, allows defining the function univocally. Therefore, the sensitivity analysis regarding the threat probability is included in the model. The use of multi-scenario criteria allows defining average economic performance of security measures combinations, weighted on all the scenarios m.

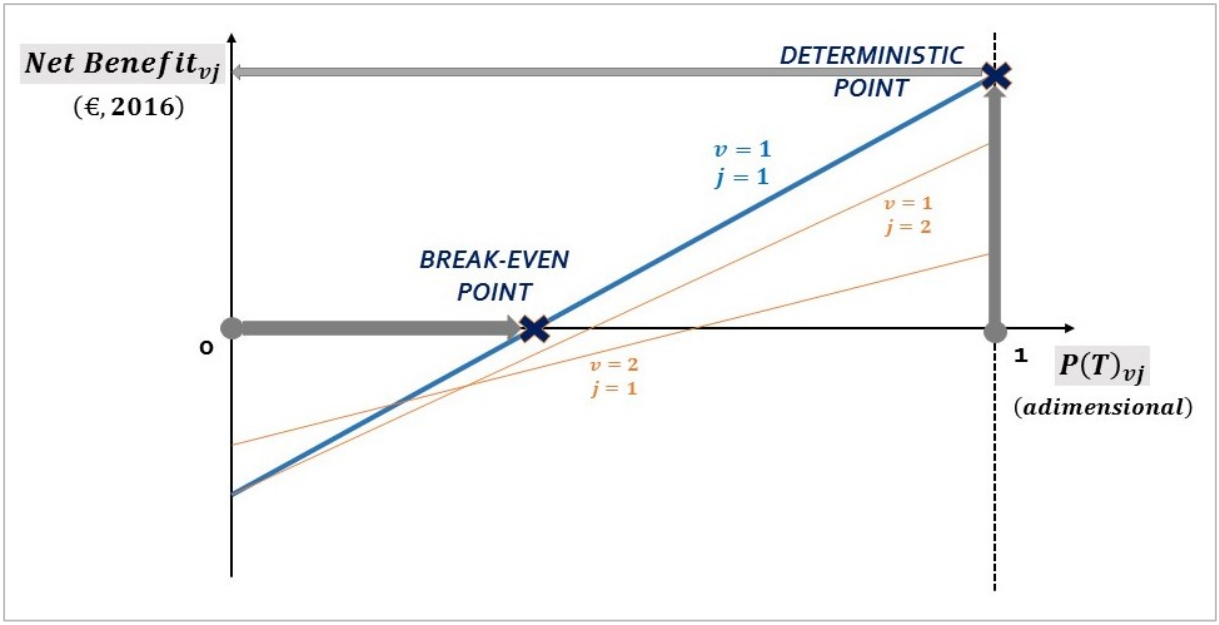


Figure 4. 9 Representation of cost-effectiveness analysis results under break-even and deterministic approaches for a combination of security measures v and a scenario j, according to model application. Two crosses represent the break-even point and the deterministic point.

The first economic indicator (KPI_1) expresses the results of deterministic cost-effectiveness analysis. KPI_1 is defined according to equation (4.29), for each possible combination of security measures v and for all the scenarios m:

$$\begin{cases} \text{If } C_v \cdot x_v \leq C_{Budget,j}\ \forall j \in \{1,\dots,m\}, m \in Z \\ KPI_1 = \left(\sum_{j=1}^{m}\left(Net\ Benefit_{vj} \cdot x_v / \left(\max\left(Net\ Benefit_{v^* j}\right)\right)\right)/m\right) \cdot 10 \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1,\dots,w\}, w \in Z \\ j \in \{1,\dots,m\}, m \in Z \\ \text{Else } KPI_1 = 0 \end{cases} \tag{4.29}$$

Therefore, KPI_1, ranging between [0,10], expresses the combined economic and technical performance of each combination of security measures, according to the deterministic approach. The value of the indicator is normalized with respect to the most cost-effective options v^* obtained from a deterministic approach for each scenario, which scores 10 and weighted on all the scenarios m. The higher the value of KPI_1, the better the overall performance of the combination. If the combination does not comply with the budget constraint for all the scenarios, the value of the indicator is 0.

The second economic indicator (KPI_2) expresses the results of break-even cost-effectiveness analysis. KPI_2 is defined according to equation (4.30), for each possible combination of security measures v and for all the scenarios m:

$$\begin{cases} \text{If } C_v \cdot x_v \leq C_{Budget,j} \ \forall j \in \{1, \dots, m\}, m \in Z \\ KPI_2 = \left(\sum_{j=1}^{m} \left(1 - \left(P(T)_{vj}{}^{*} \cdot x_v\right) / \left(1 - \min\left(P(T)_{v^{*}j}{}^{*} \cdot x_v\right)\right)\right)/m\right) \cdot 10 \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1, \dots, w\}, w \in Z \\ j \in \{1, \dots, m\}, m \in Z \\ \text{Else } KPI_2 = 0 \end{cases} \tag{4.30}$$

Therefore, KPI_2, ranging between [0,10], expresses again the combined economic and technical performance of a combination of security measures, according to the break-even approach. However, KPI_2 is normalized with respect to the most cost-effective option v^{*}obtained from a break-even approach for each scenario j, which scores 10 and weighted on all the scenarios m. Also in this case, if the combination does not respect the budget constraints for all the scenarios, the indicator value is zero.

An overall performance indicator is calculated from the combination of KPI_1 and KPI_2:

$$\begin{cases} \text{If } KPI_1 \geq \alpha \text{ and } KPI_2 \geq \beta \\ ECS = (KPI_1 + KPI_2) \cdot 0.5 \\ \text{Else } ECS = 0 \end{cases} \tag{4.31}$$

Where ECS is an overall cost-effectiveness indicator, again ranging between $[0, 10]$. Constants α and β are acceptability thresholds, having a value ranging between $[0, 10]$, which may be introduced by the security analyst and discussed with management, to warrant that combinations considered in decision-making perform above some minimum threshold values, under both the deterministic and break-even approaches.

A possible guideline for the selection of α and β values has been proposed in Table 4. 6. From a general perspective, in case of security managers that tend to put the focus of the economic analysis on the profitability of measures regardless the likelihood of the attack (i.e., high values of Net Benefit under deterministic approach and consequently high values of KPI_1), it is suggested to adopt high or very high α values. On the contrary, in case of security managers that tend to put the focus of the economic analysis on having an acceptable measure even with very low likelihood of the attack (i.e., low break-even probability and consequently high KPI_2), it is suggested to adopt high or very high β values. Other α and β values fall within the two discussed extremes.

Therefore, the submodule 6.3 provides a scoring system based on three indicators, all ranging within [0,10]: two intermediate economic indicators, expressing respectively deterministic and

break-even cost-effectiveness approaches, and an overall cost-effectiveness indicator. The scoring system provides the basis for a sound comparison of all possible security alternatives.

Table 4. 6 Guideline on α and β acceptability thresholds for security analysts.

Qualitative description of acceptability thresholds	α		β	
	Values ranges for α	**Requirements for α selection**	**Values ranges for β**	**Requirements for β selection**
Very high	(8, 10]	Very high Net benefit accepted under deterministic approach by security management	(8, 10]	Very low break-even probability accepted by security management
High	(6, 8]	High Net benefit accepted under deterministic approach by security management	(6, 8]	Low break-even probability accepted by security management
Medium	(4, 6]	Medium Net benefit accepted under deterministic approach by security management	(4, 6]	Medium break-even probability accepted by security management
Low	(2, 4]	Low Net benefit accepted under deterministic approach by security management	(2, 4]	High break-even probability accepted by security management
Very low	[0, 2]	Very low Net benefit accepted under deterministic approach by security management	[0, 2]	Very high break-even probability accepted by security management

4.3 DISCUSSION

The orginal model presented in Section 4 offers a complete framework for economic analysis, aimed at the selection and allocation of preventive security measures against terroristic attacks, within the specific chemical and process industry context. Two possible versions, depending on the focus for the application of the model, are depicted: EM-PICURES refers to generic security-based accidents and terroristic attacks, while ECO-SECURE refers to environmental and eco-terroristic attacks and related consequences.

The main advantage of the model is its completeness with respect to cost and performance of security measures, as well as to losses, and the consequent accuracy of results. Moreover, the model is relatively straightforward, enhancing its possibility to be applied in industrial practice. The model provides site-specific answers to security analysts, because it allows evaluating the performance of physical security measures present on-site and comparing several security upgrades according to technical and economic criteria, as well as possible adversary paths dependent on the layout of the facility.

The model may be applied both in predictive and in posterior analysis, as well as to different accident scenarios, in order to obtain scenario-specific economic indicators to be compared.

The precise checklist provided for costs and benefits evaluation may prevent omissions and inaccuracies. The cost assessment allows a precise definition of the most relevant cost terms due to the implementation of security measures, leaving at the same time enough space for the analyst to add specific costs. Indeed, the benefit assessment allows a detailed description of the losses derived from either perspective or retrospective accidental scenarios. The benefit assessment includes different damage categories between EM-PICTURES and ECO-SECURE versions, depending on the focus of the application (i.e., generic major accident and environmental damages respectively, both triggered by security threats). In particular, the retrospective application of the model may offer an additional tool to retrieve and validate quantitative information on security-based scenarios.

However, as all economic analyses, the results may reflect the subjectivity of the analyst, concerning the monetization of intangible costs and benefits and the choice of discount rates, whose inaccuracies may lead to misleading results. For instance, assigning monetary values to mortality and morbidity is a common practice in economic analyses, but it is still defined "a complicated situation" (Tappura et al., 2014), which might arise ethical concerns (Ale et al., 2015). Also the effectiveness assessment present several uncertainties: the analysis is site-specific and accident-specific, as it depends on the possible adversary path of actions. Therefore, the results obtained from effectiveness assessment cannot be generalized beyond a specific application. Moreover, although the model is able to take into account uncertainties that may decrease the overall performance of the PPS (e.g., possible lag-time in detection by security guards), it offers just a simplified description of a possible real accident.

Another possible limitation of the model is the choice of an appropriate pool of security upgrades and accidental scenarios that is up to the security analysis, in particular whenever a prospective analysis should be performed. Indeed, also the definition of vulnerability probabilities requires carefulness of the security analyst, as they depend on many variables. For this reason, whenever the model is applied, it is important to present the analysis in a fully transparent manner, specifying the assumptions made and discussing the uncertainties arisen.

The distinctive feature of the model is the flexibility, given by its capability to perform both cost-benefit and cost-effectiveness analysis, offering as outputs a broad spectrum of economic analyses results, which can eventually support the security decision-making process.

The application of solely cost-benefit analysis might not provide significant screening criteria, in particular with reference to very severe security-based accidents (e.g., cascading events). In this situation, the costs of security measures are several orders of magnitude inferior to overall losses, resulting therefore in the feasibility of almost all the single security measures. According to the same reasoning, security measures that are not feasible with reference to a marginal

scenario might be appropriate with reference to a catastrophic scenario. This issue makes the selection of an appropriate pool of credible scenarios even more important.

Instead, cost-effectiveness analysis may offer sound indications for the stakeholders to rationally select and allocate security measures, providing a range of economically profitable options that consider also security measures combinations within the budget constraints. A specific feature of ECO-SECURE version is the presence of two complementary approaches to the likelihood of the attack, named deterministic and break-even, leading to two different economic analysis approaches. On the other hand, in EM-PICTURES version, solely a deterministic approach is provided. The deterministic approach offers to the security manager insight on the optimal revision of the physical protection system, within the constraint of the annual security budget, after a variation regarding the likelihood of the attack (e.g., due to socio-political changes, increased visibility of the target, etc.). Therefore, it defines the optimal allocation of security upgrades, as a trade-off of two relevant parameters: cost and effectiveness improvement. The break-even approach, starting from a range of security options, allows defining the minimum likelihood of the attack that makes each option economically profitable, within the constraint of the annual security budget. The combined application of deterministic and break-even approaches to cost-benefit and cost-effectiveness analysis, provided solely by ECO-SECURE, allows inserting directly the uncertainties related to the estimation of the likelihood of the attack in the model, avoiding the necessity to perform an additional sensitivity analysis on the results. Therefore, ECO-SECURE version is more complete than EM-PICTURES one. For both versions, cost-effectiveness analyses results may vary depending also on the threshold of the security budget that is generally defined yearly by security management.

Another original feature of the model is the use of a specific scoring system, provided solely by ECO-SECURE version. The use of a scoring system was made necessary to compare the cost-effectiveness results obtained from the two approaches and to eventually combine them into an overall cost-effectiveness indicator (i.e., ECS). Eventual company-specific acceptance criteria and additional information should be considered, depending on the type of risk to be quantified (such as safety, economic, environmental, social), the focus of the stakeholders and decision-makers and the quality of information available. For instance, the application of the scoring system makes the model more understandable to decision-makers with non-technical backgrounds, because the final output of ECO-SECURE version of the model is constituted by solely one typology of indicator (i.e., ECS). Therefore, the application of an original scoring system allows to compare a limited pool of final combinations, and consequently to allocate the dedicated budget on security upgrades according to a rational criteria.

The application field of the model here in presented is limited to the selection and allocation of preventive security measures against security-based accidents, with different specific focus within EM-PICTURES and ECO-SECURE typologies of applications. This limitation is imposed by the specific features of security devices, and by the different intent of preventive measures with respect to mitigation measures (i.e., safety measures). Mitigation may consider both intentional and unintentional accidents and, as such, needs to incorporate a different analysis, including unintentional failure scenarios. Indeed, the tools required to carry out such analysis are different and address a specific legislation context. Moreover, as discussed in section 3. 5, recent applications of economic analyses are mainly focused on safety aspects. Nevertheless, the methodology may be extended to post-accident mitigation, in purpose to compare the possible role of safety and security measures with respect to major accidents. The extended methodology will allow decision-maker to have an integrated view of safety and security deficits in a chemical installation and to allocate the budget on the most critical aspect (i.e., either on preventive or on mitigation measures). Moreover, the current modelling environment is Excel® version 2013; possible further developments of the research might deal with the implementation of the model in a more user-friendly interface, including an automated tool for the selection of upgrades and accidental scenarios.

The outputs of the model might be applied in risk-informed security decision-making both at company and at regulatory level with different purposes: to increase the awareness of management towards security issues by means of non-technical and rather user-friendly outputs, to tackle security vulnerability in chemical facilities and to allocate the budget on profitable physical protection alternatives w.r.t. security-based major accidents. At company level, possible solutions for the optimal selection and allocation of security prevention investments provided by the model may be discussed by the management and eventually weighted with respect to company specific acceptance criteria, site-specific issues and additional qualitative information available. At regulatory level, the model might be applied to tackle security vulnerable chemical facilities and to propose economically feasible physical protection alternatives, which allow meeting eventual legal requirements. However, the application of the model at company level seems to be more feasible in a short-term perspective, due to the actual lack of regulation at European Union level regarding security risk assessment and related decision-making within chemical and process facilities.

Indeed, even if the framework is not over-complicated, its application requires an effort that should be avoided whenever the results are obvious from the outset, because in these situations it does not provide additional support to security decision-making. Moreover, the general concepts of this economic model are applicable beyond the industrial security domain; for instance, to support security decision-making at social level against environmental damages (e.g., selection of security measures to prevent vandalism).

Eventually, the model may be a systematic useful tool to cope with security-based accidents in chemical and process facilities; however, it requires to be validated by several applications to case studies that are available in Section 6.

4.4 CONCLUSIONS

In the present section, a novel model for cost-benefit and cost-effectiveness analyses of chemical and process-industry related preventive security measures was developed, with two specific versions, depending on the focus of the application, named EM-PICTURES and ECO-SECURE. The model, starting from the baseline physical protection system effectiveness of a process facility, allows evaluating and comparing the costs derived from the introduction of a security upgrade with the losses derived from either perspective or retrospective accidental events, named benefits, accounting also effectiveness improvement. The model developed provides to security managers indications on the most profitable single security upgrades and combinations of them needed to prevent security-based accident scenarios. Two approaches toward the estimation of the threat probability and therefore to economic analyses, named deterministic and break-even, are considered.

Results of deterministic analysis allow upgrading the physical protection system, according to possible variations in the likelihood of the attack. Break-even analysis provides the optimal allocation of the security budget, defined yearly by security management. The application of a specific scoring system allows comparing the two set of results, obtaining overall indicators. Thus, the method enables to define a more rational selection and allocation of physical security measures (or barriers) and its outputs provide a sound support to managers within the security decision-making process. Therefore, the model may support the inclusion of security hazards within quantitative risk assessment and related delated decision-making and its application may eventually contribute to the reduction of chemical and process plants vulnerability towards intentional malevolent acts.

Section 5.

Dynamic safety measures performance assessment in the prevention of major accidents and cascading events: applications to case studies

5.1 INTRODUCTION

The present section is aimed at filling the research gap identified in Section 3.5.1, by applying dynamic safety measures performance assessment in the prevention of major accidents and cascading events (i.e., domino effects). Several case studies and tutorials are presented.

In Section 5.2, existing applications of dynamic techniques, as Bayesian analysis and Bayesian Networks, to major accidents prevention within the chemical industry domain are presented, in purpose to explain in practice the potentialities of these methods. The mentioned Section is aimed at reproducing existing case studies regarding Bayesian analysis and Bayesian Networks, in purpose to derive lessons on the possible research gaps to be filled.

For instance, in Section 5.2.2, Bayesian analysis is applied to safety measures performance assessment by considering two case studies: case study A deals with the application of Bayesian failure assessment for a process tank equipped with safety systems, case study B applies Bayesian analysis to an oil spill accident.

Then, safety barriers performance assessment has been applied by means of Bayesian Networks in Section 5.2.3: tutorials illustrating the features and tools of a specific software to construct Bayesian Networks, named Hugin version 8.1, are presented. Two case studies, named case study C and D, aimed respectively at converting conventional risk assessment techniques (i.e., Fault-Tree and Bow-Tie) into Bayesian Networks, are presented. The possibility of Bayesian Networks to account safety barriers performance, including also economic elements have been explored by an additional case study (i.e., case study E).

The lesson learnt from existing contributions gives a precise direction for the original applications to be carried out, which are aimed at filling a significant research gap, by applying dynamic risk assessment method, for instance Bayesian Networks, to major accidents and cascading events prevention (i.e., domino effects), including safety barriers within the

modelling phase. Therefore, in Section 5.3, four original applications are presented, and in Section 5. 4, conclusions are drawn on their possible contributions in the broader risk assessment perpective.

5.2 LESSONS LEARNT FROM EXISTING APPLICATIONS

5.2.1 Applications of Bayesian analysis to safety measures performance assessment

5.2.1.1 Case study A: application of Bayesian failure assessment for a process tank equipped with safety system

5.2.1.1.1 Description of the case study

The current application is aimed at reproducing the relevant case study by Kalantarnia et al. (Kalantarnia et al., 2009), which is the first complete application of Dynamic Risk assessment (i.e., DRA), by means of Bayesian Analysis, within the process industry domain. The aim of the application is to put in practice the fundamental steps of DRA presented in Section 3.3.2.1.3.1 and to highlight the advantages of Bayesian analysis, as well as the possible limitations.

The case study considers a process tank containing a hazardous chemical liquid, according to the layout is reported in Figure 5. 1.

In Step 1 of DRA, the potential scenarios, their causes, consequences and related safety barriers are identified by means of Event-Tree analysis. Within the case study, the top event to be accounted is high flow. The occurrence of the top event may lead, according to Event-Tree analysis, to 11 final accidental states, which are grouped into three severity classes:

- A – Safe;
- B – fluid release;
- C – high pressure.

The safety systems (i.e., barriers) are: BPC (Basic Process Control), Bypass (Bypass Line), HLA (High Level Alarm), Manual (Manual Valve), PSV (Pressure safety valve). The Event-Tree for the case study is reported in Figure 5. 2.

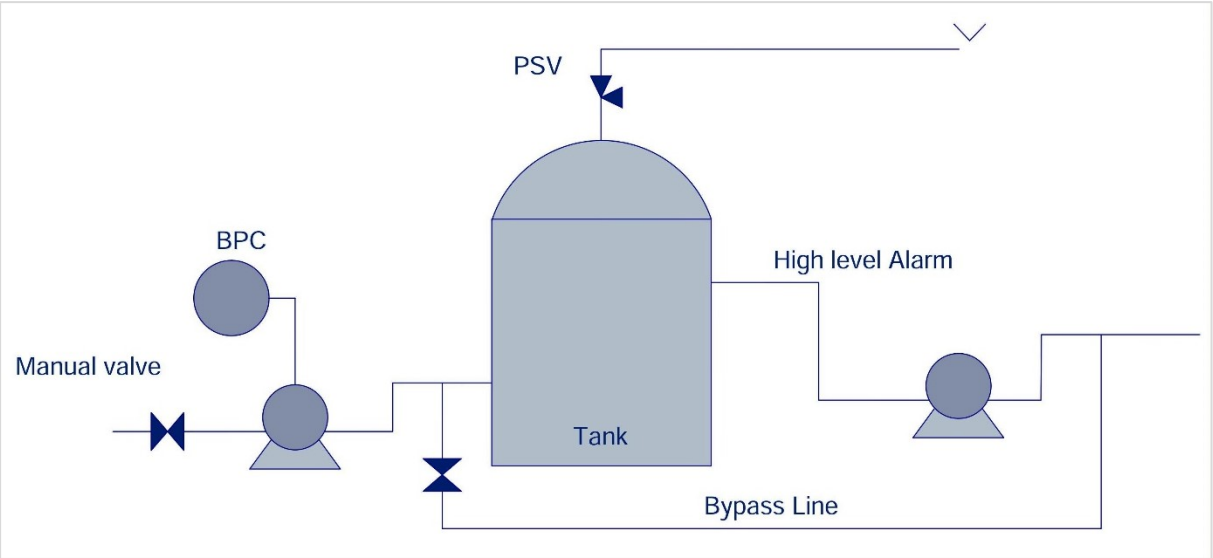


Figure 5. 1 Layout of the process tank for the case study, adapted from Kalantarnia et al. (Kalantarnia et al., 2009).

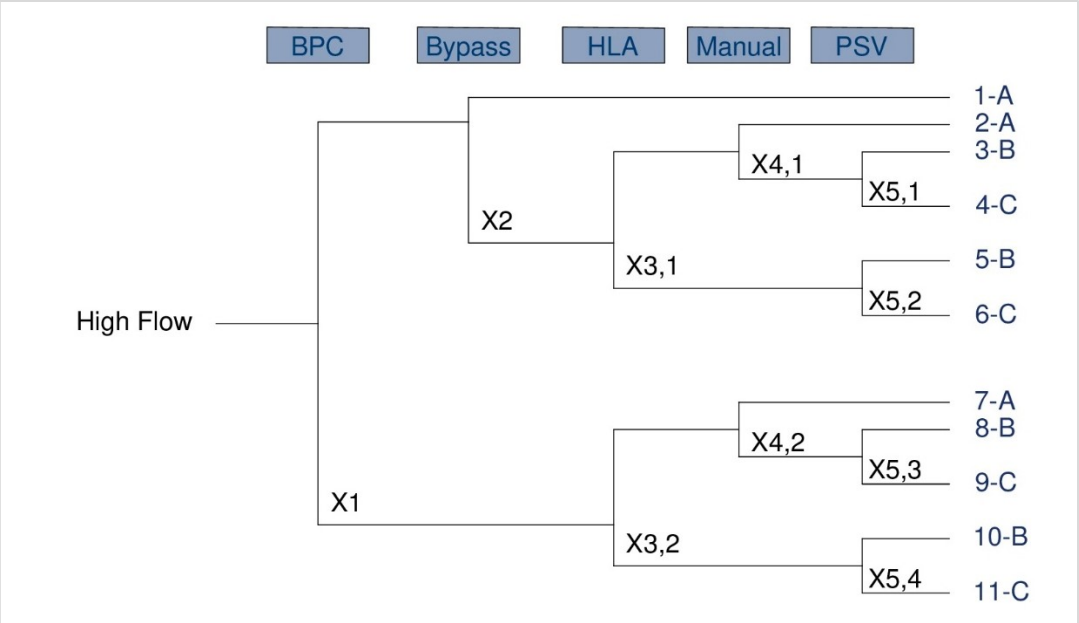


Figure 5. 2 Step 1 of DRA: Event-Tree for the failure assessment of a process tank equipped with safety systems, adapted from Kalantarnia et al. (Kalantarnia et al., 2009).

Step 2 of DRA is aimed at calculating the prior failure probability function for each barrier. Two approaches for the calculation of failure probabilities of each safety system are used:

- Deterministic approach, which applies deterministic values for failure probabilities;
- Probabilistic approach, which applies the median value of the failure probability distribution (i.e., type Beta in the case study). The median value is calculated by inserting in the inverse of Beta distribution function the value 0.5.

The values of prior failure probabilities for each safety system, according to both approaches, are reported in Table 5. 1.

Table 5. 1 Step 2 of DRA: prior values of failure probabilities for deterministic and probabilistic approaches. Inputs adapted from Kalantarnia et al. (Kalantarnia et al., 2009).

Deterministic approach							
Safety systems	***Failure Probability***			***Symbol***			
BPC	0.025			x_1			
Bypass	0.015			x_2			
HLA	0.15			$x_{3,1}$	$x_{3,2}$		
Manual	0.2			$x_{4,1}$	$x_{4,2}$		
PSV	0.045			$x_{5,1}$	$x_{5,2}$	$x_{5,3}$	$x_{5,4}$
Probabilistic approach							
Safety systems	***Alpha***	***Beta***	***Median values of distribution***	***Symbol***			
BPC	0.25	2.1	2.47 E-02	x_1			
Bypass	0.15	0.76	1.51 E-02	x_2			
HLA	1.5	7	1.51 E-02	$x_{3,1}$	$x_{3,2}$		
Manual	1	3	2.06 E-02	$x_{4,1}$	$x_{4,2}$		
PSV	0.4	3.4	4.55 E-02	$x_{5,1}$	$x_{5,2}$	$x_{5,3}$	$x_{5,4}$

Then, the prior probabilities of occurrence of each final state (i.e., end-state) of the Event-Tree are calculated according to equation (3.7) and reported in Table 5. 2.

Table 5. 2 Prior probabilities of final states according to deterministic and probabilistic approaches.

End-state	**Occurence probability (priors)**	
	Deterministic a.	**Probabilistic a.**
1 - A	9.60E-01	9.61E-01
2 - A	9.95E-03	9.90E-03
3 - B	2.37E-03	2.46E-03
4 - C	1.12E-04	1.17E-04
5 - B	2.10E-03	2.11E-03
6 - C	9.87E-05	1.01E-04
7 - A	1.70E-02	1.66E-02
8 - B	4.06E-03	4.13E-03
9 - C	1.91E-04	1.97E-04
10 - B	3.58E-03	3.55E-03
11 - C	1.69E-04	1.69E-04

5.2.1.1.2 Application of Bayesian analysis

In Step 3 od DRA, the likelihood function is created $(g(Data|x))$, according to equation (3.14), by the introduction of Accident Sequence Precursors (i.e., ASP) over 10 years of operational experience, to revise probability distributions, as reported in Table 5. 3.

Table 5. 3 Accident Sequence Precursors in cumulative form, derived from plant specific data and safety experts feedback, adapted from Kalantarnia et al. (Kalantarnia et al., 2009).

Years	1 - A	2 - A	3 - B	4 - C	5 - B	6 - C	7 - A	8 - B	9 - C	10 - B	11 - C
1	1	1	0	1	0	1	1	0	1	0	1
2	1	2	0	2	1	2	2	1	2	1	2
3	1	2	1	3	1	3	3	2	3	2	3
4	2	2	2	6	2	4	3	2	3	2	4
5	2	3	3	7	2	4	3	2	5	2	4
6	3	3	3	8	4	6	5	3	7	3	4
7	5	4	5	10	6	8	6	4	7	4	4
8	8	6	10	11	7	9	7	5	7	5	4
9	9	8	12	12	8	10	8	6	8	6	5
10	11	10	14	13	9	11	9	7	9	6	6

5.2.1.1.3 Results and discussion

In step 4 of DRA, the posterior failure function of each safety system ($f(x|Data)$) is calculated from the prior and likelihood functions using Bayesian inference, according to equation (3.15). Indeed, for each safety barriers, the parameters of the Beta distribution are changed according to ASPs, as well as safety barriers median values of failure probabilities. Posterior values of failure probabilities, dynamically revised over 10 years of operational experience, are reported in Table 5. 4.

The last step of DRA application (step 5) is the consequence analysis, carried out on the scenario in order to estimate the revised probabilities of occurrence of final states, according to the equation (3.7), by inserting the posterior failure function in the equation, to describe each safety barrier performance. Therefore, the values of posterior end-state probabilities and end-state classes are dynamically revised over 10 years of operational experience; results are available in Table 5. 5.

Table 5. 4 Step 4 of DRA: safety measures posterior failure probabilities.

Years	BPC					Bypass					HLA				
	n. failures	n. success	Alpha	Beta	Median value	n. failures	n. success	Alpha	Beta	Median value	n. failures	n. success	Alpha	Beta	Median value
1	3	4	3.25	6.1	3.36E-01	3	1	3.15	1.76	6.62E-01	2	4	3.5	11	2.29E-01
2	8	8	8.25	10.1	4.48E-01	7	1	7.15	1.76	8.26E-01	6	9	7.5	16	3.14E-01
3	13	11	13.25	13.1	5.03E-01	10	1	10.15	1.76	8.72E-01	9	14	10.5	21	3.30E-01
4	14	18	14.25	20.1	4.13E-01	16	2	16.15	2.76	8.67E-01	12	18	13.5	25	3.48E-01
5	16	21	16.25	23.1	4.11E-01	19	2	19.15	2.76	8.85E-01	12	23	13.5	30	3.07E-01
6	22	27	22.25	29.1	4.32E-01	24	3	24.15	3.76	8.74E-01	17	29	18.5	36	3.37E-01
7	25	38	25.25	40.1	3.85E-01	33	5	33.15	5.76	8.58E-01	22	36	23.5	43	3.52E-01
8	28	51	28.25	53.1	3.46E-01	43	8	43.15	8.76	8.36E-01	25	46	26.5	53	3.32E-01
9	33	59	33.25	61.1	3.51E-01	50	9	50.15	9.76	8.41E-01	29	54	30.5	61	3.32E-01
10	37	68	37.25	70.1	3.46E-01	57	11	57.15	11.76	8.33E-01	32	62	33.5	69	3.26E-01

Years	Manual					PSV				
	n. failures	n. success	Alpha	Beta	Median value	n. failures	n. success	Alpha	Beta	Median value
1	2	2	3	5	3.64E-01	4	0	4.4	3.4	5.70E-01
2	5	4	6	7	4.60E-01	8	3	8.4	6.4	5.71E-01
3	9	5	10	8	5.58E-01	12	6	12.4	9.4	5.71E-01
4	13	5	14	8	6.41E-01	17	8	17.4	11.4	6.07E-01
5	17	6	18	9	6.71E-01	20	9	20.4	12.4	6.24E-01
6	21	8	22	11	6.70E-01	25	13	25.4	16.4	6.09E-01
7	26	10	27	13	6.78E-01	29	19	29.4	22.4	5.68E-01
8	33	13	34	16	6.82E-01	31	27	31.4	30.4	5.08E-01
9	38	16	39	19	6.74E-01	35	32	35.4	35.4	5.00E-01
10	43	19	44	22	6.68E-01	39	36	39.4	39.4	5.00E-01

Table 5. 5 Step 5 of DRA: posterior probabilities over 10 years of operational experience: 1) final states probabilities; 2) category probabilities results.

1) Final state probabilities

Years	1 - A	2 - A	3 - B	4 - C	5 - B	6 - C	7 - A	8 - B	9 - C	10 - B	11 - C
1	2.24E-01	2.15E-01	5.30E-02	7.03E-02	4.33E-02	5.74E-02	1.65E-01	4.06E-02	5.38E-02	3.32E-02	4.39E-02
2	9.63E-02	1.69E-01	6.17E-02	8.20E-02	6.14E-02	8.17E-02	1.66E-01	6.06E-02	8.05E-02	6.03E-02	8.02E-02
3	6.36E-02	1.29E-01	6.95E-02	9.25E-02	6.13E-02	8.16E-02	1.49E-01	8.06E-02	1.07E-01	7.12E-02	9.47E-02
4	7.83E-02	1.19E-01	8.35E-02	1.29E-01	6.96E-02	1.07E-01	9.68E-02	6.79E-02	1.05E-01	5.66E-02	8.72E-02
5	6.74E-02	1.19E-01	9.09E-02	1.51E-01	6.02E-02	1.00E-01	9.38E-02	7.18E-02	1.19E-01	4.75E-02	7.90E-02
6	7.15E-02	1.08E-01	8.60E-02	1.34E-01	6.54E-02	1.02E-01	9.45E-02	7.50E-02	1.17E-01	5.70E-02	8.89E-02
7	8.73E-02	1.10E-01	1.00E-01	1.32E-01	8.01E-02	1.06E-01	8.04E-02	7.30E-02	9.62E-02	5.85E-02	7.71E-02
8	1.08E-01	1.16E-01	1.23E-01	1.27E-01	8.92E-02	9.22E-02	7.34E-02	7.76E-02	8.02E-02	5.65E-02	5.84E-02
9	1.03E-01	1.19E-01	1.23E-01	1.23E-01	9.06E-02	9.06E-02	7.64E-02	7.91E-02	7.91E-02	5.83E-02	5.83E-02
10	1.10E-01	1.22E-01	1.23E-01	1.23E-01	8.87E-02	8.87E-02	7.74E-02	7.80E-02	7.80E-02	5.64E-02	5.64E-02

2) Final categories probabilities

Posterior probabilities (over 10 years)											Prior probabilities
Categories	1	2	3	4	5	6	7	8	9	10	0
A	6.04E-01	4.31E-01	3.41E-01	2.94E-01	2.80E-01	2.74E-01	2.78E-01	2.97E-01	2.98E-01	3.09E-01	9.87 E-01
B	1.70E-01	2.44E-01	2.83E-01	2.78E-01	2.70E-01	2.83E-01	3.12E-01	3.46E-01	3.51E-01	3.46E-01	1.23 E-02
C	2.25E-01	3.24E-01	3.76E-01	4.28E-01	4.50E-01	4.42E-01	4.11E-01	3.57E-01	3.51E-01	3.46E-01	5.85 E-04

Results from this study show that safety systems, final state probabilities, as well as final states category probabilities, vary significantly over the time span considered, due to the introduction of ASP and the application of Bayesian analysis within DRA.

For instance, without additional information, the probability of system being Safe (i.e., Prior probability of final state category A) is largely prevailing. Nevethless, after probabilities revisions, at the end of the observation period, all three categories of final events have the same probability of occurrence.

Indeed, DRA with Bayesian analysis helps obtaining revised probabilities over time, providing safety managers an updated risk picture. However, it should be noted that Bayesian analysis should be performed by revising manually probability distribution for each safety system, so it may become an unsuitable techinque for complex case studies. Moreover, it is based on conventional Risk assessment tool (e.g., the Event-Tree), so it still suffers from some of its limitations (e.g., difficulty to account common causes).

5.2.1.2 Case study B: application of Bayesian analysis to an oil spill accident

5.2.1.2.1 Description of the case study

The current application is aimed at reproducing the relevant case study by Yang et al. (Yang et al., 2013), which is the first complete application of Dynamic Risk assessment (i.e., DRA), by means of Bayesian Analysis, to a major accidental scenario, within the process industry domain. The aim of the application is to put in practice the fundamental steps of DRA presented in Section 3.3.2.1.3.1 and to highlight the advantages of Bayesian analysis, as well as the possible limitations with respect to a complex accidental event, with several safety barriers, intermediate events and final states to be considered.

The case considers an explosion that occurred aboard the Deepwater Horizon drilling platform in the Gulf of Mexico on April 20th, 2010. Eleven people were killed, about $8.0 \cdot 10^5\ m^3$of oil spilled into the Gulf unabated until mid July when the wellhead was capped. Severe consequences affected people living in the nearby coastal region, as well as environment and assets.

In Step 1 of DRA, the potential scenario, the intermediate event and the consequences identified by means of Event-Tree analysis; the Event-Tree for the case study is reported in Figure 5. 3; the description of intermediate events reported in Table 5. 6 (Yang et al., 2013).

Table 5. 6 Description of events to be considered in the case study, adapted from Yang et al. (Yang et al., 2013).

	Description of events
0	High pressure gas in rock formation
1	Anular cement and shoe track barrier fail to isolate gas
2	Hydrostatic pressure does not hold and entered the well
3	Failure of inner pipe
4	Gas leak is not detected by the system
5	Gas leak is not detected by rig crew
6	Mud gas separator fails to control the release
7	HVAC fails to shut down, trasfers more gas-rich mixture
8	Ignition source, e.g., over-speed engine
9	Blowout preventer fails to be activated

The 27 final accidental states defined by the Event-Tree are grouped into three main categories:

- A - safe;
- B - unsafe;
- C - fire and major accident.

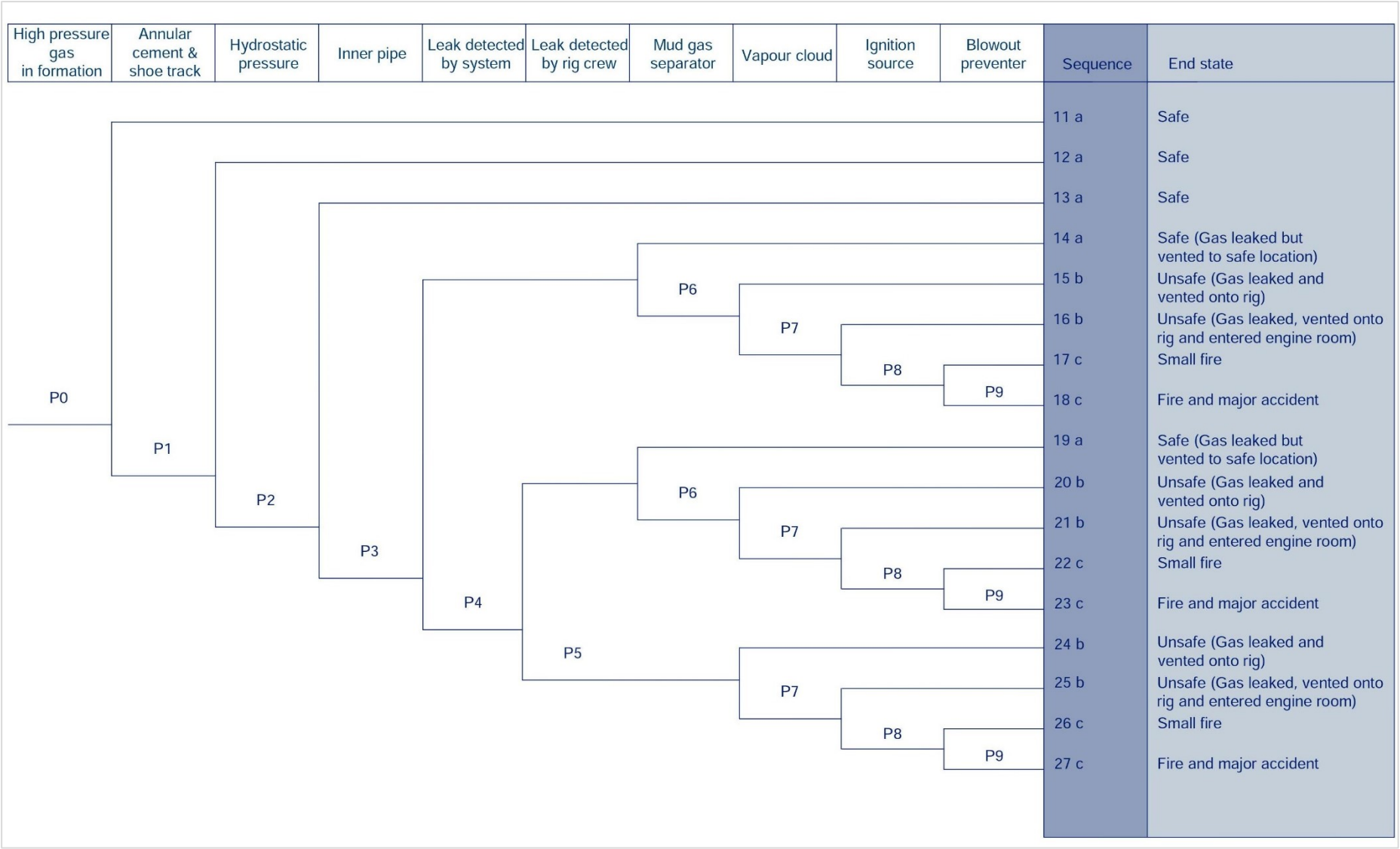


Figure 5. 3 Event-Tree for the case study, adapted from Yang et al. (Yang et al., 2013).

Step 2 of DRA is aimed at calculating the prior failure probability function for each event, by means of a probabilistic approach, using a distribution type Gamma. Prior mean values for each event are obtained (Table 5. 7), as the product of the two parameters, according to the typology of distribution (Vose and Rowe, 2000).

Table 5. 7 Step 2 of DRA: calculation of prior failure probabilities for each event; inputs adapted from Yang et al. (Yang et al., 2013).

Event	Alpha	Beta	Distribution	Prior mean
0	0.500	0.200	Gamma	**1.00E-01**
1	0.500	0.200	Gamma	**1.00E-01**
2	0.071	0.700	Gamma	**4.97E-02**
3	0.063	0.800	Gamma	**5.04E-02**
4	0.100	0.500	Gamma	**5.00E-02**
5	0.800	0.400	Gamma	**3.20E-01**
6	0.761	0.080	Gamma	**6.09E-02**
7	0.300	0.500	Gamma	**1.50E-01**
8	0.300	0.600	Gamma	**1.80E-01**
9	0.120	0.200	Gamma	**2.40E-02**

Then, the prior probabilities of occurrence of each final state (i.e., end-state) of the Event-Tree are calculated according to equation (3.7) and reported in Table 5. 8.

Table 5. 8 Step 2 of DRA: Prior probabilities for final states.

Final state ID	Probability
11 - A	9.00E-02
12 - A	9.50E-03
13 - A	4.72E-04
14 - A	2.23E-05
15 - B	1.23E-06
16 - B	1.78E-07
17 - C	3.82E-08
18 - C	9.39E-10
19 - A	8.00E-07
20 - B	4.41E-08
21 - B	6.38E-09
22 - C	1.37E-09
23 - C	3.36E-11
24 - B	3.41E-07
25 - B	4.93E-08
26 - C	1.06E-08
27 - C	2.60E-10
Total A	1.000E-01
Total B	1.85E-06
Total C	3.94E-08

5.2.1.2.2 Application of Bayesian analysis

In Step 3 of DRA, the likelihood function is created $\left(g(Data|x)\right)$, according to equation (3.14), by the introduction of Accident Sequence Precursors (i.e., ASP) over 30 years of operational experience, to revise probability distributions. Accident precursor data, obtained from plants specific data and safety expert feedback, are reported in Table 5. 9. However, no specific precursors are available for the accidental scenario that actually happened (27 – C), due to the fact that it is an HILP (i.e., High Impact, Low Probability accident). Therefore, additional sequence precursors data from contiguous process sectors, in which the same components are applied, reported in Table 5. 10, are inserted, as sensitivity analysis to DRA.

Table 5. 9 Accident sequence precursors referred to the chemical sector, in cumulative form and gathered over 30 years of operational experience (Yang et al., 2013).

End-State	Operational experience (years)		
	10	20	30
11 - A	1	1	2
12 - A	0	1	1
13 - A	0	1	1
14 - A	0	1	1
15 - B	0	0	1
16 - B	0	1	1
17 - C	0	1	1
18 - C	-	-	-
19 - A	1	1	1
20 - B	0	0	0
21 - B	0	0	0
22 - C	0	0	0
23 - C	-	-	-
24 - B	1	1	1
25 - B	1	1	1
26 - C	0	0	0
27 - C	-	-	-

Table 5. 10 Additional accident sequence precursors from contiguous sectors (Yang et al., 2013).

Event	Operational experience (years)		
	30	30	30
	Nuclear	Mining	Process
0	8	9	10
1	6	7	6
2	7	7	8
3	5	6	7
4	4	2	4
5	2	2	1
6	3	4	5
7	1	1	3
8	0	1	1
9	0	1	2

5.2.1.2.3 Results and discussion

In step 4 of DRA, the posterior failure function of each safety system ($f(x|Data)$) is calculated from the prior and likelihood functions using Bayesian inference, according to equation (3.15). Indeed, for each event, the parameters of the Gamma distribution are changed according to ASPs, and posterior median values of failure probabilities are obtained. Posterior values of failure probabilities, dynamically revised over 30 years of operational experience, according to the ASPs of Table 5. 9, referred to the chemical sector, are reported in Table 5. 11.

Then, Bayesian analysis is carried out by including also the additional ASPs data of contiguous sectors reported in Table 5. 10; the posterior median values of failure probabilities for each event is available in Table 5. 12.

The last step of DRA application (step 5) is the consequence analysis, carried out on the scenario in order to estimate the revised probabilities of occurrence of final states, according to the equation (3.7), by inserting the posterior failure function in the equation, to describe each safety barrier performance. Therefore, the values of posterior end-state probabilities and end-state classes are dynamically revised, according to ASPs from the chemical sector (Table 5. 9) and additional data from contiguous sectors (Table 5. 10). The results are available in Table 5. 13. Then, final states probabilities have been summed, according to the three severity classes (i.e., A, B and C).

Results from this study show that events, final state probabilities, as well as final states category probabilities, vary significantly over the time span considered, due to the introduction of ASP and the application of Bayesian analysis within DRA.

For instance, without additional information, the probability of system being Safe (i.e., Prior probability of final state category A) is largely prevailing. Neverthless, after probabilities revisions, at the end of the observation period, the likelihood of occurrence of categories B and C of final events is at least two orders of magnitude higher in comparison with initial data.

This demonstrates the effectiveness of Bayesian analysis in major accidents modelling. Morover, the application of a sensitivity analysis, due to the introduction of additional ASPs, demonstrates the usefulness of applying precursors of major accidents.

Table 5. 11 Step 4 of DRA: Posterior mean for events after introduction of ASP for the chemical sector.

Event	10 years					20 years					30 years				
	n. failures	**n.success**	**Alpha* (new)**	**Beta* (new)**	**Posterior mean**	**n. failures**	**n.success**	**Alpha* (new)**	**Beta* (new)**	**Posterior mean**	**n. failures**	**n.success**	**Alpha* (new)**	**Beta* (new)**	**Posterior mean**
0	4	0	4.500	0.067	**3.00E-01**	9	0	9.500	0.040	**3.80E-01**	11	0	11.500	0.029	**3.29E-01**
1	3	1	3.500	0.067	**2.33E-01**	8	1	8.500	0.040	**3.40E-01**	9	2	9.500	0.029	**2.71E-01**
2	3	0	3.071	0.088	**2.69E-01**	7	1	7.071	0.047	**3.30E-01**	8	1	8.071	0.032	**2.57E-01**
3	3	0	3.063	0.089	**2.72E-01**	6	1	6.063	0.047	**2.85E-01**	7	1	7.063	0.032	**2.26E-01**
4	3	0	3.100	0.083	**2.58E-01**	3	3	3.100	0.045	**1.41E-01**	3	4	3.100	0.031	**9.69E-02**
5	2	1	2.800	0.080	**2.24E-01**	2	1	2.800	0.044	**1.24E-01**	2	1	2.800	0.031	**8.62E-02**
6	0	1	0.761	0.044	**3.38E-02**	2	2	2.761	0.031	**8.50E-02**	3	2	3.761	0.024	**8.85E-02**
7	1	1	1.300	0.083	**1.08E-01**	3	1	3.300	0.045	**1.50E-01**	3	2	3.300	0.031	**1.03E-01**
8	0	1	0.300	0.086	**2.57E-02**	1	2	1.300	0.046	**6.00E-02**	1	2	1.300	0.032	**4.11E-02**
9	0	0	0.120	0.067	**8.00E-03**	0	1	0.120	0.040	**4.80E-03**	0	1	0.120	0.029	**3.43E-03**

Table 5. 12 Comparison of Bayesian analysis results regarding posterior failure probabilities after 30 years of operational experience (step 4 of DRA) with ASP from the chemical sector and with additional ASPs from contiguous sectors.

Event	**n. failures**	**Alpha* (new)**	**Beta* (new)**	***Conventional Bayesian method (with additional data)***	***Conventional Bayesian method (only specific plant data)***	***Difference %***
				Posterior mean	**Posterior mean**	
0	10.000	10.500	0.029	**3.00E-01**	**3.29E-01**	**9.52%**
1	7.667	8.167	0.029	**2.33E-01**	**2.71E-01**	**16.33%**
2	7.667	7.738	0.032	**2.46E-01**	**2.57E-01**	**4.31%**
3	6.500	6.563	0.032	**2.10E-01**	**2.26E-01**	**7.62%**
4	3.167	3.267	0.031	**1.02E-01**	**9.69E-02**	**5.38%**
5	1.83	2.633	0.031	**8.10E-02**	**8.62E-02**	**6.33%**
6	3.500	4.261	0.024	**1.00E-01**	**8.85E-02**	**13.29%**
7	2.333	2.633	0.031	**8.23E-02**	**1.03E-01**	**25.32%**
8	0.8333	1.133	0.032	**3.58E-02**	**4.11E-02**	**14.71%**
9	0.5000	0.620	0.029	**1.77E-02**	**3.43E-03**	**416.67%**

Table 5. 13 Step 5 of DRA: Event-Tree final states results after application of Bayesian adapting.

Years / *End-state*	**10**	**20**	**30**	**30**	***Difference %***
	Conventional Bayesian method	***Conventional Bayesian method***	***Conventional Bayesian method (only specific plant data)***	***Conventional Bayesian method (with additional data)***	
	Posterior mean	**Posterior mean**	**Posterior mean**	**Posterior mean**	
11 - A	2.30E-01	2.51E-01	2.39E-01	2.30E-01	4.08%
12 - A	5.12E-02	8.66E-02	6.63E-02	5.28E-02	25.61%
13 - A	1.37E-02	3.05E-02	1.77E-02	1.36E-02	30.20%
14 - A	3.67E-03	9.56E-03	4.26E-03	2.92E-03	45.73%
15 - B	1.15E-04	7.55E-04	3.71E-04	2.99E-04	24.09%
16 - B	1.36E-05	1.25E-04	4.09E-05	2.59E-05	58.24%
17 - C	3.55E-07	7.95E-06	1.75E-06	9.43E-07	85.17%
18 - C	2.86E-09	3.84E-08	6.00E-09	1.70E-08	183.09%
19 - A	9.92E-04	1.37E-03	4.18E-04	3.06E-04	36.73%
20 - B	3.10E-05	1.08E-04	3.64E-05	3.12E-05	16.42%
21 - B	3.66E-06	1.80E-05	4.01E-06	2.70E-06	48.47%
22 - C	9.60E-08	1.14E-06	1.71E-07	9.85E-08	73.73%
23 - C	7.74E-10	5.51E-09	5.89E-10	1.78E-09	201.72%
24 - B	2.64E-04	1.81E-04	3.87E-05	2.75E-05	41.04%
25 - B	3.13E-05	3.01E-05	4.27E-06	2.38E-06	79.86%
26 - C	8.19E-07	1.91E-06	1.82E-07	8.66E-08	110.46%
27 - C	6.60E-09	9.21E-09	6.27E-10	1.56E-09	149.07%
Total (A- safe)	**3.00E-01**	**3.79E-01**	**3.28E-01**	**3.00E-01**	**9.50%**
Total (B- unsafe)	**4.58E-04**	**1.22E-03**	**4.95E-04**	**3.89E-04**	**27.45%**
Total (C- fire and major accident)	**1.28E-06**	**1.11E-05**	**2.11E-06**	**1.15E-06**	**83.44%**

Indeed, DRA with Bayesian analysis helps obtaining revised probabilities over time, providing safety managers an updated risk picture. However, it should be noted that Bayesian analysis should be performed by revising manually probability distribution for each event, so it becomes excessively laborious for complex applications, as the one here in considered. Moreover, it is based on conventional Risk assessment tool (e.g., the Event-Tree), so it still suffers from some of its limitations (e.g., difficulty to account common causes).

Therefore, it is preferable in these situations, to apply DRA by means of Bayesian Networks, using a specific software.

5.2.2 Applications of Bayesian Networks to safety measures performance assessment

5.2.2.1 Tutorials on the use of a dedicated software for the application of Bayesian Networks

The present tutorials have been aimed at applying Bayesian Statistic Methods, in the form of Directed Acyclic Graphs, named also Bayesian Networks (BNs), by using a specific software, Hugin version 8.1, which provides decision support for reasoning under uncertainty. The formalization of BNs model appeared to be necessary in order to integrate various dimensions correlated with process system behavior within risk assessment.

5.2.2.1.1 Tutorial: how to build a basic New Bayesian Network

This tutorial is aimed at implementing a simple Bayesian Network (BN), named also as Directed Acyclic Graph (DAG), in Hugin software, version 8.1 (Hugin, 2016). The tutorial is aimed at exploring the main functions, tools and potentialies of Bayesian Networks, applying in practice the concepts described in Section 3.3.2.1.3.2

The illustrative tutorial considers two safety barriers, one technical (e.g., a sprinkler system), the other human/organizational (e.g. emergency fire-brigade intervention), whose failure may cause a fire in a chemical installation. The situation can be modelled by the Bayesian Network displayed in Figure 5. 4.

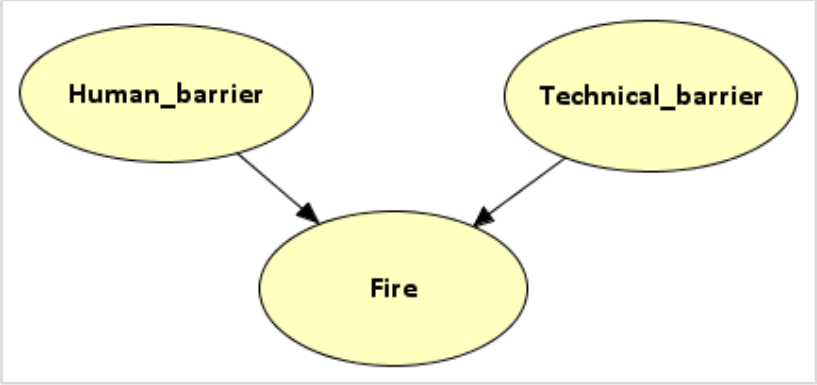


Figure 5. 4 Bayesian Network for the illustrative tutorial.

The BN consists of three nodes: "*Human_barrier*", "*Technical_barrier*" and "*Fire*" which can all be in one of two states: "*Human_barrier*" can be either in the state "*Human_barrier (failure)*" or "*not*"; "*Technical_barrier*" can be either "*Technical_barrier (failure)*" or "*not*" - and "*Fire*" can be either "*yes*" or "*not*".

The node "*Human_barrier*" tells us that the system can undergo a fire by being in state "*Human_barrier (failure)*". Otherwise, it will be in state "*not*". The nodes "*Technical_barrier*"

and "*Fire*" tell us in the same way if the system shows a technical barrier failure and if a fire is taking place, respectively. The focus of the example is on safety barriers failure, so the automatic "*yes*" state provided by the software has been renamed respectively by "*Human_barrier (failure)*" and "*Technical_barrier (failure)*" for the two nodes "*Human_barrier*" and "*Technical_barrier*" of the tutorial, with the purpose to avoid misunderstandings. The Bayesian Network in Figure 5. 4 models the causal dependence from "*Human_barrier*" to "*Fire*" and from "*Technical_barrier*" to "*Fire*". The representation in Figure 5. 4 should be considered as a qualitative representation of BN, while the quantitative representation is given by the set of Conditional Probabilities Tables (i.e., CPTs) of the nodes. In Figure 5. 5 the CPTs of the three nodes represented in Figure 5. 4 are reported. The probabilities reported in the present tutorial have been chosen arbitrarily, in purpose to demonstrate the applicability of Bayesian Network technique.

Technical_barrier

Technical barri	0.1
not	0.9

Fire

Techical barrie	Technical barrier		not	
Human barrier	Human ba	not	Human ba	not
ves	0.95	0.85	0.9	0.02
not	0.05	0.15	0.1	0.98

Human_barrier

Human barrier	0.1
not	0.9

Figure 5. 5 CPTs of the nodes; screenshot of Hugin software.

All the three tables show the probability of a node being in a specific state depending on the states of its parent nodes but since "*Human_barrier*" and "*Technical_barrier*" do not have any parent nodes, the distributions referred to them are not conditioned on anything. This step finish the construction of the networks with tools provided by Hugin development environment. In Figure 5. 6 the network window has been shown in "Run Mode", with the probabilities of each node being in a certain state. With these inputs, the probability of the system being on fire is 18.32%; in a more formal way: $P(Fire = "yes") = 0.1832$.

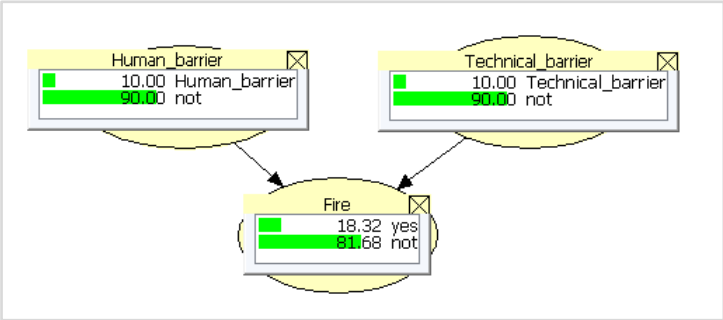


Figure 5. 6 The network window for the tutorial in run mode, with overlapped node list pane.

Then, the network can be applied by entering evidence in some of the nodes where the state is known and retrieve the new probabilities calculated in other nodes corresponding to this evidence. The use of additional information is probably the most distinctive advantage of Bayesian-based techniques. In this example, let's suppose it is known that the fire is taking place. This evidence can be entered by selecting the state *"yes"* in the *"Fire"* node. Then, the probability of the fire taking place can be read as the probability of the node *"Human_barrier"* being in state *"Human_barrier (failure)"* and the probability of the node *"Technical_barrier"* being in state *"Technical_barrier (failure)"*. In Figure 5. 7, the BN after the entrance of the evidence that the system is on fire and the "sum propagation tool" has been reported.

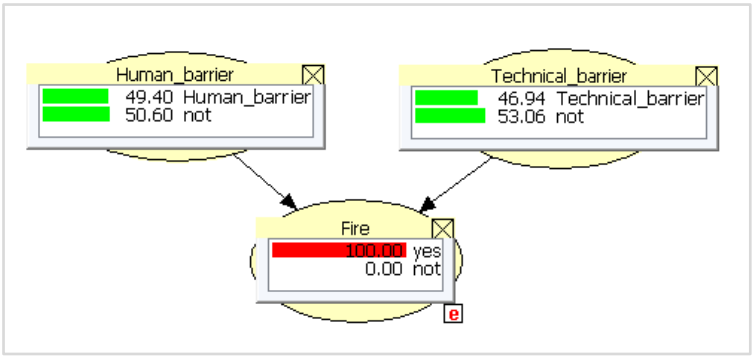


Figure 5. 7 BN after entrance of the evidence that a fire is taking place and sum propagation.

Another interesting feature, especially with the final goal of modelling domino-effect scenarios for chemical process plants, can be the identification of the most likely combination of state and the related probability (i.e., MPE). In this case the most likely combination of states, obtained by using the "maximum propagation tool", is given by *"Human_barrier"* being in the failure state and *"Technical_barrier"* being the "not" state. The monitor window has been displayed in Figure 5. 8.

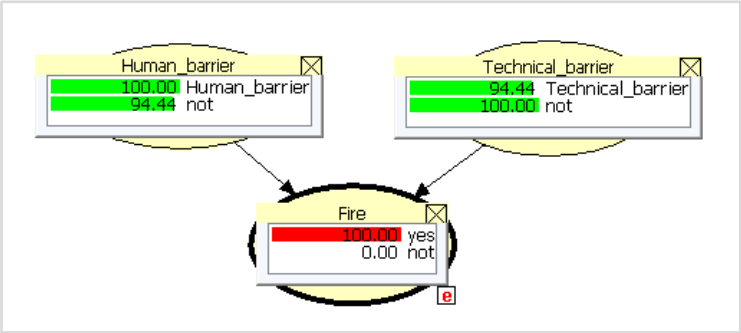


Figure 5. 8 Most likely combination of events that cause a fire in the system.

The software reports the probability of the entered evidence:

$$P(Human\_barrier = "human\_barrier(failure)", \quad Technical\_barrier = "not", \\ Fire = "yes") = 0.081 = P(All)$$

Eventually the final probability of the most likely combination of states, giving the evidence that a fire is taking place, can be calculated, according to equation (3.20):

$$P(Human\_barrier = "Human\_barrier(failure)", \\ Technical\_barrier = "not" \mid Fire = "yes")$$

$$= \frac{P(Human\_barrier = "human\_barrier(failure)", \ Technical\_barrier = "not", \ Fire = "yes")}{P(Fire = "yes")}$$

$$= \frac{0.081}{0.1832} = 0.442$$

Similarly, the final probability of other combinations of states can be computed.

The tutorial herein reported makes clear what are the main advantages of BNs application: flexibility and easy-to-update information. On the other side, when modelling causal dependence in BNs it is not always so clear in which direction a link should point, especially when nets are bigger than this one; this is a relevant drawback still affecting BN technique. In further applications, more realistic inputs probabilities coming from databases will be applied and more complex chemical process systems will be analyzed.

5.2.2.1.2 Tutorial: How to build a basic Limited Memory Influence Diagram

The tutorial conceived considers the extension of the BN, previously constructed and described, into a Limited Memory Influence Diagram (i.e., LIMID), by application of Hugin software version 8.1 (Hugin, 2016). For further information on the previous example, please go again to Section 5.2.2.1.2). The aim of the tutorial is to explain how to implement a rather simple LIMID with the software.

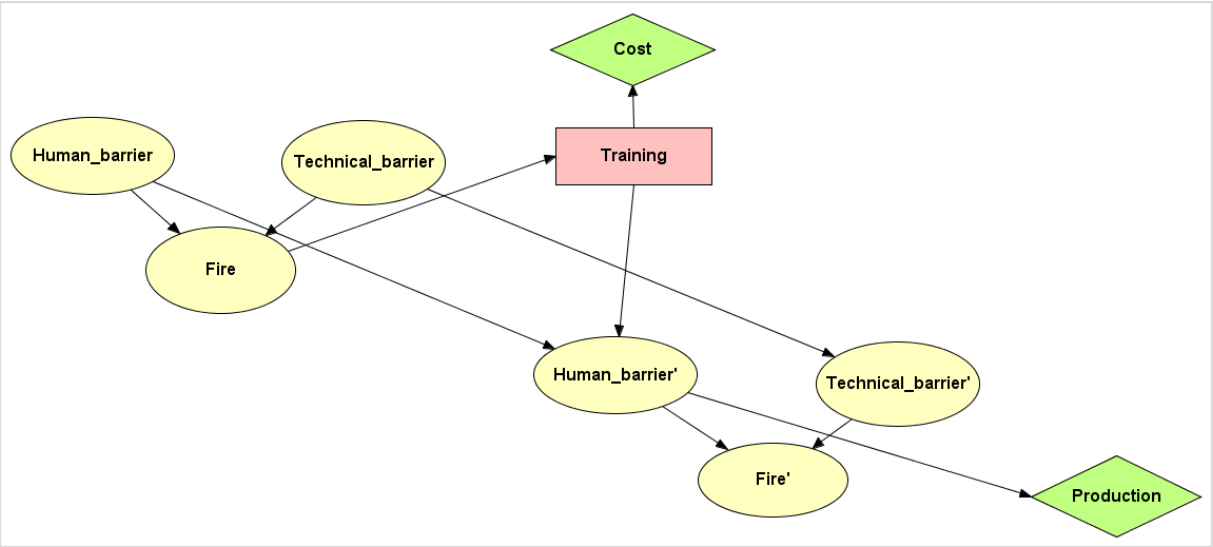


Figure 5. 9 The complete influence diagram (i.e., LIMID) for the tutorial.

The management of a small process plant wants to decide whether or not invest resources on additional training courses for employees, after an accidental event, recently happened, has raised the attention toward safety issues of the site. Since this involves a decision through time, it implies a modification of the previous BN. The complete influence diagram has been reported in Figure 5. 9.

In this case, the construction (or edit phase) of the Directed Acyclic Graph consists of different steps:

1. Editing the BN just constructed, composed by three nodes: *Human_barrier*, *Technical_barrier* and *Fire*.
2. Adding three nodes, very similar to those already present in the network. The new nodes *Human_barrier'*, *Technical_barrier'* and *Fire'* represent the same as the old nodes, except that they represent the situation at the time of normal production. The new nodes can be in the same states as the old nodes: *Human_barrier'* can be either *"Human_barrier (failure)"* or *"not"* - *Technical_barrier'* can be either *"Technical_barrier (failure)"* or *"not"* - and *Fire'* can be either *"yes"* or *"no"*. In the new model, a causal dependence from both the old *Human_barrier* node to the new *Human_barrier'* node and the old *Technical_barrier* node to the new *Technical_barrier'* node is expected. This is because if, for example, the failure of a technical barrier is expected at the present time, then this is also very likely to be the case in the future. Of course, the strength of the dependence depends on how far out in the future the net refers. It could be possible also to have a dependence from *Fire* to *Fire'*.

3. Adding a utility node, named *Production*, which represent the utility gained from the production process. Diamonds represents utility nodes; each contributes with one part of the total utility. It depends on the state of *Human_barrier'* indicating that the production of the plant depends on the human barrier integrity.
4. Adding a decision node, named *Training*, which represents the decision to give the workers an additional training on safety issues. Action nodes are represented by rectangles. The Training node has the states *"training"* and *"not"*. As it appears also a link from *Training* to *Human_barrier'* has been added. This is because we expect the training to have an impact on future events involving the process plant.
5. Linking a *Cost* – utility node to *Training* node. The utility node *Cost* gathers information about the cost of the training. The action of giving the employees a training course make the representation an influence diagram.
6. Filling the Conditional Probabilities Tables (CPTs). The CPTs referred to the nodes *Human_barrier*, *Technical_barrier* and *Fire* have already been showed in Figure 5. 10. The CPTs of *Human_barrier'* and *Technical_barrier'* are different from the previous tutorial and they are specified in the following table (Figure 5. 11).

Utility functions should be specified with the purpose to compute the expected utility of a decision. The *Production* utility node shows that if the human barrier doesn't fail (*Human_barrier'* is the state *"not"*), an income of 20000€ will be obtained, while if the barrier fails (*Human_barrier'* is state *"yes"*) the income will decrease suddenly to 3000 €. The decision node *Training* and the utility node *Cost* show that if the choice is to implement an additional training course, the management should spend 8000 €.

Cost

Training	training	not
Utility	-8000	0

Training

Fire	yes	not
training	0	0
not	1	1

Production

Human_barrier	Humanb_fa	not
Utility	3000	20000

Figure 5. 10 Screenshot of the utility nodes (*Production* and *Cost*) and the decision nodes (*Training*), which are present in the LIMID.

Technical_barrier'

Techical_barrie	Technicalb	not
Technical_barri	0.6	0.05
not	0.4	0.95

Human_barrier'

Training	training		not	
Human_barrier	Humanb_fa	not	Humanb_fa	not
Humanb_fail	0.2	0.01	0.99	0.02
not	0.8	0.99	0.01	0.98

Figure 5. 11 Screenshot of the CPTs for the nodes *Human_barrier'* and *Technical_barrier'*.

The quantitative representation of the influence diagram is given by adding conditional probability table (CPT) for each chance node and a utility table for each utility node. The utility tables are simply cost functions. A decision node does not have any table. At that point, the construction of the influence diagram has been completed and the net can be compiled.

The solution to a LIMID is determined using Single Policy Updating, as explained in Section 3.3.2.1.3.2. This is a theoretical explanation, but how to put it into practice? In the present case the "Single Policy Updating" has been applied by inserting the evidence that *Fire* is *"yes"*. This means that the management of the small process plant has to decide whether or not invest resources on additional training courses for employees, after a recent accident (e.g. a fire a couple of weeks before). The net has been propagated using the "sum propagation tool" and in the *Training* decision node the expected utility of *"training"* or *"not"* can be eventually read; a screenshot has been reported in Figure 5. 12.

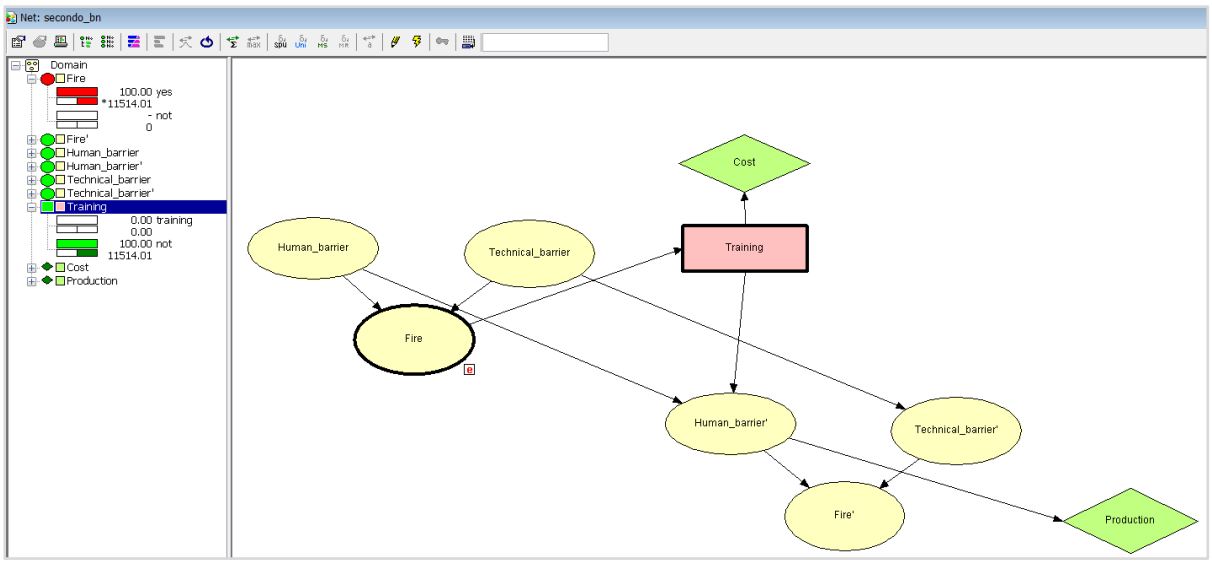


Figure 5. 12 The influence diagram propagated with the evidence that *Fire = "yes"*.

With this evidence, the expected utility of not doing anything is 11514 €. This suggests that, under the specific inputs and assumptions considered, it will be best for the management not

to implement another training course. Obviously, the final outcome, as well as consequent choices, are strongly affected by the inserted CPTs and Utility functions. Figure 5. 13 reports the probabilities and the utilities referred to each node of the net.

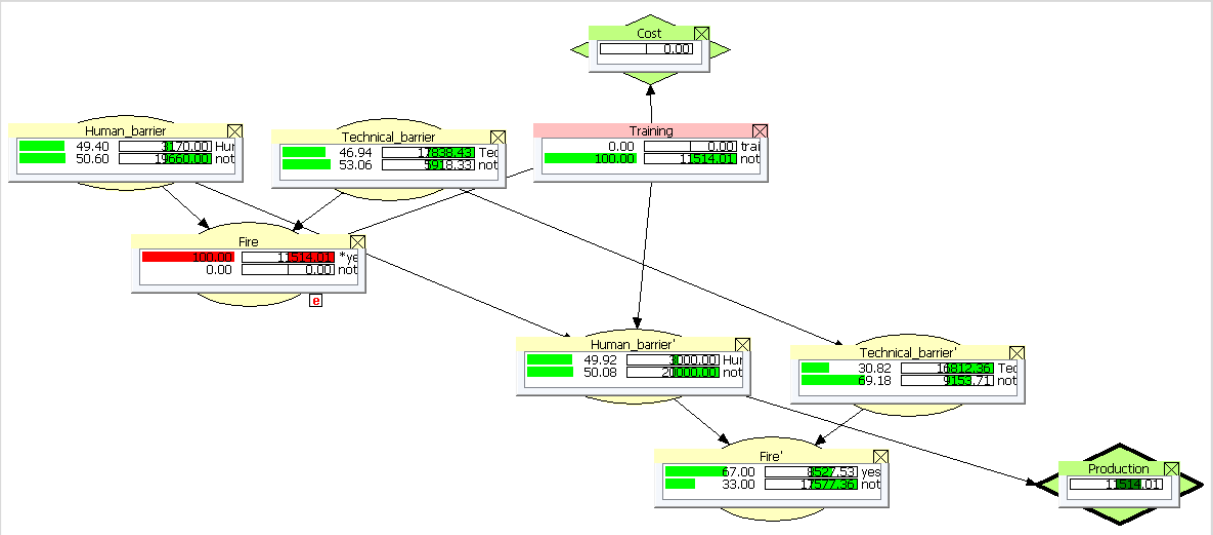


Figure 5. 13 The influence diagram (LIMID) propagated with the evidence that *Fire = "yes"*, with the probabilities and utilities for each node.

5.2.2.2 Case study C: conversion of a Fault-Tree into a Bayesian Network for the analysis of a feeding control system

5.2.2.2.1 Description of the case study

The implementation of a Bayesian Network (i.e., BN), starting from a Fault-Tree (i.e., FT), has been carried out by reproducing the case study proposed by Khakzad et al. (Khakzad et al., 2011). The aim of the case study is to show the practical application of the mapping procedure described in Section 3.3.2.1.3.3.1.

The case study deals with the performance of a feeding control system that transfers propane from a propane evaporator to a scrubbing column, so the top event considered in the case study is feed system improper control. In purpose to maintain a specified and constant pressure inside the scrubbing column, the feed pipeline is equipped with an automatic valve operated by an actuator. A manual valve has also been considered in order to avoid pressure increase in case of malfunction of the automatic valve. The automatic valve immediate and effective control depends on the mechanical failure of the actuator and the valve as well as on signals. The latter ones depend on a pressure relay and a pressure controller that received signals from a pressure transmitter. On the other side, the manual valve improper control can be due to a mechanical failure or to a human failure during the operation. All components have been assumed binary (i.e. work/fail components), at least in the first modelling step. The occurrence

probability data of primary events that would contribute to the occurrence of this accident scenario have been reported in Table 5. 14, while intermediate events, as well as the top event, have been identified by their type of gate.

Table 5. 14 Input data for Fault-Tree development regarding an accidental scenario for a feeding control system. Occurrence probabilities and type of gates applied in the case study are adapted from a previous study (Khakzad et al., 2011).

Number	Component	Symbol	Probability
1	Pressure transmitter failure	PT	1.647 E-01
2	Pressure controller failure	PC	2.818 E-01
3	No signal received by pressure controller	PC_signal	*OR-gate*
4	Pressure relay failure	PY	1.538 E-01
5	No signal received by actuator	Act_signal	*OR-gate*
6	Automatic valve mechanical failure	A_valve	3.403 E-01
7	Actuator mechanical failure	Actuator	2.015 E-01
8	Automatic valve improper control	A_valve_ctrl	*OR-gate*
9	Human failure in operating manual valve	Hum_error	2.696 E-01
10	Manual valve mechanical failure	M_valve	1.393 E-01
11	Manual valve improper control	M_valve_ctrl	*OR-gate*
12	Feed system improper control	Feed_ctrl	*AND-gate*

The starting Fault-Tree has been reported in Figure 5. 14; the mapping algorithm reported in Section 3.3.2.1.3.3.1 allows constructing the correspondent Bayesian Network (i.e., reported in Figure 5. 15), by applying the dedicated software Hugin version 8.1 (Hugin, 2016).

Bayesian Network analysis of the so-obtained net, as well as the subsequent implementation of other relevant modelling aspects allows demonstrating the ability of this technique to handle multi-state variables, sequentially dependent failure and uncertainties.

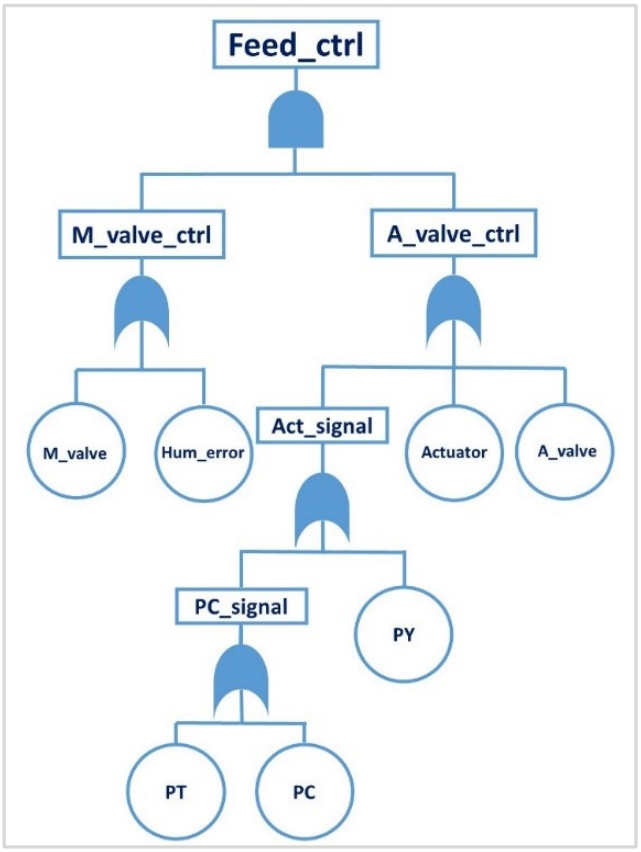


Figure 5. 14 Fault-Tree for the malfunction of a feed system for propane transfer, adapted from Khakzad et al. (Khakzad et al., 2011).

5.2.2.2.2 Conversion of Fault-Tree into a Bayesian Network and application of Bayesian analysis

The Bayesian Network reported in Figure 5. 15 represents the translation of FT in Figure 5. 14, according to the mapping process described in Section 3.3.2.1.3.3.1. The prior probability of the leaf node in the BN is calculated to be $P(Feed_{ctrl}) = 2.720 \cdot 10^{-1}$, which is the same as that of the FT. The application makes clear that, during predictive analysis to calculate the scenario occurrence probability (i.e., $P(Feed_{ctrl})$), with no additional information/evidence added to the network, the BN provides the same results to those of the traditional FT, as long as primary events are independent of each other, as in the present example. In other words, the results reported in Table 5. 15 prove that, whenever a translation of a Fault Tree is performed, the expected results in terms of prior probabilities are the same ones of the corresponding BN.

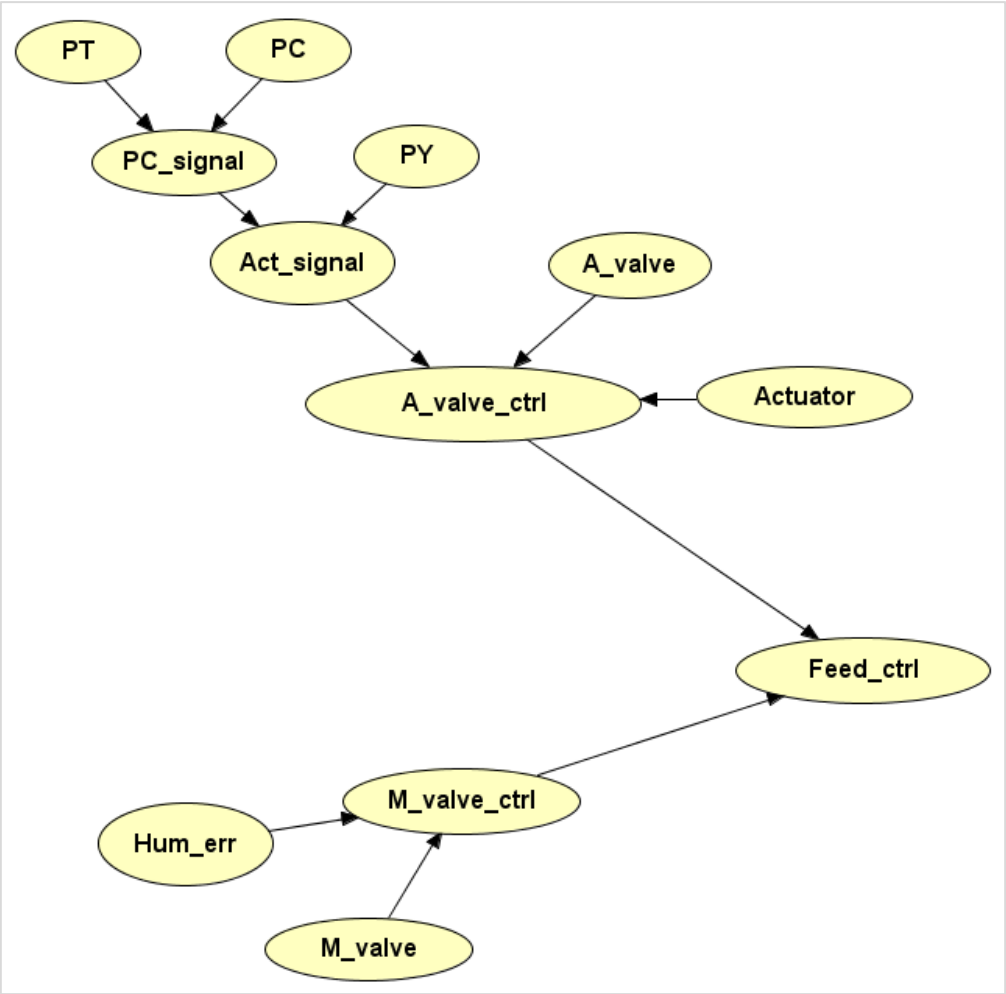


Figure 5. 15 Bayesian Network based on the fault tree reported in Figure 5. 14, named "First modelling".

However, BNs take advantage on FTs in reducing parameter uncertainty through two probability revising techniques: probability adapting and probability updating. In BN analysis, the posterior probabilities reflect the characteristics of the accident more specifically than prior probabilities, due to new observations.

A common feature is the calculation of the posterior marginal probabilities of root nodes given the scenario occurrence (as an inserted evidence); this probability revising technique is called probability adapting or abductive reasoning. The posterior probability of each root node C_i can be calculated as $P(C_i|Feed\_ctrl)$, indicating the probability of C_i conditioned to the feed system control $(P(Feed\_ctrl) = 1)$ malfunction/failure. Prior and posterior probabilities, calculated according to the "sum propagation tool" have been reported in Table 5. 15.

It may be observed from Table 5. 15 that the occurrence probability of the events $Human\_error$, M_valve and M_valve_ctrl have the highest increase.

Table 5. 15 Bayesian Analysis results referred to "First modelling" network (reported in Figure 5. 15): comparison between prior and posterior probabilities and % relative increases.

Number	Component	Fault-Tree analysis	Bayesian Network analysis: first modelling		
			Prior	Posterior	Δ rel %
1	PT	1.647E-01	1.647E-01	2.248 E-01	36.5%
2	PC	2.818 E-01	2.818 E-01	3.847 E-01	36.5%
3	PC_signal	4.001 E-01	4.001 E-01	5.461 E-01	36.5%
4	PY	1.538 E-01	1.538 E-01	2.099 E-01	36.5%
5	Act_signal	4.924 E-01	4.924 E-01	6.721 E-01	36.5%
6	A_valve	3.403 E-01	3.403 E-01	4.645 E-01	36.5%
7	Actuator	2.015 E-01	2.015 E-01	2.751 E-01	36.5%
8	A_valve_ctrl	7.326 E-01	7.326 E-01	1	36.5%
9	Hum_error	2.696 E-01	2.696 E-01	7.260 E-01	145.3%
10	M_valve	1.393 E-01	1.393 E-01	3.751 E-01	169.3%
11	M_valve_ctrl	3.713 E-01	3.713 E-01	1	169.3%
12	Feed_ctrl	2.720 E-01	2.720 E-01	1	Evidence

Another relevant feature is the determination of the most probable state of all the variables given the accident occurrence (i.e., the most probable configuration), named in statistics as posterior joint probability of all primary event, according to probability updating technique. The accident occurrence, which is expressed by $P(Feed\_ctrl) = 1$, is inserted as evidence in the net. In this case, the BN searches over each variable to identify weak links by applying the "max propagate" tool. As visible from Figure 5. 16, the most probable sequence of events given the accident occurrence is the one corresponding to the occurrence of the failure of the following components: *Hum_err*, *M_valve_ctrl*, *A_valve* and *A_valve_ctrl*. The probability of the system being in the most probable configuration has been computed, according to equation (3.20) and reported in Figure 5. 16.

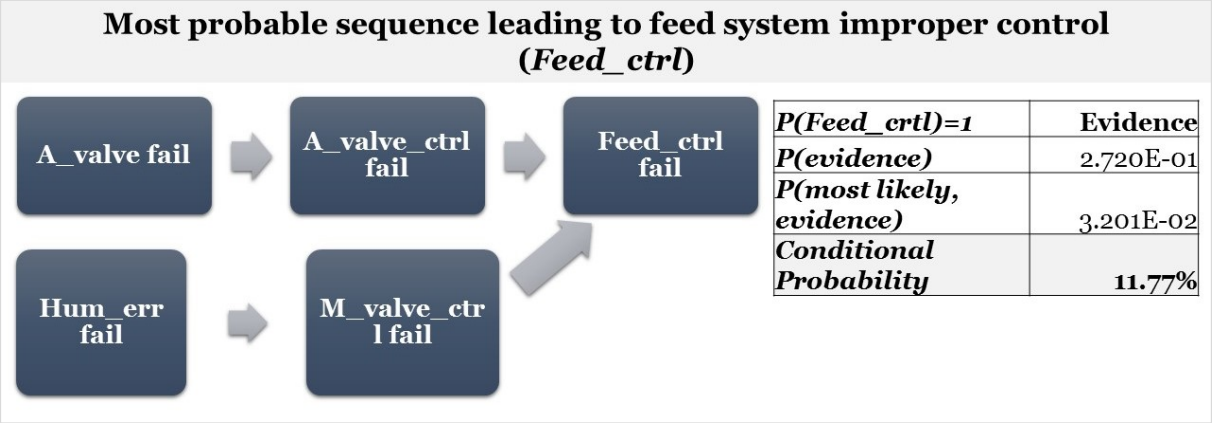


Figure 5. 16 Bayesian Updating results for the case study, aimed at calculating the most probable sequence of events leading to the top event (i.e., malfunction in feed control), according to "First modelling" Bayesian Network.

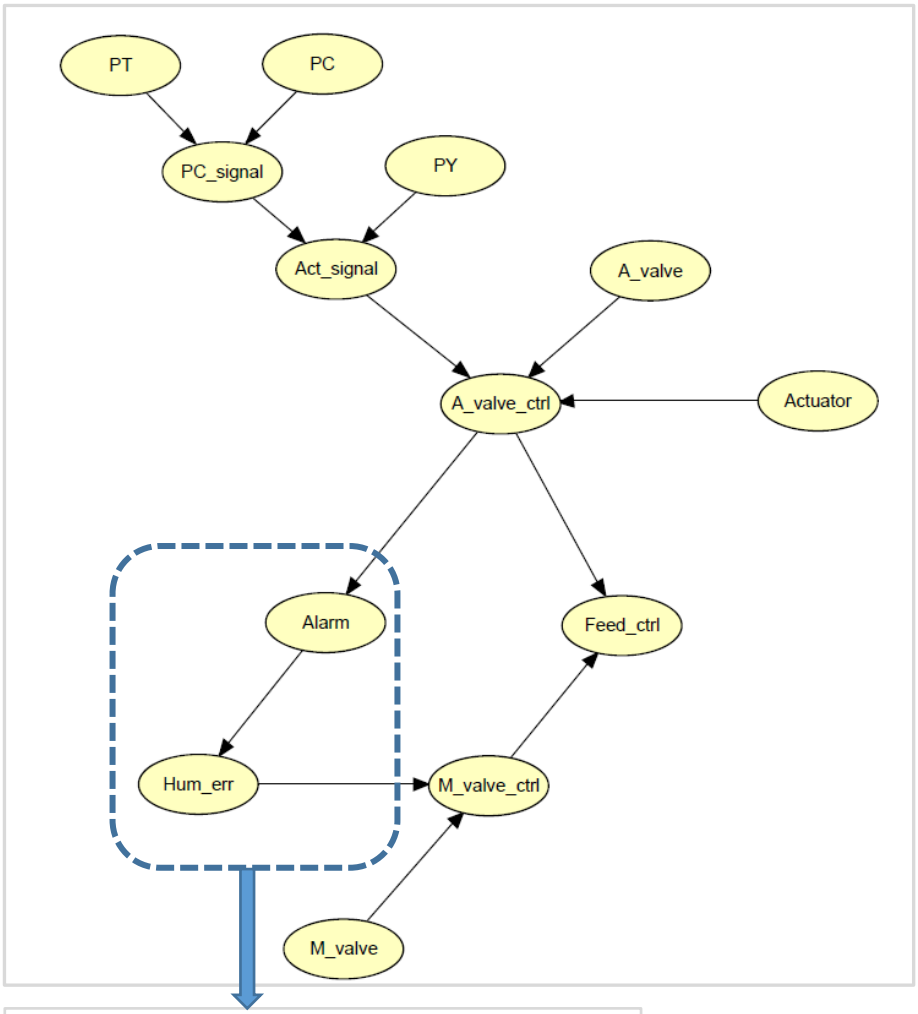
The importance of this feature for safety analysis is due to its ability in identifying critical sequence of events and allocating safety barriers not only to the primary events directly leading to the top event but also to weak links that are combination of non-critical events.

5.2.2.2.3 Extension of Bayesian Network application to multi-state variables and dependent failures

Two assumptions in the application of Fault-Tree analysis consist of considering components binary and events independent. A Bayesian Network can overcome these limitations, as shown by the following application to the case study.

Starting from the system considered in Figure 5. 15, it is assumed that the manual valve is closed by the operator only if an alarm system sounds due to the automatic valve failure (that means A_valve_ctrl occurrence). All components are assumed binary, except for the alarm system, named *Alarm*. The alarm system is considered ternary; its three states are: *No-sound* (i.e., alarm fails to sound), *Wrong-sound* (i.e., alarm sounds although automatic valve works), and *Right-sound* (i.e., alarm sounds when automatic valve fails). It has also been assumed that human failure probabilities referred to closing the manual valve (named, Hum_err) differ for wrong and right alarm sounds.

The occurrence probability of the BN components, expressed as inputs in the Conditional Probability Tables (i.e., CPTs), are the same considered in "First modelling" net and reported in Table 5. 14, except for *Alarm* and Hum_err which are assigned new CPTs, available in Figure 5. 16. For ease of comparison in subsequent calculations, CPT values have been identified such that the prior probability of Hum_err would be $2.696 \cdot 10^{-1}$ (as in "First modelling" step). The BN obtained by applying the software Hugin version 8.1. has been reported in Figure 5. 17, with the modified or newly inserted CPTs. The net has been indicated as "Alarm modelling". As before, the aim of BN is to predict the probability of improper operation of the control system (i.e., $P(Feed\_ctrl)$) . Prior probabilities for each node have been reported in Table 5. 16. It should be noticed that *Alarm* can have two different failure modes: *no-sound* and *wrong-sound*. The prior probability of the leaf node in the BN is calculated to be $P(Feed_{ctrl}) = 1.146 \cdot 10^{-1}$, inferior to the one calculated in First modelling step and reported in Section 5.2.2.2.2.



Hum_err

Alarm	no-sound	wrona-sou	right-sounc
fail	1	0.07	0.01
work	0	0.93	0.99

Alarm

A_valve_ctrl	fail	work
no-sound	0.01	0.95
wrona-sound	0	0.05
right-sound	0.99	0

Figure 5. 17 BN structure for feed control system with alarm systems (Alarm modelling step). The fraction of the net modified in comparison with the previous one has been highlighted and its CPTs for nodes *"Human error"* (modified CPT - top) and *"Alarm system"* (added CPT - bottom) have been reported.

Prior and posterior probabilities have been reported in Table 5. 16. It may be observed from Table 5. 16 that, adding the evidence $P(Feed\_ctrl) = 1$, the occurrence probability of the events M_valve and M_valve_ctrl has the highest increase. Hum_err prior probability is the same compared with the basic study case, but it decreases suddenly adding the evidence. This value highlights that adding the alarm system helps the operator to prevent accident occurrence, resulting in a decrease of $P(Feed_{ctrl})$.

Table 5. 16 Bayesian Analysis results, referred to "Alarm modelling step", whose BN is is reported in Figure 5. 17: comparison between prior and posterior probabilities and % relative variations.

Number	Component	Alarm modelling		
		Prior	Posterior	Δ rel %
1	**PT**	1.647 E-01	2.248 E-01	36.5%
2	**PC**	2.818 E-01	3.847 E-01	36.5%
3	**PC_signal**	4.001 E-01	5.461 E-01	36.5%
4	**PY**	1.538 E-01	2.099 E-01	36.5%
5	**Act_signal**	4.924 E-01	6.721 E-01	36.5%
6	**A_valve**	3.403 E-01	4.645 E-01	36.5%
7	**Actuator**	2.015 E-01	2.751 E-01	36.5%
8	**A_valve_ctrl**	7.326 E-01	1	36.5%
9	**Hum_error**	2.696 E-01	1.272 E-01	-52.8%
10	**M_valve**	1.393 E-01	8.905 E-01	539.3%
11	**M_valve_ctrl**	3.713 E-01	1	169.3%
12	**Feed_ctrl**	1.146 E-01	1	evidence
13	**Alarm (no-sound)**	2.614 E-01	6.39 E-02	-75.6%
	Alarm (wrong-sound)	1.340 E-01	0	-100.0%

The determination of the most probable state of all the variables given the accident occurrence (the most probable configuration) has been carried out also for the system including alarm (Figure 5. 17). The most probable state, given the accident occurrence, is the one corresponding to the occurrence of the events M_valve, M_valve_ctrl, A_valve and A_valve_ctrl. The probability of the system being in the most probable configuration has been computed, according to equation (3.20):

$$P(most\ likely\ configuration) = \frac{P(most\ likely\ configuration, evidence)}{P(evidence)} = \frac{0.018833}{0.114597}$$

$$= 1.643 \cdot 10^{-1}$$

It should be noted that human error is not included anymore in this configuration, as suggested by previous observations. According to the new most probable explanation, mechanical failure of the automatic valve is to blame for A_valve_ctrl occurrence, triggering the alarm system. Despite alarm system proper functioning, the manual valve cannot be closed because of mechanical failure (M_valve) , not the operator failure. So mechanical failure of the automatic and manual valve eventually caused the feed system not to work properly.

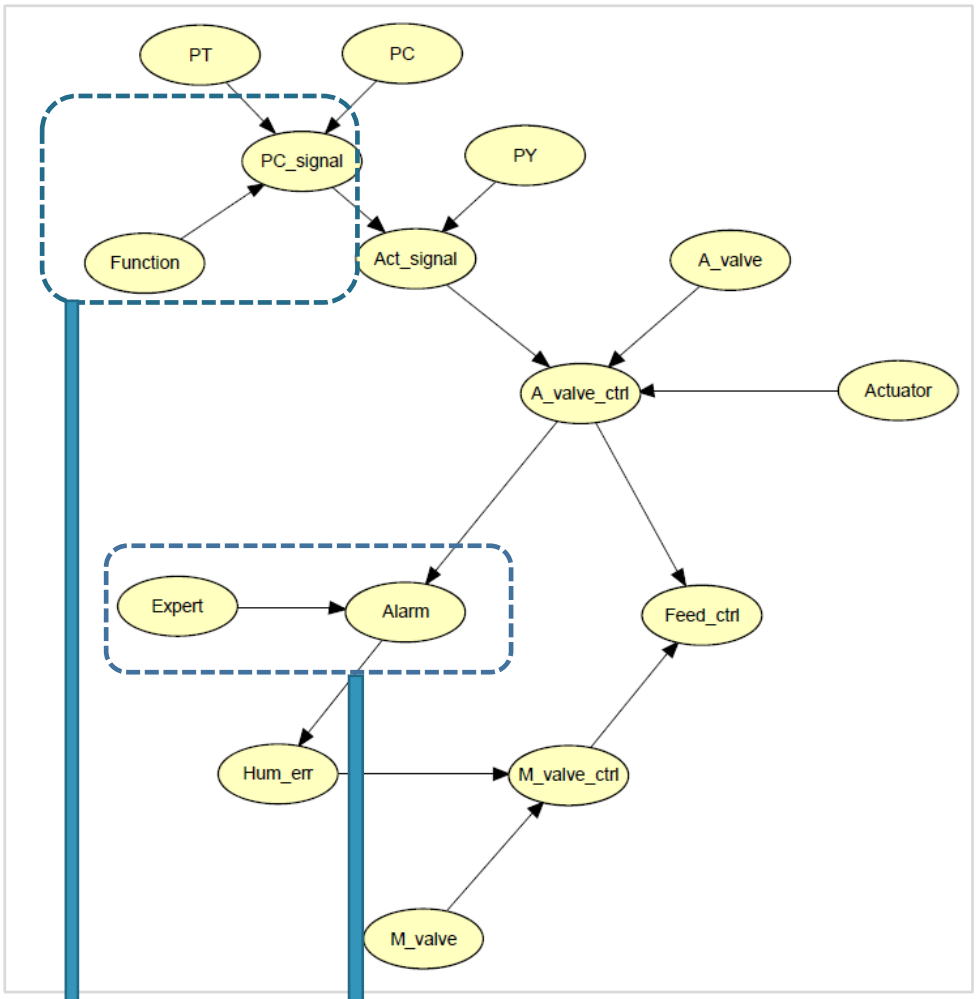
5.2.2.2.4 Application of functional uncertainties & Expert Opinion

Another interesting feature of BN is the ability to capture some types of uncertainties that are relevant for accident analysis, as functional uncertainty and uncertainty due to expert opinion.

Functional uncertainty is due to the lack of certitude in accurate determination of a causal function among nodes. In order to handle this kind of uncertainty, alternative functions and their relative frequencies should be known. In BNs the most common functions used to link a child node to its parents are intersection and union of variables (corresponding respectively to *OR-gate* and *AND-gate* in FTs), but sometimes it is not clear which is the correct relation, whose choice turns into different probabilities. As an example, it is assumed that in the BN shown in Figure 5. 17 , it is not clear whether $PC\_signal = PC \cup PT$ or $PC\_signal = PC \cap PT$, but it is known that the likelihood of the former is three times that of the latter, that means $Pr(U) = 3 \cdot Pr(\cap)$. This uncertainty can be modeled by adding another parent node to PC_signal, named $Function$. $Function$ has two states: $intersection$ and $union$ and the CPT for node $Function$ has been filled by using the information available: $Pr(Function) = Pr(\cup,\cap) = (0.75\ , 0.25)$.

This turns into a modification of the CPT for node PC_signal, as reported in Figure 5. 18. In BNs most prior beliefs used to construct the model are based on domain experts' opinions. So, it is common to have different beliefs about probability parameters due to different experts assessing the model values.

BN allows considering different judgments in the network structure by adding a node to the parent set of the node of interest. The newly added node has one state for each expert and its prior probability represents the reliability degree of each expert. For instance, it is assumed that two experts (e.g., Exp_1 and Exp_2) have been asked to assess the causal effect of A_valve_ctrl on $Alarm$. So, node $Expert$ with two states Exp_1 and Exp_2 has been added to parent set of $Alarm$. The reliability of the first expert is 60% and that of the second is 40%, so the CPT of the node has been filled consequently (i.e., $Pr(Expert) = Pr(Exp_1, Exp_2) = (0.6\ , 0.4)$. The different opinions of experts about the conditional dependence of $Alarm$ on A_valve_ctrl have been included in the corresponding CPT (Figure 5. 18). Prior and posterior probabilities of the BN expressing functional uncertainty and expert opinion (Figure 5. 18) have been listed in Table 5. 17. Posterior probabilities have been obtained by probability revision (given the accident occurrence), as explained in the previous paragraph.



Alarm

Expert	Expert1		Expert2	
A_valve_ctrl	fail	work	fail	work
no-sound	0.01	0.95	0.04	0.92
wrong-sound	0	0.05	0	0.08
right-sound	0.99	0	0.96	0

PC_signal

Function	union(AND)				intersection(OR)			
PC	fail		work		fail		work	
PT	fail	work	fail	work	fail	work	fail	work
fail	1	1	1	0	1	0	0	0
work	0	0	0	1	0	1	1	1

Figure 5. 18 Modified BN structure to capture functional uncertainty and expert opinion (Uncertainty modelling step). The fraction of the net modified in comparison with the previous one (feed system with alarm) has been highlighted and its CPTs, for nodes *PC_signal* and *Alarm* have been reported. The newly added nodes are *Function* and *Expert*.

Table 5. 17 Bayesian Analysis results (referred to Uncertainty modelling step): comparison between prior and posterior probabilities and % relative variations. Bayesian Analysis results (referred to Uncertainty modelling step): comparison between prior and posterior probabilities and % relative variations.

Number	Component	Uncertainty modelling		
		Prior	Posterior	Δ rel %
1	**PT**	1.647 E-01	2.186 E-01	32.7%
2	**PC**	2.818 E-01	3.687 E-01	30.8%
3	**PC_signal**	3.117 E-01	4.496 E-01	44.2%
4	**PY**	1.538 E-01	2.219 E-01	44.3%
5	**Act_signal**	4.175 E-01	6.024 E-01	44.3%
6	**A_valve**	3.403 E-01	4.909 E-01	44.3%
7	**Actuator**	2.015 E-01	2.907 E-01	44.3%
8	**A_valve_ctrl**	6.932 E-01	1	44.3%
9	**Hum_error**	3.112 E-01	1.907 E-01	-38.7%
10	**M_valve**	1.393 E-01	8.359 E-01	500.1%
11	**M_valve_ctrl**	4.071 E-01	1	145.6%
12	**Feed_ctrl**	1.155 E-01	1	evidence
13	**Alarm (no-sound)**	3.031 E-01	1.320 E-01	-56.5%
	Alarm (wrong-sound)	1.900 E-02	0	-100.0%
14	**Expert (Exp 1)**	6.000 E-01	5.632 E-01	-6.1%
	Expert (Exp 2)	4.000 E-01	4.368 E-01	9.2%
15	**Function (Union)**	7.500 E-01	7.926 E-01	5.7%
	Function (Intersection)	2.500 E-01	2.074 E-01	-17.0%

The results show a slight increase in the likelihood of union relationship between PT and PC: $Pr(Function) = Pr(\cup,\cap) = (0.7926\,, 0.2074)$. Regarding experts opinions. an increase in the reliability of Exp_2 has been reported: $Pr(Expert) = Pr(Exp_1, Exp_2) = (0.5632\,, 0.4368)$. The prior probability of the leaf node, indicating the failure of feed system, is: $P(Feed_{ctrl}) = 1.155 \cdot 10^{-1}$; its increase in comparison with the value previously calculated, i.e. $1.146 \cdot 10^{-1}$ (see Section 5.2.2.2.3), denotes the effect of uncertainty consideration in the model. The most probable configuration of events, given the accident occurrence, is the one corresponding to the occurrence of the events M_valve, M_valve_ctrl, A_valve and A_valve_ctrl, that is the same as before. The probability of the system being in the most probable configuration has been computed, according to equation (3.20):

$$P(most\ likely\ configuration) = \frac{P(most\ likely\ configuration, evidence)}{P(evidence)} = \frac{0.008475}{0.115520}$$

$$= 7.34 \cdot 10^{-2}$$

The new most probable configuration determines that the states of $Function$ and $Expert$ have to be $Union$ (AND) and Exp_1, respectively.

5.2.2.2.5 Discussion and conclusions on the case study

The present benchmark application has been aimed at implementing a Bayesian Network, starting from a Fault-Tree and subsequently at exploring the features of BN technique. The case study here-in considered has been adapted from Khakzad et al. (Khakzad et al., 2011), in order to have a direct comparison of the results for each modelling step. Despite this application should be considered an intermediate step in the development of a full-Bayesian approach to safety barriers performance assessment, it has been relevant in illustrating the use of BNs in both accident occurrence probability estimation and updating in the light of new information or uncertainties.

A FT was used to construct a corresponding BN by following a specific conversion algorithm. Both methods proved effective in the estimation of accident occurrence probability, but BN took advantage of probability updating. By propagating new observations through the network, BN updates the prior probabilities, yielding posterior probabilities that are more specific to case considered.

Then, the application was focused on implementing those aspects and modelling issues of BN, which FT is incapable of handling, such as multi-state variables, dependent failures and uncertainties.
The overall results, obtained from the three modelling steps, have been summarized in Table 5. 18, Figure 5. 19 and Figure 5. 20. The application made clear that each FT can be mapped to its corresponding BN, while a BN does not necessarily have an equivalent FT, due to its much more flexible structure.
Eventually the application of the conversion process from a Fault Tree to a Bayesian Network made clear the advantages of the latter one. In general, BN proved a significant ability for abductive reasoning and uncertainty handling, which may turn into real-time accident analysis and more effective design and evaluation of safety measures.

Table 5. 18 Comparison between prior and posterior probabilities in different modelling steps.

Number	Component	First modelling		Alarm modelling		Uncertainty modelling	
		Prior	Posterior	Prior	Posterior	Prior	Posterior
1	PT	1.647 E-01	2.248 E-01	1.647 E-01	2.248 E-01	1.647 E-01	2.186 E-01
2	PC	2.818 E-01	3.847 E-01	2.818 E-01	3.847 E-01	2.818 E-01	3.687 E-01
3	PC_signal	4.001 E-01	5.461 E-01	4.001 E-01	5.461 E-01	3.117 E-01	4.496 E-01
4	PY	1.538 E-01	2.099 E-01	1.538 E-01	2.099 E-01	1.538 E-01	2.219 E-01
5	Act_signal	4.924 E-01	6.721 E-01	4.924 E-01	6.721 E-01	4.175 E-01	6.024 E-01
6	A_valve	3.403 E-01	4.645 E-01	3.403 E-01	4.645 E-01	3.403 E-01	4.909 E-01
7	Actuator	2.015 E-01	2.751 E-01	2.015 E-01	2.751 E-01	2.015 E-01	2.907 E-01
8	A_valve_ctrl	7.326 E-01	1	7.326 E-01	1	6.932 E-01	1
9	Hum_error	2.696 E-01	7.260 E-01	2.696 E-01	1.272 E-01	3.112 E-01	1.907 E-01
10	M_valve	1.393 E-01	3.751 E-01	1.393 E-01	8.905 E-01	1.393 E-01	8.359 E-01
11	M_valve_ctrl	3.713 E-01	1	3.713 E-01	1	4.071 E-01	1
12	Feed_ctrl	2.720 E-01	1	1.146 E-01	1	1.155 E-01	1
13	Alarm (no-sound)	not present	not present	2.614 E-01	6.390 E-02	3.031 E-01	1.320 E-01
	Alarm (wrong-sound)	not present	not present	1.34 E-02	0	1.900 E-02	0
14	Expert (Exp 1)	not present	not present	not present	not present	6.000 E-01	5.632 E-01
	Expert (Exp 2)	not present	not present	not present	not present	4.000 E-01	4.368 E-01
15	Function (Union)	not present	not present	not present	not present	7.500 E-01	7.926 E-01
	Function (Intersection)	not present	not present	not present	not present	2.500 E-01	2.074 E-01

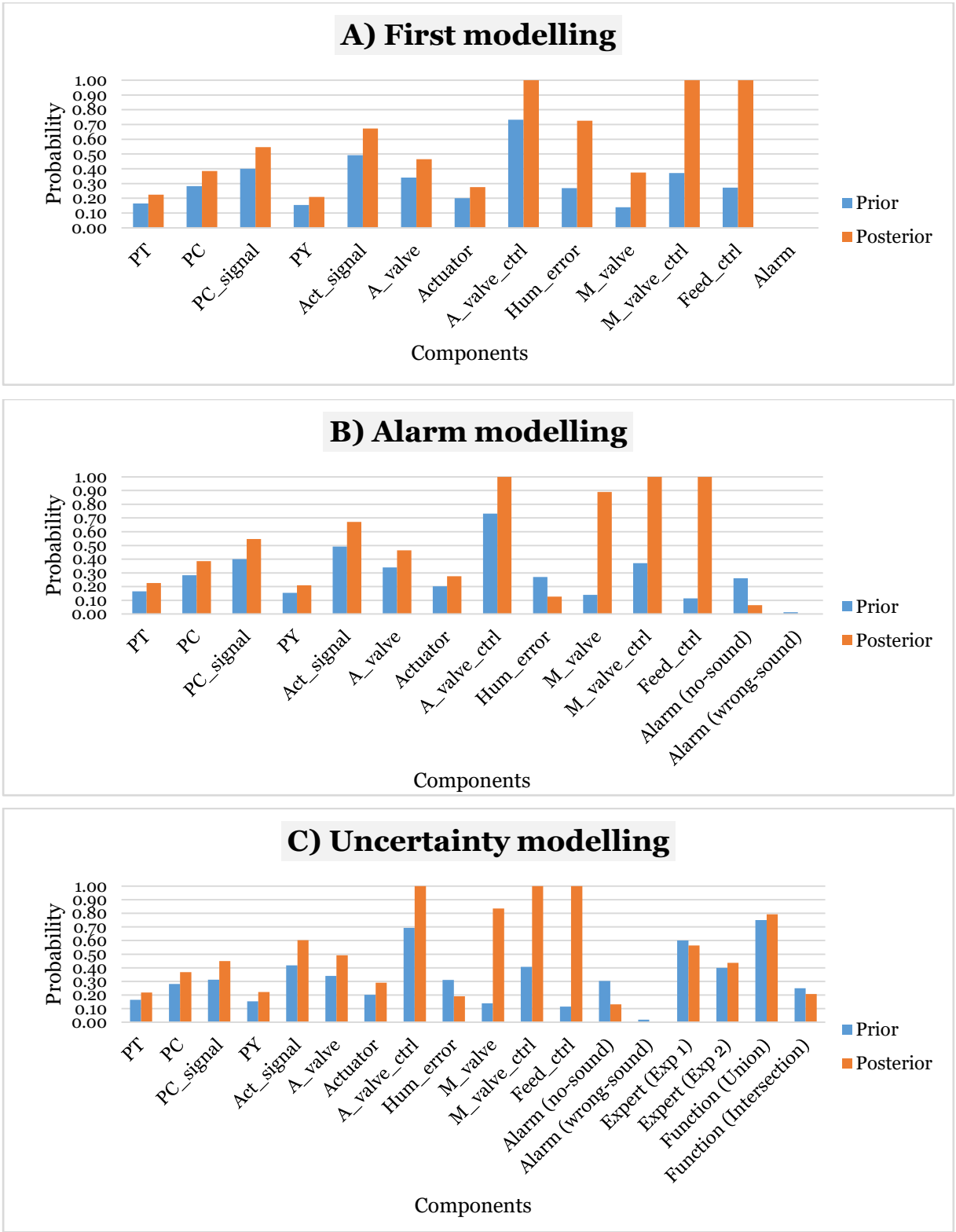


Figure 5. 19 Comparison among prior and posterior probabilities: A) First modelling (i.e. basic system), B) alarm modelling (effect of multi-state variables) and C) uncertainty modelling and expert opinion.

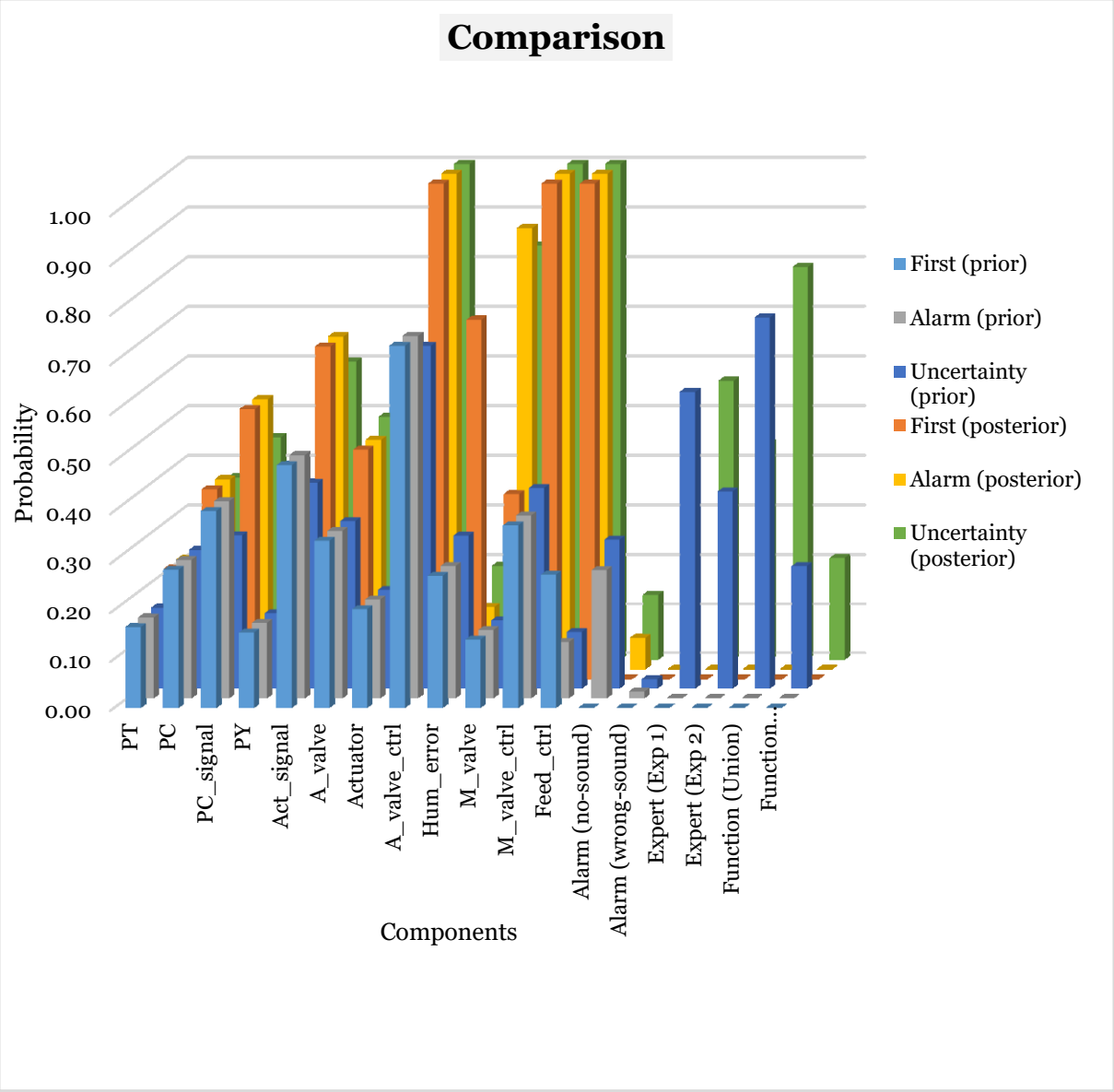


Figure 5. 20 Comparison among components probabilities before and after updating, accounting three different modelling steps.

5.2.2.3 Case study D: conversion of a Bow-Tie into a Bayesian Network for the analysis of a Vapor Cloud Explosion accident scenario

5.2.2.3.1 Definition of the case study

The implementation of a Bayesian Network, starting from a Bow-Tie diagram, has been carried out by reproducing the case study proposed by Khakzad et al. (Khakzad et al., 2013b). The aim of the case study is to put in practice the mapping procedure from a Bow-Tie into a Bayesian Network, explained in Section 3.3.2.1.3.3.2. The case study was implemented in Hugin software, version 8.1 (Hugin, 2016).

The case study deals with an accident scenario really happened at Universal Form Clamp, Inc., Bellwood, Illinois, U.S. on June 14th, 2006. The reference report, issued by the U.S. Chemical

Safety Board (CSB, 2007b), described the accident scenario as a flammable vapor cloud consisting of heptane and mineral spirits overflowed from an open top mixing and heating tank. The vapour cloud ignited as it met unknown ignition sources, leading to one death, two injuries and significant business interruption. The tank was equipped with steam coils supplying it with heat needed for the mixing process. A temperature controller composed of a temperature sensor and a pneumatic control unit was installed to operate the steam valves based on the mixture temperature. In addition to these control system, an operator was supposed to check the temperature using an infrared thermometer and to take any necessary actions. The tank was also equipped with local exhaust ventilation at the top to control vapors.

As reported by CSB (CSB, 2007b) and later by (Khakzad et al., 2013b), a malfunction of the temperature control system allowed the steam valves to remain open long enough to heat the mixture to its boiling point, generating a high volume of vapour. Consequently, the failure of the local ventilation system due to a broken fan belt caused the vapour cloud to spill from the tank and finally ignited when exposed to an ignition source. It was also found that even if the ventilation system had been working, it would not have had enough capacity to collect such a high volume of vapour.

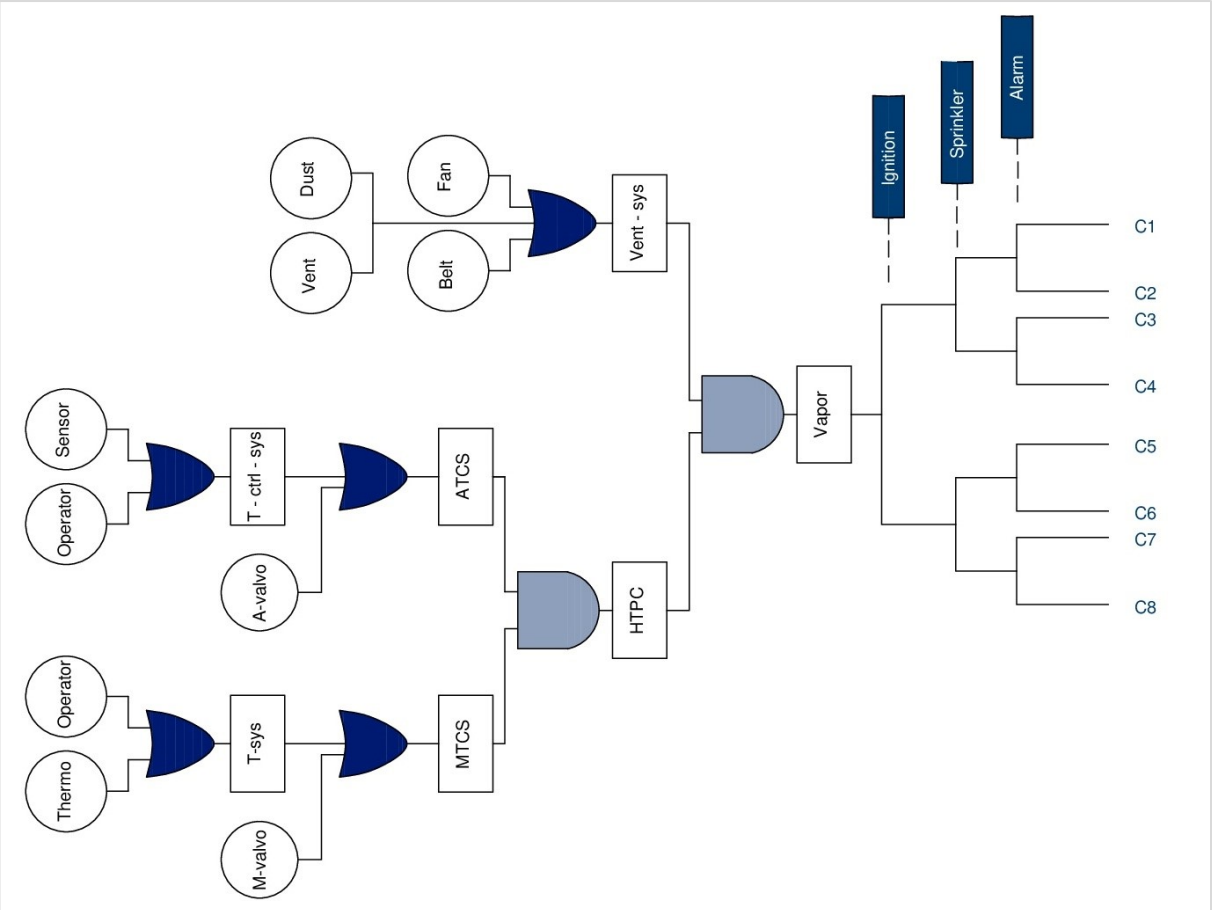


Figure 5. 21 Bow-Tie diagram for the case study (CSB, 2007b; Khakzad et al., 2013b).

Following the accident description, Khakzad et al. (Khakzad et al., 2013b) developed a Bow-Tie diagram to investigate the envisaged accident scenarios and the effectiveness of the various safety measures (Figure 5. 21). The accident components, their symbols and failure probabilities have been reported in Table 5. 19.

Because the vapour cloud is non-toxic, Khakzad et al. (Khakzad et al., 2013b) assumed that any fatalities or injuries are due to vapour ignition, not the vapour itself. It should be noted that the failure probabilities of safety barriers Sprinkler and Alarm are influenced by either safety barrier $Ignition$ or top event $Vapor$, showing the conditional dependency of the former on the latter. $Sprinkler$ and $Alarm$ are activated if vapor is ignited, i.e. when $Vapor = Overflow$ and $Ignition = Spark$, but with failure probabilities equal to $4.00 \cdot 10^{-2}$ and $1.30 \cdot 10^{-3}$, respectively.

Table 5. 19 Components of the system and their probabilities. (Khakzad et al., 2013b).

Number	Events	Symbol	Probability
1	Sensor	**Sensor**	4.00 E-02
2	Pneumatic Unit	**P_unit**	2.015 E-01
3	Temperature control system	**T_ctrl_sys**	*OR-gate*
4	Operator	**Operator**	2.00 E-02
5	Infrared Thermometer	**Thermo**	4.68 E-02
6	Temperature measurement system	**T_sys**	*OR-gate*
7	Manual steam valve	**M_valve**	2.43 E-02
8	Automatic steam valve	**A_valve**	2.76 E-02
9	Automatic temperature control system	**ATCS**	*OR-gate*
10	Manual temperature control system	**MTCS**	*OR-gate*
11	High temperature protection system	**HTPS**	*AND-gate*
12	Inadequate ventilation	**Vent**	1.50 E-02
13	Fan failure	**Fan**	100 E-02
14	Belt failure	**Belt**	5.00 E-02
15	Duct plugging	**Duct**	1.00 E-03
16	Ventilation system	**Vent_sys**	*OR-gate*
17	Vapor overflow	**Vapor**	*AND-gate*
18	Ignition barrier	**Ignition**	1.00 E-01
19	Water sprinkler system (spark)	**Sprinkler**	4.00 E-02
	Water sprinkler system (no spark)		1
20	Alarm system (spark)	**Alarm**	1.30 E-03
	Alarm system (no spark)		2.250 E-01

Alarm can also be activated by a particular amount of vapor concentration in the air even if it is not ignited, i.e. when $Vapor = Overflow$ and $Ignition = No\ spark$, but with a failure probability equal to $2.25 \cdot 10^{-1}$ (Table 5. 19). Table 5. 20 shows eight consequences that can be

envisaged for the accident scenario depending on the success or failure of the sequential safety barriers. It has been assumed that even if there is no fire (i.e.,$Ignition = No\ spark$), the operation of $Sprinkler$ will lead to a safer mode compared to its failure, due to fact that the operation of $Sprinkler$ can possibly reduce the probability of delayed ignitions. Consequences have been reported in order of increasing severity, from C_1 to C_8.

Table 5. 20 Consequence of the vapor overflow accident scenario, reported in order of increasing severity.

Consequences of the vapor overflow accident scenario	
Event	**Symbol**
Safe evacuation	C1
Wet vapour cloud near the ground	C2
Safe evacuation with possibility of delayed ignition	C3
Vapour cloud with possibility of delayed ignition	C4
Fire, moderate property damage, low death toll	C5
Fire, moderate property damage, high death toll	C6
Fire, high property damage, low death toll	C7
Fire, high property damage, high death toll	C8

Assigning the probabilities listed in Table 5. 19 to the primary events and the safety barriers of the BT, the probabilities of top event, and accident consequences are calculated and presented in Table 5. 21.

5.2.2.3.2 Conversion of Bow-Tie into a Bayesian Network

The Bayesian Network correspondent to BT (Figure 5. 21) has been implemented by applying the mapping algorithm reported in Section 3.3.2.1.3.3.2 and the dedicated software Hugin version 8.1 (Hugin, 2016). The BN has been reported in Figure 5. 22.

Attention should be posed to the consequence node that is a multi-state node, accounting all the possible outcomes (state set from C_1 to C_8); indeed, by connecting node $Vapor$ (indicating the top event) to $Consequences$, another state, namely $Safe$ state (i.e., $Vapor = Controlled$) is added to the state set. To show the dependency among the safety barriers and the top event, causal arcs are also drawn from $Ignition$ and $Vapor$ to $Sprinkler$ and $Alarm$, as suggested by the mapping algorithm. All the safety nodes of the BN are connected to node $Consequences$ because the failure/success of each safety barrier results in different consequences (i.e., different states of the $Consequences$ node).

Then, Bayesian analysis has been performed by assigning the probabilities listed in Table 5. 19 as the prior, and the so obtained results have been compared with the results of Bow-Tie analysis, in order to assure the translation algorithm has been applied correctly. The

comparison among probabilities obtained applying BT approach and the ones obtained by BN analysis have been reported in Table 5. 21.

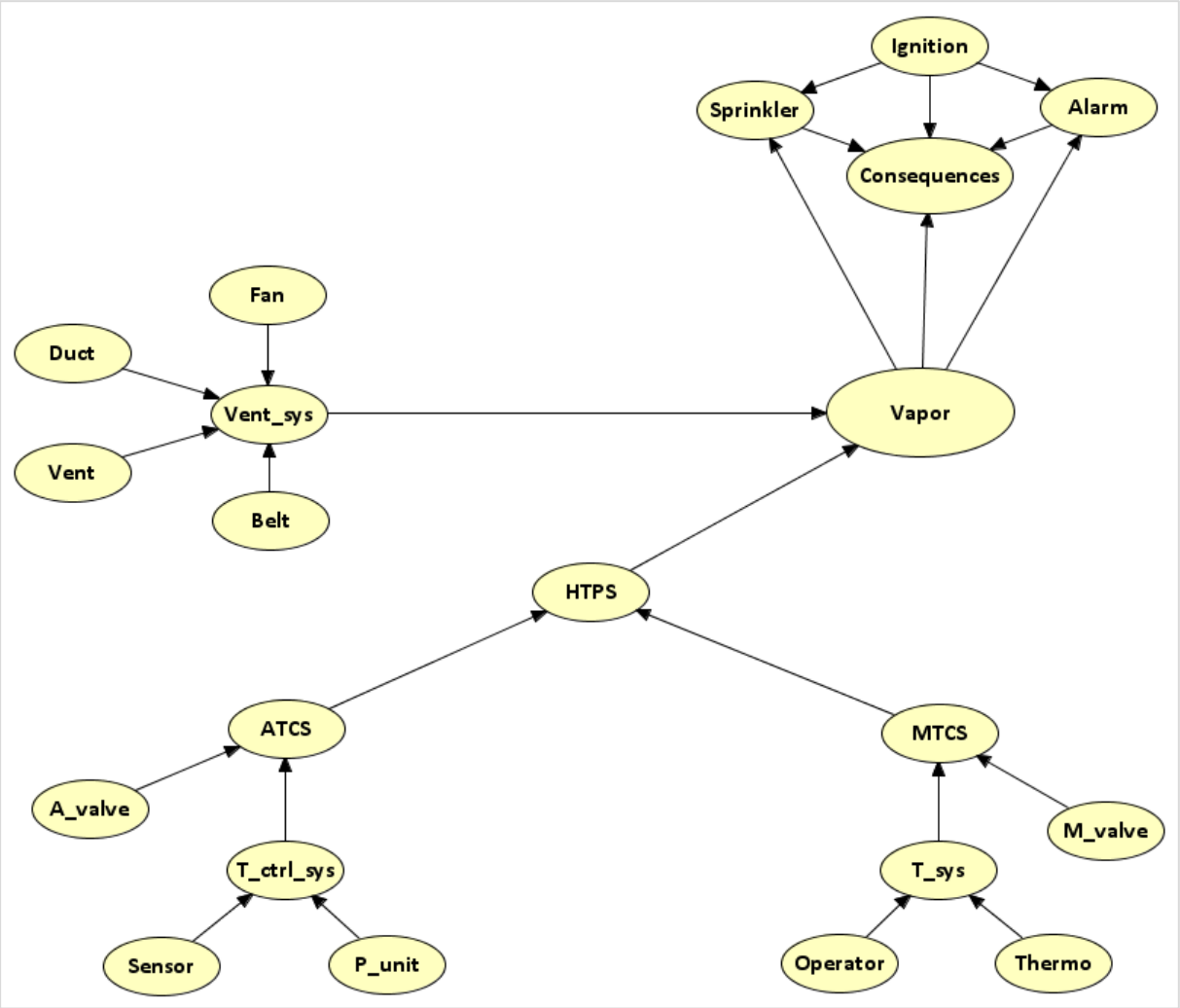


Figure 5. 22 Bayesian Net correspondent to the BT reported in Figure 5. 21.

Table 5. 21 Comparison among the results of BT analysis and BN analysis (without any additional information). The same results denote a successful mapping process.

Top Event & Consequences	BT analysis	BN analysis
C8	8.739E-09	8.739E-09
C7	6.714E-06	6.714E-06
C6	2.097E-07	2.097E-07
C5	1.611E-04	1.611E-04
C4	3.403E-04	3.403E-04
C3	1.172E-03	1.172E-03
C2	0	0
C1	0	0
Vapour (Top Event)	9.983E-01	9.983E-01

Once it is confirmed that the BT and BN are equally able to analyse the accident scenario, the BN superiority can be evidenced by the ability to update the probabilities, taking into account new evidences. In the current case, probability updating has been performed by inserting C_5 consequence (accident occurrence) and propagating it through the network. This evidence (i.e., $(x_i|Consequences) = C_5$, with x_i generic event) denotes that it is known a fire with moderate property damage and low number of fatality is observed in the process plant. Posterior probabilities obtained by Bayesian Updating have been reported in Figure 5. 23.

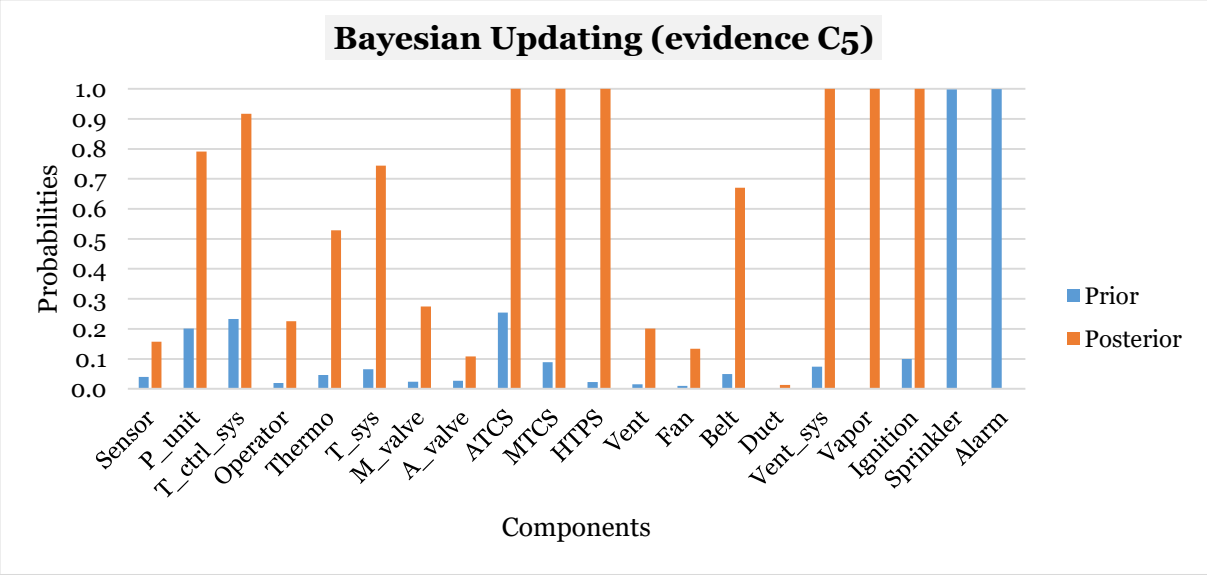


Figure 5. 23 Bayesian Updating results, after having inserted C_5 as an evidence.

The most probable state given the accident (C_5) occurrence, also known as MPE – Most probable Explanation, is the one corresponding to the failure of $Thermo$, P_unit, $Belt$ and consequently of $Vent\_sys$, T_ctrl_sys, T_sys, $ATCS$, $HTPS$, $MTCS$ and eventually $Vapor$ overflow. It results in C_5 (evidence), provided that $Ignition = Spark$, $Sprinkler = Work$ and $Alarm = Work$. The probability of the system being in the most probable configuration has been computed, according to equation (3.20):

$$P(most\ likely\ configuration) = \frac{P(most\ likely\ configuration, evidence)}{P(evidence)} = \frac{0.000161}{3.93 \cdot 10^{-5}}$$

$$= 2.441 \cdot 10^{-1}$$

The importance of this feature, often named as “Probability Updating” for safety analysis is due to its ability in identifying critical events (i.e., the failures here-in reported) and allocating preventive safety barriers not only to the primary events directly leading to the top event but also to weak links that are combination of non-critical events.

5.2.2.3.3 Bayesian Network analysis & Probability adapting (Accident Sequence Precursors)

Bayesian probability revision can be performed through "Probability updating" that is the calculation of Most Probable Explanation, as shown in the previous paragraph, or through "Probability adapting" that calculates the posterior probability of a generic event x_i given another event Q has occurred n times; that can be expressed in statistical terms as $P(x_i|Q = n)$. This means applying prior experience (in the form of cumulative information collected during a certain time span – ASP, i.e. Accident Sequence Precursors) to adapt conditional probability distributions. Probability adapting technique has been applied by several studies (Kalantarnia et al., 2010, 2009; Meel et al., 2007; Meel and Seider, 2006; Rathnayaka et al., 2011) to develop likelihood functions for probability updating using Bayes theorem, coupled with standard tools for safety assessment (i.e. Bow-Tie diagram).

In the current case study, adapted from Khakzad et al. (Khakzad et al., 2013b), an hypothetical prior experience referred to four years of operation has been applied (Table 5. 22).

Table 5. 22 Experience used in Probability adapting, in the form of ASP, referred to four years of operation.

ASP (accident sequence precursors) – Non cumulative form				
Consequence	**Year 1**	**Year 2**	**Year 3**	**Year 4**
C3	3	1	2	1
C5	0	1	0	0
C6	0	0	0	1

For example, at the end of the third year, C_3 has cumulatively occurred 6 times, C_5 has occurred only once; probability adapting can be performed by inserting $P(x_i|Consequences = 4C_3)$ and $P(x_i|Consequences = C_5)$, with x_i generic event. Bayesian adapting has been performed by applying "adaptation panel" from software Hugin version 8.1, as visible in Figure 5. 24.

The results of Bayesian Probability Adapting for four sequential years have been reported in Table 5. 23 (for safety barriers - both preventive and protective ones - and Top Event) and Table 5. 24 (for consequences). The results referred to as "Year 0" are the prior probabilities that have been already presented in the previous section.

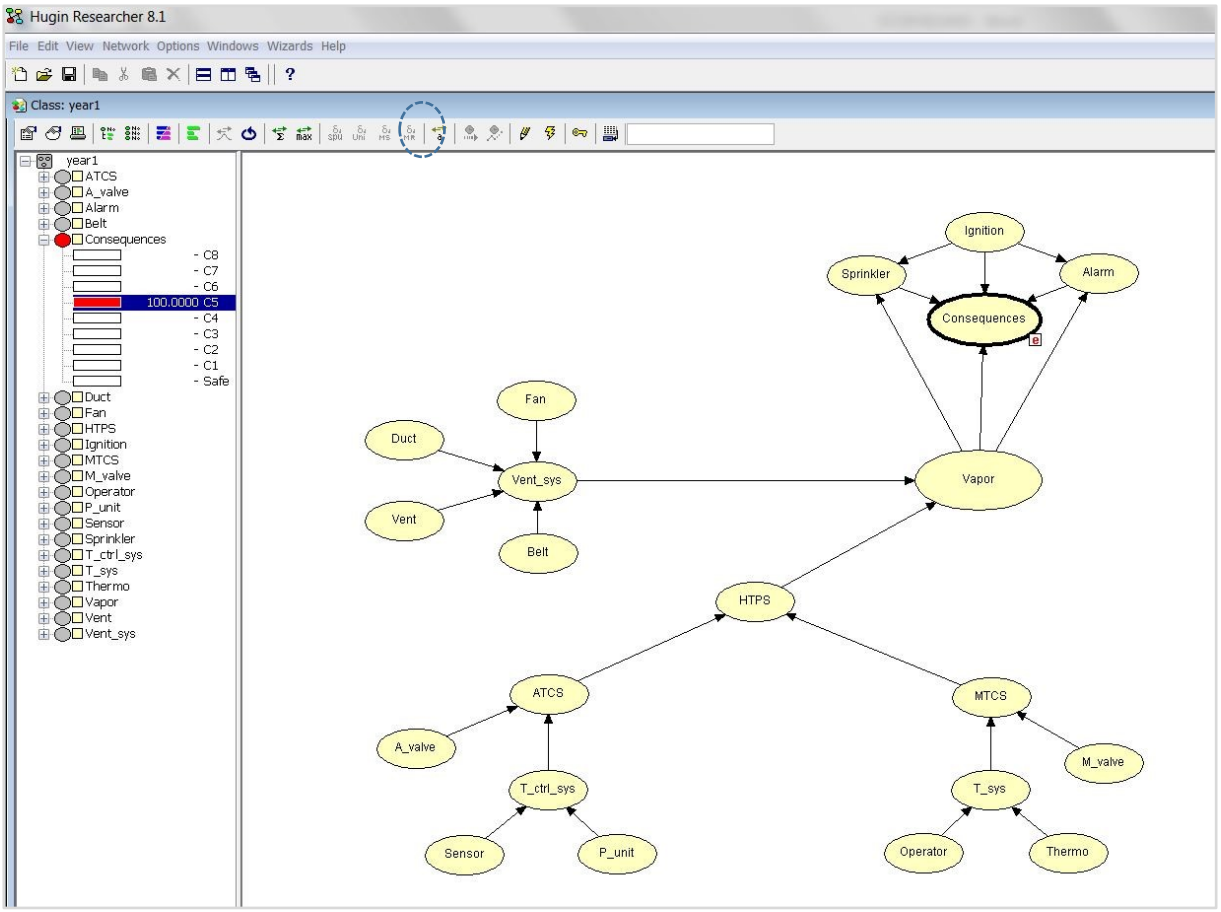


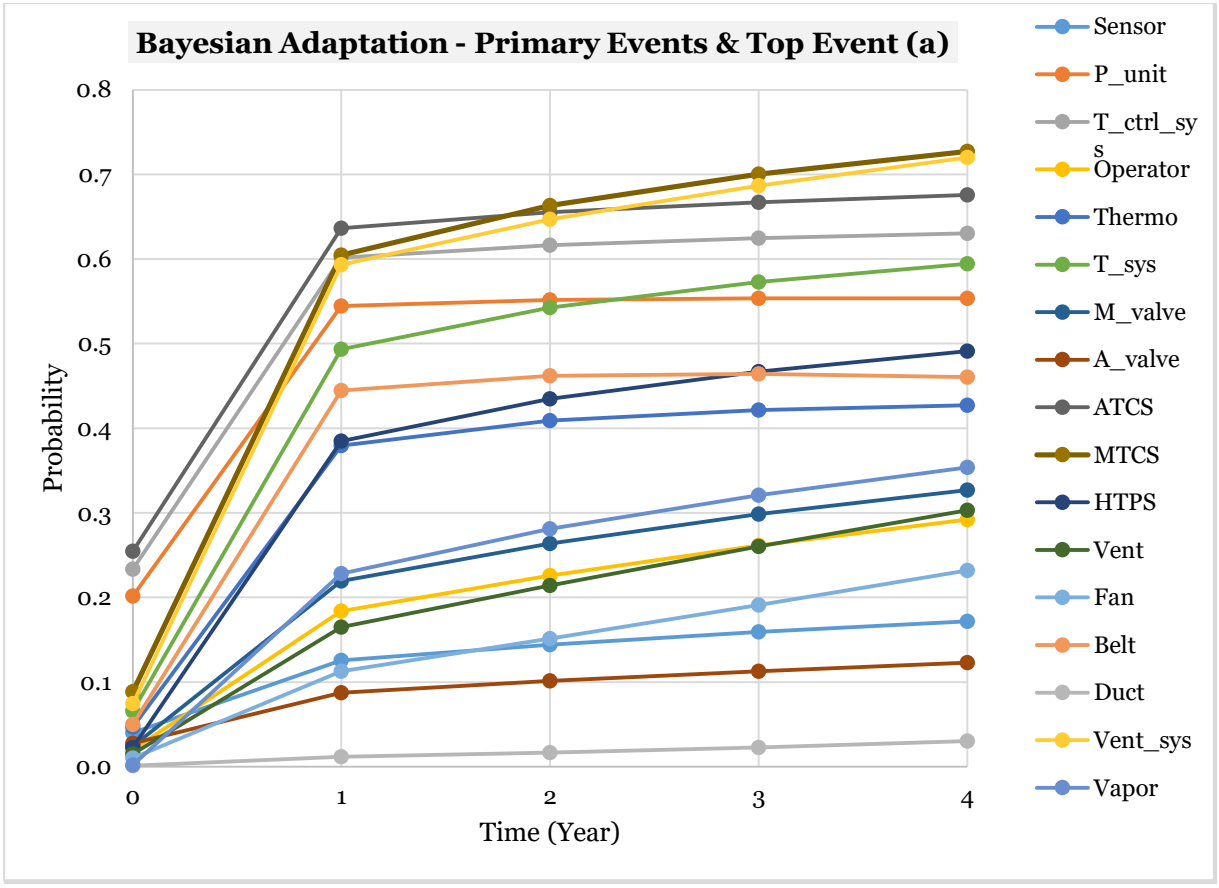
Figure 5. 24 Screenshot of BN Probability Adapting, performed through adaptation function.

The results highlights that the failure probabilities of the primary events and top event are increasing during the time interval (Figure 5. 25). This is due to fact that the top event (i.e. vapour overflow) has always occurred a number of times greater than or equal to the maximum failure numbers of each safety barrier and all the consequences applied as ASP denotes an occurrence of vapour overflow. Indeed, the occurrence probability of Top Event increases rapidly over the time span of the analysis. Moreover, the information about the occurrence probability of the top event propagates backwards through the network, increasing the probability of the primary events, with a similar trend.

The results highlights that failure probabilities for safety barriers can remain constant or decrease during the time interval (Figure 5. 26), with a trend opposite to the one of Primary Events. The explanation can be found in ASP (Table 5. 22): there are observations suggesting that each safety barrier has been equally observed working or failing during the fourth year. As emerged from Figure 5. 26, *Ignition* has the lowest failure probability among the safety barriers shown, and its failure probability illustrates an approximately constant trend, showing it has gained the lowest attention compared to the other two safety barriers, on which corrective actions should be focused on.

Table 5. 23 Results of Bayesian adapting over four years of operations for Safety Barriers and Top Event.

Safety Barriers and Top event - Bayesian Probability adapting over four years					
Year / **Probability**	***0***	***1***	***2***	***3***	***4***
Sensor	4.000E-02	1.255E-01	1.442E-01	1.592E-01	1.719E-01
P_unit	2.015E-01	5.445E-01	5.518E-01	5.534E-01	5.534E-01
T_ctrl_sys	2.334E-01	6.017E-01	6.164E-01	6.245E-01	6.302E-01
Operator	2.000E-02	1.837E-01	2.258E-01	2.613E-01	2.922E-01
Thermo	4.680E-02	3.795E-01	4.090E-01	4.216E-01	4.272E-01
T_sys	6.586E-02	4.935E-01	5.425E-01	5.728E-01	5.946E-01
M_valve	2.430E-02	2.192E-01	2.637E-01	2.985E-01	3.268E-01
A_valve	2.760E-02	8.730E-02	1.012E-01	1.128E-01	1.230E-01
ATCS	2.546E-01	6.365E-01	6.552E-01	6.669E-01	6.757E-01
MTCS	8.856E-02	6.046E-01	6.632E-01	7.003E-01	7.271E-01
HTPS	2.255E-02	3.848E-01	4.345E-01	4.670E-01	4.913E-01
Vent	1.500E-02	1.651E-01	2.140E-01	2.604E-01	3.030E-01
Fan	1.000E-02	1.127E-01	1.511E-01	1.912E-01	2.320E-01
Belt	5.000E-02	4.445E-01	4.618E-01	4.641E-01	4.605E-01
Duct	1.000E-03	1.174E-02	1.668E-02	2.271E-02	3.005E-02
Vent_sys	7.453E-02	5.933E-01	6.469E-01	6.867E-01	7.199E-01
Vapor	1.681E-03	2.283E-01	2.811E-01	3.207E-01	3.537E-01
Ignition	1.000E-01	5.000E-02	1.500E-01	1.214E-01	1.611E-01
Sprinkler	9.984E-01	9.890E-01	9.592E-01	9.624E-01	9.449E-01
Alarm	9.987E-01	7.961E-01	7.488E-01	7.135E-01	6.891E-01



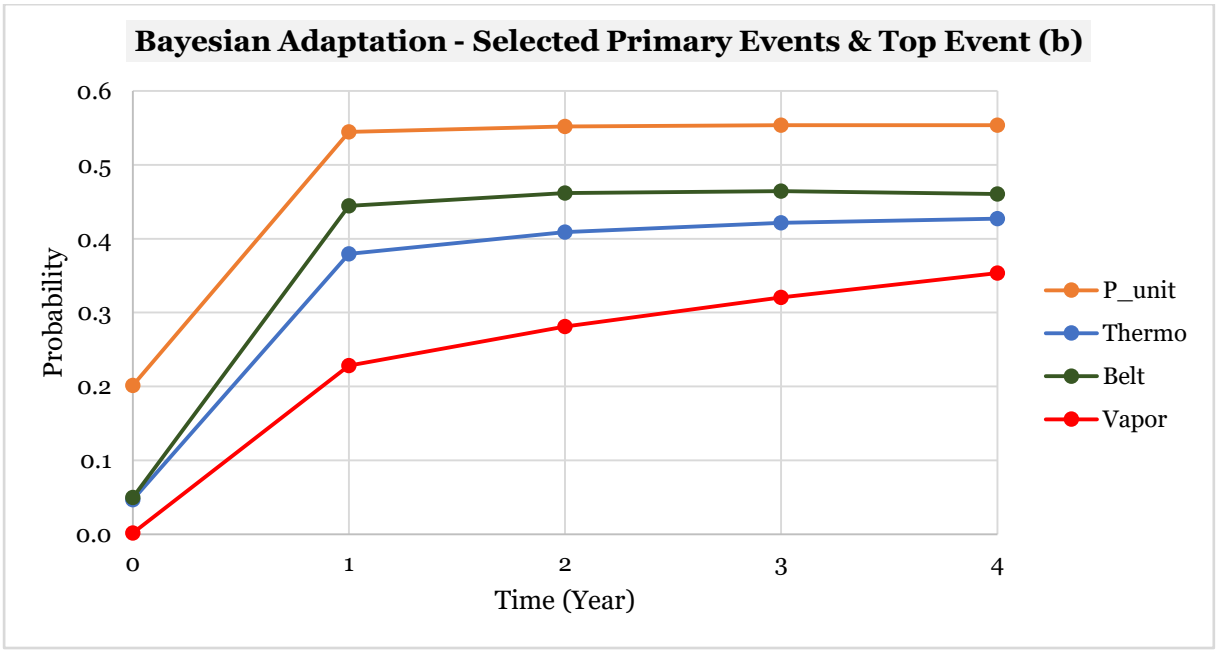


Figure 5. 25 Results of Bayesian adapting over four years of experience, referred to Primary Events and Top Event. From the top to the bottom: (a) Primary events and Top Event (b) Selected primary events and Top Events (i.e., only the ones determining MPE).

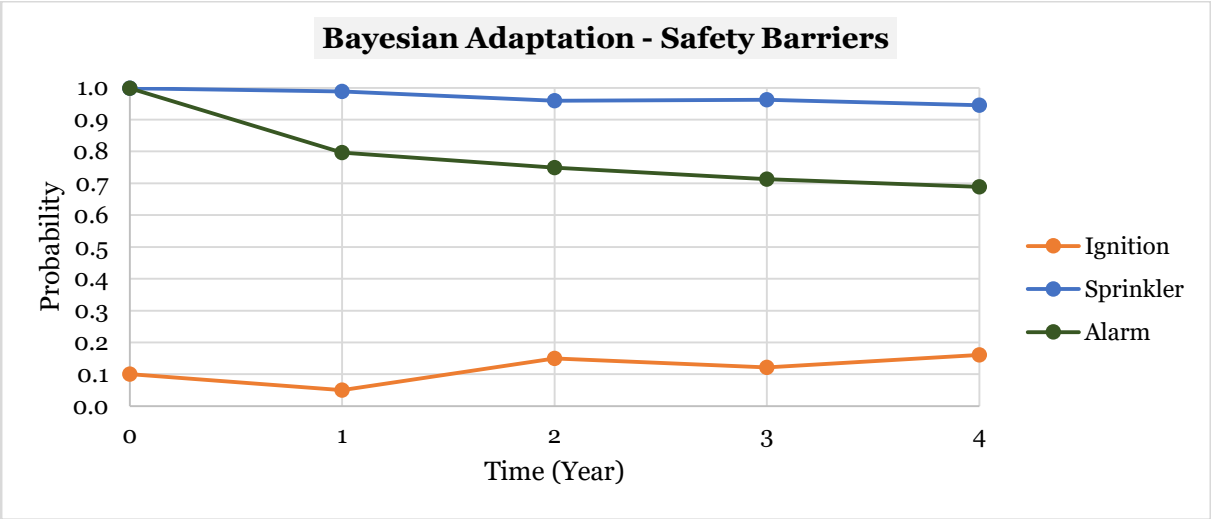


Figure 5. 26 Results of Bayesian adapting over four years of experience, referred to Safety Barriers.

Table 5. 24 Results of Bayesian adapting over four years of operations, referred to Consequences.

Consequences - Bayesian Probability adapting over four years					
Year / ***Probability***	***0***	***1***	***2***	***3***	***4***
C8	8.739E-09	5.935E-07	1.523E-06	1.550E-06	1.715E-04
C7	6.714E-06	4.560E-04	1.404E-03	1.361E-03	1.693E-03
C6	2.097E-07	1.425E-05	4.416E-05	4.275E-05	5.069E-03
C5	1.611E-04	1.094E-02	4.072E-02	3.754E-02	5.004E-02
C4	3.403E-04	2.440E-02	2.987E-02	3.414E-02	3.755E-02
C3	1.172E-03	1.925E-01	2.091E-01	2.476E-01	2.591E-01
C2	0.000E+00	0.000E+00	0.000E+00	0.000E+00	0.000E+00
C1	0.000E+00	0.000E+00	0.000E+00	0.000E+00	0.000E+00
Safe	9.983E-01	7.717E-01	7.189E-01	6.793E-01	6.463E-01

Using the revised probabilities for Top Event and safety barriers, it is possible to dynamically update the probability of all consequences that tends to increase over time, as highlighted by Figure 5. 27. This reasoning can be applied also to those consequences for which no information is available, that often are the most severe ones. For example, Figure 5. 28 represents the updated probability of consequence C_8 (the most damaging one) even though it has not been observed until the end of observation time (Table 5. 22). Its probability has increased by four orders of magnitude during the observation time, so without an appropriate improvement of safety barriers the occurrence of a major accident can be expected in the near future.

In this framework Bayesian probability adapting can be applied as a predictive tool in purpose to assess the effectiveness and adequacy of safety measures. Moreover, though the adaptation process the generality arisen from the application of reliability data can be reduced by observed accident precursors.

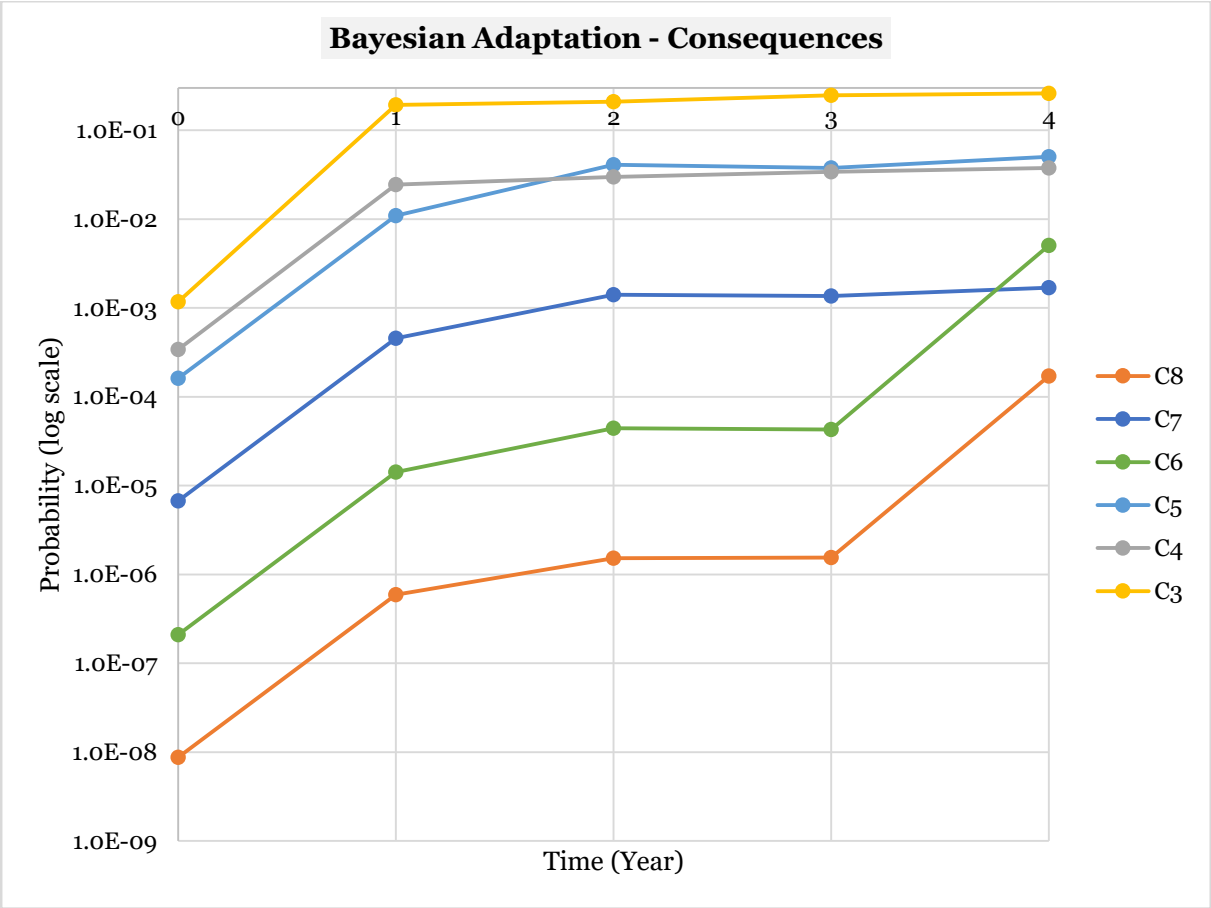


Figure 5. 27 Results of Bayesian adapting over four years of operations, referred to Consequences and reported in logarithmic scale. Graph representing probability vs time for all possible outcomes: C_1 and C_2 have been neglected because their probabilities were equal to zero.

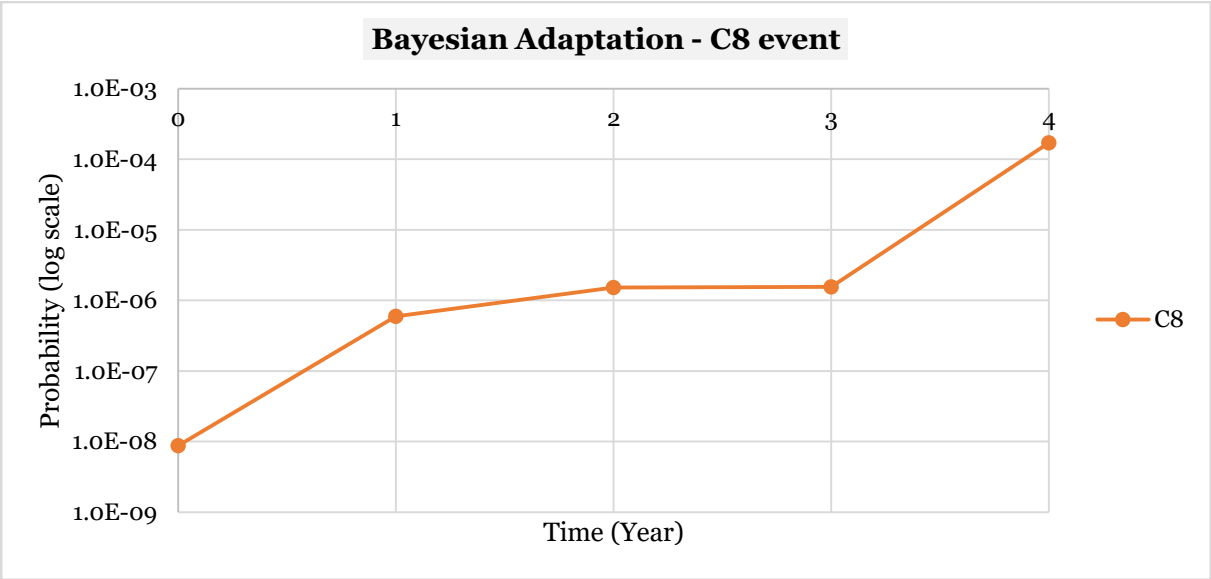


Figure 5. 28 Results of Bayesian adapting over four years of operations, referred to the worst-case consequence C_8 ; graph reported in logarithmic scale.

5.2.2.3.4 Discussion and conclusions on the case study

The present benchmark application has been aimed at implementing a Bayesian Network, starting from a Bow-Tie and subsequently at exploring the features of BN technique in evaluating the performance of Safety Barriers. The system here-in considered has been adapted from a previous contribution by Khakzad et al. (Khakzad et al., 2013b) in order to have a direct comparison of the results for each modelling step of the mapping process, whose results highlighted the superior flexibility of BN over Bow-Tie.

This application should be considered a significant step in the development of a full-Bayesian approach in safety barriers performance assessment, and it has been relevant in illustrating the flexible use of BNs in probability estimation for primary events, top event, safety barriers and consequences.

Two different approaches to Bayesian Analysis have been applied, in order to dynamically update probabilities, by means of Bayesian Networks: probability updating and probability adapting. In probability updating, the information about a node instantiated to one of its states (i.e., a certain event that had happened) is used as evidence; its main application is the determination of the most probable explanation (MPE) leading to that particular state, in order to apply consequent actions. On the other hand, in probability adapting the information about the cumulative occurrence number of an accident during a time interval is used as evidence, in order to dynamically revise probabilities over a certain time span. This feature helps in gradually replace generic priors (i.e., generic reliability data) with more case-specific posteriors, resulting in a dynamic assessment of systems safety and a reliable prediction of occurrence likelihood for each consequence.

5.2.2.4 Case study E: application of Bayesian Networks tutorials to account for the role of safety measures performance on bugdet and risk

5.2.2.4.1 Definition of tutorials

The current section is aimed at including safety barriers performance and economic evaluations within Bayesian Networks, by reproducing some tutorials by Reniers and Van Erp (Reniers and Van Erp, 2016) that illustrate the role of Bayesian Networks (BNs) and Limited Memory Influence Diagrams (LIMIDs) in relation to safety decision-making in the context of major accidents prevention. The case studies have been carried out by Hugin software version 8.1 (Hugin, 2016).

The first example is an extended BN to account the effect of safety barriers on budget and risk, with a further modification to consider uncertainties in budget availability. The second example is a similar problem, approached with LIMID, which allows considering decision alternatives and utilities in a more structured way.

5.2.2.4.2 Extended BN to account for the effect of safety barriers on the bugdet and risk considering uncertainties in budget availability

The tutorial considers an initiating event (i.e., IE), which could result in four consequences (i.e., C1, C2, C3, C4) based on the work/failure state of two safety barriers (i.e., SB1 and SB2).

Therefore, the consequence node is composed by 5 states including Safe State - depending on the state of SB1, SB2 and IE. Input data for IE, safety barriers nodes, consequence and budget nodes are reported in Table 5. 25 and Table 5. 26. A screenshot of the CPT for the risk node is reported in Figure 5. 29, considering a consequence monetary value increasing of one order of magnitude with the increasing severity of the accidental consequence, starting with a monetary value for C1 of 1000 €. The BN is reported in Figure 5. 30.

Table 5. 25 Input for BN regarding initiating event node, safety barriers node and budget node.

IE	**Initiating event**
P(IE=Yes)	0.01
P(IE=No)	0.99
Install SB_1/Install SB_2	
2 states - Yes/No	4 different nets for 4 combinations
Safety barriers (binary: work/fail state)	
SB_1	Safety barrier 1
P(SB_1 = work)	0.8
P(SB_1 = fail)	0.2
SB_2	Safety barrier 2
P(SB_2 = work)	0.9
P(SB_2 = fail)	0.1
Budget	
Cost of Safety Barriers	
Cost SB_1 (€)	1000
Cost SB_2 (€)	4000

Table 5. 26 Input for BN regarding the consequence node.

CPT for consequence node			
IE	**SB 1**	**SB 2**	**Consequence**
Yes	Work	Work	C1
Yes	Work	Fail	C2
Yes	Fail	Work	C3
Yes	Fail	Fail	C4
No	Work	Work	Safe
No	Work	Fail	Safe
No	Fail	Work	Safe
No	Fail	Fail	Safe

Risk

Consequence	C1	C2	C3	C4	Safe
EUR1000	1	0	0	0	0
EUR10000	0	1	0	0	0
EUR100000	0	0	1	0	0
EUR1000000	0	0	0	1	0
EUR0	0	0	0	0	1

Figure 5. 29 A screenshot of theCPT for the node Risk.

Then, the BN is compiled; the results are reported in Table 5. 30, according to the four possible barriers configurations (i.e., both working, none working, only SB1 working, only SB2 working).

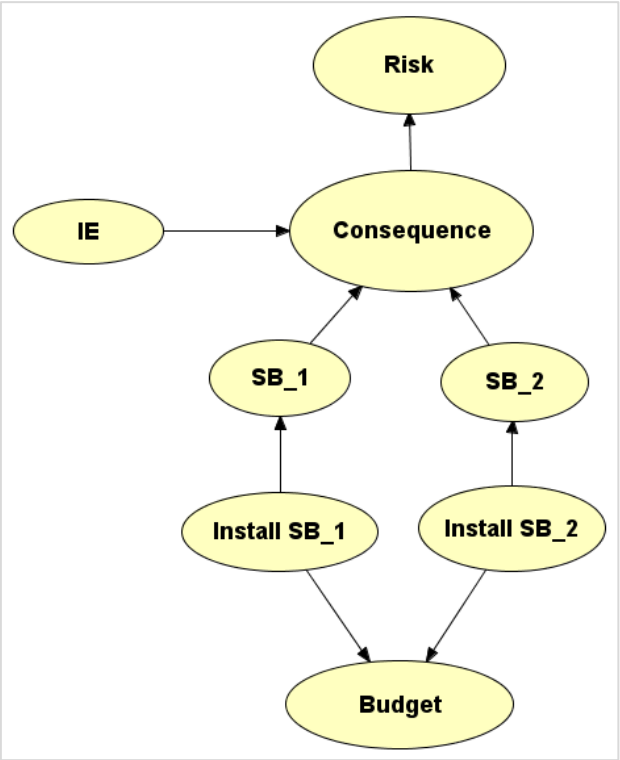


Figure 5. 30 BN to account the role of safety barriers on the budget and risk.

Table 5. 27 Results of Bayesian Network for the four possible configurations, according to safety barriers state.

Risk (cost category- €)	**Both SB working**	**None of SB working**	**SB 1**	**SB 2**
	Risk (probability)	**Risk (probability)**	**Risk (probability)**	**Risk (probability)**
1000	7.20 E-03	0	0	0
10000	8.00 E-04	0	8.00 E-03	0
100000	1.80 E-03	0	0	9.00 E-03
1000000	2.00 E-04	1.00 E-02	2.00 E-03	1.00 E-03
0	9.90 E-01	9.90 E-01	0.99	9.99 E-01
Risk (€)	**395.2**	**10000**	**2080**	**1900**
Cost (€)	**5000**	**0**	**1000**	**4000**

Then, a modification to the previous net to incorporate uncertainty in the amount of available budget for purchasing safety barriers. The following CPTs have not been modified: Initiating event, *Safety Barriers, Consequence, Risk*. On the other hand, the CPT for the node *Budget*

has been modified, introducing the same costs for SB1 and SB2, but adding a probability distribution for the budget, according to the values reported in Table 5. 28.

Table 5. 28 Input for the node Budget in the modified version to account uncertainty on safety barriers budget.

Budget (€)	Budget (probability distribution 1)	Budget (probability distribution 2)
5000	0.3	0.1
4000	0.5	0.3
1000	0.2	0.4
0	0	0.2

The following assumptions have been taken:

- In case of budget deficiency, priority will be given to SB 1;
- In comparison with previous example, the arc that connects *Budget* and *Install SB_1* nodes (as well as the one between *Budget* and *Install SB_2*) has been reverted. *Budget* node here becomes the parent node, whose information influence child nodes *Install SB_1* and *Install SB_2*;
- Due to budget constraints and SB1 priority over SB2, an additional arc has been added from the node *Install SB_1* to *Install SB_2*.

The BN obtained according to these assumptions is available in Figure 5. 31; the results are available in Table 5. 29.

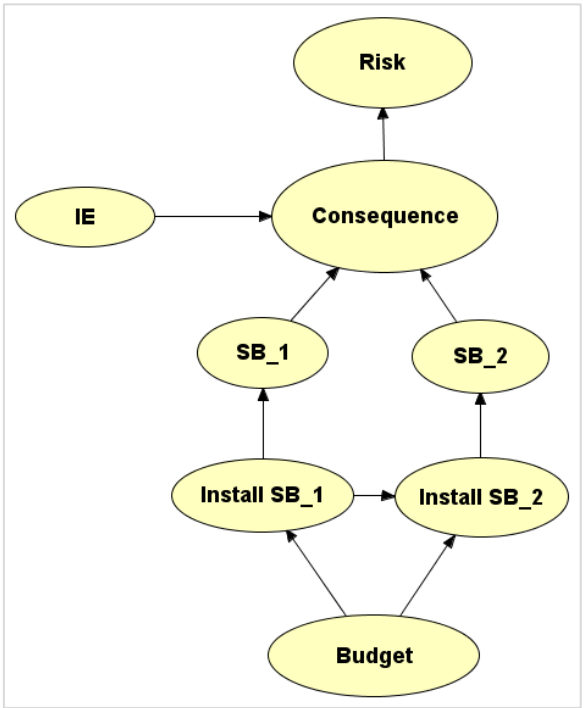


Figure 5. 31 Bayesian Network to account the role of uncertainty on budget.

Table 5. 29 Results of BN to account the effect of uncertainty on budget. Cost indicates the expected value of the budget, according to the probability distribution inserted.

Risk (cost category- €)	**Probability distribution 1**	**Probability distribution 2**
	Risk (probability)	**Risk (probability)**
1000	2.16 E-03	7.20 E-04
10000	4.64 E-03	4.96 E-03
100000	1.89 E-03	9.90 E-04
1000000	1.31 E-03	3.33 E-04
0	9.90 E-03	9.90 E-01
Risk (€)	**1547.56**	**3479.32**
Cost (€) (*)	**3700**	**2100**

5.2.2.4.3 Application of Limited Memory Influence Diagrams to support safety related decision-making

The present tutorial, adapted from Reniers and Van Erp (Reniers and Van Erp, 2016) is aimed at applying Limited Memory Influence Diagrams to support safety related decision-making. Limited Memories influences diagrams are extension of Bayesian Networks with decision nodes (i.e., rectangles) and utility nodes (i.e., diamonds). Nodes for random variables in this case are recalled "chance nodes"; further information is available in Section 3.3.2.1.3.2. The general structure of the net is available in Figure 5. 32.

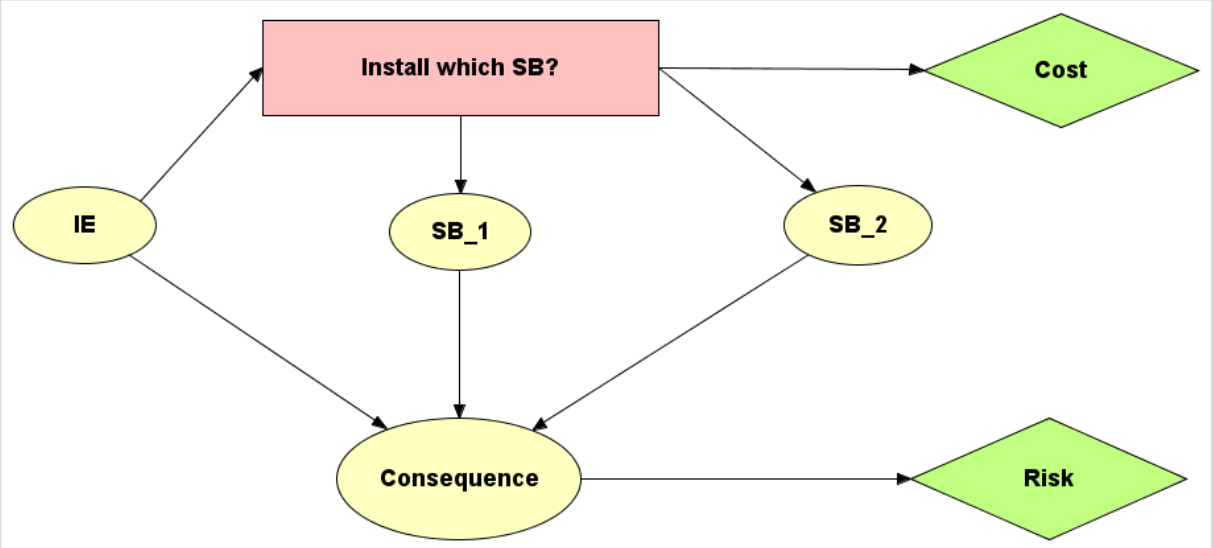


Figure 5. 32 LIMID for the case study.

Input data for LIMID are reported in Table 5. 30; the nomenclature is the same one of the previous tutorial. Safety barriers (i.e., SB1 and SB2 nodes) are assumed to be binary (i.e.,

work/fail states). The consequence node accounts 5 states including Safe state, depending on the state of SB1, SB2 and IE (i.e., initiating event). Risk and cost are utility nodes, expressed in €.

Table 5. 30 Inputs for the case study.

IE	**Initiating event**		
P(IE=Yes)	0.01		
P(IE=No)	0.99		
Install which SB?	(Decision node)		
Safety barriers (binary: work/fail state)			
SB_1	Safety barrier 1		
P(SB_1 = work)	0.8		
P(SB_1 = fail)	0.2		
SB_2	Safety barrier 2		
P(SB_2 = work)	0.9		
P(SB_2 = fail)	0.1		
Inputs for Consequence node			
IE	**SB 1**	**SB 2**	**Consequence**
Yes	Work	Work	C1
Yes	Work	Fail	C2
Yes	Fail	Work	C3
Yes	Fail	Fail	C4
No	Work	Work	Safe
No	Work	Fail	Safe
No	Fail	Work	Safe
No	Fail	Fail	Safe
Cost			
Cost of Safety Barriers			
Cost SB_1 (€) - Utility	1000		
Cost SB_2 (€) - Utility	4000		
Risk			
C1 (€) – Utility	-1000		
C2 (€) – Utility	-10000		
C3 (€) – Utility	-100000		
C4 (€) – Utility	-1000000		
Safe (€) - Utility	0		

It shoulde be noted that direct values of Cost and Risk have been applied as utility values in the utility tables of Cost and Risk (Table 5. 30).

In case of constraints, as maximum (cost) available budget for safety barriers and maximum tolerable risk of consequences, an appropriate utility function can be selected and applied to convert direct values into utility values; according to equation (3. 21). Often the approach based on utility function is preferred because it allows a better incorporation the satisfaction of the

decision making for each decision alternative. Therefore, the application of utility function is carried out, according to the values reported in Table 5. 31, in purpose to apply also this feature of LIMID.

Table 5. 31 Utility values for the case study.

Utility values corrisponding to the values of Cost		**Utility values corrisponding to the values of Risk**
Cost (€)	**Risk (€)**	**Utility**
5000	1000	2.00
4000	10000	1.95
1000	100000	1.50
0	1000000	-3.00
	0	2.00
Maximum available budget		
Max Cost (€)	4500	
Maximum tolerable Risk		
Max Risk (€)	200000	

Then, the net has been compiled, with sum propagation – normal tool. In order to evaluate the expected utility values for 8 decision alternatives, which are all the alternatives possible in this case, the node *IE* and the node *"Install which Safety Barrier?"* have be instantiated to a certain state, to obtain all possible 8 combinations. The summary of the results has been reported in Table 5. 32.

Table 5. 32 Results of the case study, reporting expected utility values for each decision alternative.

IE / *Install which SB?*	Yes	No
Both	2.69	2.89
SB1	2.74	3.78
SB2	2.16	3.11
None	-1.00	4.00

The following comments are outlined from the results of the LIMID case study:

- In case of occurrence of IE, the decision alternative SB1 has the highest expected utility. The optimal decision may be to install SB1 and not SB2.
- In case of non-occurrence of IE, the decision alternative None has the highest expected utility. The optimal decision may be to install none of the safety barriers.
- The results of the case study depend on the definition of cost and risk constraints, as well as on the difinition of the utility function. Therefore, an appropriate choice of utility function, available budget and tolerable risk is required.

Several advantages of applying Bayesian Networks/LIMID within operational safety emerge:

- BNs/LIMID are useful tools for describing past situations, even better for predicting the future, as they are able to revise probability distribution (both for cause and effect nodes), after entering new a observation or evidence. If no evidence is inserted, the prior distribution is the obtained result.
- BNs/LIMID allow the integration of different types of evidencies: both objective data and subjective opionions can be inserted.
- They give the possibility to carry out a sensitivity analysis to quantify uncertainties.
- They provide an effective visualization and communication of the results.

5.2.3 Discussion on the lessons learnt from existing applications

Existing applications make clear the adavantages of Bayesian techniques in safety barriers performance assessment within major accident prevention in the chemical and process industry.

The application of a relevant dynamic technique, DRA by Bayesian analysis, to risk assessment, with particular reference to two significant existing case studies, inherent to process systems, was carried out. The first application (i.e., case study A) was a study-case regarding a process tank equipped with safety systems, while the second one, more complex, represented real-happened major accident. The mentioned applications proved the effectiveness of Bayesian analysis method, both in everyday plant operation and in the prevention of major accidents. However, the second application (i.e., case study B), which is indeed more complex, made clear the necessity to perform Bayesian analysis by means of Bayesian Networks, using a specific software.

Tutorials and applications of Bayesian Networks, carried out by a specific software (i.e., Hugin version 8. 1) proved that BNs are able to give a flexible an updated risk picture. Two case studies investigated how to map conventional risk assessment techniques into Bayesian Networks (i.e., case study C and D). An additional application highlights the possible usefulness of BNs within safety decision-making, to support prevention investments.

However, original applications should deal, in a BN environment, with the inclusion of safety barriers performance within cascading events prevention, with particular mention to domino accident analysis, as no applications currently exist.

5.3 ORIGINAL APPLICATIONS OF BAYESIAN NETWORKS TO DYNAMIC SAFETY MEASURES PERFORMANCE ASSESSMENT IN THE PREVENTION OF MAJOR ACCIDENTS AND CASCADING EVENTS

5.3.1 Introduction

This Section illustrates several original case studies, aimed at applying Bayesian Networks to quantitative assessment of safety measures performance in the context of major accidents and cascading events prevention, within the chemical and process industry domain.

In Section 5.3.2, a preliminary application has been focused on the implementation of Bayesian Networks to safety measures performance assessment, starting from an Event-Tree based approach. The illustrative case study considers a major accident (i.e., fire triggered by an external hazard factor), whose occurrence can be prevented by the action of pertinent technical active safety measures.

In Section 5.3.3, the Bayesian Network application is extended to a realistic case study regarding the prevention of fire escalation, including active, passive and procedural safety measures performance. In both the applications, the Bayesian approach is compared with a conventional Event-Tree based one. The conversion of the Event-Tree, key element of the conventional approach to safety barriers performance assessment, into a Bayesian Network has been performed, with the aim to test the ability of Bayesian Networks in representing possible events sequences, according to the mapping procedure described in Section 3.3.2.1.3.3. In the Bayesian approach, safety measures performance has been assessed by means of specific gates, depending on barriers states and classification, described in Section 3.3.2.1.2. An adequate number of final states has been considered. Indeed, the potentialities of the Bayesian approach in revising probabilities have been explored by means of two different techniques: probability updating and probability adapting. The results of the case study will highlight the advantages of Bayesian Networks application to safety measures performance assessment, proving that its application may eventually will turn into a more flexible and realistic analysis of major accidental scenarios, in comparison with conventional techniques.

Therefore, Bayesian Networks have been applied to the prevention of cascading events, for instance to domino accident analysis, in purpose to assess the effect of safety measures inclusion in the modelling phase. Two case studies, the first regarding a simplified tank farm and the second regarding a realistic tank farm, have been carried out, in Section 5.3.4 and Section 5.3.5 respectively.

The case study presented in Section 5.3.4 deals with a simplified tank farm, composed by three atmospheric storage tanks, with heat radiation as escalation vector. The application is developed in three consequential steps: in modelling step (1), safety measures are not accounted, in modelling steps (2) and (3) safety measures on each tank, pertinent for the reference typology of installation, are considered. In step (2), only availability is considered, while in the latter step, specific gates, accounting both availability and effectiveness, are applied to describe safety barriers performance, according to the description of Section 3.3.2.1.2.

The case study presented in Section 5.3.5 deals with a realistic tank farm, composed by eight tanks, with two initiating events, synergistic effects and three domino levels to be inserted in the analysis. The application is developed in two steps: in the first step, safety measures on each tank are not considered; in the second step, safety measures are introduced in Bayesian Networks modelling, by means of specific gates. The effect of safety measures introduction in Bayesian Networks modelling is evaluated and discussed in both the case studies, in terms of domino escalation probabilities.

The general aim of the original case studies presented in this section is to demonstrate the feasibility and eventual advantages of Dynamic Risk Assessment application, by means of Bayesian Networks, to cascading events modelling and prevention, for instance domino accidents, including safety measures performance.

5.3.2 Application of Bayesian Networks to dynamic safety measures performance assessment for fire prevention in a major accident

The present illustrative case study is aimed at applying Bayesian Networks to quantitative assessment of safety measures performance in the context of major accidents triggered by an external hazard factor, within the process industry domain.

5.3.2.1 Definition of the case study

The illustrative case study considers a major accident (i.e., fire) on a storage tank, belonging to a tank farm, whose occurrence can be prevented or mitigated by the action of two pertinent technical active safety barriers. The inputs for the case study are adapted from a previous Event-Tree based application (Necci et al., 2014), in purpose to compare the results obtained from the conventional and Bayesian Network approaches. The software applied for case study development is Hugin Expert software, version 8.1 (Hugin, 2016). According to the procedure illustrated in Section 3.5.1.1, the application of quantitative safety barriers performance assessment by means of Bayesian Networks starts with the identification of the accidental scenario; the top event is a lightning strike on an atmospheric storage tank, containing

flammable liquid. The top event can determine either direct perforation or not, leading in the latter case to the action of the two active safety barriers; this intermediate event is indicated as direct damage throughout the case study. Then, the two technical active safety barriers, pertinent for the reference installation, which are a rim seal fire extinguisher and a fixed foam system, are identified.

5.3.2.2 Conversion of the Event-Tree for the case study into a Bayesian Network

The Event-Tree, which is the starting point for the application, adapted from Necci et al. (Necci et al., 2014) has been reported in Figure 5. 33, Part A. The conversion of the Event-tree has been performed, according to the mapping procedure reported in Section 3.3.2.1.3.3.2 and maintaining the same inputs, which are reported in Table 5. 33. The assessment of safety barriers performance by means of Bayesian Networks is carried out in two sequential steps:

1) Only availability, expressed by the probability of failure on demand (i.e., PFD), is accounted to represent safety barriers performance. Two Fault-Trees developed in the application by Necci et al. (Necci et al., 2014), reported in Figure 5. 33, Part B and C, to calculate the probability of failure on demand for both the barriers are directly converted and inserted into the Bayesian Network, according to the mapping procedure, reported in Section 3.3.2.1.3.3.2. Indeed, the availability (i.e., probability of failure on demand) has been calculated for each barrier as the output of several pertinent subsystems. This simplified approach to safety barriers performance assessment allows comparing directly the results obtained from Event-Tree and Bayesian Networks applications.
2) The performance of safety barriers has been accounted by means of a specific gate (i.e., type B), suitable for active safety measures and described in Section 3.3.2.1.2, which combines availability and effectiveness. The inputs regarding availability values are the same ones applied in the previous modelling step. Indeed, for effectiveness a reference value of 0.95 (Landucci et al., 2015a) has been considered for both the barriers. This approach allows avoiding over conservative assumptions regarding safety barriers performance, according to the concepts discussed in Section 3.3.2.1.2.

In the conversion process from Event-Tree to Bayesian Network attention should be posed to the consequence node, that is a multi-state node, accounting all the possible outcomes, according to an AND-gate. According to this configuration, there are six possible consequences states; consequences state set of the node range from $Cons\_1$, to $Cons\_5$, plus state Safe, which should be added in the conversion process. $Cons\_1$ indicates release and pool fire, $Cons\_2$ indicates rim seal fire extinguishment, $Cons\_3$ corresponds to full surface fire extinguishment, $Cons\_4$ represents full surface fire, $Cons\_5$ indicates no consequences. However, the most

severe consequences are *Cons*_1, and *Cons*_4. Therefore, their sum, which a useful indicator of major accidents occurrence probability, has been considered as the final output of the BN, named for instance *Results*. Indeed, by connecting node *Top_Event* (i.e., indicating the top event) to *Consequence*, another state, namely *Safe* state is added to the state set; the mentioned node is connected also to the *Damage* node, indicating the possible direct perforation of the tank, which in turn is connected, according to the mapping procedure, to the *Consequence* node.

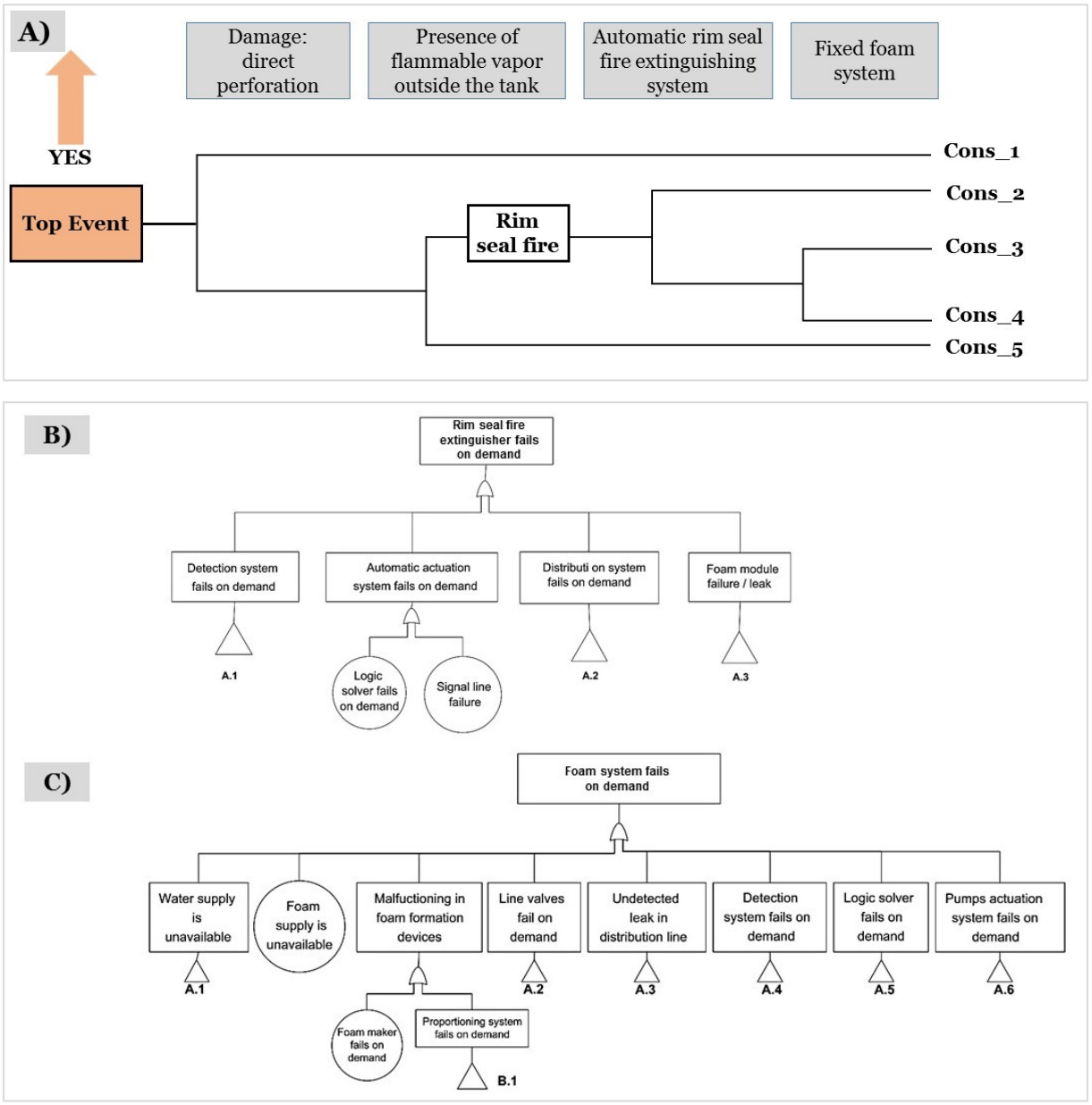


Figure 5. 33 Starting point for the conversion of a conventional application, adapted from Necci et al. (Necci et al., 2014), into a Bayesian Network. A) Event-Tree to be converted. The Top Event is the occurrence of a lightning strike on a storage tank, which can be prevented by two technical barriers: a fixed foam system and a rim seal fire extinguisher. Their performance is calculated in the conventional application by means of Fault-Trees represented in B) for a rim seal fire extinguisher and in C) for a fixed foam system.

To show the dependency among the safety barriers and the top event, causal arcs are also drawn from *Rim_seal_fire_extinguisher* and *Fixed_foam_system* to the node *Consequence*, because the failure/success of each safety barrier results in different consequences (i.e., different states of the *Consequence* node).

The Bayesian Networks obtained from the conversion of the corresponding Event-Tree, according to modelling steps 1) and 2) are reported in Figure 5. 34 and Figure 5. 35.

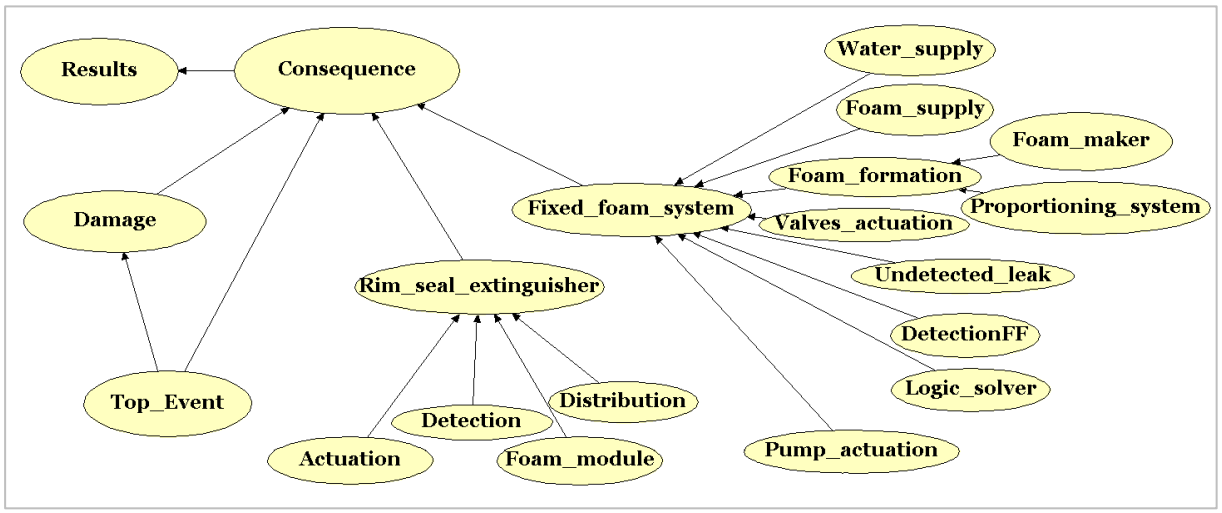


Figure 5. 34 Bayesian Network obtained from Event-Tree conversion according to modelling step 1), regarding the prevention of a major accident (i.e., fire) by means of two pertinent safety barriers: rim seal fire extinguisher and fixed foam system. The performance of safety barriers is represented only by their availabilities.

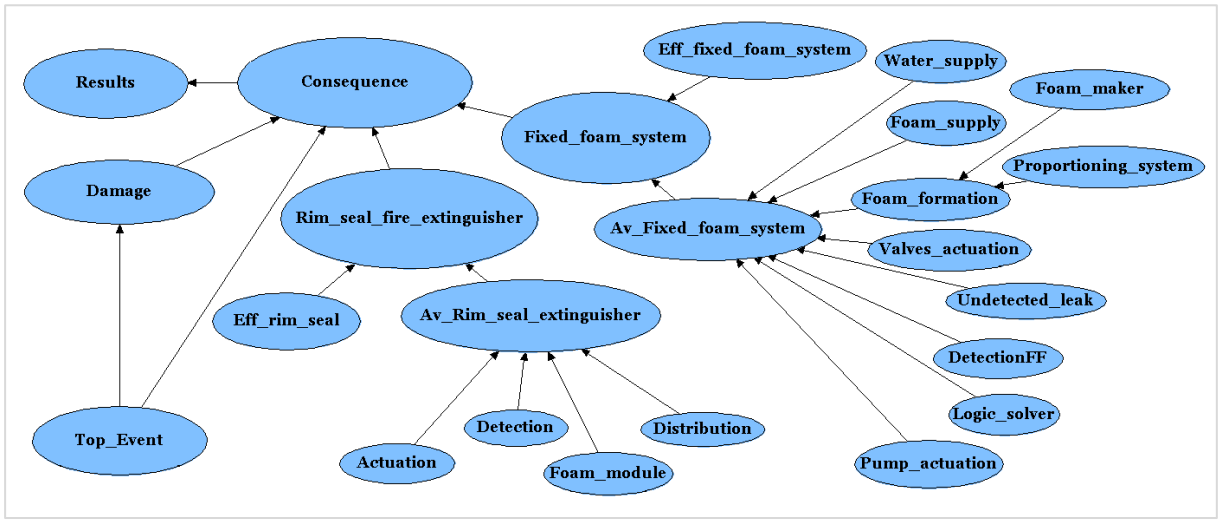


Figure 5. 35 Bayesian Network obtained from Event-Tree conversion, according to modelling step 2), regarding the prevention of a major accident (i.e., fire) by means of two pertinent safety barriers: rim seal fire extinguisher and fixed foam system. The performance of active safety barriers is represented by a specific gate accounting both availability and effectiveness.

An overview on the data applied in the case study, according to modelling steps 1) and 2) has been reported in Table 5. 33.

Table 5. 33 Data for the application of Bayesian Networks to the case study, from Event-Tree conversion.

Symbol	Description	Probability	Type
Data for modelling steps 1) and 2)			
Top_Event	Top event occurrence; lightning on storage tank	4.85E-02	Input
Damage	Intermediate event occurrence; probability of direct perforation	3.38E-04	Input
Safety barrier: Rim seal fire extinguisher			
Av_Rim_seal_extinguisher (in step 2)/ Rim_seal_extinguisher (in step 1)	**Probability of failure on demand (PFD) for rim seal fire extinguisher**	**2.38E-02**	**Output; OR-gate of 4 subsystems listed below**
Actuation	Actuation system (both automatic and manual) fails on demand	2.21E-02	Input
Detection	Detection system fails on demand	8.96E-04	Input
Foam_module	Foam module failure/leak	5.84E-04	Input
Distribution	Distribution system fails on demand	2.81E-04	Input
Safety barrier: Fixed foam system			
Water_supply	Water supply fails on demand	8.83E-04	Input
Foam_supply	Foam supply system fails on demand	1.00E-04	Input
Foam_formation	Foam formation devices fail on demand	5.14E-03	Intermediate output; OR-gate of two subsystems (i.e., proportioning system and foam maker)
Av_Fixed_foam_system (in step 2)/ Fixed_foam_system (in step 1)	**Probability of failure on demand (PFD) for fixed foam system**	**7.01E-03**	**Intermediate output; OR-gate of 8 subsystems listed below**
Proportioning_system	Proportioning system fails on demand	1.16E-03	Input
Foam_maker	Foam maker fails on demand	3.98E-03	Input
Valves_actuation	Actuation system (valves on foam and water lines) fails on demand	6.24E-04	Input
Undetected_leak	Undetected major leak	1.37E-07	Input
DetectionFF	Fixed foam detection system fails on demand	8.96E-06	Input
Logic_solver	Logic solver fails on demand	1.76E-04	Input
Pump_actuation	Pumps actuation system fails on demand	9.57E-05	Input
Data for modelling step 2)			
Eff_rim_seal	Effectiveness of rim seal fire extinguisher	0.95	Input
Eff_fixed foam_system	Effectiveness of fixed foam system	0.95	Input
Rim_seal_extinguisher	Performance of rim seal fire extinguisher by combined availability and effectiveness	7.26E-02	Intermediate output; gate type B
Fixed_foam_system	Performance of fixed foam system by combined availability and effectiveness	5.67E-02	Intermediate output; gate type B

Bayesian analysis has been performed by assigning in modelling step 1) the same probabilities of the conventional Event-Tree based application as the prior probabilities. The comparison among probabilities obtained applying Event-Tree based approach and the ones obtained by

Bayesian Network analysis have been reported in Table 5. 34. Indeed, the application of modelling step 1) to safety barriers performance assessment confirmed the equal ability of Bayesian Networks in the analysis of the specific accidental scenario, in comparison with the conventional Event-Tree based approach, as the results completely overlap. The results of Bayesian Network analysis after the application of a logic gate (type B) specific for active safety barriers, used in modelling step 2), are reported in Table 5. 34. This approach allows avoiding over conservative assumptions regarding safety barriers performance, according to the concepts discussed in Section 3.3.2.1.2. Indeed, introducing a more detailed approach to safety barriers performance in Bayesian Network analysis turns into an increase of fire probability of one order of magnitude. From a general perspective, the conversion process proved that the Event-Tree and Bayesian Network are equally able to analyse the accident scenario. Moreover, BN superiority can be evidenced by the ability to incorporate also the converted fault trees in the same net, to calculate PFD of the safety barriers.

Table 5. 34 Results of Bayesian Network application to the case study, according to modelling steps 1) and 2). The results of Bayesian Network analysis according to modelling step 1) completely overlap with Event-Tree analysis.

Symbol	**Description**	**Probability**	
		Event-Tree/ BN Modelling step 1)	**BN Modelling step 2)**
Fixed_foam_system	Probability of fixed foam system failure	7.01E-03	5.67E-02
Rim_seal_fire_extinguisher	Probability of rim seal fire extinguisher failure	2.38E-02	7.26E-02
Consequence	Consequence multistate node		
Cons_1	Release and pool fire	1.64E-05	1.64E-05
Cons_2	Rim seal fire extinguishment	3.32E-04	2.55E-03
Cons_3	Full surface fire extinguishment	1.14E-03	3.32E-03
Cons_4	Full surface fire	8.08E-06	1.99E-04
Cons_5	No consequences	4.70E-02	4.24E-02
Safe	Safe	9.52E-01	9.52E-01
Results	Fire probability	2.45E-05	2.16E-04

5.3.2.3 Results of dynamic safety measures performance assessment with Bayesian Networks

Bayesian Network analysis has been performed by applying two probability-revising techniques (i.e., probability adapting and probability updating – see Section 3.3.2.1.3.2) with Hugin software version 8.1 (Hugin, 2016), to the net obtained in modelling step 2).

The sequences of events leading to the two most critical final states (i.e., $Cons\_1$ and $Cons\_4$), named also Most Probable Explanations, have been determined by applying probability updating, according to equation (3.20); the calculations are reported in Figure 5. 36, which

illustrates also the sequences. For instance, the most probable sequence leading to $Cons\_1$, with 84.4% probability, consists in the direct perforation of the tank, leading to release and pool fire. On the other hand, the most probable sequence leading to $Cons\_4$, with 58.8% probability, is given by the availability and ineffectiveness of both safety barriers, leading to their failure and to full surface fire. Therefore, the importance of probability updating for safety barriers performance assessment lies in its ability to identify critical sequence of events and allocate safety barriers consequently.

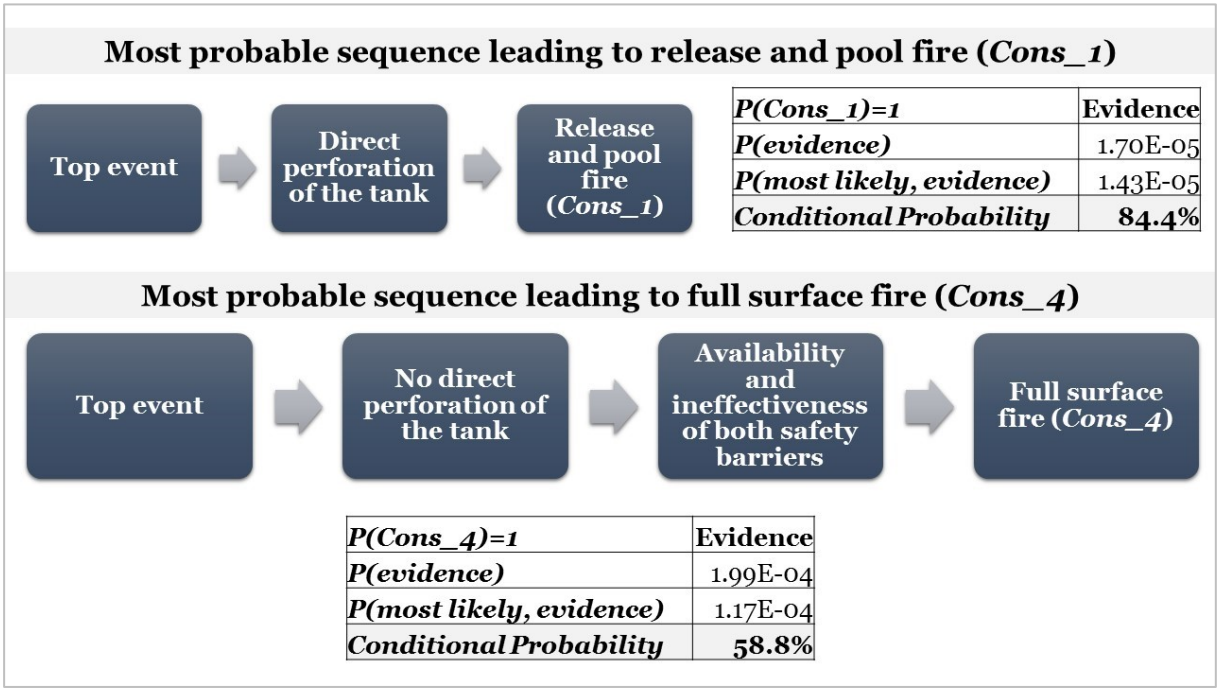


Figure 5. 36 Bayesian Updating results for the case study, aimed at calculating the most probable sequence of events leading to the most severe consequences (i.e., $Cons\_1$ and $Cons\_4$).

Then, Bayesian adapting, which calculates the posterior probability of a generic event x_i given another event Q has occurred n times, is applied. It can be expressed in statistical terms as $P(x_i|Q = n)$. Probability adapting requires as inputs prior experience data (in the form of past accident data collected during a certain time span – ASP, i.e. Accident Sequence Precursors) to adapt conditional probability distributions. In probability adapting application to the illustrative case study, fictional operational data over five years of experience, reported in Table 5. 35, have been applied to revise top event, intermediate event, safety barriers and consequences probabilities over time. Year 0 represents the baseline Bayesian Network analysis, with no additional information added to revise probabilities. For example, at the end of the third year, $Cons\_3$ has cumulatively occurred 3 times, $Cons\_5$ has occurred 5 times; probability adapting can be performed by inserting $P(x_i|Consequence = 5Cons\_5)$ and $P(x_i|Consequence = 3Cons\_3)$, with x_i generic event. Bayesian adapting has been performed by applying "adaptation panel" from software Hugin software, version 8.1.

Table 5. 35 Accident Sequence Precursors (ASP) over five years of operational experience for probability adapting application.

Consequence	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
Cons_1	0	0	0	0	0	1
Cons_2	0	0	1	0	0	0
Cons_3	0	1	1	1	0	0
Cons_4	0	0	0	0	1	0
Cons_5	0	2	2	1	1	1

The results of Bayesian adapting regarding Top event occurrence probability highlight an increasing trend during the time interval (Figure 5. 37). The trend regarding Top event can be explained considering that the accidents top event has always occurred a number of times greater than or equal to the maximum failure numbers of each safety barrier and all the consequences applied as ASP denotes an occurrence of the top event. Indeed, the occurrence probability of Top event increases rapidly over the time span of the analysis. With respect to damage probability, the trend is different, as a consequence of ASP applied in the analysis: its occurrence probability does not vary significantly, with the exception of Year 5, in which a significant increase is recorded, due to a precursor data regarding $Cons\_1$, which propagates backwards thorough the network. Therefore, the insertion of ASP led to an increase after 5 years of the top event and intermediate event probabilities of one and two order of magnitude respectively.

Concerning both the safety barriers, their PFDs, as well as the failure probabilities of their subsystems, have been revised over time by means of Bayesian adapting technique, showing a general increasing trend, which is visible in Figure 5. 38. Furthermore, their effectiveness values have changed consequently over time, with a general decreasing trend. Indeed, the application of a specific gate for the assessment of safety barriers performances hindered from performances overestimation, in comparison with the standard approach based solely on PFDs. The results regarding the failure probabilities for both safety barriers, obtained by combining PFDs and effectiveness, have been reported in Figure 5. 38. They show a global increase of the failure probability over time, which corresponds to a performance decrease over time, for both the rim seal fire extinguisher and the fixed foam system.

Consequences probabilities show a general increasing trend over time, with the obvious exception of "Safe" state, which tend to decrease over time, due to ASPs application. The results of probability adapting referred to all consequences, with a focus on the most critical ones (i.e., $Cons\_1$ and _4), have been reported in Figure 5. 39. The results show that the major accident probability (i.e., *Results* probability), either by release and pool fire or by full surface fire,

increases after five years of more than two order of magnitude, as displayed by Figure 5. 39 revealing indeed a significant change in the relative percentages of the two critical final states.

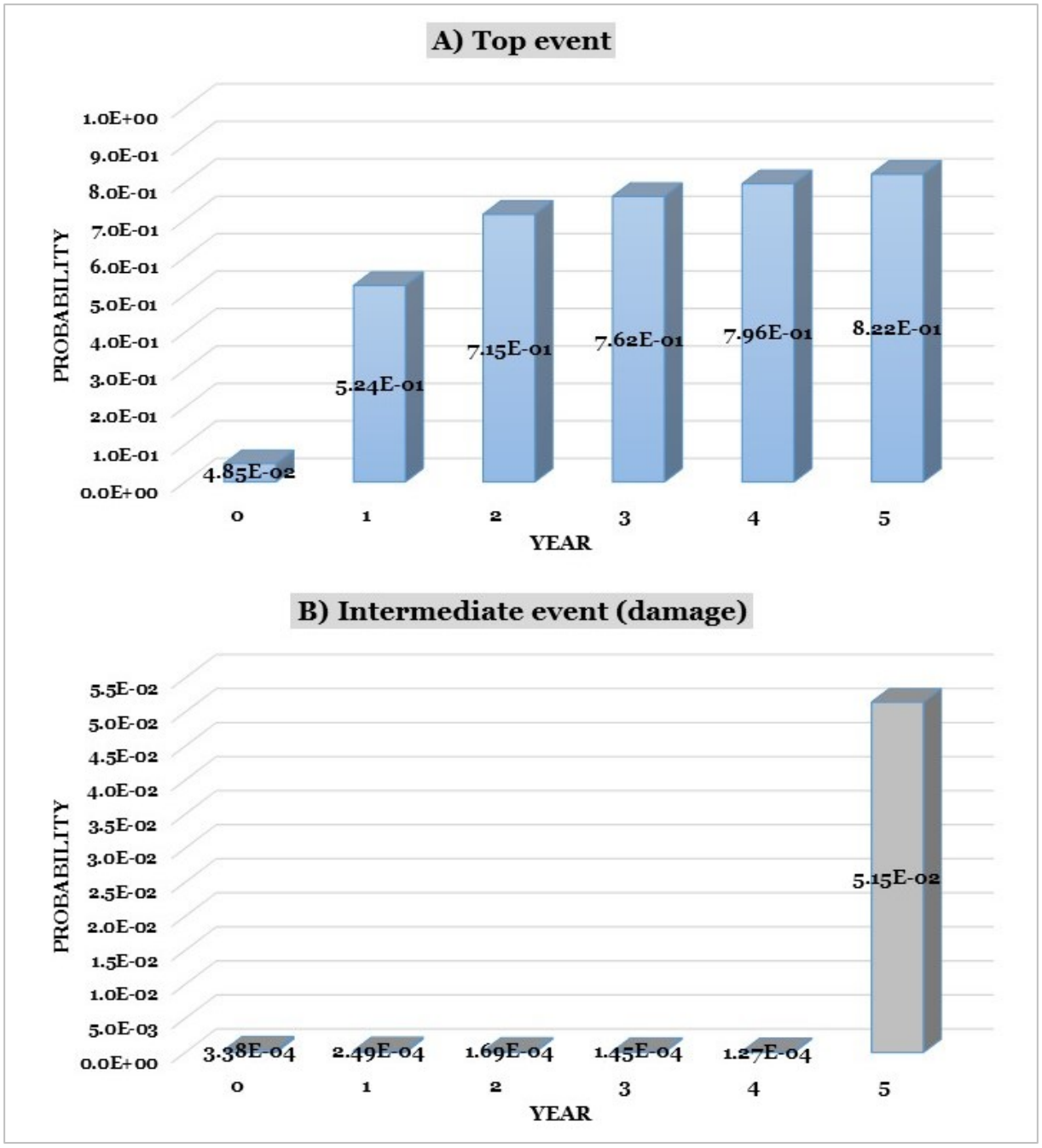


Figure 5. 37 Bayesian adapting results regarding A) Top event occurrence probability B) Direct damage occurrence probability, over five years of operational experience.

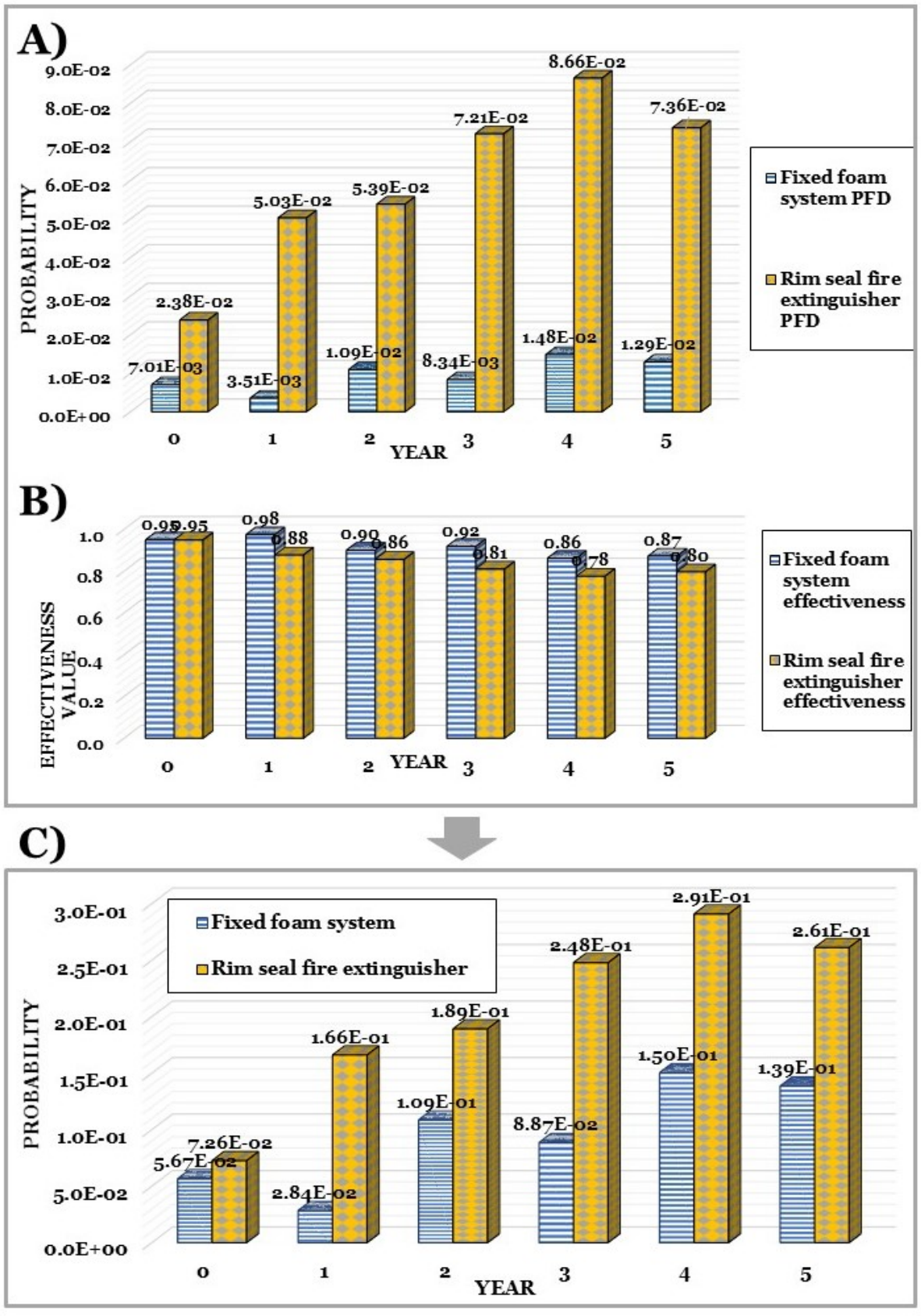


Figure 5. 38 Results of safety barriers performance assessment by means of Bayesian Networks, with Bayesian adapting application. For both the safety barriers: A) PFDs; B) Effectiveness; C) Overall performance combining PFD and effectiveness with a specific gate for active safety measures.

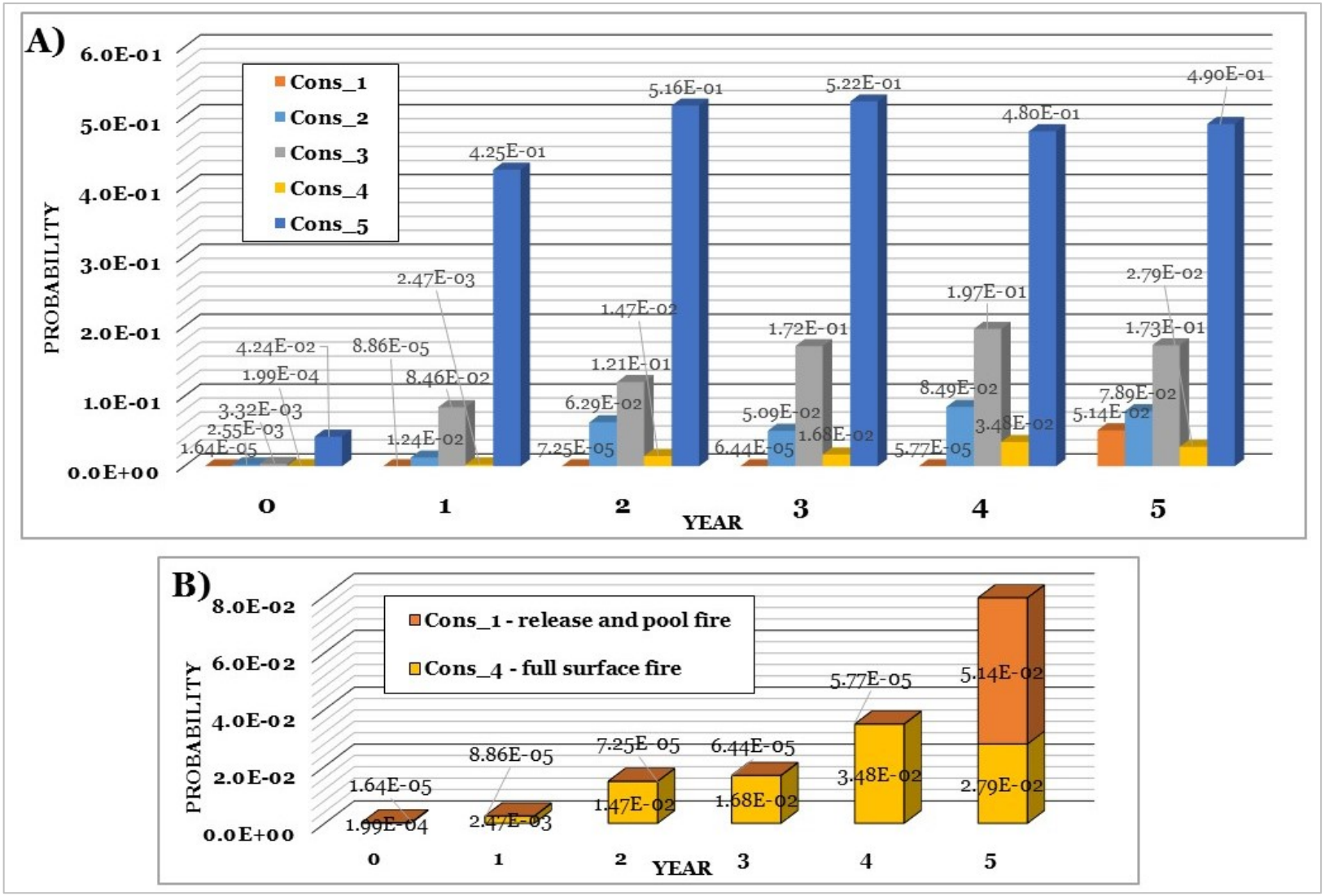


Figure 5. 39 Consequences probabilities over time, after the application of Bayesian adapting, over five years of operational experience: A) All accidental states for the case study; B) Major accident.

5.3.2.4 Discussion and conclusions on the case study

The current contribution has been aimed at comparing the application of a conventional Event-Tree based approach with a Bayesian Network based approach to safety barriers performance assessment in the context of major accidents prevention and mitigation.

The illustrative case study considered a major accident (i.e., a fire triggered by lightning as representative external hazard factor) that can be prevented by pertinent technical safety barriers. The advantages of Bayesian Networks application, in terms of enhanced flexibility and dynamic system representation, have been highlighted by the application. The case study highlighted Bayesian Networks ability to represent an accidental scenario, by the conversion of a previous Event-Tree based application. Indeed, the application of a specific gate for the assessment of active safety barriers performance, accounting both availability and effectiveness, proved to be useful in purpose to avoid performance overestimation and to provide a more accurate risk picture.

The case study is the first application of this specific gate, named gate type B, in a Bayesian framework, and indeed it provides a benchmark for further implementations. Nevertheless, two specific gates (type A and C) stills need to be tested on a more complete case study performed with Bayesian Networks, including also passive and procedural safety barriers, besides active ones.

Within the current case study, Bayesian analysis, by means of probability updating and probability adapting, was performed, leading to the revision of probabilities over time. In probability updating, the information about a node instantiated to one of its states (i.e., a certain event that had happened) is used as evidence; its main application is the determination of the most critical sequence of events, in order to revise the safety system consequently. The results demonstrate that Bayesian probability adapting can be applied as a predictive tool in purpose to assess the adequacy of a safety system. Therefore, probability adapting is a useful technique to replace generic prior probabilities (i.e., generic reliability data) with more case-specific posterior probabilities, resulting in a dynamic assessment of safety barriers performance and a more reliable prediction of occurrence likelihood for each final event.

Eventually, the results of the case study proved the applicability of Bayesian Networks in the context of quantitative safety barriers performance assessment with respect to major accidents triggered by external hazard factors in chemical facilities. However, the present case study provides just a preliminary illustrative application; further applications should deal with cascading events triggered by external hazard factors, considering realistic plant layouts and the integration of different technical and organizational safety barriers.

5.3.3 Application of Bayesian Networks to dynamic safety measures performance assessment in the prevention of a domino accident triggered by fire

The present case study is aimed at applying a Bayesian Networks based approach to safety barriers performance assessment in the prevention of fire escalation, starting from a conventional Event-tree based one, adapted from Landucci et al. (Landucci et al., 2015a), and at applying both of them to the same case study, in purpose to compare the so-obtained results.

5.3.3.1 Definition of the case study

The case study deals with the dynamic assessment of safety barriers performance by means of Bayesian Networks with respect to the prevention of a possible domino accident triggered by fire in a Liquefied Petroleum Gas (i.e., LPG) storage facility.

The inputs for the case study are adapted from a previous Event-Tree based application (Landucci et al., 2015a), in purpose to compare the results obtained from the conventional and Bayesian approaches. The software applied for case study development is Hugin Expert software, version 8.1 (Hugin, 2016). According to the procedure illustrated in Section 3.3.2.1.2 and in Section 3.5.1.1, the application of quantitative safety barriers performance assessment starts with the identification of the accidental scenario: the case study considers a pool fire of ethanol (from T1 tank) causing the top event, which is fire impingement on a second tank, named for instance T2, containing LPG. Fire escalation can be prevented by the action of four technical and organizational safety barriers, pertinent for the reference installation, which is, according to the criteria presented in Section 3.3.2.1.2, RI Type 2 with above ground pressurized vessel. The layout of the installation to be applied in the case study is available in Figure 5. 40. The barriers to be considered in the application are indeed a water deluge system (i.e., *WDS*), which is an active barrier, a pressure safety valve (i.e., *PSV*) and a passive fire protection coating (i.e., *PFP*), belonging both to the class of passive barriers, and emergency team intervention (i.e., *Em_Team*), which is a procedural/organizational barrier.

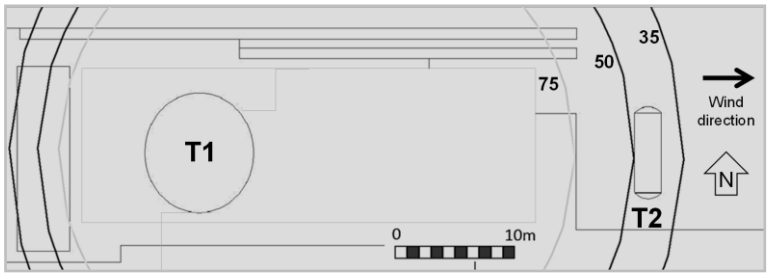


Figure 5. 40 Layout of the reference installation to be applied in the case study (Landucci et al., 2015a).

Both in the starting application and its Bayesian conversion, safety barriers performance is carried out by means of specific gates, depending on barriers states and classification, and

accounting both availability and effectiveness. In detail, for water deluge system, pressure safety valve and passive fire protection performance is described by a gate Type A; emergency tem intervention is represented by a gate Type C.

The final accidental states to be considered in the case study are 16 (i.e., indicated as FE1.1, FE1.2, FE.2.1, etc.), grouped into three main severity classes: no domino, mitigated domino (partial/delayed fire escalation) and unmitigated domino.

5.3.3.2 Application of an Event-Tree based approach to the case study

The starting point for the case study is the Event-Tree reported in Figure 5. 41. The Event-Tree based application, provided by Landucci et al. (Landucci et al., 2015a), was reproduced, in purpose to provide a starting point for the implementation of the corresponding Bayesian Network and to compare the results.

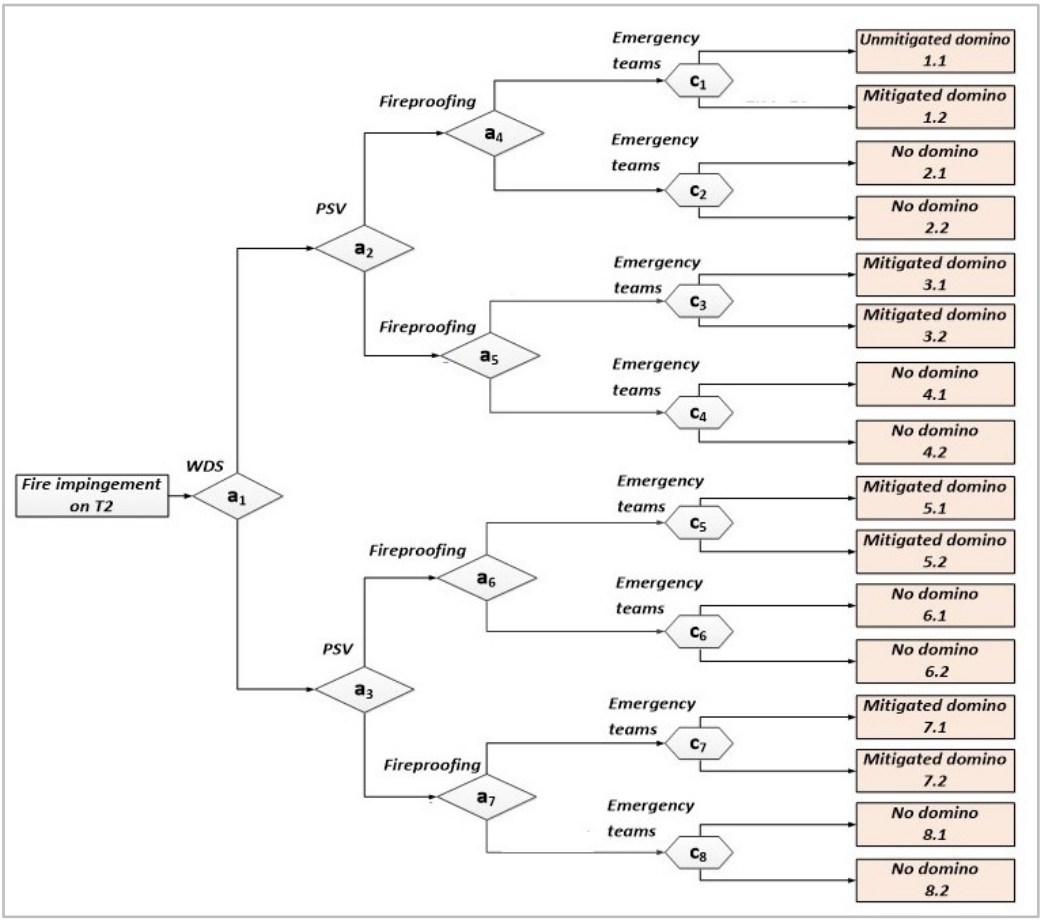


Figure 5. 41 Event-Tree for escalation assessment (Landucci et al., 2015a), which is the starting point for the application a Bayesian Network. The case study considers the probabilistic assessment of a domino accident resulting from pool fire impingement on a storage tank, considering the action of relevant safety barriers. The upper branch always indicates the failure state.

Both the approaches require the calculation of associated escalation probability values (P_d), according to the procedure described in Section 3.3.2.1.2, depending on safety barriers states.

Concerning the two branches defined by water deluge system in Figure 5. 41 (i.e., the first branch on the left, starting from the top event), the heat load (Q_{WDS}) is calculated according to equation (3.8), considering a full heat load value (Q_{HL}) of $50\frac{\text{kW}}{\text{m}^2}$ which can be reduced, according to an intensity reduction factor φ of 0.5 when the safety barrier is available; else way φ is equal to 1. Indeed, WDS is charaterized by a gate type A (Figure 3. 6).

For all barriers represented by a gate type A, OUT 1 represents failure state, with barrier unavailability expressed by PFD; OUT 2 represent barrier success, corresponding to availability of the barrier, but its effectiveness η should be considered. The PFD of WDS was assumed $4.33 \cdot 10^{-2}$, according to the Fault-Tree analysis provided by Landucci et al. (Landucci et al., 2015a); the effectiveness value was assumed unitary. The values of heat loads for each accidental final states are reported in Table 5. 38 (i.e., third column from the left).

Concerning the four branches defined by pressure safety valve in Figure 5. 41, a gate type A has been considered: the availability value is $1.00 \cdot 10^{-2}$, according to literature data (Landucci et al., 2015a) and the effectiveness value was assumed unitary.

Concerning the eight branches defined by fireproofing coating in Figure 5. 41, a gate type A was applied with a PFD value of $1.00 \cdot 10^{-3}$ and $\eta = 1$. The calculation of the time to failure (ttf_P) was carried out according to equation (3.10), according to the following inputs:

- ttf is calculated according to equation (3.9), using the coefficients listed in Table 5. 36;
- Q_{HL} is substituted by Q_{WDS} if WDS available;
- In equation (3.10), if PFP is available and effective, with $ttf_C = 70\ min$.

Table 5. 36 Coefficients for time to failure calculation to be applied in the case study.

V (m^3)		**Vessel description**		
T1 (first tank)	229	Ethanol, atmospheric tank		
T2 (second tank)	25	LPG (propane), pressurized vessel		
Coefficients for ttf calculation				
Item	f	e	d	c
Atmospheric vessel	9.877	-1.13	1	-2.667E-05
Pressurized vessel	0	-0.95	0.032	8.845

Indeed, according to the Event-Tree presented in Figure 5. 41, branches FE1.1, FE1.2, FE3.1, FE3.2, FE5.1., FE5.2, FE7.1., FE7.2 indicate fireproofing failure; time to failure values for each final state have been reported in Table 5. 38 (i.e., fourth column from the left).

Concerning the sixteen branches defined by emergency team intervention in Figure 5. 41, a gate type C has been applied; in the present application the gate has two states. OUT 1 represents the upper branch of the gate, corresponding to unavailability of the emergency

teeam, expressed by PFD, whose value is $1.00 \cdot 10^{-1}$. The lower branch of the gate is either in state OUT 2 or in state OUT 3; OUT 2 and OUT 3 are mutually exclusive states. According to OUT 2, emergency response is activated but uneffective ($\eta = 0$), as the time for final mitigation (i.e., maximum time required by the external emergency team to provide and keep constant the amount of water for fire suppression and cooling action, indicated with tfm) overcomes the time to failure. According to OUT 3, the emergency response is activated, mitigation action is successful and therefore fire escalation is prevented ($\eta = 1$).

The calculation of tfm is carried according to the data reported in Table 5. 37, applying the concepts described in Section 3.3.2.1.2. The values of the difference between time to failure and tfm for each final accidental state are reported in Table 5. 38 (i.e., fifth column from the left).

Table 5. 37 Calculation of the time for final mitigation.

Calculation of time for final mitigation (*tfm*)		
Description	***Value***	***Unit***
Time to alert external emergency team	5	*minutes*
Overall response time	12	*minutes*
Time for equipment deployement	7	*minutes*
Other set up operations	8	*minutes*
tfm	**32**	*minutes*
	1920	*s*

Then, the calculation of associated escalation probability (P_d) is carried out for each final accidental state, according to the following steps:

1) Calculation of Probit variable (Y), according to equation (3.2), using coefficients $a = 9.261$ and $b = -1.85$;
2) Calculation of normalized Probit variable ($Y - 5$);
3) Application of standard cumulative distribution to get P_d values, according to equation (3.4).

Probit values and associated escalation probability values are reported in Table 5. 38 (i.e., sixth and seventh column from the left respectively). Indeed, consequences probabilities for each final state are calculated and reported in Table 5. 38 (i.e, second to last column).

Then, the root frequency of the top event, indicating fire impingement on T2, $f_{Top\ event} = 1.0 \cdot 10^{-5}\ ev/y$ is introduced to calculate final events frequencies, according to the conventional Event-Tree approach, by applying equation (3. 12); the results are reported in the last column of Table 5. 38. Then, final events consequences probabilities and frequencies are grouped into the three mentioned severity categories: no domino, mitigated domino and unmitigated

domino, whose values are calculated by summing all the contribution to each category and reported in Table 5. 39.

It should be noted that without considering safety barriers, the probability of escalation for the case study is 0.715, therefore unmitigated domino escalation frequency value is $7.15 \cdot 10^{-6} y^{-1}$, significantly higher than the value reported by Purple Book (TNO, 2005a) for a catastrophic loss of containment (i.e., $5.00 \cdot 10^{-7} y^{-1}$).

Therefore, the introduction of safety barriers in the modelling phase of fire escalation avoid unrealistic over estimation of a possible domino event occurrence. This observation makes the use of accurate tools for the evaluation of safety barriers performances even more important within risk assessment.

Table 5. 38 Results of Event-Tree application for the case study, which is the starting point for the conversion into a Bayesian Network approach.

Final event ID	Type of resulting scenario	Heat Load (kW/m^2)	*ttf (s)* - total	*ttf-tsm (s)*	Escalation Probit (*Y*)	Associated Escalation Probability (P_d)	Barriers states				Consequence probability	Event-Tree results Final event probabilities
							WDS	PSV	PFP	EM-TEAM		
FE1.1	Unmitigated domino	50	442	-1478	5.568	7.15E-01	OUT1	OUT1	OUT1	OUT1	4.33E-08	**3.10E-08**
FE1.2	Mitigated domino	50	442	-1478	5.568	7.15E-01	OUT1	OUT1	OUT1	OUT2	3.90E-07	**2.79E-07**
FE2.1	No domino	50	4642	2722	1.216	7.72E-05	OUT1	OUT1	OUT2	OUT1	4.33E-05	**3.34E-09**
FE2.2	No domino	50	4642	2722	1.216	7.72E-05	OUT1	OUT1	OUT2	OUT3	3.89E-04	**3.01E-08**
FE3.1	Mitigated domino	50	442	-1478	5.568	7.15E-01	OUT1	OUT2	OUT1	OUT1	4.29E-06	**3.07E-06**
FE3.2	Mitigated domino	50	442	-1478	5.568	7.15E-01	OUT1	OUT2	OUT1	OUT2	3.86E-05	**2.76E-05**
FE4.1	No domino	50	4642	2722	1.216	7.72E-05	OUT1	OUT2	OUT2	OUT1	4.28E-03	**3.31E-07**
FE4.2	No domino	50	4642	2722	1.216	7.72E-05	OUT1	OUT2	OUT2	OUT3	3.85E-02	**2.98E-06**
FE5.1	Mitigated domino	25	853	-1067	4.350	2.58E-01	OUT2	OUT1	OUT1	OUT1	9.57E-07	**2.47E-07**
FE5.2	Mitigated domino	25	853	-1067	4.350	2.58E-01	OUT2	OUT1	OUT1	OUT2	8.61E-06	**2.22E-06**
FE6.1	No domino	25	5053	3133	1.059	4.06E-05	OUT2	OUT1	OUT2	OUT1	9.56E-04	**3.88E-08**
FE6.2	No domino	25	5053	3133	1.059	4.06E-05	OUT2	OUT1	OUT2	OUT3	8.60E-03	**3.49E-07**
FE7.1	Mitigated domino	25	853	-1067	4.350	2.58E-01	OUT2	OUT2	OUT1	OUT1	9.47E-05	**2.44E-05**
FE7.2	Mitigated domino	25	853	-1067	4.350	2.58E-01	OUT2	OUT2	OUT1	OUT2	8.52E-04	**2.20E-04**
FE8.1	No domino	25	5053	3133	1.059	4.06E-05	OUT2	OUT2	OUT2	OUT1	9.46E-02	**3.84E-06**
FE8.2	No domino	25	5053	3133	1.059	4.06E-05	OUT2	OUT2	OUT2	OUT3	8.52E-01	**3.46E-05**

Table 5. 39 Final events probabilities and frequencies, according to the Event-Tree methodology and grouped into three main classes, depending on scenario severity.

Type of resulting scenario	Final event evaluated probability	Final event frequency (y^{-1})
Unmitigated domino	3.10E-08	3.10E-13
Mitigated domino	2.78E-04	2.78E-09
No domino	4.21E-05	4.21E-10

5.3.3.3 Conversion of the Event-Tree into a Bayesian Network for the case study

The application of an Event-Tree based approach to safety barriers performance assessment proved its limitations in terms of flexibility and ability to insert additional information. Therefore, the conversion of the Event-Tree for escalation assessment into a Bayesian Network was carried out for the case study, using Hugin software version 8.1 (Hugin, 2016). The mapping procedure to be applied is described in Section 3.3.2.1.2; the same inputs listed in Section 5.3.3.2 were maintained in BN application.

Regarding the four technical and organizational safety barriers in place (i.e., water deluge system, pressure safety valve, fireproofing coating and emergency team intervention) they are represented by four safety nodes, whose performances have been evaluated by means of the same specific gates, accounting both availability and effectiveness that have been applied in the Event-Tree based approach. The nomenclature has been kept coherent with the Event-Tree application. The implementation of the logic gates Type A and Type C in a Bayesian Network environment has been realized, implementing the equations reported in Figure 3. 6. The inputs for the safety nodes, regarding availability and effectiveness values, are the same ones applied in the previous modelling step and reported in Section 5.3.3.2; these are called prior probabilities throughout the development of the Bayesian approach to the case study.

The Top Event node (*TE_PFT2*), indicating fire impingement on LPG tank T2, was defined, considering a probability unitary, in purpose to keep the focus of Bayesian analysis on safety barriers and consequences.

In the conversion process from Event-Tree to Bayesian Network attention should be posed to the consequence node, named *Cons_prob*, which is a multi-state node, accounting all the possible outcomes, according to an AND-gate, implemented manually, whose screenshot is reported in Figure 5. 42. According to this configuration, the consequence node include sixteen possible accidental consequences states, corresponding to the Event-Tree application. Indeed, by connecting the top event to the consequence node, another state, namely *Safe* state is added to the consequence state set. As in the Event-Tree based approach, final states have been grouped analogously into three classes: unmitigated domino, delayed/mitigated domino and no domino.

Cons_prob

Em_team	OUT1															
Fireproofing	OUT 1								OUT 2							
PSV	OUT 1				OUT 2				OUT 1				OUT 2			
WDS	OUT 1		OUT 2		OUT 1		OUT 2		OUT 1		OUT 2		OUT 1		OUT 2	
TE_PFT2	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...
FE11	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE21	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
FE22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE31	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
FE32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE41	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
FE42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE51	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
FE52	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE61	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
FE62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE71	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
FE72	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
FE82	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Safe	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Cons_prob

Em_team	OUT2-3															
Fireproofing	OUT 1								OUT 2							
PSV	OUT 1				OUT 2				OUT 1				OUT 2			
WDS	OUT 1		OUT 2		OUT 1		OUT 2		OUT 1		OUT 2		OUT 1		OUT 2	
TE_PFT2	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...	Impinq...	No-im...
FE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE12	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE22	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
FE31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE32	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
FE41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE42	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
FE51	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE52	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
FE61	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE62	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
FE71	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE72	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
FE81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FE82	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Safe	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Figure 5. 42 Conditional Probability Table for the consequence node of BN, including 16 final accidental states plus state *Safe*.

An overview on the inputs and nomenclature applied in the development of Bayesian approach to the case study is available in Table 5. 40. The Bayesian Network application, derived from the conversion of the corresponding Event-Tree, is displayed in Figure 5. 43. The results obtained by running the net with the sum propagation tool of Hugin software, completely overlaps with the results previously obtained with the Event-Tree based approach, as visible from Table 5. 41, as inputs data and assumptions are the same ones and no application of Bayesian inference has been carried out at this stage of the case study.

This confirms that Event-Tree and Bayesian Network are equally able to perform escalation assessment referred to a possible cascading event.

Table 5. 40 Data for the application of Bayesian Networks to the case study, from Event-Tree conversion.

Symbol	Description	Probability	Type
TE_PFT2	Top event occurrence; fire impingement on LPG tank T2	1	Input. In the BN $P(TE\_PFT2) = 1$ to focus on safety barriers.
Safety barrier node: water deluge system (WDS)			
Av_WDS	Probability of failure on demand (PFD) for water deluge system	4.33E-02	Input
Eff_WDS	Effectiveness of water deluge system	1	Input
WDS	Performance of water deluge system by combined availability and effectiveness	4.33 E-02	Intermediate output; gate type A
Safety barrier node: pressure safety valve (PSV)			
Av_PSV	Probability of failure on demand (PFD) for pressure safety valve	1.00E-02	Input
Eff_PSV	Effectiveness of pressure safety valve	1	Input
PSV	Performance of pressure safety valve by combined availability and effectiveness	1.00E-02	Intermediate output; gate type A
Safety barrier node: fireproofing coating (PFP)			
Av_PFP	Probability of failure on demand (PFD) for fireproofing coating	1.00E-03	Input
Eff_PFP	Effectiveness of fireproofing coating	1	Input
Fireproofing	Performance of fireproofing coating by combined availability and effectiveness	1.00E-03	Intermediate output; gate type A
Safety barrier node: emergency team intervention (Em_team)			
Av_Emt	Probability of failure on demand (PFD) for emergency team intervention	1.00E-01	Input
Eff_Emt	Effectiveness of emergency team	1	Input
Em_team	Performance of emergency team by combined availability and effectiveness	1.00E-01	Intermediate output; gate type C
Consequence node			
Cons_prob	Consequence multistate node with 16 final accidental states + state *Safe*	-	Outputs of AND-gate; results available in Table 5. 41
P_d	Escalation probability for each final accidental state	-	Inputs added externally from Bayesian Network; values available in Table 5. 38

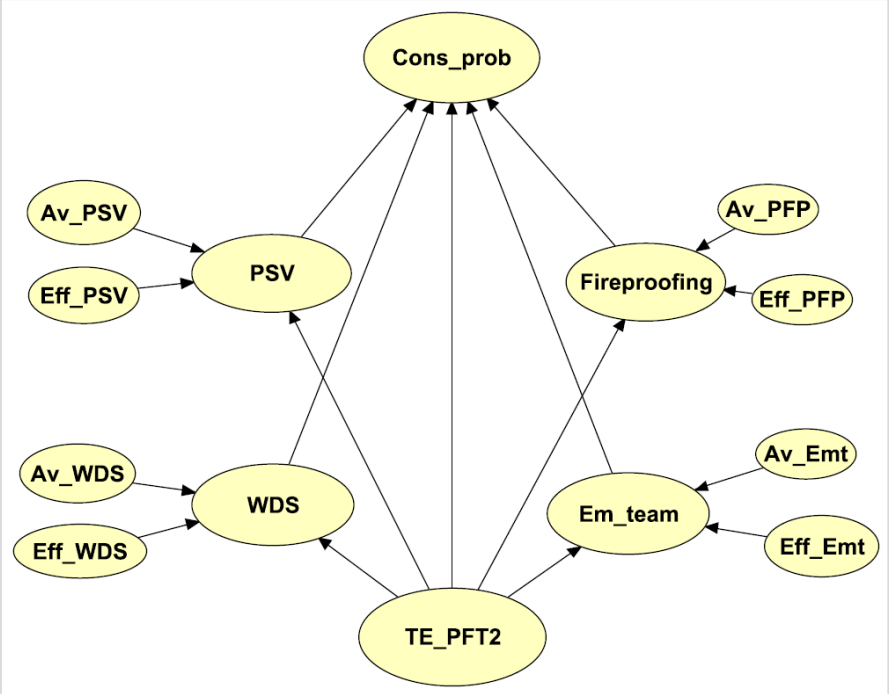


Figure 5. 43 Bayesian Network for fire escalation resulting from pool fire impingement on an LPG tank, considering the action of four relevant safety barriers. The net has been obtained from the conversion of the corresponding Event-Tree.

Table 5. 41 Comparison of results obtained from Event-Tree analysis and Bayesian Network analysis.

Final event ID	Type of resulting scenario	Event-Tree analysis		Bayesian Network analysis	
		Consequence probability	Final event probability	Consequence probability	Final event probability
FE 1.1	Unmitigated domino	4.33E-08	3.10E-08	4.33E-08	3.10E-08
FE 1.2	Mitigated domino	3.90E-07	2.79E-07	3.90E-07	2.79E-07
FE 2.1	No domino	4.33E-05	3.34E-09	4.33E-05	3.34E-09
FE 2.2	No domino	3.89E-04	3.01E-08	3.89E-04	3.01E-08
FE 3.1	Mitigated domino	4.29E-06	3.07E-06	4,29E-06	3.07E-06
FE 3.2	Mitigated domino	3.86E-05	2.76E-05	3.86E-05	2.76E-05
FE 4.1	No domino	4.28E-03	3.31E-07	4.28E-03	3.31E-07
FE 4.2	No domino	3.85E-02	2.98E-06	3.85E-02	2.98E-06
FE 5.1	Mitigated domino	9.57E-07	2.47E-07	9.57E-07	2.47E-07
FE 5.2	Mitigated domino	8.61E-06	2.22E-06	8.61E-06	2.22E-06
FE 6.1	No domino	9.56E-04	3.88E-08	9.56E-04	3.88E-08
FE 6.2	No domino	8.60E-03	3.49E-07	8.60E-03	3.49E-07
FE 7.1	Mitigated domino	9.47E-05	2.44E-05	9.47E-05	2.44E-05
FE 7.2	Mitigated domino	8.52E-04	2.20E-04	8.52E-04	2.20E-04
FE 8.1	No domino	9.46E-02	3.84E-06	9.46E-02	3.84E-06
FE 8.2	No domino	8.52E-01	3.46E-05	8.52E-01	3.46E-05

5.3.3.4 Results of dynamic safety measures performance assessment with Bayesian Networks

Once it is confirmed that the Event-Tree based approach and Bayesian Networks are equally able to perform escalation assessment, the BN superiority can be evidenced by the ability to update the probabilities, taking into account new evidences. Bayesian Analysis has been applied in order to demonstrate the superior flexibility of this technique in comparison with Event-Tree and exploring its features in safety barriers performance evaluation. Two different approaches to Bayesian Analysis have been applied, in order to dynamically update probabilities: probability updating and probability adapting (see Section 3.3.2.1.3.2).

Probability updating is the determination of the most probable state of all the variables given the accident occurrence (i.e., the most probable configuration or explanation - MPE), named in statistics as posterior joint probability of all events. The information about a node is used as evidence, determining the most probable explanation (MPE) leading to that state.

In the case study, final state FE 7.2, which is the most probable final state according to Table 5. 41, is added as an evidence, and by means of the "max propagate tool", the BN searches over each variable to identify weak links. The probability of the system being in the most probable configuration leading to final state FE 7.2 is 85.2%; the most critical sequence, which is reported in Figure 5. 44, corresponds to Passive Fire Protection failure state (i.e., OUT 1) and working state for all the other safety barriers in place (i.e., WDS, PSV and Emergency Team).

Bayesian updating results suggests revising and upgrading fireproofing coating, as it represents the weak point of the critical sequence of events leading to the most probable final state. Therefore, the importance of probability updating for safety barriers performance assessment lies in its ability to identify critical sequence of events and allocate safety barriers consequently to prevent fire escalation.

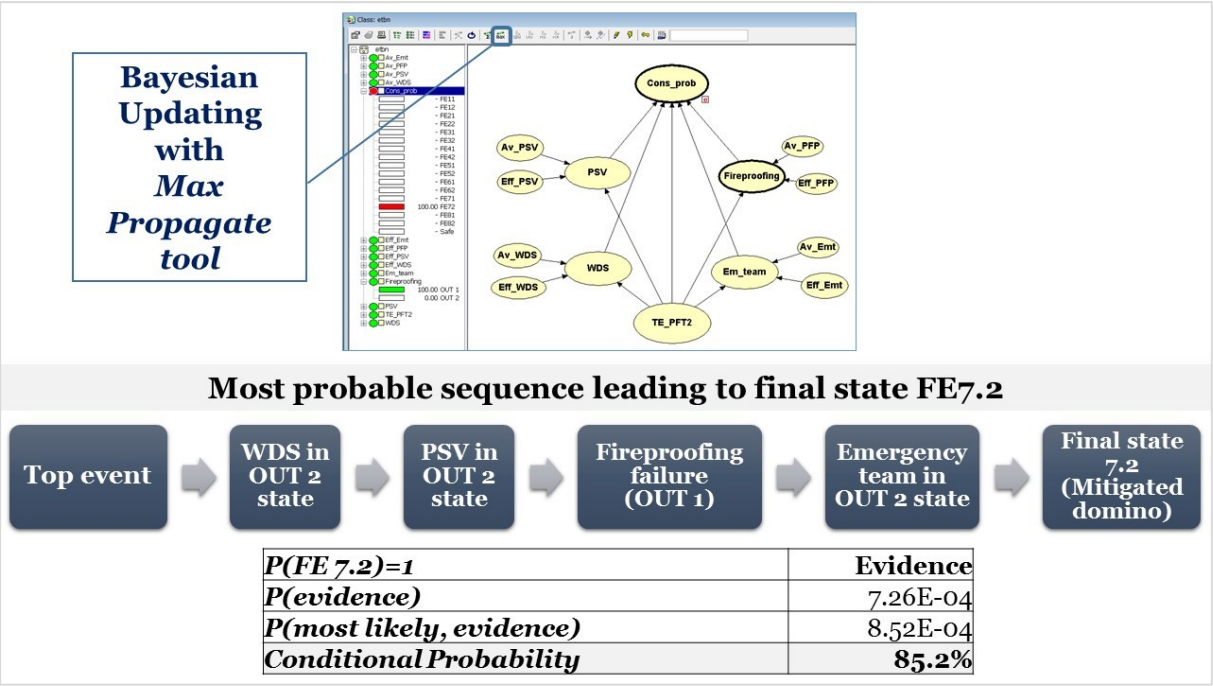


Figure 5. 44 Bayesian Updating results for the case study, aimed at calculating the most probable sequence of events leading to the most probable consequence (i.e., *FE* 7.2).

Then, Bayesian probability adapting is applied. In probability adapting, the additional information during a time interval is used as evidence (e.g, in the form of Accident Sequence Precursors), in order to dynamically revise probabilities for safety barriers, final events and domino probabilities. In statistical terms, this can be expressed as $P(x_i|Q = n)$.

Indeed, probability adapting requires as inputs prior experience data (in the form of past accident data collected during a certain time span – ASP, i.e. Accident Sequence Precursors) to adapt conditional probability distributions. In probability adapting application to the case study, fictional operational data over five years of experience, reported in Table 5. 42, have been applied to dynamically revise safety barriers, final events and domino probabilities over time; ASP are referred to top-4 most probable final events. Year 0 represents the baseline Bayesian Network analysis, with no additional information added to revise probabilities, whose results have already been presented in Table 5. 41. For example, according to the data reported in Table 5. 42 at the end of the second year, FE 8.2 has cumulatively occurred 4 times, FE 7.2 has occurred only once; probability adapting can be performed by inserting $P(x_i|\, Consequences) = 4P(FE\ 8.2)$ and $P(x_i|\, Consequences) = P(FE\ 7.2)$, with x_i generic event. Bayesian adapting has been performed by applying "adaptation panel" from software Hugin software, version 8.1 (Hugin, 2016), inserting manually the values of ASP reported in Table 5. 42 and developing a specific net corresponding to each year of operational experience.

Table 5. 42 Accident Sequence Precursors (ASP) over five years of operational experience for probability adapting application.

Consequence	Year 1	Year 2	Year 3	Year 4	Year 5
FE 3.2	0	0	0	1	0
FE 7.1	0	0	0	0	2
FE 7.2	0	1	0	0	1
FE 8.2	3	1	2	1	0

The information about the occurrence probability of selected final events propagates backwards through the network, varying the performance of the safety barriers over time, as well as the values of final events probabilities and final events categories probabilities.

The results of Bayesian adapting over 5 years of operational experience concerning the performance of the four safety barriers in place, evaluated by means of specific gates combining availability and effectiveness are reported in Figure 5. 45 and Figure 5. 46 with reference to failure (i.e., OUT1) and work (i.e., OUT 2-3) states respectively.

Indeed, the application of a specific gate for the assessment of safety barriers performances hindered from performances overestimation, in comparison with the standard approach based solely on PFDs. As visible from both the figures, it is possible to have either decreasing trend, increasing trend or constant values of safety barriers performance depending on the ASP introduced. As highlighted by Figure 5. 45, the barriers show slightly different behaviors: WDS, PSV and Emergency team failure probabilities tend to increase moderately over time, while PFP gains more attention compared to the other three barriers, due to a significant increase of the failure probability of two orders of magnitude after the application of 5 years long operational experience.

Barriers	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
WDS	4.33E-02	2.17E-02	2.17E-02	2.17E-02	7.72E-02	6.33E-02
PSV	1.00E-02	5.00E-03	5.00E-03	5.00E-03	5.00E-03	5.00E-03
PFP	1.00E-03	5.00E-04	1.01E-01	7.19E-02	1.12E-01	2.09E-01
Em.Team	1.00E-01	5.00E-02	5.00E-02	5.00E-02	5.00E-02	1.33E-01

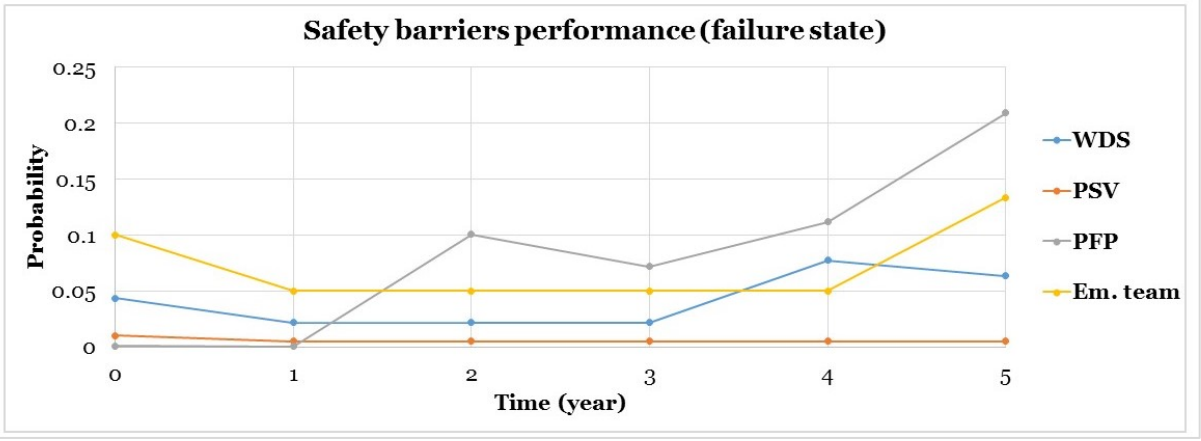


Figure 5. 45 Results of safety barriers performance assessment by means of Bayesian Networks, with Bayesian adapting application over five years of operational experience. The results refers to failure state (i.e., OUT 1) and are obtained by means of specific gates for four safety barriers in place in the reference installation: water deluge system (i.e., WDS), pressure safety valve (i.e., PSV), fireproofing coating (i.e, PFP) and emergency team intervention (i.e., Em. Team).

Barriers	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
WDS	9.57E-01	9.78E-01	9.78E-01	9.78E-01	9.23E-01	9.37E-01
PSV	9.90E-01	9.95E-01	9.95E-01	9.95E-01	9.95E-01	9.95E-01
Fireproofing	9.99E-01	1.00E+00	9.00E-01	9.28E-01	8.88E-01	7.91E-01
Em. Team	9.00E-01	9.50E-01	9.50E-01	9.50E-01	9.50E-01	8.67E-01

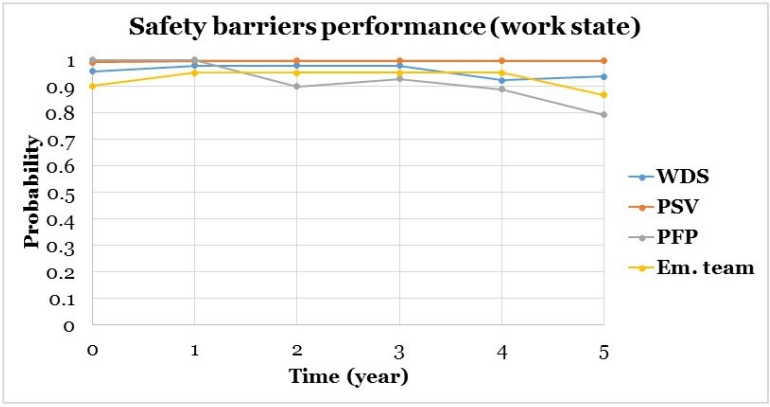


Figure 5. 46 Results of safety barriers performance assessment by means of Bayesian Networks, with Bayesian adapting application over five years of operational experience. The results refers to work state (i.e., OUT 2-3) and are obtained by means of specific gates for four safety barriers in place in the reference installation: water deluge system (i.e., WDS), pressure safety valve (i.e., PSV), fireproofing coating (i.e, PFP) and emergency team intervention (i.e., Em. Team).

Table 5. 43 Final events probabilities for sixteen final accidental states obtained by means of Bayesian Networks, with Bayesian adapting application over five years of operational experience.

Final event ID - consequences	Type of resulting scenario	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
FE 1.1	Unmitigated domino	3.10E-08	1.94E-09	3.89E-07	2.78E-07	1.54E-06	6.30E-06
FE 1.2	Mitigated domino	2.79E-07	3.68E-08	7.39E-06	5.29E-06	2.93E-05	4.10E-05
FE 2.1	No domino	3.34E-09	4.18E-10	3.76E-10	3.88E-10	1.32E-09	2.58E-09
FE 2.2	No domino	3.01E-08	7.94E-09	7.14E-09	7.37E-09	2.52E-08	1.68E-08
FE 3.1	Mitigated domino	3.07E-06	3.85E-07	7.74E-05	5.54E-05	3.07E-04	1.25E-03
FE 3.2	Mitigated domino	2.76E-05	7.32E-06	1.47E-03	1.05E-03	5.83E-03	8.15E-03
FE 4.1	No domino	3.31E-07	8.31E-08	7.48E-08	7.72E-08	2.64E-07	5.13E-07
FE 4.2	No domino	2.98E-06	1.58E-06	1.42E-06	1.47E-06	5.01E-06	3.34E-06
FE 5.1	Mitigated domino	2.47E-07	3.15E-08	6.34E-06	4.54E-06	6.64E-06	3.36E-05
FE 5.2	Mitigated domino	2.22E-06	5.99E-07	1.20E-04	8.62E-05	1.26E-04	2.19E-04
FE 6.1	No domino	3.88E-08	9.92E-09	8.93E-09	9.21E-09	8.32E-09	2.01E-08
FE 6.2	No domino	3.49E-07	1.89E-07	1.70E-07	1.75E-07	1.58E-07	1.30E-07
FE 7.1	Mitigated domino	2.44E-05	6.28E-06	1.26E-03	9.03E-04	1.32E-03	6.69E-03
FE 7.2	Mitigated domino	2.20E-04	1.19E-04	2.40E-02	1.72E-02	2.51E-02	4.35E-02
FE 8.1	No domino	3.84E-06	1.97E-06	1.78E-06	1.83E-06	1.66E-06	3.99E-06
FE 8.2	No domino	3.46E-05	3.75E-05	3.38E-05	3.48E-05	3.15E-05	2.59E-05

The results of probability adapting referred to all final states, with have been reported in Table 5. 43. The final events consequences have been obtained by keeping the top event probability equal to one and by inserting escalation probabilities values externally from the network, as discussed in Section 5.3.3.3.

Final events (i.e., consequences) probabilities show a general increasing trend over time, due to ASP application, with few exceptions. Most of final states (i.e., FE 1.1, FE 1.2, FE 3.2, FE 5.1,

FE 5.2, FE 7.1, FE 7.2) show an increase, either around two orders of magnitude or three (i.e., FE 3.1) ones in their occurrence probabilities.

Other accidental states reveal just a slight increase in their occurrence probabilities, inferior to one order of magnitude (i.e., FE 4.1, FE 4.2, FE 8.1). Few final accidental states (i.e., FE 2.1, FE 2.2, FE 6.1, FE 6.2, FE 8.2) show a slight decrease of their probabilities, inferior to one order of magnitude. It should be noted that, despite ASP refer only to 4 possible final states, all the consequences are dynamically revised over time, even those for whom no information is available, that are often the most severe ones (e.g., FE 1.1 - unmitigated domino in the case study).

The results of Bayesian adapting for selected final states, which includes the top four most probable ones in the initial Bayesian Network configuration at Year 0 (i.e., the final states to whom ASPs are referred – FE 3.2, FE 7.1, FE 7.2, FE 8.2) and the most severe final state (i.e., FE 1.1) are reported in Figure 5. 47. For instance, even though FE 1.1 has not been observed until the end of observation time, which equals 5 years in the case study, its probability has increased by two orders of magnitude at the end of the fifth year.

The probability of the consequence node being in the $Safe$ state is equal to zero throughout the time interval considered in the case study, due to the assumption of unitary top event probability of occurrence.

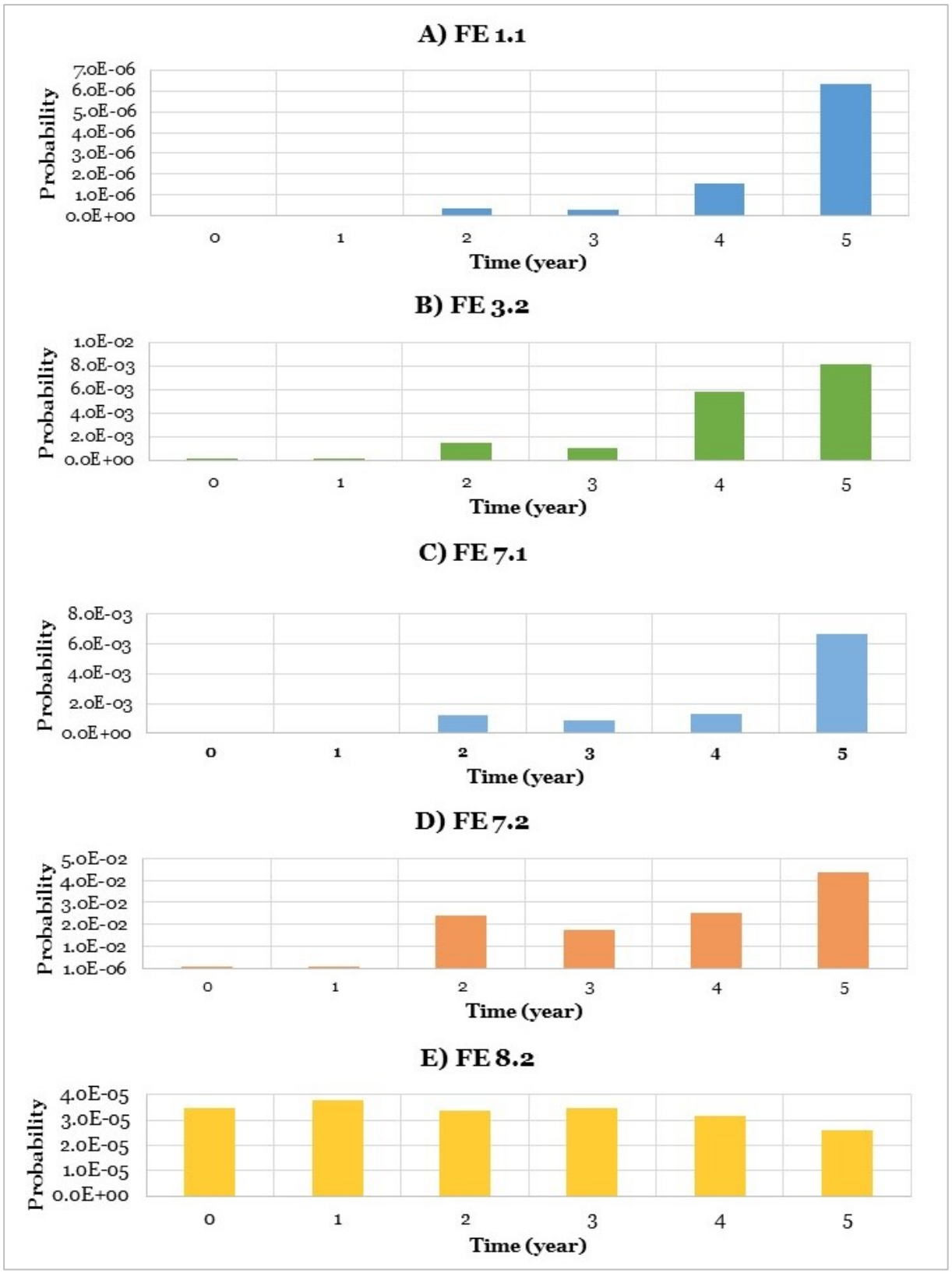


Figure 5. 47 Final events probabilities for selected final accidental states obtained by means of Bayesian Networks, with Bayesian adapting application over five years of operational experience. From the top to the bottom: A) FE 1.1 regarding unmitigated domino; B) FE 3.2; C) FE 7.1; D) FE 7.2 and E) FE 8.2. The latter four final events are the ones associated with ASPs.

Then, final events probabilities referred to the same year are grouped into the three mentioned final events categories: no domino, mitigated domino and unmitigated domino. The dynamic evolution over time of the occurrence probability for each final event category is available in Figure 5. 48. The results reveal that mitigated domino and unmitigated domino categories have a significant increase of two orders of magnitude. On the other hand, no domino category shows a slight decrease of occurrence probability over time.

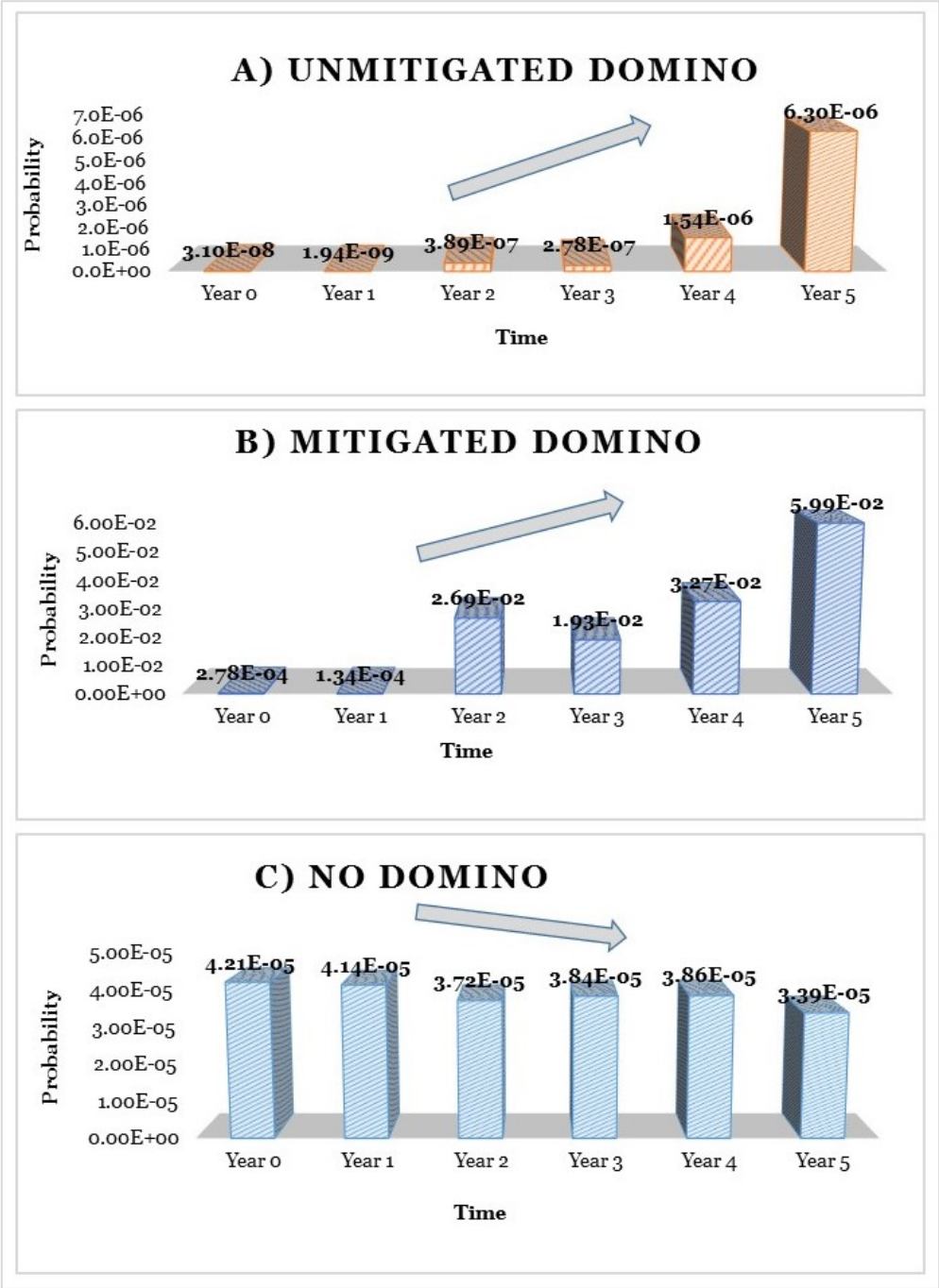


Figure 5. 48 Final events categories probabilities results, referred to fire escalation, obtained by means of Bayesian Network, applying Bayesian adapting over five years of operational experience. From the top to the bottom: A) Unmitigated domino probabilities; B) Mitigated domino probabilities and C) No domino probabilities.

In Figure 5. 49 the percentage relative compositions of final events categories for each year considered in the Bayesian adapting application (i.e., from Year 0 to Year 5) are reported.

The results confirm that final events categories compositions vary over time after the introduction of ASPs.

For instance, no domino probability is significant at Year 0 (i.e., with no additional information), but it turns into a very low value starting from Year 2; this trend confirms the decrease of the absolute values displayed in Figure 5. 48. Consequently, the relative percentage of mitigated domino category tend to increase over time and from Year 2 it overcomes 99%, becoming very predominant, according to the absolute value increase displayed in Figure 5. 48.

Indeed, it should be remarked that, even if unmitigated domino category assumes an irrelevant percentage value throughout the operational time considered (Figure 5. 49), the increase of its absolute value of almost two orders of magnitude, displayed in Figure 5. 48, joined with its severity, makes the consideration of this final event category significant.

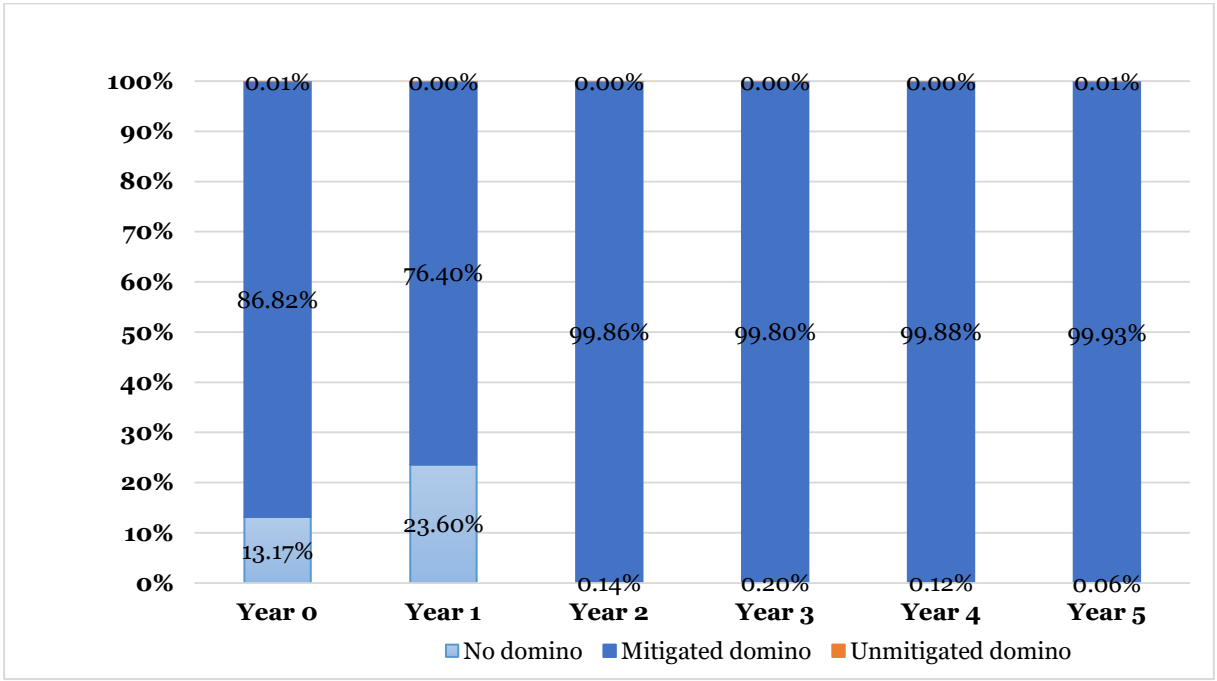


Figure 5. 49 Percentage relative compositions of final events categories obtained from Bayesian adapting over five years of experience. From each year, the categories are: A) Unmitigated domino; B) Mitigated domino and C) No domino.

5.3.3.5 Discussion and conclusions on the case study

The present application has been aimed at implementing a Bayesian approach to safety barriers performance assessment, by means of Bayesian Networks, starting from a conventional Event-Tree based approach and applying them to the same case study in purpose to compare the results. The case study refers to the prevention of fire escalation into a cascading event (i.e., domino accident), which can be prevented by the action of four active, passive and procedural safety barriers, pertinent for the reference installation.

The conversion of an Event-Tree for escalation assessment into a Bayesian Network has been performed, highlighting equal ability to consider the escalation pathway. Indeed, the mapping process has highlighted the advantages of Bayesian Networks application, in terms of enhanced flexibility and dynamic system representation. Safety barriers performance have been assessed by means of specific gates (i.e., type A and C), depending on barriers states and classification, combining availability and effectiveness. Indeed, the present case study provides validation for the application of these specific gates within a Bayesian framework, as it represents their first application within a Bayesian Network. The application of specific gates for the assessment of safety barriers performance proved definitively to be useful in purpose to avoid performance overestimation and to provide a more accurate risk picture.

Escalation probabilities as well as sixteen final accidental states have been considered in the case study and grouped into three severity categories related to the possible final states (i.e., no domino, mitigated/delayed domino and unmitigated domino); this allows a more effective visualization of domino probabilities over time than the application of final accidental states.

Bayesian Analysis has been applied in order to demonstrate the superior flexibility of this technique in comparison with Event-Tree and to explore its features in safety barriers performance evaluation with respect to the prevention and mitigation of domino escalation. Two different approaches to Bayesian Analysis have been applied, in order to dynamically revise probabilities: probability updating and probability adapting. In probability updating to the case study, the information about the occurrence of a final accidental state is used as evidence; its main application is the determination of the most critical sequence of events, in order to revise safety barriers consequently.

However, as highlighted by the results, the most significant feature of Bayesian Network is the application of probability adapting technique that allows revising dynamically safety barriers performance and final events probability over time, as a function of additional information in the form of Accident Sequence Precursors added to the net. The results of the case study demonstrates that probability adapting is a useful technique to replace generic prior probabilities (i.e., generic reliability data) with more case-specific posterior probabilities, resulting in a dynamic assessment of safety barriers performance and a more reliable

prediction of final events, with reference to the prevention and mitigation of fire escalation into a cascading event. Indeed final events categories probabilities have been dynamically revised over time, demonstrating that additional information revise significantly both their absolute values and their relative percentage compositions, giving a more realistic and exhaustive picture of the possible escalation of the accident into a cascading event, and allowing to perform consequently custom-made revision of safety barriers.

Therefore, the case study proved the feasibility of Bayesian Networks application to safety barriers performance assessment with respect to accident escalation into a cascading event.

This advanced application allows obtaining detailed and updated information regarding safety barriers technical performance, to be inserted within the risk evaluation step of QRA, in the extended version that includes external hazard factors (i.e., domino accidents).

However, the present application considers just a simplified two-tank process plant layout and one top event, whose probability was assumed unitary, in purpose to focus on safety barriers and final events. Further applications should extend safety barriers performance assessment to domino accident analysis by means of Bayesian Networks, considering process tank farms, occurrence probabilities of the top event(s), eventual synergistic effects and several domino levels.

5.3.4 Application of Bayesian Networks to domino accident analysis including safety measures performance for a simplified tank farm

5.3.4.1 Definition of the case study

The present case study applies domino accident analysis by means of Bayesian Networks for a simplified tank farm. The original application is aimed at extending safety barriers performance assessment by means of Bayesian Networks to domino accident analysis, filling the research gap identified in Section 3.5.1.2.

The case study has been developed in three sequential steps.

The starting point for the case study (i.e., named step 1 thoughout Section 5.3.4) is an existing application of domino accident analysis by means of BNs (Khakzad et al., 2013d), which applied an innovative methodology for domino accident propagation (see Section 3.3.2.1.3.4), with no safety barriers included in the modelling phase. The existing application is reproduced as the starting point for further implementations.

In step 2, which is an original application, safety barriers are introduced in domino accident analysis by means of BNs. Domino accident analysis is performed according to the same

methodology of the previous step. The safety barriers to be accounted are pertinent for the reference installation, according to the classification presented in Section 3.3.2.1.2, but their performance is evaluated with a standard approach based solely on availability.

In the step 3, safety barriers are included in domino accident analysis by means of BNs. Domino accident analysis is performed according to the same methodology of step 1) and 2). The safety barriers to be accounted are pertinent for the reference installation (i.e., the same ones applied in the previous step), but safety barriers performance is improved by applying specific gates accounting availability and effectiveness and depending on barriers classification (see Section 3.3.2.1.2 for further information on logic gates).

The inputs data applied for the case study are adapted from Khakzad et al. (Khakzad et al., 2013d), in purpose to provide a sound comparison between the original application (with safety barriers included) and the starting point (where safety barriers are neglected). The installation to be considered is a simplified tank farm, where the possible cascading event is a domino accident triggered by fire. The following inputs regarding the tank farm, shared among all modelling steps of the case study, are reported:

- The tank farm includes 3 atmospheric storage tanks (*T1, T2* and *T3*);
- *T1* is selected as primary unit; $P(Fire) = 1.00 \cdot 10^{-5}$;
- One Top-event (Fire) is included; heat radiation is the solely escalation vector;
- *DL1, DL2* indicates respectively the probability of first and second level domino obtained with AND gates, according to the procedure of Section 3.3.2.1.3.4;
- Escalation probabilities are embedded in the Conditional Probability Table (CPTs) of each tank (*T1,T2* and *T3*), according to the procedure of Section 3.3.2.1.3.4;

Further explanations on these assumptions are available below. The layout of the simplified tank farm is reported in Figure 5. 50; a description of tanks characteristics is available in Table 5. 44.

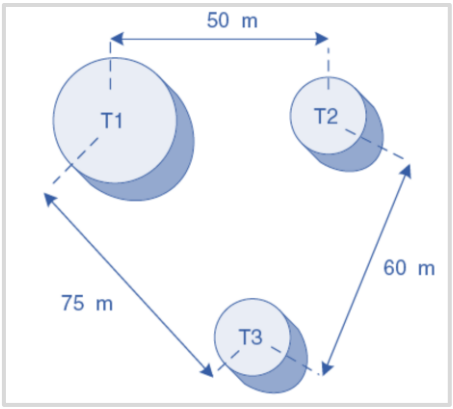


Figure 5. 50 Layout of the simplified tank farm, adapted from Khakzad et al. (Khakzad et al., 2013d).

Table 5. 44 Vessels characteristics for the simplified tank farm case study, adapted from Khakzad et al. (Khakzad et al., 2013d).

Vessel	Type	Substance	Content (t)	Accident scenario	Primary probability	Escalation vector
T1	Atmospheric	Gasoline	500	Pool fire	1.00E-05	Heat radiation
T2	Atmospheric	Xylene	200	Pool fire	1.00E-05	Heat radiation
T3	Atmospheric	Gasoline	200	Pool fire	1.00E-05	Heat radiation

To determine the possible secondary units, the intensity of heat radiation received by *T2* and *T3* in the case of a PF in *T1* is calculated (Table 5.45). As can be seen, *T2* is more likely to be the secondary unit impacted by *T1*. Accordingly, in the corresponding BN, a causal arc should directed from node *T1* to node *T2* (Figure 5. 51). *T3* did not exceed the threshold criteria; but, considering the synergistic effect of *T1* and *T2*, it can be seen that the total heat radiation received by *T3* because of both *T1* and *T2* would be sufficiently above the threshold value to damage *T3*. Therefore, in BN configuration *T3* should receive two arcs, both from *T2* and *T1*.

DL0 overlaps with the primary event. Nodes *DL1* and *DL2*, representing first level and second level domino should be added to the network. To account for the first level domino effect, *DL1* is connected to the primary unit *T1* and the secondary unit *T2* and the CPT is filled with an AND gate. Similarly, to consider the second level domino effect, *DL2* is connected to the first-level domino effect node *DL1* and the tertiary unit *T3* with an AND gate.

Table 5. 45 Data for escalation probabilities (P_d) calculations for the simplified tank farm, adapted from (Khakzad et al., 2013d).

Data for calculation of escalation probabilities				
Ref.	**Heat Load (kW/m²)**	**ttf (s)**	**Probit (Y)**	**Escalation Probability (P_d)**
$P(T_2 \mid T_1)$	19.3	686.37	0.4764	3.041E-06
$P(T_3 \mid T_1, T_2)$	17.6	762.15	0.2830	1.197E-06
Data for time to failure calculation (ttf)				
Volume of *T2* (m^3)	247	Volume of *T3* (m^3)	220	
c	$-2.667 \cdot 10^{-5}$			
d	1			
e	-1.13			
f	9.877			
Probit coefficients for probit calculation (Y)				
a	12.54			
b	-1.847			

Preliminary calculations allows defining escalation probabilities, according to the procedure reported in Section 3.3.2.1.3.4; the data are reported in Table 5. 45. Time to failure calculation is carried out according to equation (3.9); escalation Probit calculation for heat radiation is carried out according to equation (3.2) with the Probit coefficients presented in Table 5. 45; the calculation of associated escalation probability is obtained by the application of normal standard distribution (equation (3.4)).

5.3.4.2 Application of Bayesian Networks to domino accident analysis without safety measures

In modelling step 1), which is adapted from Khakzad et al. (Khakzad et al., 2013d), safety barriers are not included in domino accident analysis, which is performed according to the methodology of Section 3.3.2.1.3.4. Bayesian Network is constructed using Hugin Software version 8.1 (Hugin, 2016); a qualitative representation of the net is available in Figure 5.51, the inputs and reasoning that lead to the accident propagation modelling are listed in the previous subsection.

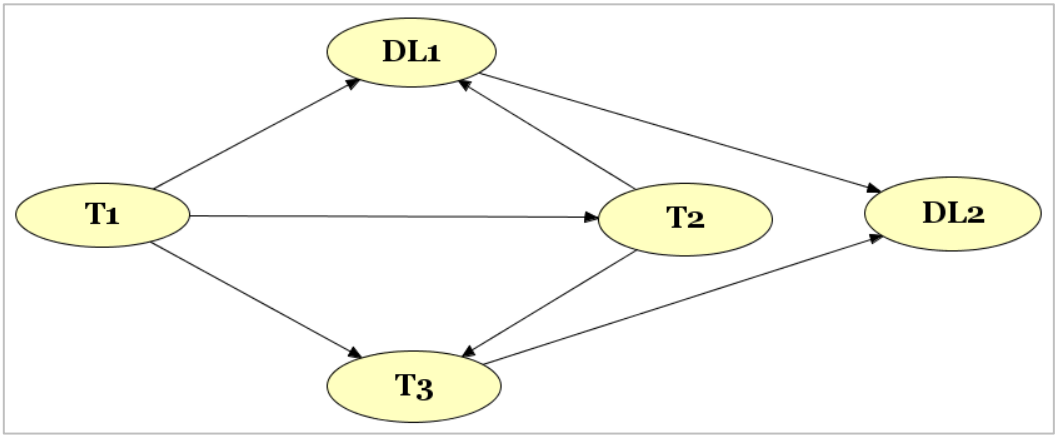


Figure 5. 51 Bayesian Network for domino accident analysis in a simplified tank farm with no safety barriers included in the analysis (modelling Step 1), adapted from Khakzad et al. (Khakzad et al., 2013b).

Table 5. 46 Results of Bayesian Network for domino accident analysis in a simplified tank farm with no safety barriers included in the analysis (modelling Step 1).

Results (probabilities)	
Modelling step 1	**No safety barriers**
T1	1.00E-05
T2	3.041E-11
T3	3.640E-17
DL0	1.00E-05
DL1	3.041E-11
DL2	3.640E-17

The outputs of the net obtained from modelling step 1), which consist on tank accident probabilities (i.e., *T1, T2, T3*) and domino level probabilities (i.e., *DL0*, *DL1* and *DL2*) are available in Table 5.46. It should be noted that modelling step 1) demonstrate the usefuleness and ease of application of Bayesian Network aplication to domino accident modelling, at least with reference to a simplified plant layout. Neverthless, step 1) provide only a baseline situation for further implementations, as cascading events realistic representation demands for introduction of safety barriers in the modelling phase.

5.3.4.3 Application of safety measures performance assessment to domino accident analysis by means of Bayesian Networks

According to modelling step 2) and 3) an extension of the previous case study with introduction of pertinent safety barriers on each tank is provided, obtaining therefore two original applications of domino accident analysis with Bayesian Networks, filling the research gaps identified in Section 5.1.1.2. The accident propagation and the input data are the same ones applied in the previous section.

Safety barriers pertinent for the reference installation are defined, based on the approach presented in Section 3.3.2.1.2. As the installation is considered RI Type 1, the presence of 3 safety barriers on each tank is accounted. They are respectively: sprinkler (*Sprinkler_TX*), PSV (*PSV_TX*) and emergency team intervention (*Em_Team_TX*), represented by three nodes in BNs modelling, which are connected as child node of *TX* with $X = \{1,2,3\}$; each safety barrier has a binary behavior (i.e., fail/work). A consequence node is defined for each tank (*Cons_TX*), according to an AND - gate, as displayed in previous safety barriers performance assessment by means of BNs (e.g., see Section 5.3.2 and 5.3.3). According to the configuration of the case study (i.e., one top event, three safety barriers on each tank), the consequence node on each tank accounts for 8 accidental states plus state Safe, as displayed in Table 5. 47.

Table 5. 47 Safety barriers states for each resulting final accidental state, for a generic tank X of the simplified tank farm.

Consequence ID - Tank X	**Safety barrier ID_TX**		
	Sprinkler_TX	**PSV_TX**	**Em_team_TX**
CTX_1	fail	fail	fail
CTX_2	fail	fail	work
CTX_3	fail	work	fail
CTX_4	fail	work	work
CTX_5	work	fail	fail
CTX_6	work	fail	work
CTX_7	work	work	fail
CTX_8	work	work	work

The escalation occurs only when all the barriers on a tank are not working, according to the approximation taken from Landucci et al. (Landucci et al., 2015a). In this situation, the consequence node is in state *CTX1* (Table 5. 47)); this is represented in the net by an additional node (*WCons_TX*) on each tank, which is a child node of the respective consequence node. Therefore, *WCons_TX* node represents the "reduced" accident probability on each tank, due to the introduction of safety barriers. Indeed, *WCons_TX* , which has a binary behavior (i.e., accident/safe), should concour to the determination of domino level probabilities in modelling steps 2) and 3). The methodology for domino accident modelling displayed in Section 3.3.2.1.3.4, and previously applied in modelling step 1) has been applied also in these modelling steps; the introduction of safety barriers did not modified the accident propagation pattern. Therefore, *WCons_TX* is linked to the following tanks considering the same propagation pattern as in modelling step 1).With reference to the specific case plant layout, for example *WCons_T1* is connected to *T2*, *WCons_T2* is connected to *T3* and *WCons_T1* is connected to *T3*. Instead of considering the unprotected tank accident probability *TX, WCons_TX* is considered to define domino level probabilities. For example, the probability of a first level domino (*DL*1) is obtained from an AND gate of *WCons_T1* and *WCons_T2*; the probability of a second level domino (*DL*2) is obtained from an AND gate of *WCons_T3* and *DL*1. *DLO* overlaps with *WCons_T1*.

Table 5. 48 Input data for the inclusion of safety barriers performance assessment within domino accident analysis by means of Bayesian Networks. Data retrieved from a data repository (Landucci et al., 2015a).

Safety barrier ID	Safety barrier description	Input data for modelling step 2		Input data for modelling step 3	
Sprinkler	Foam water sprinkler system with electric actuation	Availability	2.00E-03	Gate Type	B
				Availability	5.39E-03
				Effectiveness (η)	0.954
PSV	Pressure safety valve	Availability	1.00E-02	Gate Type	A
				Availability	1.00E-02
				Effectiveness (η)	1
Em.Team	Emergency team intervention	Availability	1.00E-01	Gate Type	C
				Availability	1.00E-01
				Effectiveness (η)	1

With regards to Bayesian Network modelling, in modelling steps 2) and 3), two approaches to safety barriers performance assessement are considered:

2) Only availability, expressed by the probability of failure on demand (i.e., PFD), is accounted to represent safety barriers performance. Availability values for safety barriers on each tank are taken from a standard reference and reported in Table 5. 48.
3) The performance of safety barriers has been accounted by means of the three typologies of specific gates described in Section 3.3.2.1.2, which combine availability and

effectiveness. Therefore, the performance of safety barriers on each tank (i.e., *Sprinkler_TX, PSV_TX, Em_Team_TX*) is the output of a logic gate, whose inputs are the nodes regarding the availability of each barrier (*Av_Spr_TX, Av_PSV_TX, Av_Emt_TX)* and the respective effectiveness (*Eff_Spr_TX, Eff_PSV_TX, Eff_Emt_TX)*. Input data are reported in Table 5. 48. This approach allows avoiding over conservative assumptions regarding safety barriers performance, according to the concepts discussed in Section 3.3.2.1.2.

5.3.4.4 Results of the case study

The results obtained from modelling step 2) are reported below; the qualitative part of BN, obtained with Hugin software 8.1 (Hugin, 2016) is reported in Figure 5. 52; the outputs of the net, obtained from Bayesian Network analysis, are available in Table 5. 49.

According to modelling step 2), for each tank of the tank farm ($X = \{1,2,3\}$);, the following results have been reported in Table 5. 49:

- Safety barriers performance probabilities, referred to failure state (i.e., *Sprinkler_TX, PSV_TX, Em_Team_TX*);
- Tank node probabilities (*TX*);
- Consequence node probabilities *(Cons_TX)*, specifying the one possibly leading to further escalation *(WCons_TX)*;
- Domino probabilities *(DLO, DL1, DL2)*.

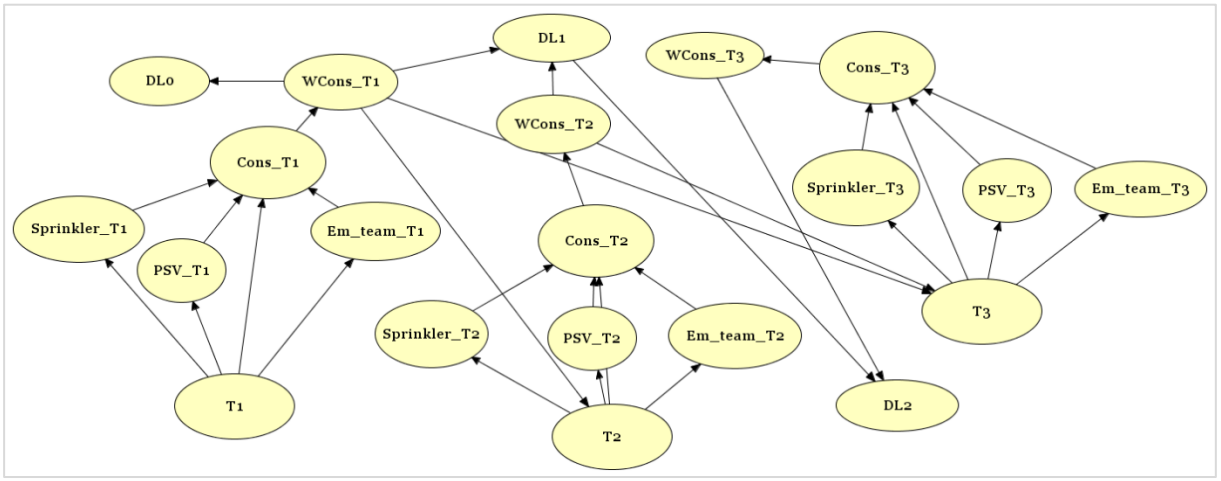


Figure 5. 52 Bayesian Network for domino accident analysis in a simplified tank farm with safety barriers included in the analysis. Their performance is evaluated with a standard approach, based solely on availability (modelling Step 2).

Table 5. 49 Results of Bayesian Network for domino accident analysis in a simplified tank farm with safety barriers included in the analysis. Their performance is evaluated with a standard approach, based solely on availability (modelling Step 2). All the results are referred to accidental/failure state.

Symbol	***Tank X (X=1,2,3)***		
	X=1	***X=2***	***X=3***
TX	1.000E-05	6.082E-17	1.456E-28
Sprinkler_TX	2.000E-08	1.216E-19	2.912E-31
PSV_TX	1.000E-07	6.082E-19	1.456E-30
Em_team_TX	1.000E-06	6.082E-18	1.456E-29
Cons_TX	***X=1***	***X=2***	***X=3***
CTX_1	2.000E-11	1.216E-22	2.912E-34
CTX_2	1.800E-10	1.095E-21	2.621E-33
CTX_3	1.980E-09	1.204E-20	2.883E-32
CTX_4	1.782E-08	1.084E-19	2.595E-31
CTX_5	9.980E-09	6.070E-20	1.453E-31
CTX_6	8.982E-08	5.463E-19	1.308E-30
CTX_7	9.880E-07	6.009E-18	1.439E-29
CTX_8	8.892E-06	5.408E-17	1.295E-28
WCons_TX	2.000E-11	1.216E-22	2.912E-34
Domino probability			
DLo	2.000E-11		
DL1	1.216E-22		
DL2	2.912E-34		

The results obtained from modelling step 3) are reported below; the qualitative part of BN, obtained with Hugin software 8.1 (Hugin, 2016) is reported in Figure 5. 53; the outputs of the net, obtained from Bayesian Network analysis, are available in Table 5. 50.

According to modelling step 2), for each tank of the tank farm ($X = \{1,2,3\}$);, the following results have been reported in Table 5. 50:

- Safety barriers nodes performance probabilities, referred to failure state – OUT 1 (i.e., *Sprinkler_TX, PSV_TX, Em_Team_TX*);
- Tank node probabilities (*TX*);
- Consequence node probabilities *(Cons_TX)*, specifying the one possibly leading to further escalation *(Cons_TX)*;
- Domino probabilities *(DLO, DL1, DL2)*.

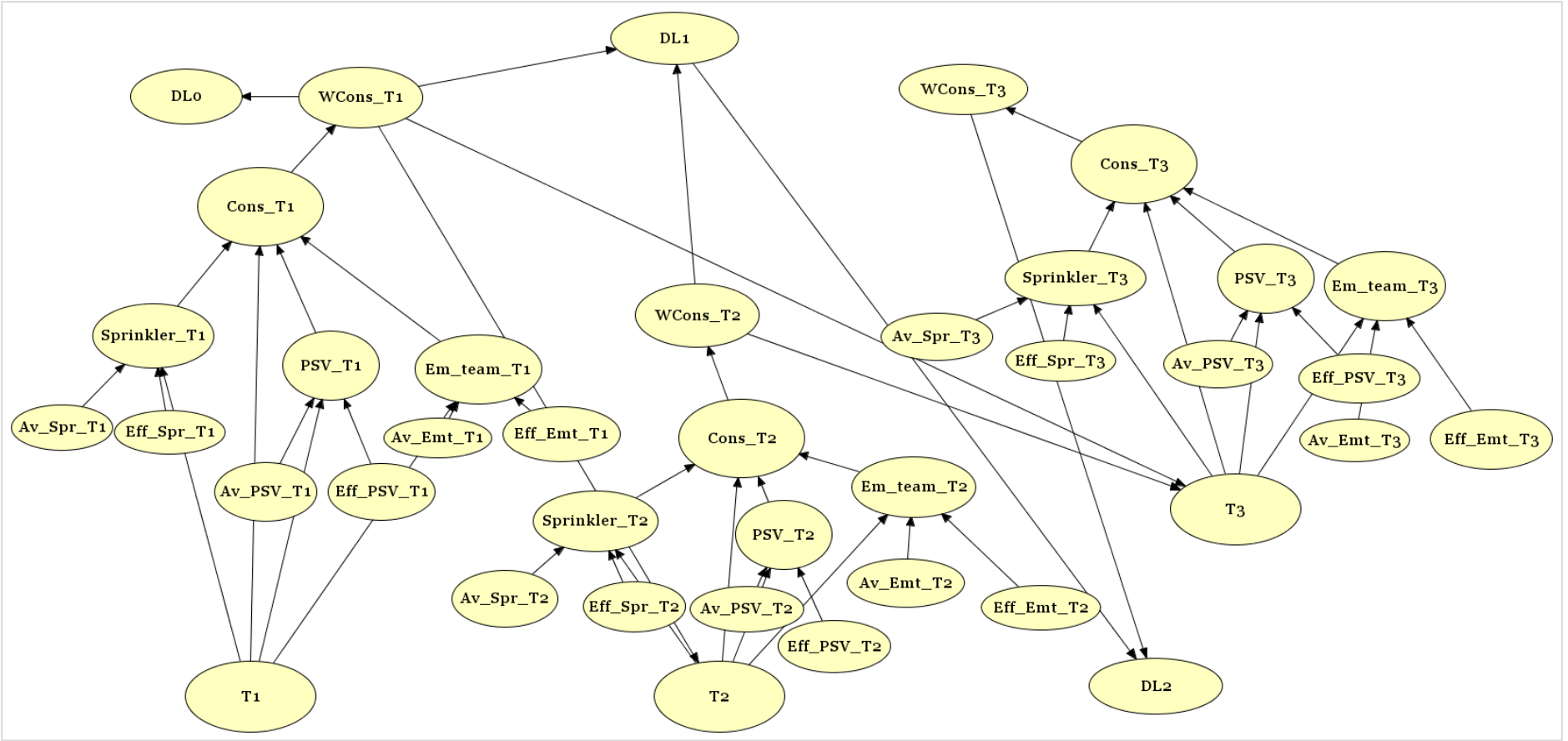


Figure 5. 53 Bayesian Network for domino accident analysis in a simplified tank farm with safety barriers included in the analysis. Their performances are evaluated with specific gates, based on availability and effectiveness (modelling Step 3).

Table 5. 50 Results of Bayesian Network for domino accident analysis in a simplified tank farm with safety barriers included in the analysis. Their performances are evaluated with specific gates, based on availability and effectiveness (modelling Step 3). All the results refer to accident/failure state (i.e., OUT1).

Symbol	***Tank X (X=1,2,3)***		
	X=1	***X=2***	***X=3***
TX	1.000E-05	1.555E-15	9.521E-26
Sprinkler_TX	5.114E-07	7.954E-17	4.869E-27
PSV_TX	1.000E-07	1.555E-17	9.521E-28
Em_team_TX	1.000E-06	1.555E-16	9.521E-27
Cons_TX	***X=1***	***X=2***	***X=3***
CTX_1	5.114E-10	7.954E-20	4.869E-30
CTX_2	4.603E-09	7.158E-19	4.382E-29
CTX_3	5.063E-08	7.874E-18	4.820E-28
CTX_4	4.557E-07	7.087E-17	4.338E-27
CTX_5	9.489E-09	1.476E-18	9.034E-29
CTX_6	8.540E-08	1.328E-17	8.130E-28
CTX_7	9.394E-07	1.461E-16	8.943E-27
CTX_8	8.454E-06	1.315E-15	8.049E-26
WCons_TX	5.114E-10	7.954E-20	4.869E-30
Domino probabilities			
DLo	5.114E-10		
DL1	7.954E-20		
DL2	4.869E-30		

As seen in previous case studies, one of the advantage of Bayesian Networks is the possibility to revise probabilities, due to new evidencies. Therefore, the application of a probability revising technique is carried out to the net obtained from modelling step 3), in purpose to identify weak links leading to a specific final accidental state, for instance *WCons_T2*. The evidence of *WCons_T2* in accidental state is inserted in the net, and the sum propagation normal tool is applied to compile the net. The results, reported in Table 5. 51, show posterior probabilities for each tank of the tank farm ($X = \{1,2,3\}$), in particular:

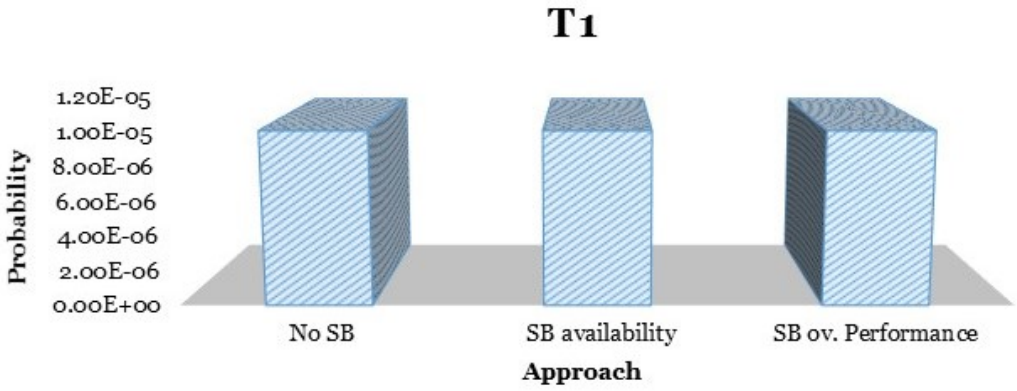
- Tank node probabilities (*TX*);
- Consequence node probabilities *(Cons_TX)*, specifying the one possibly leading to further escalation *(WCons_TX)*;
- Domino probabilities *(DLO, DL1, DL2)*.

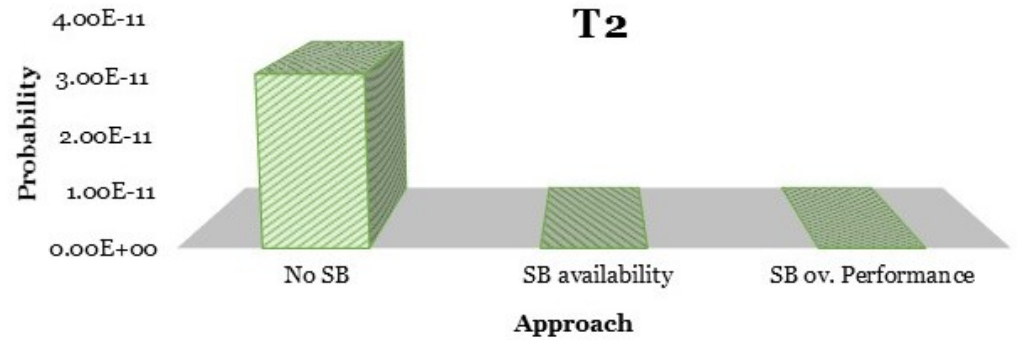
Table 5. 51 Results of Bayesian probability revision for domino accident analysis in a simplified tank farm with safety barriers included in the analysis. The evidence of *WCons_T2* is inserted in the net, obtained according to modelling Step 3). All the results refer to accident/failure state.

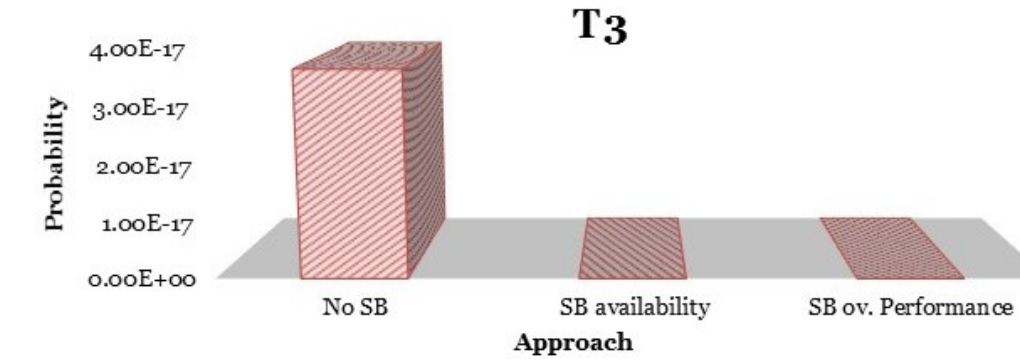
Symbol	***Tank X (X=1,2,3)***		
	X=1	***X=2***	***X=3***
TX	1	1	1.197E-06
Sprinkler_TX	1	1	6.122E-08
PSV_TX	1	1	1.197E-08
Em_team_TX	1	1	1.197E-07
Cons_TX	***X=1***	***X=2***	***X=3***
CTX_1	1	1	6.122E-11
CTX_2	0	0	5.510E-10
CTX_3	0	0	6.060E-09
CTX_4	0	0	5.454E-08
CTX_5	0	0	1.136E-09
CTX_6	0	0	1.022E-08
CTX_7	0	0	1.124E-07
CTX_8	0	0	1.012E-06
WCons_TX	1	1	6.122E-11
Domino probability			
DL0	1		
DL1	1		
DL2	6.122E-11		

However, it should be noted that the application of probability revising techniques, which are very useful with respect to major accident scenarios and generally rather simple case studies, might be not the most significant advantage of domino accident analysis by means of Bayesian Network, due to the scarcity of accidental data to be applied.

On the other hand, it might be relevant to carry out a comparison of the results, obtained from modelling steps 1), 2) and 3), in purpose to evaluate the effect of safety barriers introduction within modelling phase. For each tank of the tank farm ($X = \{1,2,3\}$), the results referred to tank accident probabilities *(TX)* according to the three different modelling steps have been reported in Figure 5. 54. For instance, the ratio between tank accident probability in modelling step 3) and 1) clearly shows a reduction up to 9 orders of magnitude. The gap tends to be very significant in the last unit affected by domino effect (i.e., *T3*). Therefore, modelling step 3), which includes a complete approach to safety barriers performance assessment, is able to represent the systems in detailed way, avoiding overestimation of accident probabilities.

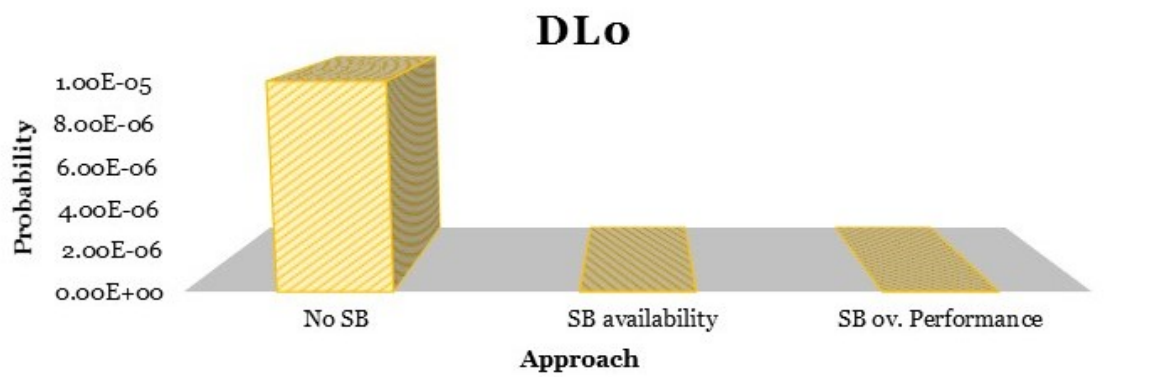


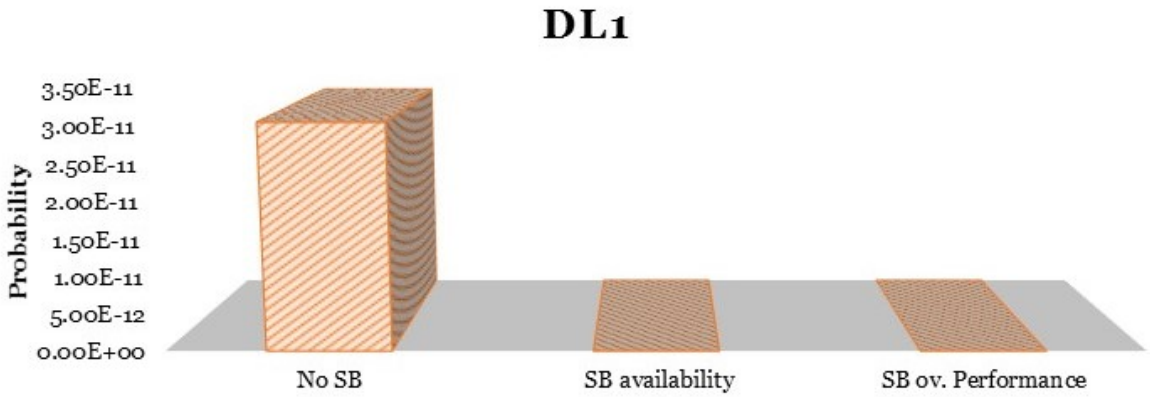


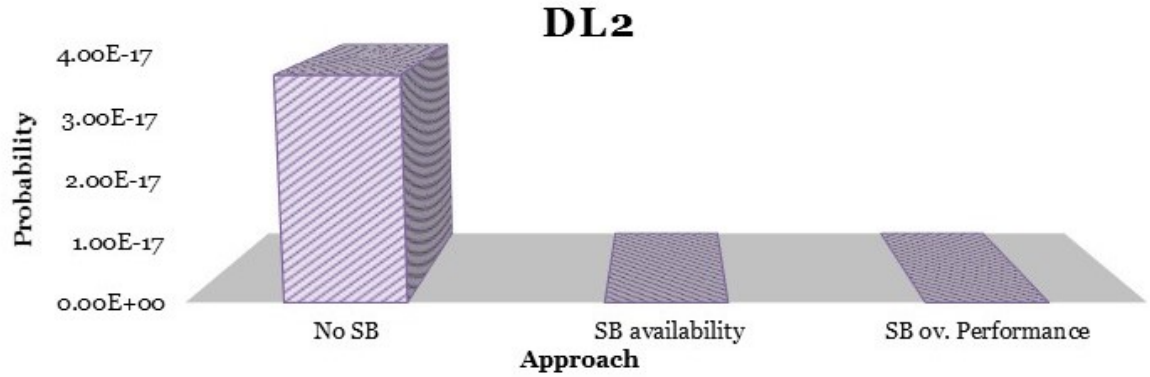


Modelling step/approach				
	1	*2*	*3*	
Tank ID	**No SB**	**SB availability**	**SB ov. Performance**	**Ratio step 3 vs 1**
T1	1.000E-05	1.000E-05	1.000E-05	1
T2	3.041E-11	6.082E-17	1.555E-15	5.114E-05
T3	3.640E-17	1.456E-28	9.521E-26	2.616E-09

Figure 5. 54 Comparison of tank probabilities (*T1*, *T2* and *T3*) obtained from domino accident analysis by means of Bayesian Networks, following different modelling steps/approaches: 1) No safety barriers (i.e., SB); 2) safety barriers performance expressed by availability only; 3) safety barriers overall performance, expressed by specific gates accounting availability and effectiveness.







Modelling step/approach				
	1	*2*	*3*	
Domino level	**No SB**	**SB availability**	**SB ov. Performance**	**Ratio step 3 vs 1**
DLo	1.00E-05	2.000E-11	5.114E-10	5.114E-05
DL1	3.04E-11	1.216E-22	7.954E-20	2.616E-09
DL2	3.64E-17	2.912E-34	4.869E-30	1.338E-13

Figure 5. 55 Comparison of domino probabilities (*DLo*, *DL1* and *DL2*) obtained from domino accident analysis by means of Bayesian Networks, following different modelling steps/approaches: 1) No safety barriers (i.e., SB); 2) safety barriers performance expressed by availability only; 3) safety barriers overall performance, expressed by specific gates accounting availability and effectiveness.

Domino probabilities at different levels *(DLO, DL1, DL2)* have been reported separately for the three modelling steps in Figure 5. 55: without Safety Barriers (step 1), with safety barriers (only availability considered, according to step 2) and with safety barriers overall performance (i.e., combination of availability and effectiveness, according to step 3). The ratio between modelling steps 3) and 1) shows a reduction from 5 to 13 order of magnitude in domino probabilities after the introduction of safety barriers, confirming that safety barriers introduction within domino accident modelling provides a more realistic framework for domino effects analysis.

5.3.4.5 Discussion and conclusions on the case study

The present application has been aimed at implementing safety barriers performance assessment, by means of Bayesian Networks, to domino accident analysis. The case study refers to the prevention of fire escalation into a cascading event (i.e., domino accident), considering a simplified tank farm of three tanks and one top event. The methodology for the definition of domino accident modelling by means of BNs has been recently defined, but none of existing applications accounted for safety barriers within the modelling phase. Therefore, the present original case study was aimed at filling this research gap, by introducing safety barriers in the modelling phase and comparing the so obtained results.

Safety barriers of different typologies (i.e., active, passive and procedural ones) have been introduced in the modelling phase on each tank of the tank farm; their performances have been assessed both by standard approach and by means of specific gates (i.e., type A, B and C), depending on barriers states and classification, combining availability and effectiveness. The application of specific gates for the assessment of safety barriers performance proved definitively to be useful in purpose to avoid performance overestimation and to provide a more accurate risk picture within domino effect modelling and prevention.

Indeed, the results of the case study demonstrated a decrease of several order of magnitude of domino probabilities at different levels after the introduction of safety barriers within the modelling phase. Therefore domino accident analysis, performed by means of an advanced technique as Bayesian Networks, joined with safety barriers performance assessment may be able to model realistically severe accidental scenarios and cascading events triggered by external hazard factors (i.e., domino effect triggered by fire). The information obtained by domino accident modelling may offer a more accurate risk picture, avoiding overestimation of accident probabilities, within the framework of QRA extension to external hazard factor, with specific reference to domino effect.

However, the case study deals with a simplified tank farm, with few units and just one top event. Therefore, the inclusion of safety barriers performance assessment within domino accident analysis by means of Bayesian Networks should be tested to complex systems,

considering for instance realistic tank farm, with multiple top events, synergistic effects and a congruous number of units and domino levels.

5.3.5 Application of Bayesian Networks to domino accident analysis including safety measures performance for a realistic tank farm

5.3.5.1 Definition of the case study

The present case study applies domino accident analysis by means of Bayesian Networks for a realistic tank farm. The original application is aimed at extending safety barriers performance assessment by means of Bayesian Networks to domino accident analysis, filling the research gap identified in Section 3.5.1.2. The case study has been developed in two sequential steps.

The starting point for the case study (i.e., named step 1 thoughout Section 5.3.5) is an existing application of domino accident analysis by means of BNs (Khakzad et al., 2013d), which applied an innovative methodology for domino accident propagation (see Section 3.3.2.1.3.4), with no safety barriers included in the modelling phase. The existing application is reproduced as the starting point for further implementations.

In the step 2, which is an original application, safety barriers are included in domino accident analysis by means of BNs. Domino accident analysis is performed according to the same methodology of step 1). The safety barriers to be accounted are pertinent for the reference installation and their performance is evaluated by applying specific gates accounting availability and effectiveness and depending on barriers classification (see Section 3.3.2.1.2 for further information on the logic gates applied in the case study).

The inputs data applied for the case study are adapted from Khakzad et al. (Khakzad et al., 2013d), in purpose to provide a sound comparison between the original application (with safety barriers included) and the starting point (where safety barriers are neglected). The installation to be considered is a realistic tank farm, where the possible cascading event is a domino accident triggered by fire and overpressure as escalation vectors.

The following inputs regarding the tank farm, shared among all modelling steps of the case study, are reported:

- The tank farm includes 8 atmospheric storage tanks (TX with $X = \{1,2,3 \dots,8\}$), represented by eight nodes;
- *T1* is selected as primary unit;
- Two Top-Events are accounted: Pool Fire (*PF*) and Vapor Cloud Explosion (*VCE*) with probabilities of $1.00 \cdot 10^{-5}$ and $2.00 \cdot 10^{-6}$ respectively;
- Heat radiation and overpressure should be considered as escalation vectors;

- Each unit impacted has the same likelihood to develop a *PF* or a *VCE* (i.e., 0.5);
- *DLO, DL1, DL2* and *DL3* indicate respectively the probability of zero, first, second and third level domino obtained with AND gates, according to the procedure of Section 3.3.2.1.3.4. They have 2 states: Accident and Safe;
- *L1, L2, L3* are auxiliary nodes obtained with OR gates, according to the procedure of Section 3.3.2.1.3.4, to connect all the tanks concurring to same domino level;
- Escalation probabilities are embedded in the Conditional Probability Table of each tank (*TX*) node. Each tank can be in one of these three states: *PF* (i.e., pool fire), *VCE*, *Safe*.

Further explanations on these assumptions are available below. The layout of the realistic tank farm is reported in Figure 5. 56; a description of tanks characteristics is available in Table 5. 52.

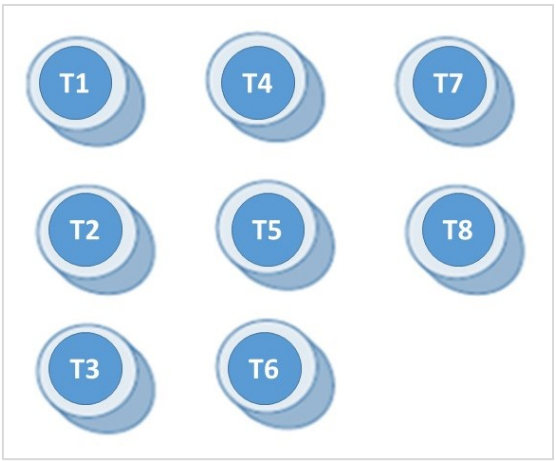


Figure 5. 56 Layout of the realistic tank farm (Khakzad et al., 2013d).

Overpressure and heat radiation escalation vectors are available in the reference (Khakzad et al., 2013d); the threshold values of heat radiation and overpressure are selected respectively as 15 kW/m^2 and 7 kPa for atmospheric storage tanks with fixed roofs. The accident propagation pattern is defined according to the methodology described in Section 3.3.2.1.3.4.

Preliminary calculations aimed at defining escalation probabilities (P_d), corresponding to each value of each escalation vector, according to the procedure reported in Section 3.3.2.1.3.4; the inputs are reported in Table 5. 52.

Regarding heat radiation, the time to failure calculation is carried out according to equation (3.9); then, escalation Probit calculation for heat radiation is carried out according to equation (3.2) with the Probit coefficients presented in Table 5. 52; the calculation of associated escalation probability is obtained by the application of normal standard distribution (equation (3.4)).

Regarding overpressure escalation vector, escalation Probit calculation for overpressure is carried out according to equation (3.3) with the Probit coefficients presented in Table 5. 52; the calculation of associated escalation probability is obtained by the application of normal standard distribution (equation (3.4)).

Because the likely accident scenarios for *T1* are *PF* and *VCE*, *T1* can impact nearby units by means of either heat radiation or overpressure. Based on a comparison among the threshold values and the escalation vectors, *T1* can impact *T2* and *T4* by either heat radiation or overpressure, although it affects *T5* only by overpressure. Thus, *T2* and *T4* are secondary units, which in turn can result in *PF* or *VCE* (with equal likelihood, as described before). Therefore, causal arcs are directed from *T1* to *T2* and *T4*. *T3*, *T5*, and *T7* can be involved in the domino effect as tertiary units. Similarly, units *T6* and *T8* are impacted as quaternary units in the domino effect. Causal arcs are drawn from the parent units to the associated children units, to model accident propagation in the realistic tank farm. The propagation pattern has been maintened in the two modelling steps.

To calculate the domino effect probabilities, auxiliary nodes *L1, L2, L3*, are added to the net, as well as *DL0, DL1, DL2*, and *DL3*. *DL0* overlaps with the primary event. To account for the first level domino effect, *DL1* is connected to the primary unit *T1* and the auxiliary node *L1* with an AND gate. *L1* represents the output of an OR gate between *T2* and *T4*. Then, *L2* auxiliary node is obtained as an OR gate among *T3, T5* and *T7*. *DL2* is connected to the unit *DL1* and the auxiliary node *L2* with an AND gate. Similarly, *L3* auxiliary node is obtained as an OR gate between *T6* and *T8*. *DL3* is connected to the unit *DL2* and the auxiliary node *L3* with an AND gate.

Table 5. 52 Input data for escalation probabilities calculations for the realistic tank farm, adapted from Khakzad et al. (Khakzad et al., 2013d).

Values for ttf calculation	
V (m^3)	2770
c	$-2.667 \cdot 10^{-5}$
d	1
e	-1.13
f	9.877
Probit coefficient for heat radiation	
a	12.54
b	-1.847
Probit coefficient for overpressure	
a	-18.96
b	2.44

The calculated values of escalation probabilities corresponding to the specific values of heat radiation and overpressure considered in the case study are reported in Table 5. 53.

Table 5. 53 Inputs for the calculation of escalation probabilities due to single escalation vectors (i.e., heat radiation and overpressure) for the case study.

A) Calculation of escalation probabilities due to heat radiation			
Heat Load (kW/m^2)	ttf (s)	Probit (Y)	Escalation Probability (P_d)
2.2	7.433E+03	-3.924E+00	2.255E-19
3.6	4.265E+03	-2.898E+00	1.421E-15
4.6	3.235E+03	-2.387E+00	7.511E-14
9.3	1.462E+03	-9.203E-01	1.607E-09
19.3	6.417E+02	6.008E-01	5.432E-06
B) Calculation of escalation probabilities due to overpressure			
Peak overpressure (Pa)		Probit (Y)	Escalation Probability (P_d)
2000		-0.41380	3.085E-08
4000		1.2775	9.862E-05
8000		2.9688	2.112 E-02
10000		3.5132	6.854 E-02

The escalation probabilities derived from the two effects (i.e., heat radiation and overpressure) have been calculated for each tank as reported in Table 5. 54, and then combined in purpose to account synergistic effects.

The Conditional Probability Tables that considers escalation probabilities to be inserted in Bayesian Network modelling (in both steps) have been reported in Table 5. 55, Table 5. 56 and Table 5. 57, for each unit TX with $X = \{1,2,3 \dots ,8\}$. The values of escalation probabilities, have been calculated by noisy OR-gates, considering the synergistic effects of heat radiation and overpressure. The CPTs are the same ones in both modelling steps, as the accident propagation pattern does not vary.

Table 5. 54 Results of escalation probabilities calculation due to heat radiation and overpressure.

Heat radiation - escalation probabilities								
	T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**
T1	0	5.4315E-06	7.5112E-14	5.4315E-06	1.6066E-09	1.4210E-15	7.5112E-14	1.4210E-15
T2	5.4315E-06	0	5.4315E-06	1.6066E-09	5.4315E-06	1.6066E-09	1.4210E-15	7.5112E-14
T3	7.5112E-14	5.4315E-06	0	1.4210E-15	1.6066E-09	5.4315E-06	2.2551E-19	1.4210E-15
T4	5.4315E-06	1.6066E-09	1.4210E-15	0	5.4315E-06	7.5112E-14	5.4315E-06	1.6066E-09
T5	1.6066E-09	5.4315E-06	1.6066E-09	5.4315E-06	0	5.4315E-06	1.6066E-09	5.4315E-06
T6	1.4210E-15	1.6066E-09	5.4315E-06	7.5112E-14	5.4315E-06	0	1.4210E-15	1.6066E-09
T7	7.5112E-14	1.4210E-15	2.2551E-19	5.4315E-06	1.6066E-09	1.4210E-15	0.0000E+00	5.4315E-06
T8	1.4210E-15	7.5112E-14	1.4210E-15	1.6066E-09	5.4315E-06	1.6066E-09	5.4315E-06	0
Overpressure – escalation probabilities								
	T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**
T1	0	6.8538E-02	9.8623E-05	6.8538E-02	2.1115E-02	9.8623E-05	9.8623E-05	9.8623E-05
T2	6.8538E-02	0	6.8538E-02	2.1115E-02	6.8538E-02	2.1115E-02	9.8623E-05	9.8623E-05
T3	9.8623E-05	6.8538E-02	0	9.8623E-05	2.1115E-02	6.8538E-02	3.0851E-08	9.8623E-05
T4	6.8538E-02	2.1115E-02	9.8623E-05	0	6.8538E-02	9.8623E-05	6.8538E-02	2.1115E-02
T5	2.1115E-02	6.8538E-02	2.1115E-02	6.8538E-02	0	6.8538E-02	2.1115E-02	6.8538E-02
T6	9.8623E-05	2.1115E-02	6.8538E-02	9.8623E-05	6.8538E-02	0	9.8623E-05	2.1115E-02
T7	9.8623E-05	9.8623E-05	3.0851E-08	6.8538E-02	2.1115E-02	9.8623E-05	0	6.8538E-02
T8	9.8623E-05	9.8623E-05	9.8623E-05	2.1115E-02	6.8538E-02	2.1115E-02	6.8538E-02	0

Table 5. 55 CPTs for the case study (from T1 to T5).

CPT T1	
PF	1.00E-05
VCE	2.00E-06
Safe	9.9999E-01

CPT T2			
T1	PF	VCE	Safe
PF	2.71577E-06	0.034268925	0
VCE	2.71577E-06	0.034268925	0
Safe	9.9999E-01	9.3146E-01	1

CPT T3			
T2	PF	VCE	Safe
PF	2.71577E-06	0.034268925	0
VCE	2.71577E-06	0.034268925	0
Safe	9.9999E-01	9.3146E-01	1

CPT T4			
T1	PF	VCE	Safe
PF	2.71577E-06	0.034268925	0
VCE	2.71577E-06	0.034268925	0
Safe	9.9999E-01	9.3146E-01	1

CPT T5									
T4	PF								
T2	PF			VCE			Safe		
T1	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	5.4323E-06	1.0563E-02	0	3.4271E-02	4.4105E-02	0	2.7166E-06	1.0560E-02	0
VCE	5.4323E-06	1.0563E-02	0	3.4271E-02	4.4105E-02	0	2.7166E-06	1.0560E-02	0
Safe	9.9999E-01	9.7887E-01	1	9.3146E-01	9.1179E-01	1	9.9999E-01	9.7888E-01	1
T4	VCE								
T2	PF			VCE			Safe		
T1	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	3.4271E-02	4.4105E-02	0	6.6189E-02	7.5349E-02	0	3.4269E-02	4.4103E-02	0
VCE	3.4271E-02	4.4105E-02	0	6.6189E-02	7.5349E-02	0	3.4269E-02	4.4103E-02	0
Safe	9.3146E-01	9.1179E-01	1	8.6762E-01	8.4930E-01	1	9.3146E-01	9.1179E-01	1
T4	Safe								
T2	PF			VCE			Safe		
T1	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	2.7166E-06	1.0560E-02	0	3.4269E-02	4.4103E-02	0	8.0328E-10	1.0558E-02	0
VCE	2.7166E-06	1.0560E-02	0	3.4269E-02	4.4103E-02	0	8.0328E-10	1.0558E-02	0
Safe	9.9999E-01	9.7888E-01	1	9.3146E-01	9.1179E-01	1	1.0000E+00	9.7888E-01	1

Table 5. 56 CPTs for the case study (from T6 to T7).

CPT T6									
T2	PF								
T5	PF			VCE			Safe		
T3	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	5.4323E-06	3.4271E-02	2.7166E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7166E-06	3.4269E-02	8.0328E-10
VCE	5.4323E-06	3.4271E-02	2.7166E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7166E-06	3.4269E-02	8.0328E-10
Safe	9.9999E-01	9.3146E-01	9.9999E-01	9.3146E-01	8.6762E-01	9.3146E-01	9.9999E-01	9.3146E-01	1
T2	VCE								
T5	PF			VCE			Safe		
T3	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	1.0563E-02	4.4105E-02	1.0560E-02	4.4105E-02	7.5349E-02	4.4103E-02	1.0560E-02	4.4103E-02	1.0558E-02
VCE	1.0563E-02	4.4105E-02	1.0560E-02	4.4105E-02	7.5349E-02	4.4103E-02	1.0560E-02	4.4103E-02	1.0558E-02
Safe	9.7887E-01	9.1179E-01	9.7888E-01	9.1179E-01	8.4930E-01	9.1179E-01	9.7888E-01	9.1179E-01	9.7888E-01
T2	Safe								
T5	PF			VCE			Safe		
T3	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	5.4315E-06	3.4271E-02	2.7158E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7158E-06	3.4269E-02	0
VCE	5.4315E-06	3.4271E-02	2.7158E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7158E-06	3.4269E-02	0
Safe	9.9999E-01	9.3146E-01	9.9999E-01	9.3146E-01	8.6762E-01	9.3146E-01	9.9999E-01	9.3146E-01	1

CPT T7			
T4	PF	VCE	Safe
PF	2.71577E-06	0.034268925	0
VCE	2.71577E-06	0.034268925	0
Safe	9.9999E-01	9.3146E-01	1

Table 5. 57 CPTs for the case study (T8).

CPT T8									
T4	PF								
T7	PF			VCE			Safe		
T5	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	5.4323E-06	3.4271E-02	2.7166E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7166E-06	3.4269E-02	8.0328E-10
VCE	5.4323E-06	3.4271E-02	2.7166E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7166E-06	3.4269E-02	8.0328E-10
Safe	9.9999E-01	9.3146E-01	9.9999E-01	9.3146E-01	8.6762E-01	9.3146E-01	9.9999E-01	9.3146E-01	1.0000E+00
T4	VCE								
T7	PF			VCE			Safe		
T5	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	1.0563E-02	4.4105E-02	1.0560E-02	4.4105E-02	7.5349E-02	4.4103E-02	1.0560E-02	4.4103E-02	1.0558E-02
VCE	1.0563E-02	4.4105E-02	1.0560E-02	4.4105E-02	7.5349E-02	4.4103E-02	1.0560E-02	4.4103E-02	1.0558E-02
Safe	9.7887E-01	9.1179E-01	9.7888E-01	9.1179E-01	8.4930E-01	9.1179E-01	9.7888E-01	9.1179E-01	9.7888E-01
T4	Safe								
T7	PF			VCE			Safe		
T5	PF	VCE	Safe	PF	VCE	Safe	PF	VCE	Safe
PF	5.4315E-06	3.4271E-02	2.7158E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7158E-06	3.4269E-02	0
VCE	5.4315E-06	3.4271E-02	2.7158E-06	3.4271E-02	6.6189E-02	3.4269E-02	2.7158E-06	3.4269E-02	0
Safe	9.9999E-01	9.3146E-01	9.9999E-01	9.3146E-01	8.6762E-01	9.3146E-01	9.9999E-01	9.3146E-01	1

5.3.5.2 Application of Bayesian Networks to domino accident analysis without safety measures

In modelling step 1), which is adapted from Khakzad et al. (Khakzad et al., 2013d), safety barriers are not included in domino accident analysis, which is performed according to the methodology of Section 3.3.2.1.3.4. Bayesian Network is constructed using Hugin Software version 8.1 (Hugin, 2016); a qualitative representation of the net is available in Figure 5.57, the inputs and reasoning that lead to the accident propagation modelling are listed in the previous subsection.

The outputs of the net obtained from modelling step 1), which consists on tank accident probabilities *TX* with $X = \{1,2,3 \ldots,8\}$, auxiliary nodes probabilities (i.e., *L1, L2* and *L3*) and domino level probabilities (i.e., *DL0*, *DL1* and *DL2*) are available in Table 5. 58. It should be noted that modelling step 1) demonstrates the usefuleness and ease of application of Bayesian Network application to domino accident modelling, with reference to a realistic plant layout.

Neverthless, step 1) provides only a baseline situation for further implementations, as cascading events realistic representation demands for introduction of safety barriers in the modelling phase.

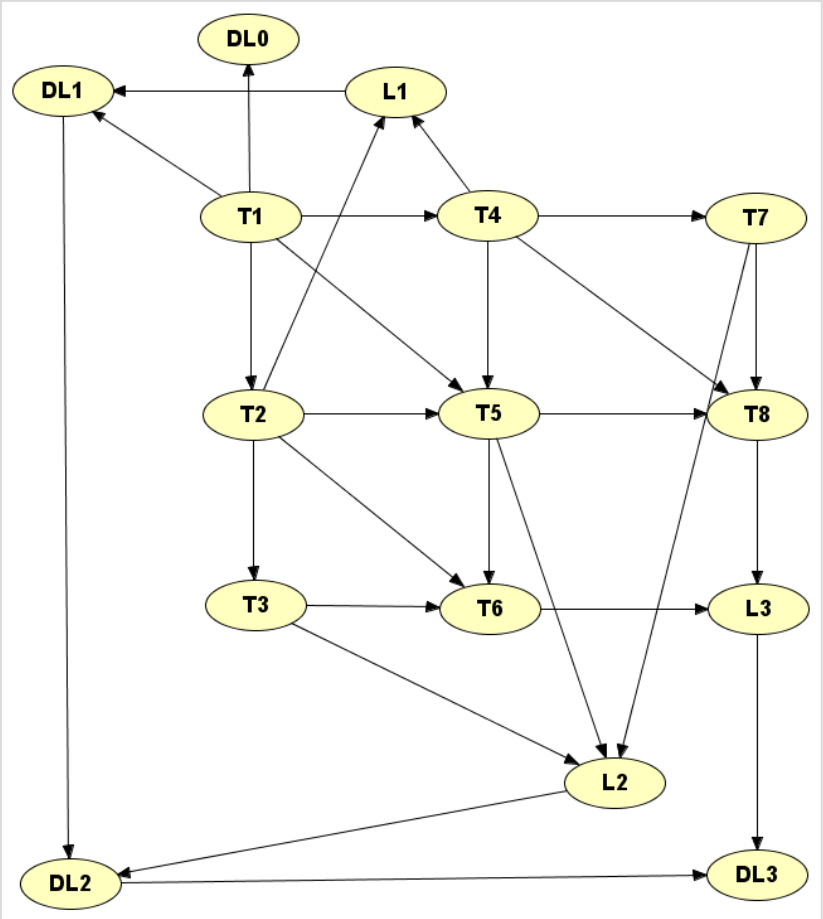


Figure 5. 57 Bayesian Network for domino accident analysis in a realistic tank farm with no safety barriers included in the analysis (modelling Step 1), adapted from Khakzad et al. (Khakzad et al., 2013b).

As seen in previous case studies, one of the advantage of Bayesian Networks is the possibility to revise probabilities, due to new evidencies. Therefore, the application of a probability revising technique is carried out to net obtained from modelling step 1), in purpose to identify weak links leading to a specific final accidental state, for instance *T6*. The evidence of *T6* in PF state is inserted in the net, and the sum propagation normal tool is applied to compile the net. The results, reported in Table 5. 58, show posterior probabilities for each tank of the tank farm ($X = \{1,2, \dots ,8\}$), in particular:

- Tank node probabilities (*TX*);
- Auxiliary nodes probabilities *(L1, L2, L3);*
- Domino probabilities *(DLO, DL1, DL2, DL3).*

Table 5. 58 Results of Bayesian Network for domino accident analysis in a realistic tank farm with no safety barriers included in the analysis (modelling Step 1). Column on the left refers to prior probabilities; column on the right reports posterior probabilities, after the introduction of T6 in Pool Fire state as evidence.

Modelling step 1	**No safety barriers Prior probabilities**		**No safety barriers Posterior probabilities**	
Tank probabilities				
Tank ID	**PF**	**VCE**	**PF**	**VCE**
T1	1.000E-05	2.000E-06	2.300E-04	9.998E-01
T2	6.857E-08	6.857E-08	1.630E-02	5.371E-01
T3	2.350E-09	2.350E-09	1.681E-02	6.337E-02
T4	6.857E-08	6.857E-08	3.240E-02	7.910E-02
T5	2.590E-08	2.590E-08	2.152E-02	5.458E-01
T6	1.688E-09	1.688E-09	1.000E+00	0.000E+00
T7	2.350E-09	2.350E-09	2.710E-03	2.710E-03
T8	1.688E-09	1.688E-09	1.958E-02	1.958E-02
Auxiliary nodes probabilities				
L1	2.649E-07		6.241E-01	nd
L2	6.033E-08		6.374E-01	nd
L3	6.619E-09		1.000E+00	nd
Domino probabilities				
DL0	1.200E-05		**1.000E+00**	nd
DL1	2.649E-07		**6.241E-01**	nd
DL2	2.331E-08		**2.615E-01**	nd
DL3	1.721E-09		**2.615E-01**	nd

5.3.5.3 Application of safety measures performance assessment to domino accident analysis by means of Bayesian Networks

According to modelling step 2, an extension of the previous case study with introduction of pertinent safety measures, named also safety barriers, on each tank is provided, obtaining therefore an original application of domino accident analysis with Bayesian Networks, filling the research gap identified in Section 5.1.1.2. The accident propagation and the input data are the same ones applied in the previous section. The results obtained in the two different modelling steps will be compared to assess the influence of safety barriers introduction on domino probabilities. BNs modelling has been performed with Hugin Expert Software version 8.1 (Hugin, 2016).

Safety barriers pertinent for the reference installation are defined, based on the approach presented in Section 3.3.2.1.2; they are the same ones of the tank farm case study with 3 tanks (Section 5.3.4). As the installation is considered RI Type 1, the presence of 3 safety barriers on each tank is accounted. They are respectively: sprinkler (*Sprinkler_TX*), PSV (*PSV_TX*) and emergency team intervention (*Em_Team_TX*), represented by three nodes in BNs modelling,

which are connected as child node of *TX* with $X = \{1,2,\dots,8\}$; each safety barrier has a binary behavior (i.e., OUT 1 – fail / OUT 2 – work).

The performance of safety barriers has been accounted by means of the three typologies of specific gates described in Section 3.3.2.1.2, which combine availability and effectiveness. Therefore, the performance of safety barriers on each tank (i.e., *Sprinkler_TX, PSV_TX, Em_Team_TX*) is the output of a logic gate, whose inputs are the nodes regarding the availability of each barrier (*Av_Spr_TX, Av_PSV_TX, Av_Emt_TX)* and the respective effectiveness (*Eff_Spr_TX, Eff_PSV_TX, Eff_Emt_TX)*. Input data for safety barriers performance assessment are reported in Table 5. 59. It should be noted that safety barriers behavior is independent from the typology of top event (i.e., *PF* or *VCE*). This approach, applied also in the previous case study (Section 5.3.4) allows avoiding over conservative assumptions regarding safety barriers performance, according to the concepts discussed in Section 3.3.2.1.2. It should be noted that, despite the increased complexity of the net (more units and variables, increased maximum domino level), the inclusion of safety barriers performance in domino accident modelling for the current case study (i.e., tank farm of 8 tanks) has been carried out by applying the same typologies of safety barriers, with the same inputs regarding availability and effectiveness, as for the case study with 3 tanks (i.e., described in Section 5.3.4).

Table 5. 59 Input data for the inclusion of safety barriers performance assessment within domino accident analysis by means of Bayesian Networks. Data retrieved from a data repository (Landucci et al., 2015).

Safety barrier ID	Safety barrier description	Input data for modelling step 2	
Sprinkler	Foam water sprinkler system with electric actuation	Gate Type	B
		Availability	5.39E-03
		Effectiveness (η)	0.954
PSV	Pressure safety valve	Gate Type	A
		Availability	1.00E-02
		Effectiveness (η)	1
Em.Team	Emergency team intervention	Gate Type	C
		Availability	1.00E-01
		Effectiveness (η)	1

Regarding the definition of tank probabilities for the eight tanks composing the tank farm, the values reported in Table 5. 55, Table 5. 56, Table 5. 57 have been inserted in CPTs; CPTs remain the same ones of the previous modelling step. A consequence node is defined for each tank (*Cons_TX*), according to an AND gate, as displayed in previous safety barriers performance assessment by means of BNs (e.g., see Section 5.3.2, Section 5.3.3 and Section 5.3.4). According to the configuration of the case study (i.e., two top events, three safety barriers on each tank),

the consequence node on each tank accounts for 16 accidental states plus state Safe, as displayed in Table 5. 60. On each tank, 8 final accidental states are due to *PF* and 8 are due to *VCE*; in this way propagation due to *VCE* and *PF* can be considered correctly.

The escalation occurs only when all the barriers on a tank are not working, according to the approximation taken from Landucci et al. (Landucci et al., 2015a). In this situation, the consequence node is in state *CTX_1* with reference to *PF* and in state *CTX_9* with reference to *VCE* (Table 5. 60)), for each tank *TX* with $X = \{1,2,3 \dots,8\}$. This is represented in the net by an additional node (*WCons_TX*) on each tank, which is a child node of the respective consequence node. Therefore, *WCons_TX* node represents the "reduced" accident probability on each tank, due to the introduction of safety barriers. Indeed, *WCons_TX* should concour to the determination of domino level probabilities in modelling step 2). According to the methodology for domino accident modelling displayed in Section 3.3.2.1.3.4, and previously applied in modelling step 1), the introduction of safety barriers did not modified the accident propagation pattern. Therefore, *WCons_TX* is linked to the following tanks considering the same propagation pattern as in modelling step 1).

Table 5. 60 Safety barriers states for each resulting final accidental state, for a generic tank *X* of the realistic tank farm, with $X = \{1,2,3 \dots,8\}$.

Top event	Consequence ID - Tank X	Sprinkler_TX	PSV_TX	Em_team_TX
PF	**CTX_1**	fail	fail	fail
PF	**CTX_2**	fail	fail	work
PF	**CTX_3**	fail	work	fail
PF	**CTX_4**	fail	work	work
PF	**CTX_5**	work	fail	fail
PF	**CTX_6**	work	fail	work
PF	**CTX_7**	work	work	fail
PF	**CTX_8**	work	work	work
VCE	**CTX_9**	fail	fail	fail
VCE	**CTX_10**	fail	fail	work
VCE	**CTX_11**	fail	work	fail
VCE	**CTX_12**	fail	work	work
VCE	**CTX_13**	work	fail	fail
VCE	**CTX_14**	work	fail	work
VCE	**CTX_15**	work	work	fail
VCE	**CTX_16**	work	work	work

Auxiliary nodes *L1, L2, L3*, are added to the net, as well as *DL0, DL1, DL2*, and *DL3*. *DL0* overlaps with the primary event. With reference to the specific case plant layout, for example, to account for the first level domino effect, *DL1* is connected to *WCons_T1* and the auxiliary node *L1* with an AND gate. *L1* represents the output of an OR gate between *WCons_T2* and *WCons_T4*. Then, *L2* auxiliary node is obtained as an OR gate among *WCons_T3, WCons_T5* and *WCons_T7*. *DL2* is connected to the unit *DL1* and the auxiliary node *L2* with an AND gate.

Similarly, *L3* auxiliary node is obtained as an OR gate between *WCons_T6* and *WCons_T8*. *DL3* is connected to the unit *DL2* and the auxiliary node *L3* with an AND gate.

5.3.5.4 Results of the case study

The results obtained from modelling step 2) are reported below; the qualitative part of BN, obtained with Hugin software 8.1 (Hugin, 2016) is reported in Figure 5. 58; the outputs of the net, obtained from Bayesian Network analysis, are available in Table 5. 61 and Table 5. 62.

According to modelling step 2), for each tank X of the tank farm ($X = \{1,2,3,\dots,8\}$);, the following results have been reported in Table 5. 61 and Table 5. 62:

- Safety barriers performance probabilities, referred to failure state (i.e., *Sprinkler_TX, PSV_TX, Em_Team_TX*);
- Tank node probabilities (*TX*);
- Consequence node probabilities *(Cons_TX)*, specifying the one possibly leading to further escalation *(WCons_TX)*;
- Auxiliary nodes probabilities *(L1, L2, L3)*;
- Domino probabilities *(DLO, DL1, DL2, DL3)*.

As seen in previous case studies, one of the advantages of Bayesian Networks is the possibility to revise probabilities, due to new evidencies. Therefore, the application of a probability revising technique is carried out to net obtained from modelling step 2), in purpose to identify weak links leading to a specific final accidental state, for instance *WCons_T6* is in *PF* state. The evidence is inserted in the net, and the sum propagation normal tool is applied to compile the net. The results, reported in Table 5. 63, show posterior probabilities for each tank X of the tank farm ($X = \{1,2,\dots,8\}$), in particular:

- Tank node probabilities (*TX*);
- Consequence node probabilities *(Cons_TX)*, specifying the one possibly leading to further escalation *(WCons_TX)*;
- Auxiliary nodes probabilities *(L1, L2, L3)*;
- Domino probabilities *(DLO, DL1, DL2, DL3)*.

However, it should be noted that the application of probability revising techniques, which are very useful with respect to major accident scenarios and generally rather simple case studies, might be not the most significant advantage of domino accident analysis by means of Bayesian Network, due to the scarcity of accidental data to be applied.

Table 5. 61 Part 1 - Results of Bayesian Network for domino accident analysis in realistic tank farm of 8 tanks with safety barriers included in the analysis. Their performance is evaluated with specific gates, based on availability and effectiveness (modelling Step 2). All the results refer to accident/failure state.

Tank ID (X=1,2,…,8)																
	X=1		***X=2***		***X=3***		***X=4***		***X=5***		***X=6***		***X=7***		***X=8***	
Top event	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**
Tank probabilities																
TX	1.000E-05	2.000E-06	3.507E-12	3.507E-12	6.146E-18	6.146E-18	3.507E-12	3.507E-12	1.091E-12	1.091E-12	3.806E-18	3.806E-18	6.146E-18	6.146E-18	3.806E-18	3.806E-18
Safety barriers																
Sprinkler_TX	6.137E-07		3.587E-13		6.286E-19		3.587E-13		1.116E-13		3.893E-19		6.286E-19		3.893E-19	
PSV_TX	1.200E-07		7.013E-14		1.229E-19		7.013E-14		2.182E-14		7.612E-20		1.229E-19		7.612E-20	
Em_team_TX	1.200E-06		7.013E-13		1.229E-18		7.013E-13		2.182E-13		7.612E-19		1.229E-18		7.612E-19	
Cons_TX																
CTX_1	5.114E-10	-	1.793E-16	-	3.143E-22	-	1.793E-16	-	5.581E-17	-	1.946E-22	-	3.143E-22	-	1.946E-22	-
CTX_2	4.603E-09	-	1.614E-15	-	2.829E-21	-	1.614E-15	-	5.022E-16	-	1.752E-21	-	2.829E-21	-	1.752E-21	-
CTX_3	5.063E-08	-	1.775E-14	-	3.112E-20	-	1.775E-14	-	5.525E-15	-	1.927E-20	-	3.112E-20	-	1.927E-20	-
CTX_4	4.557E-07	-	1.598E-13	-	2.801E-19	-	1.598E-13	-	4.972E-14	-	1.734E-19	-	2.801E-19	-	1.734E-19	-
CTX_5	9.489E-09	-	3.327E-15	-	5.832E-21	-	3.327E-15	-	1.035E-15	-	3.611E-21	-	5.832E-21	-	3.611E-21	-
CTX_6	8.540E-08	--	2.995E-14	-	5.249E-20	-	2.995E-14	-	9.318E-15	-	3.250E-20	-	5.249E-20	-	3.250E-20	-
CTX_7	9.394E-07	-	3.294E-13	-	5.773E-19	-	3.294E-13	-	1.025E-13	-	3.575E-19	-	5.773E-19	-	3.575E-19	-
CTX_8	8.454E-06	-	2.965E-12	-	5.196E-18	-	2.965E-12	-	9.225E-13	-	3.218E-18	-	5.196E-18	-	3.218E-18	-
CTX_9	-	1.023E-10	-	1.793E-16	-	3.143E-22	-	1.793E-16	-	5.581E-17	-	1.946E-22	-	3.143E-22	-	1.946E-22
CTX_10	-	9.206E-10	-	1.614E-15	-	2.829E-21	-	1.614E-15	-	5.022E-16	-	1.752E-21	-	2.829E-21	-	1.752E-21
CTX_11	-	1.013E-08	-	1.775E-14	-	3.112E-20	-	1.775E-14	-	5.525E-15	-	1.927E-20	-	3.112E-20	-	1.927E-20
CTX_12	-	9.114E-08	-	1.598E-13	-	2.801E-19	-	1.598E-13	-	4.972E-14	-	1.734E-19	-	2.801E-19	-	1.734E-19
CTX_13	-	1.898E-09	-	3.327E-15	-	5.832E-21	-	3.327E-15	-	1.035E-15	-	3.611E-21	-	5.832E-21	-	3.611E-21
CTX_14	-	1.708E-08	-	2.995E-14	-	5.249E-20	-	2.995E-14	-	9.318E-15	-	3.250E-20	-	5.249E-20	-	3.250E-20
CTX_15	-	1.879E-07	-	3.294E-13	-	5.773E-19	-	3.294E-13	-	1.025E-13	-	3.575E-19	-	5.773E-19	-	3.575E-19
CTX_16	-	1.691E-06	-	2.965E-12	-	5.196E-18	-	2.965E-12	-	9.225E-13	-	3.218E-18	-	5.196E-18	-	3.218E-18

Table 5. 62 Part 2 - Results of Bayesian Network for domino accident analysis in realistic tank farm of 8 tanks with safety barriers included in the analysis. Their performance is evaluated with specific gates, based on availability and effectiveness (modelling Step 2). All the results refer to accident/failure state.

Tank ID (X=1,2,…,8)																
	X=1		***X=2***		***X=3***		***X=4***		***X=5***		***X=6***		***X=7***		***X=8***	
Top event	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**	**PF**	**VCE**
WCons_TX	5.114E-10	1.023E-10	1.793E-16	1.793E-16	3.143E-22	3.143E-22	1.793E-16	1.793E-16	5.581E-17	5.581E-17	1.946E-22	1.946E-22	3.143E-22	3.143E-22	1.946E-22	1.946E-22
Auxiliary nodes probabilities																
L1	7.173E-16															
L2	1.116E-16															
L3	7.786E-22															
Domino probabilities																
DL0	6.137E-10															
DL1	7.173E-16															
DL2	3.260E-21															
DL3	1.222E-26															

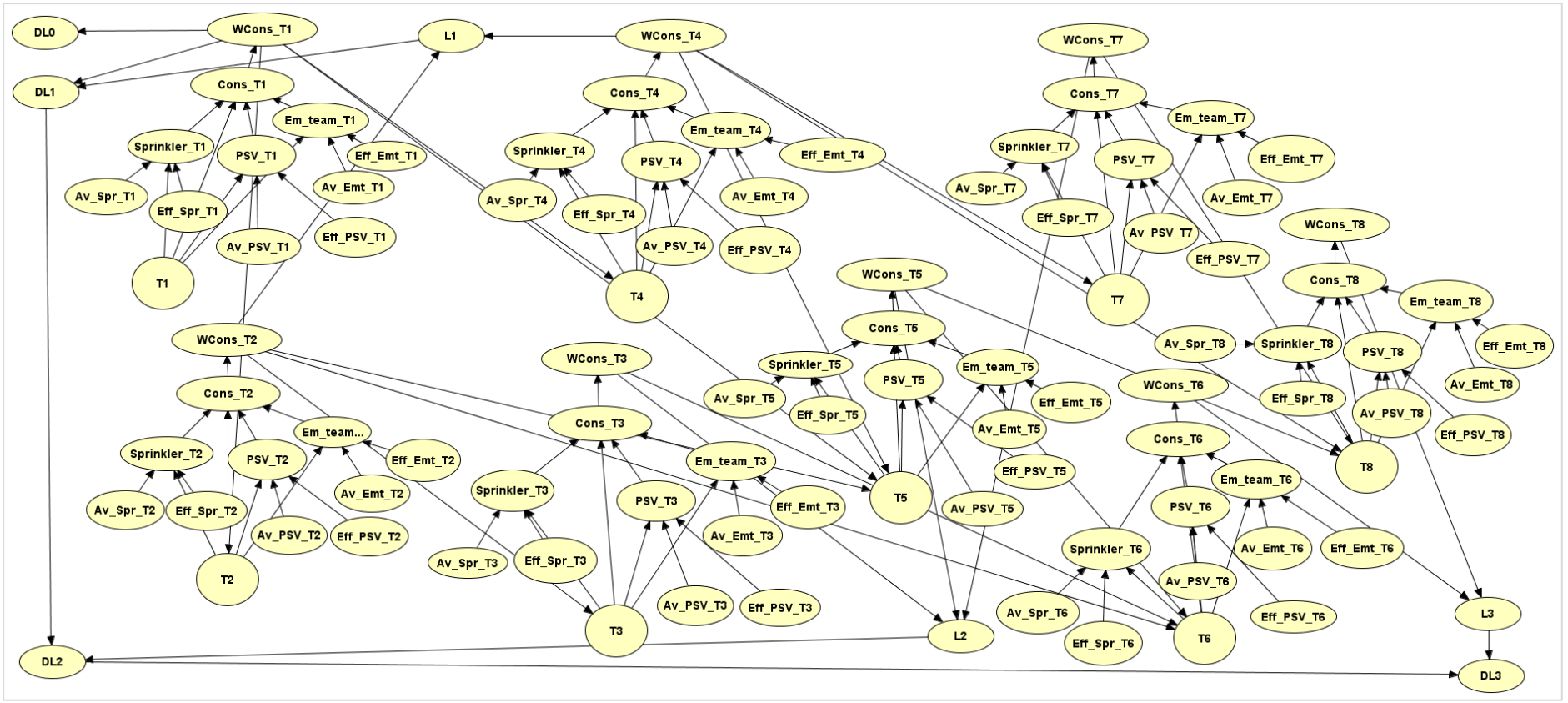


Figure 5. 58 Bayesian Network for domino accident analysis in a realistic tank farm with safety barriers included in the analysis. Their performance is evaluated with specific gates, based on availability and effectiveness (modelling Step 2).

Table 5. 63 Comparison between posterior probabilities and priors for domino accident analysis in realistic tank farm of 8 tanks with safety barriers included in the analysis. The evidence of *WCons_T6* in *PF* state is added to the net to obtain posterior probabilities.

Posterior probabilities			***Prior probabilities***		
Tank probability	**PF**	**VCE**	***Tank probability***	**PF**	**VCE**
T1	1.972E-05	9.998E-01	***T1***	1.000E-05	2.000E-06
T2	1.722E-02	5.147E-01	***T2***	3.507E-12	3.507E-12
T3	1.705E-02	1.705E-02	***T3***	6.146E-18	6.146E-18
T4	3.426E-02	3.426E-02	***T4***	3.507E-12	3.507E-12
T5	2.198E-02	5.244E-01	***T5***	1.091E-12	1.091E-12
T6	1.000E+00	0.000E+00	***T6***	3.806E-18	3.806E-18
T7	1.547E-07	1.547E-07	***T7***	6.146E-18	6.146E-18
T8	1.722E-02	1.722E-02	***T8***	3.806E-18	3.806E-18
Worst Consequences	**PF**	**VCE**	***Worst Consequences***	**PF**	**VCE**
Wcons_T1	1.972E-04	9.998E-01	***Wcons_T1***	5.114E-10	1.023E-10
Wcons_T2	9.099E-07	4.975E-01	***Wcons_T2***	1.79E-16	1.79E-16
Wcons_T3	8.721E-07	3.640E-06	***Wcons_T3***	3.143E-22	3.143E-22
Wcons_T4	1.730E-06	4.510E-06	***Wcons_T4***	1.793E-16	1.793E-16
Wcons_T5	4.094E-05	5.025E-01	***Wcons_T5***	5.580E-17	5.580E-17
Wcons_T6	1.000E+00	0.000E+00	***Wcons_T6***	1.946E-22	1.946E-22
Wcons_T7	7.911E-12	7.911E-12	***Wcons_T7***	3.143E-22	3.143E-22
Wcons_T8	8.806E-07	8.806E-07	***Wcons_T8***	1.946E-22	1.946E-22
Domino Level probability			***Domino Level probability***		
DL0	1.000E+00		***DL0***	6.137E-10	
DL1	4.975E-01		***DL1***	7.173E-16	
DL2	1.570E-05		***DL2***	3.260E-21	
DL3	1.570E-05		***DL3***	1.222E-26	

On the other hand, it might be relevant to carry out a comparison of the results, obtained from modelling steps 1) and 2), in purpose to evaluate the effect of safety barriers introduction within modelling phase. For each tank of the tank farm ($X = \{1,2, \dots ,8\}$), the results referred to tank accident probabilities *(TX)*, according to the two different modelling steps have been reported in Table 5. 64. For instance, the ratio between tank accident probability in modelling step 2) and 1) clearly shows a reduction up to 9 orders of magnitude. The gap tends to be particularly significant in the last units affected by domino effect (i.e., *T6, T7, T8*). Therefore, modelling step 3), which includes a complete approach to safety barriers performance assessment, is able to represent the systems in detailed way, avoiding overestimation of accident probabilities.

Domino probabilities at different levels *(DLO, DL1, DL2, DL3)* have been reported separately for the two modelling steps in Table 5. 64: without safety barriers (modelling step 1) and with safety barriers overall performance, by a combination of availability and effectiveness (modelling step 2). The ratio between modelling steps 2) and 1) shows a reduction from 5 to 18 order of magnitude in domino probabilities after the introduction of safety barriers, confirming that safety barriers introduction within domino accident modelling provides a more realistic framework for domino effects analysis.

Table 5. 64 Comparison of results obtained from domino accident analysis by means of Bayesian Networks, before (i.e., modelling step 1) and after introduction of safety barriers (i.e., modelling step 2) in the modelling phase.

Tank probability	***Modelling step 2 SB performance***		***Modelling step 1 No safety barriers***		***Ratio - modelling step 2 /modelling step 1***	
	PF	**VCE**	**PF**	**VCE**	**PF**	**VCE**
T1	1.00E-05	2.00E-06	1.000E-05	2.000E-06	1.000E+00	1.000E+00
T2	3.507E-12	3.507E-12	6.857E-08	6.857E-08	5.114E-05	5.114E-05
T3	6.146E-18	6.146E-18	2.350E-09	2.350E-09	2.616E-09	2.616E-09
T4	3.507E-12	3.507E-12	6.857E-08	6.857E-08	5.114E-05	5.114E-05
T5	1.091E-12	1.091E-12	2.590E-08	2.590E-08	4.214E-05	4.214E-05
T6	3.806E-18	3.806E-18	1.688E-09	1.688E-09	2.255E-09	2.255E-09
T7	6.146E-18	6.146E-18	2.350E-09	2.350E-09	2.616E-09	2.616E-09
T8	3.806E-18	3.806E-18	1.688E-09	1.688E-09	2.255E-09	2.255E-09
Domino Level prob.	***Modelling step 2 SB performance***		***Modelling step 1 No safety barriers***		***Ratio - modelling step 2 /modelling step 1***	
DLo	6.137E-10		1.200E-05		5.114E-05	
DL1	7.173E-16		2.649E-07		2.708E-09	
DL2	3.260E-21		2.331E-08		1.399E-13	
DL3	1.222E-26		1.721E-09		7.104E-18	

5.3.5.5 Discussion and conclusions on the case study

The present application has been aimed at implementing safety barriers performance assessment, by means of Bayesian Networks, to domino accident analysis. The case study refers to the prevention of fire escalation into a cascading event (i.e., domino accident), considering a realistic tank farm of eight tanks, with multiple top events, three domino levels and synergistic included in the analysis.. The methodology for the definition of domino accident modelling by means of BNs has been recently, but only the simplified case study presented in the previous Section (Section 5.3.4) accounted for safety barriers within the modelling phase. Therefore, the present original case study is aimed at definitely proving the advantage of safety barriers performance assessment inclusion within domino accident analysis by means of Bayesian Networks.

Safety barriers of different typologies (i.e., active, passive and procedural ones) have been introduced in the modelling phase on each tank of the tank farm; their performances have been assessed by means of specific gates (i.e., type A, B and C), depending on barriers states and classification, combining availability and effectiveness. Indeed, the application of specific gates for the assessment of safety barriers performance has proved in previous case studies (e.g., see Section 5.3.4) to be useful in purpose to avoid performance overestimation and to provide a more accurate risk picture within domino effect modelling and prevention.

Despite the increasing complexity of the present case study with respect to the previous one (Section 5.3.4), the results were analogous. Indeed, the results of the current case study have revealed a decrease of several order of magnitude in the domino probabilities at all the levels (i.e., 3 levels of domino), as well as in the tanks accident probability, in comparison with the results obtained not including safety barriers in the modelling phase.

Therefore, it is confirmed that the information obtained by domino accident modelling, with the inclusion of safety barriers, offers an accurate risk picture, avoiding overestimation of accident probabilities.

Eventually domino accident analysis, performed by means of an advanced dynamic technique as Bayesian Networks, joined with safety barriers performance assessment is able to model realistically severe accidental scenarios and cascading events triggered by external hazard factors (i.e., domino effect). This typology of application has demonstrated its full potential and may become a fundamental tool to support QRA application (i.e., risk evaluation phase) to external hazard factor-driven accidents, with specific reference to domino effects.

5.4 CONCLUSIONS

The present section of the research project has been aimed at applying dynamic approaches to safety measures performance assessment in the prevention of major accidents and cascading events (i.e., domino accidents), by means of Bayesian analysis techniques, in particular Bayesian Networks.

Initial tutorials and applications, the latter derived from existing works, were aimed at exploring the potentialities of the mentioned Bayesian techniques. Initial applications, which considered Bayesian failure assessment for a process tank equipped with safety system and Bayesian analysis to an oil spill accident, emphasized the necessity to perform dynamic risk assessment by means of specific software, in purpose to support calculations.

Therefore, a specific software, named Hugin, was applied to construct Bayesian Networks: tutorials have been carried out to show tools and features of the software. Then, safety barriers performance assessment has been applied by means of Bayesian Networks: two case studies were aimed at converting conventional risk assessment techniques (i.e., Fault-Tree and Bow-Tie) into Bayesian Networks. The possibility of Bayesian Network to account safety barriers performance, including also economic elements has been explored by an additional tutorial.

The lesson learnt by existing case studies and tutorials made clear the advantages of Bayesian Networks in terms of flexibility, ability to consider multi state variables and ease to update probabilities over time, according to experience. However, few original applications of dynamic techniques, in particular Bayesian Networks, are focused on safety barriers performance and none of them included safety barriers in domino accident modelling.

Then, original applications aimed at implementing a Bayesian Network approach to safety measures (or barriers) performance assessment with reference to major accidents and cascading events prevention, have been carried out.

A preliminary application has been focused on the implementation of Bayesian Networks to safety measures performance assessment, starting from a conventional approach, and including only active measures. Safety barriers performance was accounted by means of specific gates, depending on barriers states and classification, accounting both availability and effectiveness. The case study demonstrate the feasibility of the approach.

Then, the Bayesian Network application was extended to a realistic case study regarding the prevention of fire escalation, including active, passive and procedural safety measures performance. The case study proved the feasibility of Bayesian Networks application to safety

barriers performance assessment with respect to accident escalation into a cascading event. Indeed, both these applications highlighted the easiness to dynamically revise top event, intermediate event, safety measures performance and final events probabilities over time, in purpose to obtain an updated and more realistic risk picture, by means of Bayesian Networks.

Therefore, Bayesian Networks have been applied to cascading events prevention, for instance to domino accident analysis, in purpose to assess the effect of safety measures inclusion in the modelling phase. Two case studies, the first regarding a simplified tank farm and the second regarding a realistic tank farm, have been carried out. Despite the increasing level of complexity of the realistic tank farm case study, which included multiple top events, three levels of domino and synergistic effects, the results of the two case study were analogous. They both showed a reduction of domino accident probabilities of several orders of magnitude demonstrating that domino accident analysis by means of Bayesian Networks, joined with safety barriers performance assessment is able to model realistically cascading events.

Eventually the case studies have demonstrated that the application of an advanced technique for safety barriers performance assessment, as Bayesian Networks, allows providing a very accurate identification of risk reducing measures within the risk evaluation phase of QRA, with reference to external hazard factors driven accidents (i.e., domino effects), offering a sound tool to support safety analysts.

Extension of Quantitative Risk Assessment to the Analysis of External Hazard Factors in the Chemical and Process Industry

Section 6.

Application of an economic model for the allocation of preventive security measures against terroristic attacks in chemical facilities

6.1 INTRODUCTION

The present section includes the applications to case studies of the original economic model for the selection and allocation of preventive security measures in chemical facilities, presented in Section 4, according to its two versions, called EM-PICTURES (i.e., Economic Model for Process-Industry related Counter Terrorism measURES) and ECO-SECURE (i.e., ECOnomic model for the selection of SECurity measUREs). The mentioned applications provide a benchmark for the validation of the model.

The section starts in Section 6.2 with tutorials on the application of existing methodologies for physical security measures performance assessment, which are required for the application of the economic model, as discussed in Section 4.2.3. In particular, the tutorial focuses on the application of Estimate of Adversary Sequence Interruption (i.e., EASI) model, which is inserted in the economic model, presented in Section 4 (Sections 4.2.2 and 4.2.3).

Then, in Sections 6.3 and 6.4, two original applications to case studies of the economic model, in EM-PICTURES version (i.e., Economic Model for Process-Industry related Counter Terrorism measURES), are presented.

The illustrative simplified case study, introduced in Section 6.3, deals with the prevention of a possible sabotage to a storage tank farm in a process facility, whose occurrence may lead to a major accident. The aim of the case study is to prove that the application of the model provides an economic aid or criterion for selecting additional security measures in a simplified chemical installation. Starting from a credible sequence of adversary actions regarding an illustrative plant layout, the uncertainties related to the threat probability have been accounted and possible security measures in place have been considered, determining the baseline physical security system performance. Therefore, three pertinent security upgrades have been proposed; for each of them the performances improvement and realistic total costs have been calculated; the losses derived from an expected accidental scenario have been estimated. Then,

economic analysis is applied to prove that model application may allow defining a rational selection of security measures for a simplified chemical installation.

In Section 6.4, EM-PICTURES application is tested using an illustrative case study, based on a possible security-related event that took place in France, within a storage tank farm. EM-PICTURES application starts with the definition of the adversary sequence of actions, which includes multiple targets, and the realistic site-specific analysis of the baseline physical security system performance. The application includes the comparison and evaluation of the costs and performance improvements of a wide range of security upgrades with the (hypothetical) benefits related to the avoided losses, derived from different scenarios, including a possible cascading event. The application of cost-benefit and cost-effectiveness analysis is provided, according to EM-PICTURES version of the model, to enable selecting economically feasible security measures, or a combination of such measures with a maximum net present value, within the budget constraints of a chemical plant. An uncertainty analysis regarding threat and vulnerabilities probabilities is carried out, in purpose to evaluate their effects on economic analyses results. The complexity of the case study and the use of realistic site-specific information for a chemical installation provide a sound benchmark for the application of EM-PICTURES version of the original economic model within a real industrial context.

Section 6.5 presents an example of application to a relevant original case study of ECO-SECURE version of the economic model, specifically aimed at the allocation of preventive security measures against environmental and ecological terroristic attacks within chemical installations. The application of ECO-SECURE to an illustrative case study, freely adapted from a possible security-related environmental disaster that took place in Italy, show the capabilities and specific features of this economic model version. Site-specific analysis of the baseline physical security system performance allows comparing the costs of different security upgrades with the benefits related to the actual losses, derived from an environmental accident. The application of both deterministic and break-even approaches, provided by ECO-SECURE, allows considering directly the uncertainties regarding the threat probability within model application. Deterministic analysis allows upgrading the existing physical protection system, according to possible variations in the likelihood of the attack. Break-even analysis application provides the optimal allocation of the security budget, defined yearly by security management. Therefore, the selection of the most profitable security measures within budget constraints and definition of economic indicators are the main outputs of the case study. The complexity of the case study and the use of realistic site-specific information for a chemical installation provide a sound benchmark for the application of ECO-SECURE version of the original economic model within a real industrial context.

In Section 6.6, conclusions on the case studies are summarized to define the possible contribution of economic model application with respect to the reduction of chemical plants vulnerability toward security-based accidents, including terroristic attacks.

6.2 TUTORIALS ON SECURITY MEASURES PERFORMANCE ASSESSMENT

6.2.1 Introduction to tutorials

The present tutorials, adapted from Garcia (Garcia, 2007), are aimed at clarifying how to evaluate the performance of a physical security system, with reference to a site-specific adversary path of actions.

The analysis of available methodologies for the evaluation of physical security measures performance, provided in Section 3.4.3, highlighted that the Estimate of Adversary Sequence Interruption (i.e., EASI) model, based on the simplified methodology of timely detection, is a complete analytical method to calculate the probability of interruption (P_I), referred to a sequence of adversary actions aimed at theft or sabotage. Indeed, according to the methodology developed in Section 4 (see Sections 4.2.2 and 4.2.3), the site-specific evaluation of physical security system performance is a fundamental step for the application of economic analysis aimed at the allocation of security resources and the EASI model is applied to that extent.

The first tutorial applies the concept of timely detection; the second one provides an example of application of the EASI model. For both, the modelling environment is Excel® version 2013 datasheet.

6.2.2 Tutorial on timely detection model

This tutorial considers a sabotage path to a critical pump (i.e., the sabotage target) in a process facility, with multiple layers of protection standing between the adversary and the target. The evaluation of baseline physical security system performance (i.e., effectiveness) and possible upgrades are provided, by means of timely detection model.

In Figure 6. 1, information regarding adversary sequence of actions, detection and delay elements present along the path are reported. Details on the timely detection equations to be applied in the tutorial can be retrieved from Section 3.4.3.

The following assumptions are taken into account for model application:

- Detection occurs before delay;
- Non-detection probabilities $(P_{ND,i})$, assessed detection probabilities $(P_{AD,i})$ and delay times $(t_{D,i})$ for each security element $(i = 1, \dots, 5)$ present in the baseline system have been reported in Table 6. 1;
- Response force time (t_G) applied in the calculation is 90 s.

$P_{ND,i}$ indicates the non-detection probability provided by element i. In other words, $P_{ND,i}$ represent the probability that element i will not detect the defined adversary, and its value is the complement to one of $P_{AD,i}$ (i.e., probability of assessed detection).

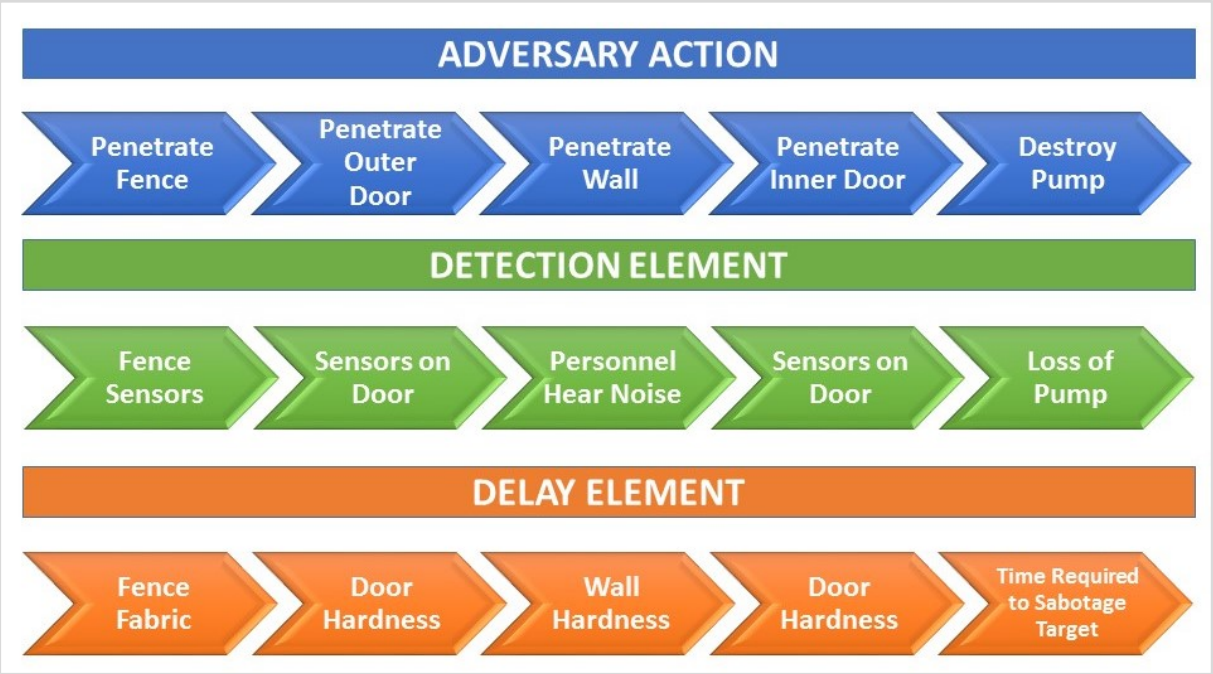


Figure 6. 1 Example of physical protection system (i.e., PPS) effectiveness calculation, for the sabotage of a critical pump in a process facility. From the top to the bottom: adversary path of actions, detection elements, delay elements.

Table 6. 1 Data for the calculation of baseline effectiveness with timely detection methodology.

Task description	Task number	Delay time $t_{D,i}$ (s)	$P_{ND,i}$	$P_{AD,i}$
Penetrate Fence	1	6	1	0
Penetrate Outer Door	2	84	0.9	0.1
Penetrate Wall	3	120	0.7	0.3
Penetrate Inner Door	4	84	0.1	0.9
Destroy Pump	5	30	1	0

First, the analyst should define the Critical Detection Point (i.e., CDP), that is the first point in the adversary path in which the adversary is more than $90\ s$ away from the target (i.e., the pump).

The delay time remaining after the CDP in the baseline PPS can be calculated as follows:

$$t_{R,old} = t_{destroy\ pump} + t_{penetrate\ inner\ door} = (30 + 84)\ s = 114\ s > t_G$$

The CDP is located at the wall and the time remaining on the path after it is $114\ s$; this means that if the adversary is not detected at the wall, there won't be enough time remaining for the guards to interrupt the adversary. The probability of interruption should be computed by considering only the detection elements before the CDP, which are fence sensors (not present in this case, as $P_{ND,fence} = 1$), outer door sensors and wall sensors. According to the concept of timely detection (see Section 3.4.3) the Probability of interruption (P_I), which expresses the baseline PPS effectiveness for the specific adversary's path of actions, is:

$$\eta_{PPS,old} = P_I^{\ *} = 1 - \left(P_{ND,1} \cdot P_{ND,2} \cdot P_{ND,3}\right) = 1 - (1 \cdot 0.9 \cdot 0.7) = 1 - 0.63 = 0.37$$

The same procedure should be repeated for all the other possible existing adversary paths p; the one with the minimum P_I , indicated as critical path (p^*), represents PPS effectiveness. In this tutorial, it is assumed, for sake of simplicity, that the path considered is the critical one. P_I should be compared with acceptability criteria defined by the security analyst; if it does not fulfill it, the Physical Protection System must be improved, by proposing modifications to the existing protection elements and/or additional elements to be added.

In the present example, it is clear that the PPS should be improved, as a possible adversary has 63% chance of reaching the sabotage target. Therefore, a possible upgrading of the PPS has been proposed and the information regarding the upgraded PPS have been reported in Table 6. 2. The possible modifications to the PPS include:

- Reduction of response force time (t_G) to $40\ s$, obtained by dispatching guards in a point closer to the high-value asset;
- Additional delay to the pump, obtained by placing the pump inside a locked metal enclosure;
- Improvement of detection sensors at outer and inner doors level, using sensors with higher $P_{AD,i}$.

The CDP of the upgraded system is now located at the pump, as shown by the calculation of the delay time remaining after the CDP:

$$t_{R,new} = t_{destroy\ pump} = 50\ s > t_G$$

Table 6. 2 Example of calculation of upgraded system performance with timely detection method. The possible upgrades in comparison with baseline PPS have been indicated in bold printing.

Task description	Task number	Delay time $t_{D,i}$ (s)	$P_{ND,i}$	$P_{AD,i}$
Penetrate Fence	1	6	1	0
Penetrate Outer Door	2	84	0.2	0.8
Penetrate Wall	3	120	0.7	0.3
Penetrate Inner Door	4	84	**0.9**	0.1
Destroy Pump	5	**50**	0	1

Apart from the benefits obtained by the upgrading of single security elements, it should be noted that it turns into the addition of a layer of protection into the system (i.e., the inner door), whose contribution can be added in the computation of upgraded system effectiveness $(\eta_{PPS,new})$, according to the following expression:

$$\eta_{PPS,new} = P_I^* = 1 - \left(P_{ND,1} \cdot P_{ND,2} \cdot P_{ND,3} \cdot P_{ND,4}\right) = 1 - (1 \cdot 0.2 \cdot 0.7 \cdot 0.9) = 1 - 0.13 = 0.87$$

The comparison between the values of baseline and upgraded PPS effectiveness shows that the effectiveness improvement $(\overline{\Delta\eta})$ is significant:

$$\overline{\Delta\eta} = \eta_{PPS,new} - \eta_{PPS,old} = 0.87 - 0.37 = 0.50$$

Indeed, also the reduction of delay time after the introduction of PPS upgrades is relevant:

$$t_{R,new} = 50\ s < t_{R,old} = 114\ s$$

Therefore, this tutorial made clear how to assess the performance of an illustrative physical protection system, according to the methodology of timely detection, and how to account PPS upgrades in the calculations.

6.2.3 Tutorial on Estimate of Adversary Sequence Interruption model

This tutorial, adapted from Garcia (Garcia, 2007), explains how to implement the Estimate of Adversary Sequence Interruption (i.e., EASI) model for the calculation of baseline and upgraded physical protection system (i.e., PPS) effectiveness, referred to a sequence of adversary tasks, by using an Excel version 2013 datasheet. EASI model is applied within the original economic model presented in Section 4, in purpose to assess both the baseline and the upgraded physical protection system effectiveness. Further details on the equations composing the EASI model are available in Section 3.4.3; its insertion within the original economic model is presented in Sections 4.2.2 and 4.2.3.

The current tutorial considers a possible sabotage to a target (i.e., a pump located in an internal area of a chemical installation). According to the EASI model, a possible critical site-specific adversary sequence path, connecting the adversary starting point with the target, in relation

with physical protection elements present on the reference site, is defined and reported in Table 6. 3, Part A. The adversary starting point is assumed outside the plant border, at the outer fence level. In this tutorial, the adversary is supposed to carry out the sabotage by foot, with no additional tools hindering his action. If a sabotage is considered, as in the present tutorial, the way back from the target up to the plant borders should not be accounted for in effectiveness calculations, because it is not relevant for the fulfillment of the malevolent action scope.

The calculation of baseline system effectiveness is carried out, with the aim to determine the probability of interruption ($P_I{}^*$) of the critical adversary path. The calculation of the baseline system effectiveness requires the following inputs:

1) Detection elements present along the path. The solely detection elements present are cameras on the wall delimiting the two storage areas, with $P_{AD,3} = P_{AD,5} = 0.9$. The probability of assessed detection $(P_{AD,i})$ expresses the likelihood of detecting an adversary within the zone covered by cameras or intrusion detection sensors. In addition, the location of detection elements was included in the analysis, according to the EASI model, identifying all of them with a standard B location, indicating detection before delay. All the data inherent to the detection function for the path considered in the case study have been reported in Table 6. 3, Part A.
2) Delay elements present along the path. For all delay elements with the exception of running times, specific data have been retrieved (Garcia, 2007) and reported in Table 6. 3, Part A.
3) Data for the calculation of running delay times. Distances among delay elements were retrieved from site layout and reported in Table 6. 3, Part B. For the calculation of running times, the standard adversary velocity of $10\ ft/s = 3.048\ m/s$ has been assumed, considering a reduction factor due to additional weights carried by the adversary unitary (i.e., no additional weight carried by the adversary).
4) Data for the calculation of response function. Inputs for the calculation of response element have been reported in Table 6. 3, Part C; for the probability of guard communication (P_C) a conventional value for industrial facilities was assumed (Garcia, 2007), with a response force time of 300 s, considering that security guards are present on site.

Standard deviation for the delay parameter of each security element and for the response force time parameter was assumed as 3/10 of the mean value throughout the tutorial, according to the conservative assumption on data dispersion reported in the EASI model (Garcia, 2007). This assumption allows considering that guards will not always respond exactly after the same

time, and that adversaries may take more or less time to penetrate barriers with respect to average values.

The critical probability of interruption (P_I^*) has been calculated according to equation (3.26) and its value is 0.4760; P_I^* represents the value of the baseline PPS effectiveness (i.e., $\eta_{PPS,old}$). The value was obtained by inserting in the EASI model datasheet (Garcia, 2007) the inputs listed in Table 6. 3, according to the approach described in Section 3.4.3 and in Section 4.2.2. Therefore, the calculation of baseline system effectiveness highlights moderate security weaknesses, which may be tackled by the introduction of pertinent security upgrades.

Table 6. 3 Inputs for the calculation of baseline PPS effectiveness referred to the critical path. Part A) Adversary sequence and inputs for the calculation of detection and delay elements referred to the identified adversary path; Part B) Additional data for the calculation of running delay times; Part C) Inputs for the calculation of the response function. Standard deviation was assumed 3/10 of the mean value. Values retrieved from data repository (Garcia, 2007) and plant layout.

Part A) Adversary Sequence Diagrams and Inputs for Detection and Delay elements				
ADVERSARY TASKS		***DETECTION***	***DELAY***	
Task number	***Task Description***	***Detection elements and assessed detection probabilities $P_{AD,i}$***	***Delay elements***	***Mean delays $t_{D,i}$ (s)***
1	**Cut fence**	None	Fence fabric	10.0
2	**Run to building**	None	Running time	12.0
3	**Open door**	Camera on the door ($P_{AD,3} = 0.9$)	Door hardness	90.0
4	**Run to vital area**	None	Running time	10.0
5	**Open door**	Camera on the door ($P_{AD,5} = 0.9$)	Door hardness	90.0
6	**Sabotage target**	None	Time required for sabotage	180

Part B) Data for Calculation of running delay times			
Description of the action	***Symbol***	***Value***	***Unit***
Adversary velocity during running	v	3.048	*m/s*
Distance starting point/ building (Task 2)	d_2	36.6	*m*
Distance building/ vital area (Task 4)	d_4	30.5	*m*
Reduction factor due to additional weight carried by adversary	φ	1	*Adim.*

Part C) Data for the calculation of Response function			
Probability of guard communication P_C	0.95	***Mean Response Force Time t_G (s)***	300

Starting from the value of baseline PPS effectiveness $(\eta_{PPS,old} = 0.4760)$, six PPS upgrades have been proposed, according to technical references (Garcia, 2007):

A) Adding fence sensors as perimeter detection system;

B) Adding fence sensors at perimeter level at fence and additional delay at target level (i.e., by enclosing the target in an hardened case);

C) Adding detection elements (i.e., surveillance cameras) at sabotage target level;

D) Adding a delay element (i.e., a wall) at perimeter level;

E) Reducing response force time by relocating the guard dispatch and additional fence sensors at perimeter level.

It should be noted that upgrades A and C refer to the detection function, upgrades D refers to the delay function, upgrade B refers to the combination of detection and delay functions and upgrade E refers to the response function. Moreover, upgrades A and D refer to the external perimeter of the facility, upgrades B, C, E refer to the proximity of the sabotage target.

Table 6. 4 Effectiveness results for five different possible PPS upgrades. From the left to the right, in column order: Upgrade identity, description of the upgrade, Physical protection function modification, reference number of adversary sequence diagram modified tasks, modified inputs for the effectiveness calculations, upgraded PPS effectiveness ($\eta_{PPS,new\ i}$). (*) Reduction of response force time does not affect a single task. A data repository regarding modified inputs values for security upgrades is available in Garcia (Garcia, 2007).

Upgrade ID	*Description*	*PPS - function modification*	*N° of modified tasks*	*Modified inputs*	$\eta_{PPS,\ new\ i}$
A	**Addition of fence sensors at perimeter level**	Detection; fence sensors	1	$P_{AD,1} = 0.9$	**0.5781**
B	**Addition of fence sensors at perimeter level and hardened case for target**	Detection; fence sensors. Delay; wall hardness	1; 6	$P_{AD,1} = 0.9$ $t_{D,6} = 240\ s$	**0.8432**
C	**Addition of detection element at sabotage target (cameras)**	Detection; camera	6	$P_{AD,6} = 0.9$	**0.4763**
D	**Construction/ additional height to external concrete-reinforced perimeter wall (3m high)**	Delay; wall hardness	1	$t_{D,1} = 30\ s$	**0.4760**
E	**Reduction of responsed force time and addition of fence sensors at perimeter level**	Detection; fence sensors.	(*)	$P_{AD,1} = 0.9$ $t_G = 200\ s$	**0.8960**

The upgraded values of effectiveness, indicated as $\eta_{PPS,new\ i}$, for each of the five options have been calculated by inserting the modified input items, listed in Table 6. 4 (i.e., third to last column), in the effectiveness model previously applied to calculate baseline PPS effectiveness (i.e., the EASI model), according to the approach presented in Section 3.4.3 and summarized in Section 4.2.2. The modified inputs regarding each security upgrade, with the exception of upgrade E, affect only specific tasks of the adversary sequence diagram; for all the remaining tasks, the values reported in Table 6. 3 have been applied.

The results regarding upgraded effectiveness (i.e., $\eta_{PPS,new\ i}$), corresponding to each of these upgrades, have also been reported in Table 6. 4.

The results in Table 6. 4 clearly show that, from the effectiveness point of view, the best option is the reduction of response force time with an upgrade of detection at fence (upgrade E), followed by the combined application of detection elements at fence and delay elements at

target level (upgrade B). On the other hand, the presence of an additional delay element at perimeter level (upgrade D) and detection element at sabotage target (upgrade C), proved to be ineffective in increasing PPS effectiveness. The addition of detection elements (i.e, fence sensors) at perimeter level, represented respectively by upgrade A, shows an intermediate performance in terms of upgraded PPS effectiveness.

The EASI model, here applied, can be performed analogously in other case studies and tutorials, according to the same approach; however, the results are site-specific as they require data regarding distances on site and security measures in place. Therefore, the specific values of baseline and upgraded effectiveness obtained in the present tutorial cannot be extended beyond the current PPS configuration and plant layout.

6.3 SELECTION OF PREVENTIVE SECURITY MEASURES AGAINST SABOTAGE IN A STORAGE TANK FARM (EM-PICTURES APPLICATION)

6.3.1 Definition of the case study

The economic model was applied, in EM-PICTURES version, to an illustrative case study, freely inspired by a real incident that took place in summer 2015 in France, consisting in the sabotage of storage tanks in a process facility (Le Guernigou and Revilla, 2015). In the case study, the sabotage of one storage tank containing naphtha has been considered.

The analysis carried out focuses on the selection and management of the security measures, given the likelihood of the attack ($P(T)_{ij}$, renamed $P(T)$ for a single scenario) with reference to a perspective security-based accident. A range of values regarding the likelihood of the attack has been accounted (i.e., 0.01; 0.20; 0.50; 0.75; 1), in purpose to derive a broad set of economic indicators. Vulnerabilities probabilities (i.e., $P(H \mid T)$ and $P(L \mid H)$) have been assumed equal to 1, following the conservative assumptions reported in Table 4. 5.

The fictional simplified plant layout applied in the case study consists on a tank farm, to which the target belongs, including 8 atmospheric storage tanks containing naphtha, with a volume of 40000 m^3 each. The adversary was supposed to carry out the sabotage by foot, following a possible critical path that starts from the facility boundary.

Figure 6. 2 Site-specific adversary sequence of actions for the case study, regarding the sabotage to a single process storage tank.

6.3.2 Development of adversary sequence diagrams and effectiveness calculation

6.3.2.1 Definition of site-specific adversary sequence diagrams and calculation of the baseline system effectiveness

The critical adversary site-specific sequence of actions is reported in Figure 6. 2. After cutting the perimeter fence, the adversary is supposed to run 200 m up to external tank protected area, open a security door with camera on it, run for 200 m up to the target and placing explosives and detonators on it, in purpose to trigger a major accident (i.e., fire). The identification of key protection elements and key distances, reported in Table 6. 5 (Part A) regarding the simplified plant layout is necessary to calculate the baseline physical protection system effectiveness. The calculation of baseline system effectiveness was carried out according to the approach described in Section 4.2.2, with the aim to determine the probability of interruption ($P_I{}^*$) of the critical adversary path. The solely detection elements present are cameras on the wall delimiting external tank protected area, with a probability of assessed detection $P_{AD,3} = 0.9$. In addition, the location of detection elements was included in the analysis, according to the EASI model, considering a standard B location. For all delay elements with the exception of running times, specific data have been retrieved (Garcia, 2007) and reported in Table 6. 5, Part A, jointly with all the data inherent to the detection function for the path considered in the case study. For the calculation of running times, the standard adversary velocity of $10\ ft/s = 3.048\ m/s$ has been assumed, considering a reduction factor due to additional weights carried by the adversary of 0.75 (i.e., additional weight due to explosives and detonators). Distances among delay elements for a typical plant layout were reported in Table 6. 5, Part B. Standard deviation for the delay parameter of each security element and for the response force time parameter was assumed as 3/10 of the mean value throughout the case study, according to the conservative assumption on data dispersion reported in the EASI model (Garcia, 2007). Inputs for the calculation of response element have been reported in Table 6. 5, Part C; for the probability of guard communication (P_C) a conventional value for industrial facilities was assumed (Garcia, 2007), with a response force time of 5 minutes, considering that security guards are present on site.

The critical probability of interruption (P_I^*) has been calculated according to equation (4.1) and its value is 0.1759. P_I^*will be considered in the development of the case study and represents the value of the baseline PPS effectiveness (i.e., $\eta_{PPS,old}$). The value was obtained by inserting in the EASI model datasheet (Garcia, 2007) the inputs listed in Table 6. 5, according to the approach described in Section 4.2.2. The baseline effectiveness calculations can be performed in other case studies, according to the same approach, described in Section 4.2.2; however, the results are site-specific as they require data regarding distances on site and security measures in place. Therefore, the value of baseline effectiveness obtained (i.e., 0.1759) cannot be extended beyond the current case study.

Table 6. 5 Inputs for the calculation of baseline PPS effectiveness referred to the critical path. Part A) Adversary sequence and inputs for the calculation of detection and delay elements referred to the adversary path; Part B) Additional data for the calculation of running delay times; Part C) Inputs for the calculation of the response function. Standard deviation was assumed 3/10 of the mean value. Values retrieved from data repository (Garcia, 2007) and plant layout.

Part A) Adversary Sequence Diagrams and Inputs for Detection and Delay elements				
ADVERSARY TASKS		***DETECTION***	***DELAY***	
Task number	***Task Description***	***Detection elements and assessed detection probabilities*** $P_{AD,i}$	***Delay elements***	***Mean delays*** $t_{D,i}$ ***(s)***
1	**Cut simple wired external perimeter fence**	None	Fence fabric	10.0
2	**Run to external tank protected area**	None	Running time	87.5
3	**Open door**	Camera on the door ($P_{AD,3} = 0.9$)	Door hardness	10.0
4	**Run to the storage tank**	None	Running time	87.5
5	**Sabotage target**	None	Time required for sabotage	120.0

Part B) Data for Calculation of running delay times			
Description of the action	***Symbol***	***Value***	***Unit***
Adversary velocity during running	v	3.048	*m/s*
Distance starting point/ wall of external tank protected area (Task 2)	d_2	36.6	*m*
Distance wall of external tank protected area/ target (Task 4)	d_4	30.5	*m*
Reduction factor due to additional weight carried by adversary	φ	0.75	*Adim.*

Part C) Data for the calculation of Response function			
Probability of guard communication P_C	0.95	***Mean Response Force Time*** t_G ***(s)***	300

6.3.2.2 Proposal of three security upgrades and calculation of upgraded system effectiveness

The calculation of baseline system effectiveness highlights a rather low value of baseline PPS effectiveness (i.e., 0.1759), which may be increased by the introduction of pertinent security upgrades. Therefore, three security upgrades have been proposed, according to technical references (Garcia, 2007):

A) Adding fence sensors as perimeter detection system;

B) Adding a delay element by building a concrete wall with security door at sabotage target level;

C) Reducing response force time by building a closer guard dispatch.

The upgraded value of PPS effectiveness ($\eta_{PPS\,new,i}$), and therefore the effectiveness improvements (i.e., $\overline{\Delta\eta_i}$) have been calculated for each of the proposed security measures (Table 6. 6). The upgraded values of effectiveness, indicated as $\eta_{PPS,new\,i}$, for each of the three options have been calculated by inserting the modified input items, listed in Table 6. 6 (i.e., third to last column), in the effectiveness model previously applied to calculate baseline PPS effectiveness (i.e., the EASI model), according to the approach presented in Section 4.2.3. The modified inputs regarding each security upgrade, with the exception of upgrade C, affect only specific tasks of the adversary sequence diagram; for all the remaining tasks, the values reported in Table 6. 5 have been applied.

The results regarding upgraded effectiveness (i.e., $\eta_{PPS,new\,i}$) and effectiveness improvement index (i.e., $\overline{\Delta\eta_i}$), corresponding to each of these upgrades, have also been reported in Table 6. 6. These values have been obtained for each security upgrade according to the equations of Section 4.2.3, using the baseline effectiveness value (i.e., $\eta_{PPS,old} = 0.1759$) and the upgraded effectiveness value (i.e., $\eta_{PPS,new\,i}$).

Table 6. 6 Effectiveness results for six different possible PPS upgrades. From the left to the right, in column order: Upgrade identity, description of the upgrade, Physical protection function modification, reference number of adversary sequence diagram modified tasks, modified inputs for the effectiveness calculations, upgraded PPS effectiveness ($\eta_{PPS,new\,i}$) and effectiveness improvement index ($\overline{\Delta\eta_i}$). (*) Reduction of response force time does not affect a single task. A data repository regarding modified inputs values for security upgrades is available in Garcia (Garcia, 2007).

Upgrade ID	***Description***	***PPS - function modification***	***N° of modified tasks***	***Modified inputs***	$\eta_{PPS,\,new\,i}$	$\overline{\Delta\eta_i}$
A	**External fence sensors as perimeter detection system (at fence level)**	Detection; fence sensors	1	$P_{AD,1} = 0.9$	0.4941	**0.3182**
B	**Additional delay element by building a concrete wall with security door at sabotage target**	Delay; door hardness	2	$t_{D,5} = 150\ s$	0.2624	**0.0865**
C	**Reduction of response force time (by creating a closer guard dispatch)**	Response; relocation of guards closer to storage area	- (*)	$t_G = 180\ s$ (*)	0.6016	**0.4257**

The results in Table 6. 6 clearly show that, from the effectiveness point of view, the best option is the reduction of response force time (upgrade C), followed by the application of fence sensors (upgrade A). On the other hand, the presence of additional delay elements at sabotage target, represented by options B, proved to be almost ineffective in increasing PPS effectiveness. However, even if upgrade C is the best ones from the effectiveness intermediate calculation, it does not mean automatically that it will be the best options in the end of the application, due to additional terms that are still to be considered in the analysis (e.g., costs, benefits, budget threshold, etc.). The approach presented in Section 4.2.3, here applied, can be used analogously in other case studies. However, the results of effectiveness calculations are site-specific and accident-specific; consequently they cannot be generalized beyond the current case study.

6.3.3 Cost calculation for security upgrades

Cost calculations have been realized for each of the three PPS upgrades proposed in the case study, according to the six main categories mentioned in Section 4.2.4, subcategories and formula, presented in EM-PICTURES version of the methodology (see Section 4.2.4), considering the time span of one year and the implementation of a single security upgrade. Further information on cost assessment is reported in Section 4.2.4. It should be noted that many subcategories consist of wages, so realistic annual salaries have been retrieved from a specific database (PayScale, 2016) and converted into hourly wages considering 1920 hours/year.

Indeed, several data regarding cost calculation have been retrieved in U.S.A. dollars of year 2016; the conversion rate from U.S.A. dollars to € has been assumed 0.8683 $€/U.S.A.$ \$ (X-Rates, 2016) throughout the case study. Moreover, a location factor of 1.20 (Richardson Products & Cost Data On Line Inc., 2008) was applied in order to adjust US prices and salaries to those of Italy (i.e., Milan industrial area). The use of location factor throughout the analysis allowed a site-specific cost calculation. In the estimation of wages, several professional profiles, which are typically involved in the selection, design, installation and maintenance of a security system in a process facility, have been considered. According to their different job tasks, the following security-related jobs have been accounted for the calculation of appropriate cost subcategories: purchasing office staff and manager, security manager, security engineer, security guards and officers, training expert (i.e., security consultant), masons, installation and maintenance technicians.

In the calculation of Initial costs for each security upgrade, wages for the job profiles involved, costs of auxiliary materials have been considered. In the calculation of Installation costs, with

particular reference to Equipment costs, specific information of market prices has been retrieved from vendor websites for each security upgrade and reported in Table 6. 7.

In the calculation of Operating costs, Utility costs consist of the costs of annual electric power consumption, which are significant only for upgrade A. For upgrade A the power has been calculated through the standard power law, retrieving data on intensity and voltage from products datasheet (Shenzhen P&H Electronic Co. Ltd, 2016) and accounting the number of devices in place, which have been assumed to be working continuously all the yearlong. The estimated annual electric power consumption has been $4.73 \cdot 10^3 kWh$ for upgrade A. Considering an average industrial electric energy market price in Italy of 0.17 $€/kWh$ (Eurostat, 2016), utilities costs have been finally calculated. Human resources operating costs have been calculated by considering the manpower, in terms of security officers and guards wages for each of the security countermeasures, which was not negligible for upgrade A. It should be noted that for security upgrades B, which consists on an additional wall with door close to the possible targets (i.e., all the tanks of the tank farm), this subcategory is equal to zero. For upgrade C, the security guards have been just relocated, so no additional human resources operating costs have been accounted in comparison with the baseline situation.

Table 6. 7 Data for the calculation of Equipment costs for three different PPS upgrades.

UPGRADE ID	***DATA FOR THE CALCULATION OF EQUIPMENT COSTS***			
	Description	***Unit***	***Value***	***Reference/ Notes***
A	Cost of a couple of fence sensors (i.e., unit cost)	$€/unit$	20	(Shenzhen P&H Electronic Co. Ltd, 2016)
	Total number of fence sensors in place	$n°units$	330	8% of spare items not included
	Number of tanks	$n°units$	8	Layout of the facility
	Length and height of the concrete wall around unit type 1 (*) and unit type 2 (**)	m	650; 3	Layout of the facility
	Cost of the wall for each unit	$€/unit$	1700	(Get A Quote, 2016)
	Cost of security doors to be applied on each unit (both type 1 and type 2)	$€/unit$	1000	(Grainger, 2016)
C	Unit cost for the new building (standard warehouse with concrete floor and metal clad)	$€/m^2$	548	(BMT, 2016)
	Area of the building	m^2	50	Layout of the facility

In the calculation of Maintenance, inspection and sustainability costs the following assumptions have been applied for each security upgrade: material costs have been estimated by assuming an annual substitution rate for equipment and other materials in the range

between 3% and 5%, 2 scheduled maintenances, 1 unscheduled maintenances and 2 scheduled inspections per year have been accounted. License and renewal costs appeared to be negligible for all the three upgrades. Other running costs have been calculated for each security upgrade; only for upgrade C this cost category has a significant role, provided that the construction of a new building for security guards requires additional office furniture and utilities. In the calculation of Specific costs, the contribution offered by False-positive costs should be considered only for upgrade A (i.e., detection upgrade). For both these upgrades, despite a single false-alarm cost, according to expert judgement, is about $2.80 \cdot 10^3$ € and $P(alarm \mid no\ attack) = 0.143$ (Garcia, 2007), assuming the probability of the attack unitary turns false-positive costs to zero. Site-specific costs, as revisions of safety measures and procedures, have been accounted in particular for upgrade B (i.e., additional delay element), whose implementation might require a revision of emergency routes, as well as entrance and exit doors.

For each of the three security upgrades, the main results obtained from cost calculations, according to the six cost categories of EM-PICTURES, as well as the Overall costs ($C_{Security,i}$) have been summarized in Figure 6. 3 and reported in detail in Table 6. 8 for upgrade A, Table 6. 9 for upgrade B and Table 6. 10 for upgrade C respectively.

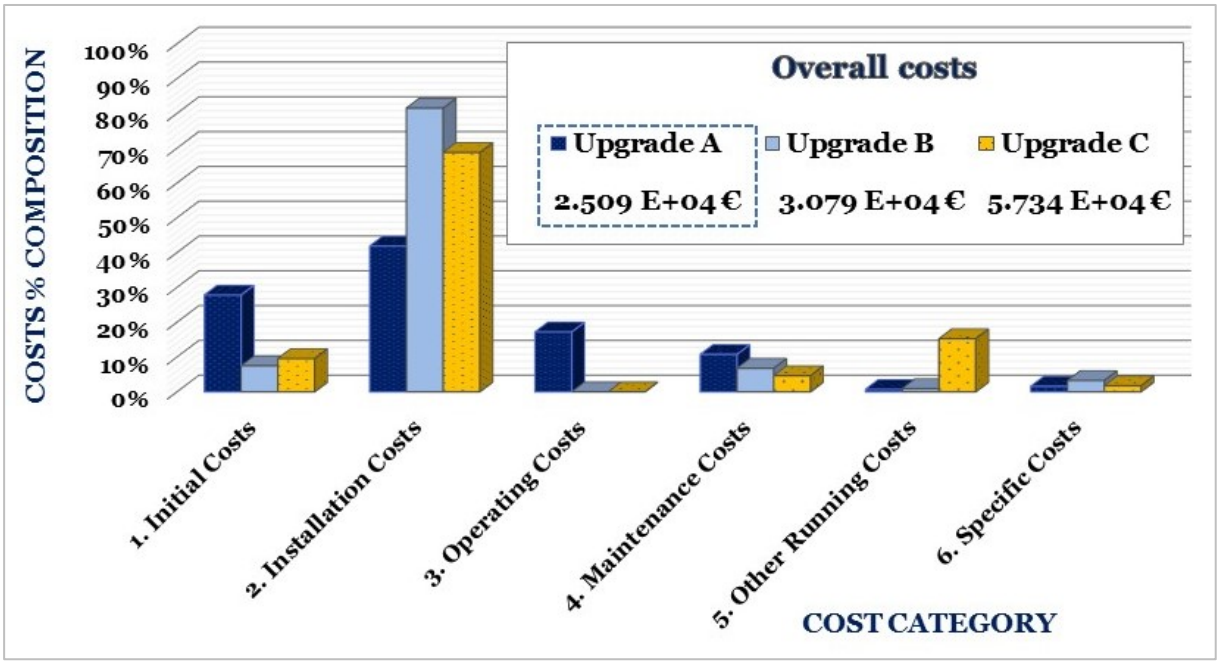


Figure 6. 3 Percentage composition of Overall costs for each upgrade of the PPS, according to six main cost categories, for $\boldsymbol{P(T)_{ij}}$. For each cost category, from the left to the right: A) Adding fence sensors as perimeter detection system; B) Adding a delay element by building a concrete wall with security door at sabotage target level; C) Reducing response force time by building a closer guard dispatch.

The cost calculations results, reported in Figure 6. 3 showed that the order of magnitude of the Overall costs is the same one for all the security upgrades. Nevertheless, despite cost distributions are slightly different, according to the security function, installation costs are the

prevailing ones for all the three security upgrades, with a percentage of 41.9 % for upgrade A, 81.5 % for upgrade B and 68.8 % for upgrade C respectively.

Table 6. 8 Overall costs results for upgrade A (i.e., fence sensors as perimeter detection system).

Calculation of Overall Costs for upgrade A				
Symbol	***Category/subcategory description***	***Unit***	***Value***	***Assumption***
$C_{INITIAL,OV}$	**1. Overall Initial costs**	**€**	**6.98E+03**	**See assumptions for subcategories**
C_{INV}	Investigation costs	€	6.46E+02	Purchasing officers, purchasing officer manager and security manager wages
$C_{S\&D}$	Selection and design costs	€	5.51E+02	Security engineer, purchasing officer manager and security manager wages
$C_{MAT,I}$	Material costs	€	3.50E+03	Cost of cables at perimeter level and monitoring software
C_T	Training costs (start-up/in service)	€	1.98E+03	Training expert (security consultant) and security guards/officers wages
$C_{G\&I}$	Changing of guidelines and informing costs	€	3.00E+02	Cost of leaflets for internal use
$C_{INSTALL,OV}$	**2. Overall Installation costs**	**€**	**1.05E+04**	**See assumptions for subcategories**
C_{START}	Start-up costs	€	1.21E+03	Maintenance technicians and security engineer wages
C_E	Equipment costs (including P - purchase & R - rental costs, space requirement costs)	€	6.60E+03	Costs of fence sensors, no space requirement costs, no rented equipment costs
$C_{INSTALL}$	Installing costs	€	2.70E+03	External personnel, maintenance technicians, IT engineer and security manager wages
$C_{OPERATION,OV}$	**3. Overall Operating costs**	**€**	**4.32E+03**	**See assumptions for subcategories**
$C_{U,OP}$	Utilities costs	€	8.04E+02	Electric power consumption
C_{HRO}	Human resources operating costs	€	3.52E+03	Security guards and officer wages for monitoring action
$C_{MIS,OV}$	**4. Overall Maintenance, Inspection and Sustainability costs**	**€**	**2.70E+03**	**See assumptions for subcategories**
$C_{MAT,M}$	Material costs	€	3.00E+02	Cables and sensors components substitution
C_{MNT}	Maintenance team costs (A- scheduled m. /B- unscheduled m.)	€	1.72E+03	Maintenance technicians and security engineer wages
C_{INSP}	Inspection team costs	€	6.87E+02	Maintenance technicians and security engineer wages
C_{LIC}	License and rental renewal	€	0	No license and rental renewal costs
$C_{OR,OV}$	**5. Other Running costs**	**€**	**1.80E+02**	**See assumptions for subcategories**
C_{OF}	Office furniture costs	€	0	No additional office furniture required
C_T	Transport costs	€	1.00E+02	Assumption based on expert judgement
C_{COMM}	Additional communication costs	€	6.00E+01	Assumption based on expert judgement
C_I	Insurance costs	€	0	No additional insurance costs
C_{OU}	Office utilities costs	€	2.00E+01	Assumption based on expert judgement
C_{OS}	Office supplies costs	€	0	No office supplies required
$C_{SPEC,OV}$	**6. Overall Specific costs**	**€**	**4.00÷8.00 E+02**	**See assumptions for subcategories**
C_{FP}	False-positive case costs	€	0 ÷ 4.00 E+02	False-positive costs equal to zero with $P(T)_{ij} = 1$
C_{SITE_SP}	Site-specific costs	€	1.80E+02	Cleaning of plant perimeter to limit false-positive cases
$C_{Security,i}$	***Overall Costs***	**€**	**2.51 ÷ 2.56 E+04**	-

Table 6. 9 Overall costs results for upgrade B (i.e., additional delay element by building a concrete wall with security door at sabotage target level).

Calculation of Overall Costs for upgrade B				
Symbol	***Category/subcategory description***	***Unit***	***Value***	***Assumption***
$C_{INITIAL,OV}$	**1. Overall Initial costs**	**€**	**2.31E+03**	**See assumptions for subcategories**
C_{INV}	Investigation costs	€	6.46E+02	Purchasing officers, purchasing officer manager and security manager wages.
$C_{S\&D}$	Selection and design costs	€	1.04E+03	Security engineer, purchasing officer manager and security manager wages.
$C_{MAT,I}$	Material costs	€	0	Reinforced concrete wall considered as equipment, no additional materials considered to produce it
C_T	Training costs (start-up/in service)	€	3.30E+02	Training expert (security consultant) and security guards/officers wages
$C_{G\&I}$	Changing of guidelines and informing costs	€	3.00E+02	Cost of leaflets for internal use
$C_{INSTALL,OV}$	**2. Overall Installation costs**	**€**	**2.51E+04**	**See assumptions for subcategories**
C_{START}	Start-up costs	€	9.22E+02	Masons, security engineer for supervision
C_E	Equipment costs (including P - purchase & R - rental costs, space requirement costs)	€	2.19E+04	Price of concrete wall installation around each tank, price of security doors, costs due to rented tools for construction works
$C_{INSTALL}$	Installing costs	€	2.28E+03	Masons, maintenance technicians and security manager wages
$C_{OPERATION,OV}$	**3. Overall Operating costs**	**€**	**0**	**See assumptions for subcategories**
$C_{U,OP}$	Utilities costs	€	0	No utilities required
C_{HRO}	Human resources operating costs	€	0	No human resources required
$C_{MIS,OV}$	**4. Overall Maintenance, Inspection and Sustainability costs**	**€**	**2.09E+03**	**See assumptions for subcategories**
$C_{MAT,M}$	Material costs	€	6.48E+02	Annual substitution costs
C_{MNT}	Maintenance team costs (A-scheduled m. /B- unscheduled m.)	€	1.10E+03	Maintenance technicians and security engineer wages
C_{INSP}	Inspection team costs	€	3.44E+02	Maintenance technicians and security engineer wages
C_{LIC}	License and rental renewal	€	0	No license and rental renewal costs
$C_{OR,OV}$	**5. Other Running costs**	**€**	**2.80E+02**	**See assumptions for subcategories**
C_{OF}	Office furniture costs	€	0	No additional office furniture required
C_T	Transport costs	€	2.00E+02	Assumption based on expert judgement
C_{COMM}	Additional communication costs	€	6.00E+01	Assumption based on expert judgement
C_I	Insurance costs	€	0	No additional insurance costs
C_{OU}	Office utilities costs	€	2.00E+01	Assumption based on expert judgement
C_{OS}	Office supplies costs	€	0	No office supplies required
$C_{SPEC,OV}$	**6. Overall Specific costs**	**€**	**1.00E+03**	**See assumptions for subcategories**
C_{FP}	False-positive case costs	€	0	No false-positive costs
C_{SITE_SP}	Site-specific costs	€	1.00E+03	Revision of safety systems (e.g. emergency door/entrance and exit doors)
$C_{Security,i}$	***Overall Costs***	**€**	**3.08E+04**	-

Table 6. 10 Overall costs results for upgrade C (reduction of response force time by guard relocation in a closer dispatch).

Calculation of Overall Costs for upgrade C				
Symbol	**Category/subcategory description**	**Unit**	**Value**	**Assumption**
$C_{INITIAL,OV}$	**1. Overall Initial costs**	**€**	**5.48E+03**	**See assumptions for subcategories**
C_{INV}	Investigation costs	€	6.46E+02	Purchasing officers, purchasing officer manager and security manager wages.
$C_{S\&D}$	Selection and design costs	€	5.51E+02	Security engineer, purchasing officer manager and security manager wages.
$C_{MAT,I}$	Material costs	€	2.00E+03	Cost of cables and connections
C_T	Training costs (start-up/in service)	€	1.98E+03	Training expert (security consultant) and security guards/officers wages
$C_{G\&I}$	Changing of guidelines and informing costs	€	3.00E+02	Cost of leaflets for internal use
$C_{INSTALL,OV}$	**2. Overall Installation costs**	**€**	**3.94E+04**	**See assumptions for subcategories**
C_{START}	Start-up costs	€	5.57E+02	Masons and security engineer wages
C_E	Equipment costs (including P - purchase & R - rental costs, space requirement costs)	€	3.22E+04	Cost of building for hosting security guards, rented tools for construction works and space requirement costs
$C_{INSTALL}$	Installing costs	€	6.67E+03	Masons, maintenance technicians, security engineer and security manager wages
$C_{OPERATION,OV}$	**3. Overall Operating costs**	**€**	**0**	**See assumptions for subcategories**
$C_{U,OP}$	Utilities costs	€	0	No utilities required
C_{HRO}	Human resources operating costs	€	0	No additional human resources required in comparison with baseline
$C_{MIS,OV}$	**4. Overall Maintenance, Inspection and Sustainability costs**	**€**	**2.67E+03**	**See assumptions for subcategories**
$C_{MAT,M}$	Material costs	€	9.22E+02	Equipment annual substitution
C_{MNT}	Maintenance team costs (A- scheduled m. /B- unscheduled m.)	€	1.06E+03	Maintenance technicians and security engineer wages
C_{INSP}	Inspection team costs	€	6.87E+02	Maintenance technicians and security engineer wages
C_{LIC}	License and rental renewal	€	0	No license and rental renewal costs
$C_{OR,OV}$	**5. Other Running costs**	**€**	**8.75E+03**	**See assumptions for subcategories**
C_{OF}	Office furniture costs	€	6.09E+03	Additional office furniture required, based on expert judgement
C_T	Transport costs	€	1.00E+02	Assumption based on expert judgement
C_{COMM}	Additional communication costs	€	6.00E+01	Assumption based on expert judgement
C_I	Insurance costs	€	0	No additional insurance costs
C_{OU}	Office utilities costs	€	2.50E+03	Assumption based on expert judgement
C_{OS}	Office supplies costs	€	0	No office supplies required
$C_{SPEC,OV}$	**6. Overall Specific costs**	**€**	**1.00E+03**	**See assumptions for subcategories**
C_{FP}	False-positive case costs	€	0	No false-positive costs for this security upgrade
C_{SITE_SP}	Site-specific costs	€	1.00E+03	Revision of emergency routes/plan after guards relocation
$C_{Security,i}$	***Overall Costs***	**€**	**5.73E+04**	-

6.3.4 Benefit calculation for an expected scenario

In the present study, an expected scenario has been considered, as a prospective analysis is carried out. Expected benefits are the losses derived from a hypothetical scenario, which considers the average benefits, weighted by probabilities of occurrence, of four possible outcomes (i.e., indicated with T1, T2, T3 and T4 in decreasing order of severity, and named catastrophic, critical, marginal and negligible accident respectively), as described in Section 4.2.5.

Illustrative probabilities were defined for each category of scenario and listed in Table 6. 11, together with a description of the losses for each scenario. Benefit calculations have been carried out according to according to the nine categories and subcategories proposed in EM-PICTURES version of the model, suitable for a generic security-based accident; the results of benefit calculations for the four scenarios are available in Figure 6. 4.

In the calculation of Supply chain benefits, a realistic production rate for the facility has been estimated by assuming a production rate of $2.66 \cdot 10^5\ kg/h$; for the conversion into mass flow rate a reference density for naphtha has been considered (Engineering ToolBox, 2017). The profit per unit sold that is the market price equal to $4.08 \cdot 10^{-4}$€ (Wang and Kim, 2015). For Schedule benefits, the fine for a cancelled contract has been assumed, based on expert judgment, $1.00 \cdot 10^5\ €/contract$ and the fine for delay in deliveries per day, $1.00 \cdot 10^4\ €/(delay \cdot day)$.

In the calculation of Damage benefits, illustrative commercial equipment costs for storage tanks have retrieved from vendors (Shanghai Iven Pharmatech Engineering Co. Ltd, 2016): a commercial value of $8.00 \cdot 10^4$ € for $40000\ m^3$ tank has been assumed throughout the case study. For the estimation of finished goods damages, the naptha market price has been applied.

In the calculation of Legal benefits and after, it should be noted that, as for costs calculations, many benefits subcategories consist of wages; the expression for converting annual salaries into hourly wages applied has been the same one reported in Section 6.3.3. Moreover, also the same values regarding conversion rate from U.S.A. dollars to € and location factor have been applied (Section 6.3.3). In the case of Legal benefits, the job profiles involved are junior lawyers and seniors lawyers, specialized lawyers, security manager, security engineer, security analyst and security consultant. The total security budget prior to the accident has been assumed, based on expert judgment, $8.00 \cdot 10^4$ €, but the percentage increase of the security budget is scenario dependent.

In the calculation of Insurance benefits, the value of the current total premium cost of the facility has been considered, based on expert judgment, $5.00 \cdot 10^7$€, while the percentage increase of the premium due to the accident is scenario dependent. In the calculation of Human

benefits, the value of a statistical life (VSL) has been retrieved from a previous study (Viscusi and Aldy, 2003) and converted from $U.S.A.\$(2000)$ into €(2016) by the application of appropriate conversion rate (X-Rates, 2016) and inflation rate (Friedman, 2017); the final VSL is $7.07 \cdot 10^6$€. Following the same reference and approach, the monetary values for a light and a serious injury are respectively $1.41 \cdot 10^4$ € and $2.06 \cdot 10^5$ €.

In the calculation of Intervention benefits, a different flat rate has been assumed for the three scenarios. In the calculation of Reputation benefits, a current total market price for the company of $1.84 \cdot 10^8$€ has been accounted, but the expected percentage drop is scenario dependent. In the calculation of Other benefits, wages for security manager and cleaning employees have been accounted, while in the estimation of Specific benefits, transportation delays costs and psychological counselling for accident witnesses have been considered. The data applied for the calculation of benefit categories and subcategories were retrieved from a collection of references and validated by a panel of security managers and academic security experts.

The comparison among benefits percentage compositions obtained for each scenario by using the respective Overall benefits as reference and reported in Figure 6. 4, shows that benefits distributions depend on the scenario selection: for catastrophic (i.e., T1) and critical scenarios (i.e., T2), the costs due to casualties and injuries are prevailing, while for marginal (i.e., T3) and negligible (i.e., T4) accidents, the prevailing losses are related to legal issues and assets damages. Indeed, as stated in previous studies referred to benefit assessment for major accidents within the chemical industry domain (Gavious et al., 2009; Reniers and Brijs, 2014b), the value of indirect losses, which include for instance reputational losses, human and environmental losses, legal and insurance losses, is generally superior to direct losses. The gap tends to increase with the increasing severity of the accident (Gavious et al., 2009), as confirmed also by Figure 6. 4. The Overall expected benefit value is $2.436 \cdot 10^5$ €; the expected benefits apportionment is reported in Figure 6. 5; it confirmes that human and environmental benefits are prevailing, followed by legal benefits and assets damages.

Table 6. 11 Description of the scenarios applied in the case study for expected benefit assessment. Expected benefits have been calculated as the average of four possible outcomes (i.e., T1, T2, T3 and T4), weighted by respective probabilities of occurrence. T1 benefits overlaps with worst-case scenario. Vulnerability probabilities are considered unitary within the present case study.

SCENARIO ID / BENEFITS	EXPECTED			
	T1 **Catastrophic accident**	**T2** **Critical accident**	**T3** **Marginal accident**	**T4** **Negligible accident**
	Probability of occurrence			
	1.00E-05	2.00E-01	7.50E-01	5.00E-02
	Description			
1. Overall supply chain benefits	Stop in production for 24 hours; 0% production rate at reactivation; 48 hours start-up; fines for delays in deliveries and 1 order cancelled	Stop in production for 6 hours; delays in the supply chain	Production slowed for few hours; delays in the supply chain, facility at 80% of its production rate at reactivation	Negligible
2. Overall damage benefits	3 tanks destroyed with content; severe damage to piping; severe damages to other company's and public properties; severe damage to surrounding living areas	One tank completely destroyed and other assets damages (e.g., contiguous tanks).	Two tanks damaged (20%); minor other assets damages	Minor damages to 2 tanks (5%)
3. Overall legal benefits	Civil liability fine for pollution; lawyers' wages; 80% increase of the Security budget; possible closing down (10%)	Fines; salaries; 50% increase of Security budget	Fines; salaries; 30% increase of Security budget	Fines; salaries; 8% increase of Security budget
4. Overall insurance benefits	1% premium increase	0.1% premium increase	10^{-2}%premium increase	10^{-3}% premium increase
5. Overall human and environmental benefits	2 casualties; 3 serious injuries and 5 light injuries; several new recruitments; content of the three tanks burnt; severe environmental damages	2 serious injuries; 4 light injuries; environmental damages	1 light injury; marginal environmental damages	Negligible
6. Overall intervention benefits	Massive Emergency intervention, with special units	Critical	Marginal	Negligible
7. Overall reputation benefits	0.5% expected drop in the share-price	10^{-4}% share price drop	$5 \cdot 10^{-5}$%share price drop	10^{-5}% share price drop
8. Other benefits	Significant manager work-time benefits and cleaning benefits	Critical	Marginal	Negligible
9. Overall specific benefits	Severe airport and traffic delays; relevant immaterial consequences	Critical	Marginal	Negligible

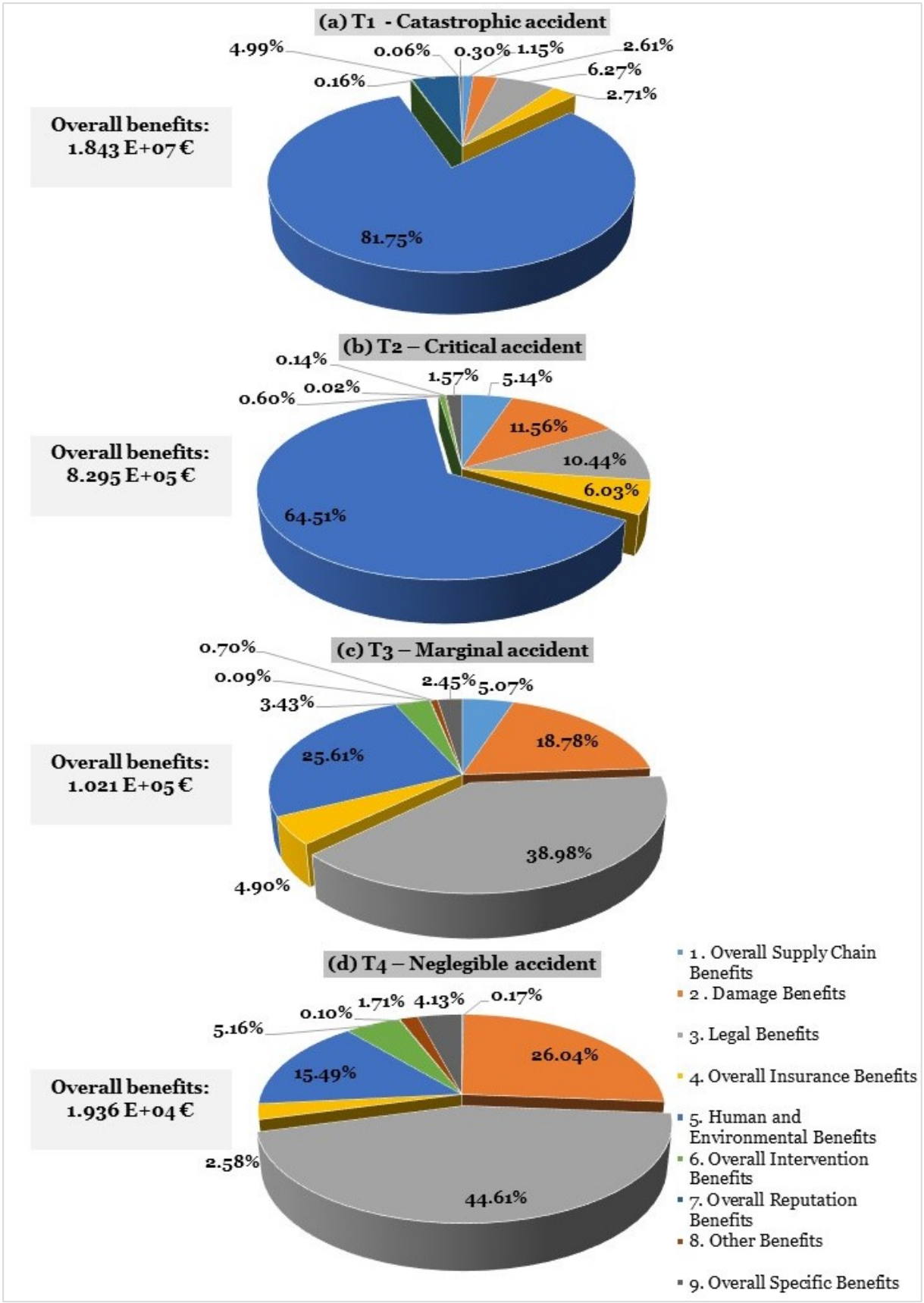


Figure 6. 4 Percentage composition of Overall benefits for four different scenarios: (a) T1, (b) T2, (c) T3 and (d) T4, composing the expected scenario, calculated according to the categories of the model, in EM-PICTURES version. Overall benefits values are reported in the box on the left for each scenario.

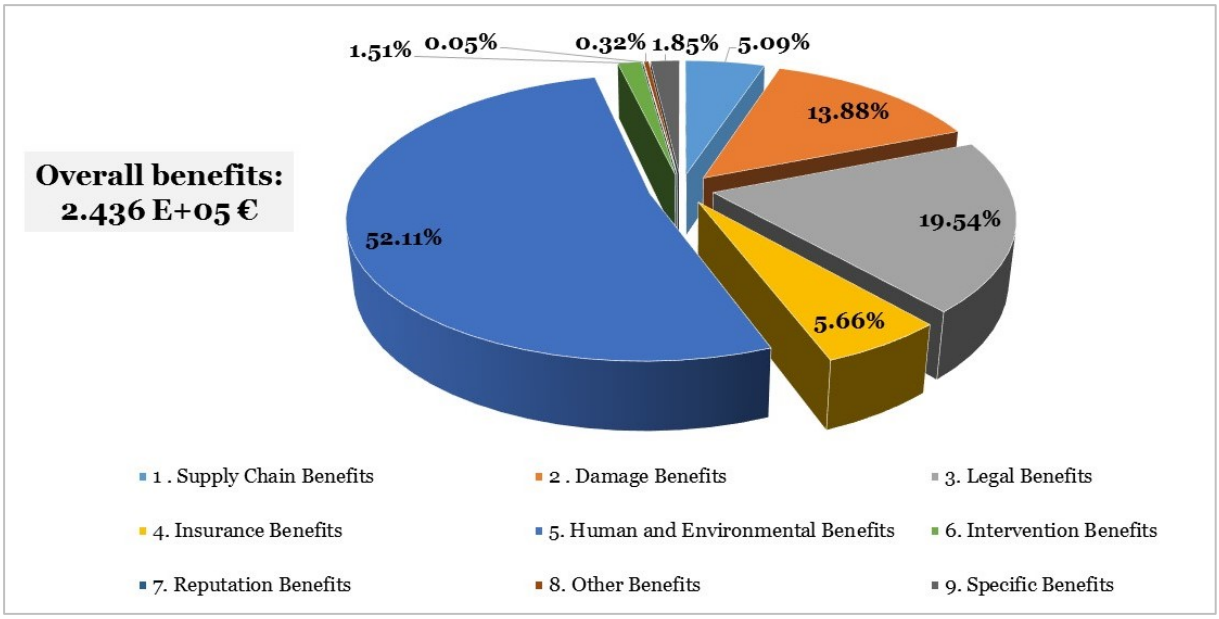


Figure 6. 5 Percentage composition of Overall benefits for the expected scenario, according to nine benefits categories proposed in EM-PICTURES version of the model.

6.3.5 Results of the case study

The results of the assessment of the case study consist in cost-benefit analysis results, which are the values of actualized Net benefits, for three PPS upgrades with reference to the expected scenario, according to EM-PICTURES version of the economic model.

Overall costs for each security measure and Overall expected benefits have been made comparable by applying appropriate discount rates (i.e., 3.5 % and 1.5 % respectively (HSE - Health and Safety Executive, 2016)) over a 10 year time-span. The latter is a conventional number of operational years for a security measure. Considering several values for the likelihood of the attack $(P(T))$, the values of Net Benefit, also named Net Present Value (NPV), have been calculated for each of the three PPS upgrades, according to the expected losses, by applying equation (4.20). The values have been compared with respect to the acceptability criteria, expressed by equation (4.21).

The results of cost-benefit analysis, reported in Figure 6. 6, prove the coherency of the model, highlighting that the feasibility of all the security upgrades is dependent on the value assumed for the likelihood of the attack. Indeed, all the three upgrades are feasible under the assumption of likelihood of the attack unitary, even if the values of Net Benefit are higher for Upgrades A and C than for Upgrade B. Nevertheless, the results of cost-benefit analysis for different values of the likelihood of the attack show that Upgrade A is feasible even for low values of the likelihood of the attack (i.e., 0.2), while Upgrade C is not. Therefore, the possible suggestion derived from the economic indicators may be to adopt security upgrade A, due to

its feasibility even with low probabilities of the attack and to its high Net Benefit under deterministic assumption.

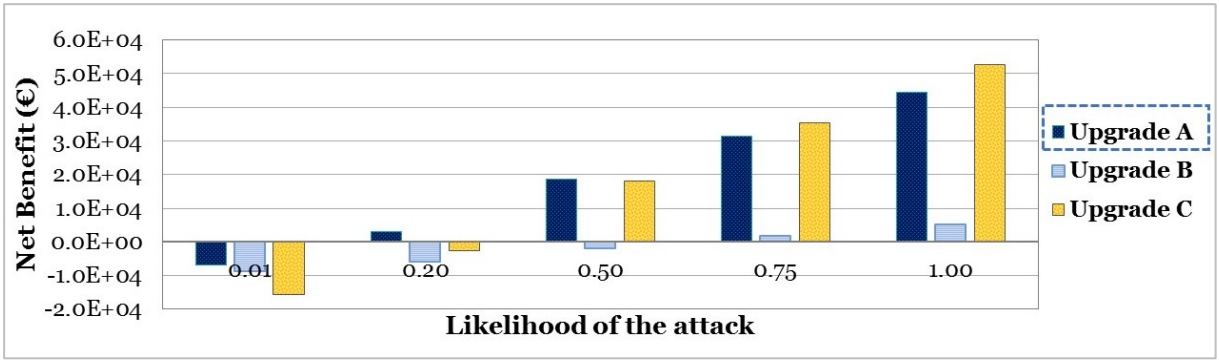


Figure 6. 6 Results of cost-benefit analysis for three security upgrades, with reference to different values of the likelihood of the attack $(\boldsymbol{P(T)})$ and to an expected scenario.

Cost-effectiveness analysis has been applied in order to determine the most profitable combination of security upgrades within the security budget constraint for the expected scenario, according to the deterministic approach proposed in EM-PICTURES version of the model (Section 4.2.8.1). All the possible 7 combinations of PPS upgrades have been considered, starting from each single security measure, to couples and triplet. Actualized Overall costs have been calculated for each combination by applying a 3.5% discount rate to the pertinent cost categories of each option taken and by summing the actualized costs (HSE - Health and Safety Executive, 2016), then Overall costs have been compared with the actualized security budget. For each scenario, only the combinations respecting the budget criteria have been selected and their Net Benefits have been calculated and compared, according to equation (4.27). For instance, the triplet of security measures A+B+C is the only combination not respecting the security budget among all the possible ones.

The results of cost-effectiveness analyses, reported in Figure 6. 7, show that the combination of security upgrades A and C (i.e., application of fence sensors at external fence level and relocation of security guards) is the one with the highest Net Benefit for all the values of the likelihood of the attack considered in the analysis, with the exception of $P(T) = 0.01$. For the latter value of the threat probability, the application of upgrade A is the most profitable option. However, the second most profitable combination varies with the likelihood of the attack.

Figure 6. 7 shows the complete ranking of all possible combinations of security measures, according to cost-effectiveness analysis, for the values of the likelihood of the attack considered in the analysis. The results show that several profitable combinations offer an integration of different security functions (i.e., detection and response), providing therefore a more complete security protection.

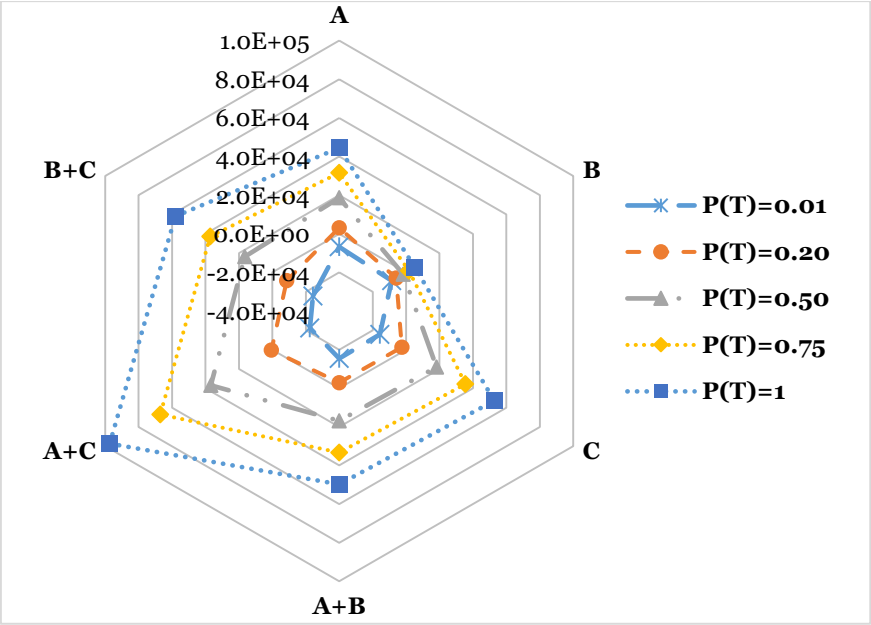


Figure 6. 7 Results of cost-effectiveness analysis, expressed as Net Benefit in €(2016), for the combinations of security upgrades respecting budget, with reference to different values of the likelihood of the attack $(P(T))$ and to an expected scenario.

6.3.6 Discussion and conclusions on the case study

The current section has been aimed at applying the EM-PICTURES version of the economic model to an original case study, regarding a sabotage to a storage tank farm. The case study dealt with a simplified plant layout and a sabotage action with one target, in purpose to test the model.

The application demonstrated that the model provides site-specific answers to security analysts, because it allows evaluating the performance of physical security measures present on-site and proposing several pertinent security upgrades, in relation with the specific adversary action and according to the security functions of detection, delay and response. Therefore, effectiveness assessment is site-specific and accident-specific, as it depends on the possible adversary path of actions. Therefore, the results obtained from effectiveness assessment, which suggest guard relocation in a closer dispatch as possible security upgrade, cannot be generalized beyond this case study. The cost assessment allows defining the most relevant cost items due to the implementation of security measures, which are indirect costs for all the upgrades proposed; the analyst, according to the model structure, can add site-specific information. Information regarding certain cost voices needs to be retrieved from vendors; as visible in Section 6.3.3 it is necessary to present cost calculations in a detailed manner and to discuss possible assumptions made and uncertainties arisen.

The case study included benefit assessment, which was carried out considering an expected scenario, as proposed in the methodology section for prospective applications (see Section

4.2.5). The precise categories and subcategories elaborated for benefit calculations allows preventing omissions and inaccuracies; nevertheless, its inputs are validated for the case study by a panel of security experts, in purpose to avoid misleading conclusions.

As discussed in Section 4.3, also the assumptions regarding discount rates for overall costs and benefits might be affected by subjectivity of the analyst, therefore specific guidance values have been considered in the case study. Indeed, simplifying assumptions have been assumed for threat and vulnerability probabilities. Different values of threat probabilities were considered to provide a broad spectrum of economic indicators. Vulnerabilities probabilities were assumed unitary throughout the case study. The deterministic approach provided by EM-PICTURES here-in applied provide guidance for the choice of threat probabilities and it allows focusing on the role of security measures in the prevention of accidental scenarios.

The results of the case study made clear that model application, even to a simplified extent, provides useful insights on the profitable security measures to be adopted in a process facility, by means of its outputs, which are a set of economic security-related indicators. Model outputs are a broad spectrum of economic analyses results, which can eventually support the security decision-making process. Indeed, the interpretation of the economic analyses results derived from the case study is particularly important, as demonstrated by the case study. Within this specific application, the results provided by cost-benefit and cost-effectiveness analyses are coherent. For instance, cost-benefit analysis results suggest to apply either additional detection at perimeter level or to relocate guards; cost-effectiveness analysis results confirm that the combination of these two measures is generally the most profitable option, according to different values of the threat probability. The results of cost-effectiveness analysis depend on the security budget threshold that is generally defined yearly by security management, which in the present case study is not particularly strict, as it excludes only one possible combination of security upgrades (i.e., a triplet of upgrades). Moreover, it should be noted that in the simplified case study here in considered, cost-effectiveness analysis results do not offer relevant additional guidance to decision-makers because the pool of possible security upgrades is very limited.

Indeed, several aspects regarding the application of EM-PICTURES version of the model need to be tested to an additional case study, as they have not been investigated in the present case study, before proposing the use of EM-PICTURES within chemical and process industry and related regulatory bodies:

- Benchmark application to a case study inspired by a real terroristic attack to a chemical plant, in purpose to apply realistic plant layout, site-specific and accident-specific information is required;

- Application of adversary sequence diagrams to multiple paths, considering a complex terroristic action with multiple targets should be carried out;
- Proposal of more than one security upgrade belonging to each security function should be considered, with the aim to extend effectiveness and cost assessment and to offer a broader pool of protection alternatives within economic analyses;
- Benefit assessment may be extended to multiple scenarios, in purpose to evaluate the role of scenario selection on security budget, model outputs and to apply multi-scenario economic criteria provided by the model;
- Retrospective application of the model should be carried out to validate occurrence probabilities for accidental scenarios;
- Specific information on the terroristic organization responsible for the accident should be applied, with the aim to evaluate threat and vulnerabilities probabilities realistically;
- Sensitivity analysis on cost-benefit and cost-effectiveness results may be performed, considering the effect of threat and vulnerabilities variations on model outputs.

In conclusion, the application of EM-PICTURES to a simplified case study demonstrated that this model version might provide a sound support to managers and regulators within the decision-making process, suggesting possible solutions for the optimal selection of security prevention investments, but the full potential of EM-PICTURES still needs to be tested to a more extended case study.

6.4 SELECTION OF PREVENTIVE COUNTER-TERRORISM MEASURES IN CHEMICAL FACILITIES (EM-PICTURES APPLICATION)

In this Section, the economic model for the selection and allocation of preventive physical security measures against terroristic attacks in chemical facilities, presented in Section 4, is tested to a realistic case study, according to EM-PICTURES version. The application is aimed at better understanding the full potential and possible outcomes of the approach developed, by means of an illustrative case study, freely inspired by a possible terrorism-related event that took place in a chemical facility in France.

6.4.1 Definition of the case study

The proposed EM-PICTURES version of the model was applied to an illustrative case study, inspired by a real incident that took place on July 14th, 2015 in Berre l'Étang, France, consisting in the sequential sabotage of two storage tanks in a chemical facility (Associated Press, 2015;

BBC News, 2015b; Le Guernigou and Revilla, 2015; Le Huffington Post, 2015; Pardini, 2016; RFI News, 2015).

Figure 6. 8 A picture of the accident, happened on July 14th 2015 in a refinery in Berre l'Étang, France that freely inspired the case study.

The analysis carried out focuses on the selection and management of the security measures, given the probability of the attack. Considering the analysis temporary posterior to the event and in purpose to maintain the focus on the role of security measures, the probability of the attack was assumed equal to one throughout the case study. Indeed, the assumption of $P(T)_{ij} = 1$ was justified by guidance values reported in Section 4.2.6 (Table 4. 5). Due to the limited amount of information available, $P(H \mid T)$ and $P(L \mid H)$ have been assumed equal to 1, following the conservative assumptions reported in Table 4. 5. The effect of these assumptions on the case study results has been evaluated by means of an uncertainty analysis.

The tank farm considered in the case study includes 40 atmospheric storage tanks, but 6 of them are dismissed. The scope of introducing dismissed tanks in the illustrative case study is to give security analysts a practical answer on security strategies to be adopted on dismissed areas of the plant/dismissed equipment, located close to the possible targets, but not containing hazardous substances anymore. The tanks have two different sizes: 10 have a volume of 40000 m^3 and contain naphtha, while 30 have a volume of 10000 m^3 and contain gasoline. The accidental scenario considered consists of a sequential sabotage to two storage tanks (i.e., multiple targets), named after respectively "first sabotage target" and "second sabotage target" as shown in Figure 6. 9. "First target" is a 40000 m^3 naphtha tank, while "second target" is a gasoline tank. The distance between the two targets is 500 m. The starting point for the adversary was chosen in correspondence of a pedestrian route just outside the border of the facility (i.e., 300 m from the first target). Indeed, investigations have shown holes in the perimeter of the fence close to one of the sabotage target (BBC News, 2015b). The adversary was supposed to carry out the sabotage action by foot, placing improvised explosives on the targets, as confirmed by recent investigations (Pardini, 2016). Electronic devices, compatible with detonators, were found in proximity of the targets (BBC News, 2015b). The

realistic damages, derived from the actual event, consisted on fire, environmental damage, but no casualties. The two tanks involved in the accident were completely destroyed, as well as their content. It was assumed that during emergency intervention, which lasts 13 hours, refinery activities were not shut down, but production rates were decreased. Moreover, additional consequences on public transportation (i.e., temporary highway closing-down, delays in the local airport) were derived from the actual event. In conclusion, the media screening highlighted several key aspects of the accident, as size and content of tanks, probable accident dynamic, features of emergency team intervention, and main consequences of the accident, which allowed carrying out the EM-PICTURES application in a realistic manner.

The determination of PPS in place was carried out comparing the description of PPS usually present in chemical facilities (Reniers et al., 2015) with photos and maps of the layout of a reference installation, reported in Figure 6. 9. The screening allowed the identification of key protection elements and key distances, which are data necessary to calculate the baseline physical protection system effectiveness. Further information on the PPS in place has been reported in Section 6.4.2.2. The application was carried out in Excel® modelling environment, using 7 different datasheets, corresponding to EM-PICTURES modules, as explained in Section 4.2.1.

6.4.2 Development of adversary sequence diagrams and effectiveness calculation

6.4.2.1 Definition of site-specific adversary sequence diagrams and calculation of the baseline system effectiveness

A possible site-specific adversary sequence path, in relation with physical protection elements present on the site, has been found. Two segments related to the two sabotage targets have been identified: “Segment n°1” connects the starting point with the first target; “Segment n°2” connects the first target with the second one. The details have been reported in Table 6. 12, Part A and Figure 6. 9. The calculation of baseline system effectiveness was carried out accordingly to Section 4.2.2, following EM-PICTURES version of the model, suitable for multi-target malevolent actions, with the aim to determine the probability of interruption (P_I), for the critical paths of the two segments.

The detection elements present in both the segments are cameras on doors, at level of both the sabotage targets, whose $P_{AD} = 0.9$. In addition, the location of detection elements has been included in the analysis, according to EASI model. For all delay elements with the exception of running times, specific data have been retrieved (Garcia, 2007) and reported in Table 6. 12, Part A, joined with all the data inherent to the detection function, for both the paths considered in the case study. For the calculation of running times, the standard adversary velocity of

$10\ ft/s = 3.048\ m/s$ has been assumed, considering a reduction factor due to the weight of explosives and detonators. Distances among delay elements have been retrieved from the map and reported in Table 6. 12, Part B. Inputs for the calculation of response element have been reported in Table 6. 12, Part C.

Figure 6. 9 Layout of a reference installation considered in the case study, with adversary starting point, sabotage targets and critical adversary paths, divided into two segments. Segment n°1 connects the starting point with the first target. Segment n°2 connects the first target with the second target. The ending point of adversary sequence of actions is the second target.

The EASI model, applied for the calculation of the effectiveness, takes into account uncertainties regarding each task (e.g., presence of a lag time in the detection) by applying probability distribution. According to the conservative assumption on data dispersion of the model (Garcia, 2007), standard deviation for each security element has been assumed as 3/10 of the mean value throughout the case study. This assumption allows considering uncertainties, as guards that will not always respond exactly after the same time and adversary that may take more or less time to penetrate barriers with respect to average values.

The critical probabilities of interruption (P_I) are respectively 0.27 for segment n°1 and 0.16 for segment n°2; these values represent the baseline PPS effectiveness for the two segments (i.e., $\eta_{PPS,old\ k}$) that will be considered in the following developments of the case study.

Table 6. 12 Inputs for the calculation of baseline PPS effectiveness. From the top to the bottom: Part A) Adversary sequence and inputs for the calculation of detection and delay elements for critical segment n°1 and critical segment n°2; Part B) Additional data for the calculation of running delay times for both the segments; Part C) Inputs for the calculation of the response function, valid for both the segments.

Part A) Adversary Sequence Diagrams and Inputs for Detection and Delay elements				
ADVERSARY TASKS – CRITICAL PATH - SEGMENT N°1		***DETECTION***	***DELAY***	
Task n°	***Task Description***	***Detection elements***	***Delay elements***	***Mean delays (s)***
1	**Cut simple wired perimeter fence**	none	Fence fabric	10.0
2	**Run to first tank protected area**	none	Running time	65.6
3	**Open door**	camera on the door; $(P_{AD,3} = 0.9)$	Height of the wall	30.0
4	**Run to first tank (target)**	none	Running time	131.2
5	**Sabotage first target**	none	Place explosives and detonators	120.0
ADVERSARY TASKS – CRITICAL PATH - SEGMENT N°2		***DETECTION***	***DELAY***	
Task n°	***Task Description***	***Detection elements***	***Delay elements***	***Mean delays (s)***
6	**Exit first target zone**	none	Running time	21.9
7	**Run to second tank protected area**	none	Running time	196.9
8	**Open door**	camera on the door $(P_{AD,8} = 0.9)$	Door hardness	30.0
9	**Reach second tank (target)**	none	Running time	91.9
10	**Sabotage second target**	none	Place explosives and detonators	120.0

Part B) Data for Calculation of running delay times							
Description of the action	***Symbol***	***Value***	***Unit***	***Description of the action***	***Symbol***	***Value***	***Unit***
Adversary velocity during running	v	3.048	*m/s*	**Distance first wall/first target (Task 4 – segment n°1)**	d_2	200	*m*
Reduction velocity factor due to additional weight - a (before first sabotage – segment n°1)	φ_1	0.5	*adim.*	**Distance first target/exit first target zone (Task 6 – segment n°2)**	d_3	50	*m*
Reduction velocity factor due to additional weight - b (after first sabotage – segment n°2)	φ_2	0.75	*adim.*	**Distance exit first target zone/ second wall (Task 7 – segment n°2)**	d_4	450	*m*
Distance out/first wall (Task 2 – segment n°1)	d_1	100	*m*	**Distance second wall/second target (Task 9 – segment n°2)**	d_5	210	*m*

Part C) Data for the calculation of Response function			
Probability of guard communication	0.95	***Mean Response Force Time (s)***	300

6.4.2.2 Proposal of five security upgrades and calculation of upgraded system effectiveness

Starting from the values of baseline PPS effectiveness for the two segments ($\eta_{PPS,old\,1} = 0.27$ and $\eta_{PPS,old\,2} = 0.16$), five PPS upgrades have been proposed, according to technical references (Garcia, 2007; Reniers et al., 2015):

A) Adding fence sensors as perimeter detection system;
B) Adding a perimeter delay element by building a concrete-reinforced external wall;
C) Adding detection elements (i.e., cameras) at sabotage targets level;
D) Adding delay elements at sabotage targets level;
E) Reducing response force time by building a closer guard dispatch.

It should be noted that upgrades A and C refer to the detection function, upgrades B and D refer to the delay function and upgrade E refers to the response function. Moreover, upgrades A and B refer to external perimeter of the facility, and consequently only to segment n°1, while C, D and E refer to the proximity of the storage tank farm and consequently belong both to segment n°1 and segment n°2.

The upgraded values of effectiveness, indicated as $\eta_{PPS,new\,i\,1}$ and $\eta_{PPS,new\,i\,2}$, for each of the five options have been calculated by inserting in the effectiveness model for the two segments (i.e., the same model previously applied to calculate baseline PPS effectiveness) the modified inputs listed in Table 6. 13. The results regarding upgraded effectiveness index (i.e., $\Delta\eta_{i,1}$ and $\Delta\eta_{i,2}$) and overall effectiveness improvement for a sequential action (i.e., $\overline{\Delta\eta_i}$, calculated according to equation (4.6)), correspondent to each of these upgrades have been reported indeed in the same table.

The results, reported in Table 6. 13, clearly show that, from the effectiveness point of view, two options belonging to different security functions are the best ones: the addiction of detection elements at external fence level (upgrade A) and guard relocation (upgrade E). Neverthless, the presence of additional delay elements at fence level, represented by upgrade B, and the addition of detection elements at sabotage targets proved to be uneffective in increasing PPS effectiveness. Additional delay at targets level, indicated with upgrade D, appeared as an intermediate option in terms of effectiveness improvement. However, even if upgrades A and E are the best ones from the effectiveness intermediate calculation, it does not mean automatically that they are the best options in the end of the application, due to additional terms that are still to be considered in the analysis (e.g., costs, benefits, budget threshold, etc.).

Furthermore, the results of effectiveness assessment are site-specific and accident-specific; consequently they cannot be generalized beyond the current case study.

Table 6. 13 Effectiveness results for five different possible PPS upgrades. From the left to the right, in column order: Upgrade identity, description of the upgrade, Physical protection function modification, reference number of modified tasks for segment n°1 and segment n°2, effectiveness improvement index for segment n°1 ($\Delta\eta_{i,1}$)and segment n°2 ($\Delta\eta_{i,2}$) and overall effectiveness improvement index ($\overline{\Delta\eta_i}$). (*) Reduction of response force time does not affect a single task.

Upgrade ID	*Description*	*PPS function modification*	*N° of modified tasks (segment n°1)*	*N° of modified tasks (segment n°2)*	*Modified inputs*	$\Delta\eta_{i,1}$	$\Delta\eta_{i,2}$	$\overline{\Delta\eta_i}$
A	**External infrared fence sensors as perimeter detection system (at fence level)**	Detection; infrared fence sensors	1	none	$P_{D,1} = 0.9$	0.3541	0	**0.3541**
B	**Construction of an external reinforced concrete wall (instead of the fence)**	Delay; wall hardness	1	none	$t_{D,1} = 180\ s$	0	0	**0**
C	**Addition of detection elements at sabotage targets**	Detection; exterior cameras	5	10	$P_{AD,5} = P_{AD,10} = 0.9$	0.0027	0.0027	**0.0054**
D	**Addition of delay elements at sabotage targets**	Delay; additional wall with doors	5	10	$t_{D,5} = t_{D,10} = 150\ s$	0.0945	0.0836	**0.1781**
E	**Reduction of response force time (by creating a closer guard dispatch)**	Response; relocation of guards closer to storage area	- (*)	- (*)	$t_G = 180\ s$	0.1961	0.1535	**0.3496**

6.4.3 Cost calculation for security upgrades

Cost calculations were carried out for each of the five PPS upgrades proposed in the case study, according to six main categories, 22 subcategories and formula presented in the methodology (i.e., Section 4), considering the time span of one year and the implementation of a single security upgrade. Further information on cost assessment is reported in Section 4.2.4. It should be noted that many subcategories consist of wages, so realistic annual salaries have been retrieved from a specific database (PayScale, 2016) and converted into hourly wages considering 1920 hours/year.

Indeed, several data regarding cost calculation have been retrieved in U.S.A. dollars of year 2016; the conversion rate from U.S.A. dollars to € has been assumed 0.8683 $€/U.S.A.$ \$ (X-Rates, 2016) throughout the case study. Moreover, a location factor of 1.13 (Richardson Products & Cost Data On Line Inc., 2008) was applied in order to adjust US prices and salaries to those of France.

The use of location factor throughout the analysis allowed a site-specific cost calculation. In the estimation of wages, several professional profiles, which are typically involved in the selection, design, installation and maintenance of a security system in a process facility, have been considered. According to their different job tasks, the following security-related jobs have been accounted for the calculation of appropriate cost subcategories: purchasing office staff and manager, security manager, security engineer, security guards and officers, training expert (i.e., security consultant), masons, installation and maintenance technicians.

In the calculation of Initial costs for each security upgrade, wages for the job profiles involved, costs of auxiliary materials and publications of leaflets for internal use have been considered. In the calculation of Installation costs, with particular reference to Equipment costs, specific information of market prices has been retrieved from vendor websites for each security upgrade and reported in Table 6. 14.

In the calculation of Operating costs, Utility costs consist of the costs of annual electric power consumption, which are significant only for upgrades A and C. For both the upgrades the power has been calculated through the standard power law, retrieving data on intensity and voltage from products datasheets (Alibi, 2016; Shenzhen P&H Electronic Co. Ltd, 2016) and accounting the number of devices in place, which have been assumed to be working continuously all the yearlong.

The estimated annual electric power consumption has been $9.07 \cdot 10^3 kWh$ for upgrade A and $3.89 \cdot 10^3 kWh$ for upgrade C. Considering an average industrial electric energy market price in France of 0.095 $€/kWh$ (Eurostat, 2016), utilities costs have been finally calculated. Human resources operating costs have been calculated by considering the manpower, in terms of security officers and guards wages for each of the security countermeasures, which was not negligible for upgrade A and C.

It should be noted that for security upgrades B and D, which are walls in different position, this subcategory is equal to zero. For upgrade E the guards have been just relocated, so no additional human resources operating costs have been accounted in comparison with the baseline situation.

Table 6. 14 Data for the calculation of Equipment costs for five different PPS upgrades.

UPGRADE ID	*DATA FOR THE CALCULATION OF EQUIPMENT COSTS*			
	Description	***Unit***	***Value***	***Reference/ Notes***
	Cost of a couple of fence sensors (i.e., unit cost)	€/*unit*	20	(Shenzhen P&H Electronic Co. Ltd, 2016)
	Total number of fence sensors in place	*n°units*	575	8% of spare items not included
B	Length and height of the concrete wall, with footings	*m*	5750; 3	Layout of the facility
	Cost of the wall (according to these specifications)	€	13530	(Get A Quote, 2016)
C	Number of cameras for each operative (*) and dismissed (**) tank	*n°units/tank*	2 (*); 1 (*)	-
	Cost of an outdoor camera	€/*unit*	178	(Alibi, 2016)
	Total number of cameras in place	*n°units*	74	8% of spare items not included
D	Number of couples of small tanks	*n°units type* 1	15	Layout of the facility
	Number of major tanks	*n°units type* 2	10	Layout of the facility
	Length and height of the concrete wall around unit type 1 (*) and unit type 2 (**)	*m*	600 (*); 650 (**); 3	Layout of the facility
	Cost of the wall for each unit (type 1 (*) and type 2 (**))	€/*unit*	1412 (*); 1530 (**)	(Get A Quote, 2016)
	Cost of security doors to be applied on each unit (both type 1 and type 2)	€/*unit*	1000	(Grainger, 2016)
E	Unit cost for the new building (standard warehouse with concrete floor and metal clad)	€/m^2	548	(BMT, 2016)
	Area of the building	m^2	50	Layout of the facility

In the calculation of Maintenance, inspection and sustainability costs the following assumptions have been applied for each security upgrade: material costs have been estimated by assuming an annual substitution rate for equipment and other materials in the range between 3% and 5%, 2 scheduled maintenances, 1 unscheduled maintenances and 2 scheduled

inspections per year have been accounted. License and renewal costs appeared to be negligible for all the five upgrades.

Other running costs have been calculated for each security upgrade; only for upgrade E this cost category has a significant role, provided that the construction of a new building for security guards requires additional office furniture and utilities.

In the calculation of Specific costs, the contribution offered by False-positive costs should be considered only for detection elements (i.e., upgrade A and C). For both these upgrades, despite a single false-alarm cost, according to expert judgement, is about $2.80 \cdot 10^3$ € and $P(alarm \mid no\ attack) = 0.143$ (Garcia, 2007), assuming the probability of the attack unitary turn false-positive costs to zero. Nevertheless, site-specific costs, as revisions of safety measures and procedures, have been accounted in particular for delay elements, whose implementation might require a revision of emergency routes, as well as entrance and exit doors.

For each of the five security upgrades, the main results obtained from cost calculations, according to the six cost categories of EM-PICTURES, as well as the Overall costs ($C_{Security,i}$) have been illustrated in Figure 6. 10 and Table 6. 15.

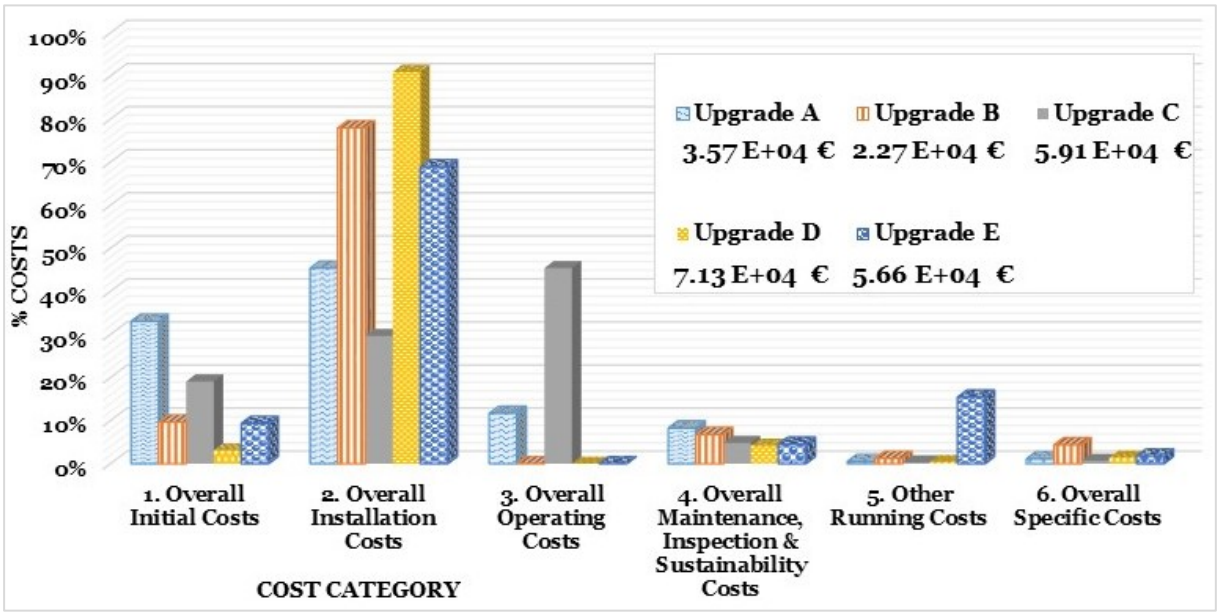


Figure 6. 10 Percentage composition of Overall costs for each upgrade of the PPS, according to six main cost categories. For each cost category, from the left to the right: A) Adding fence sensors as perimeter detection system, B) Adding a perimeter delay element by building a concrete-reinforced external wall, C) Adding detection elements at sabotage targets level, D) Adding delay elements at sabotage targets level, E) Reducing response force time by relocating guards closer to the targets. Overall cost of each security upgrade is reported in the box on the right.

Despite the values of Overall costs ($C_{Security,i}$) belong to the same order of magnitude (i.e., 10^4 €) for all the security upgrades, the same consideration does not apply to the percentage composition of each cost category, as it is visible in Figure 6. 10.

Table 6. 15 Calculation of Overall annual costs for five security upgrades, as the sum of six main categories, for $P(T)_{ij} = 1$: 1) Overall initial costs, 2) Overall installation costs, 3) Overall operating costs, 4) Overall maintenance, inspection & sustainability costs, 5) Other running costs, 6) Overall specific costs.

CALCULATION OF OVERALL COSTS ($C_{Security,i}$)			UPGRADE A	UPGRADE B	UPGRADE C	UPGRADE D	UPGRADE E
Symbol	***Description***	***Unit***	***Value***	***Value***	***Value***	***Value***	***Value***
$C_{INITIAL,OV}$	***1. Overall initial costs***	**€**	**1.18E+04**	**2.20E+03**	**1.13E+04**	**2.20E+03**	**5.29E+03**
C_{INV}	Investigation costs	€	6.08E+02	6.08E+02	6.08E+02	6.08E+02	6.08E+02
$C_{S\&D}$	Selection and design costs	€	5.19E+02	9.78E+02	5.19E+02	9.78E+02	5.19E+02
$C_{MAT,I}$	Material costs	€	8.50E+03	0	8.00E+03	0	2.00E+03
C_T	Training costs (start-up/in service)	€	1.86E+03	3.11E+02	1.86E+03	3.11E+02	1.86E+03
$C_{G\&I}$	Changing of guidelines and informing costs	€	3.00E+02	3.00E+02	3.00E+02	3.00E+02	3.00E+02
$C_{INSTALL,OV}$	***2. Overall installation costs***	**€**	**1.62E+04**	**1.77E+04**	**1.76E+04**	**6.48E+04**	**3.90E+04**
C_{START}	Start-up costs	€	1.14E+03	1.74E+03	6.73E+02	8.68E+02	5.24E+02
C_E	Equipment costs (including P - purchase & R - rental costs, space requirement costs)	€	1.25E+04	1.38E+04	1.62E+04	6.18E+04	3.22E+04
$C_{INSTALL}$	Installing costs	€	2.54E+03	2.15E+03	6.65E+02	2.15E+03	6.28E+03
$C_{OPERATION,OV}$	***3. Overall operating costs***	**€**	**4.17E+03**	**0**	**2.69E+04**	**0**	**0**
$C_{U,OP}$	Utilities costs	€	8.61E+02	0	3.69E+02	0	0
C_{HRO}	Human resources operating costs		3.31E+03	0	2.65E+04	0	0
$C_{MIS,OV}$	***4. Overall maintenance, inspection & sustainability costs***	**€**	**2.95E+03**	**1.54E+03**	**2.86E+03**	**2.98E+03**	**2.57E+03**
$C_{MAT,M}$	Material costs	€	6.88E+02	4.06E+02	6.00E+02	1.84E+03	9.22E+02
C_{MNT}	Maintenance team costs (A- scheduled m. /B- unscheduled m.)	€	1.62E+03	8.09E+02	1.62E+03	8.09E+02	9.96E+02
C_{INSP}	Inspection team costs	€	6.47E+02	3.24E+02	6.47E+02	3.24E+02	6.47E+02
C_{LIC}	License and rental renewal	€	0	0	0	0	0
$C_{OR,OV}$	***5. Other running costs***	**€**	**1.80E+02**	**2.80E+02**	**1.80E+02**	**2.80E+02**	**8.75E+03**
C_{OF}	Office furniture costs	€	0	0	0	0	6.09E+03
C_T	Transport costs	€	1.00E+02	2.00E+02	1.00E+02	2.00E+02	1.00E+02
C_{COMM}	Additional communication costs	€	6.00E+01	6.00E+01	6.00E+01	6.00E+01	6.00E+01
C_I	Insurance costs	€	0	0	0	0	0
C_{OU}	Office utilities costs	€	2.00E+01	2.00E+01	2.00E+01	2.00E+01	2.50E+03
C_{OS}	Office supplies costs	€	0	0	0	0	0
$C_{SPEC,OV}$	***6. Overall specific costs***	**€**	**4.00E+02**	**1.00E+03**	**4.00E+02**	**1.00E+03**	**1.00E+03**
C_{FP}	False-positive case costs	€	0	0	0	0	0
C_{SITE_SP}	Site-specific costs	€	4.00E+02	1.00E+03	4.00E+02	1.00E+03	1.00E+03
$C_{Security,\ i}$	***Overall costs***	**€**	**3.57E+04**	**2.27E+04**	**5.91E+04**	**7.13E+04**	**5.66E+04**

The comparison among percentage compositions (Figure 6. 10), obtained for each security measure by using the respective Overall cost as reference, shows that for detection elements (i.e., upgrades A and C) Installation costs are the prevailing ones, followed by relevant Initial costs and Operational costs. For delay elements (i.e., upgrades B and D) Installation costs are predominant, but Operating costs are negligible. For response element (i.e., upgrade E) Installation costs are the prevailing ones, followed by Other running costs; the latter ones are almost negligible for all the other security upgrades. Eventually, Maintenance, inspection and sustainability costs are around 5% of the Overall costs for all the five security upgrades considered in the case study.

6.4.4 Benefit calculation for different scenarios

The losses derived from a successful attack should include the fatalities and other damages, both direct and indirect, which will accrue because of a successful attack, taking into account the value and vulnerability of people and infrastructures, as described in Section 4.2.5. Consequently, benefits calculation is dependent on the choice of an appropriate accidental scenario.

In the present case study, three possible scenarios have been analyzed for benefit calculation, with the purpose to illustrate the potentiality of EM-PICTURES: realistic scenario, worst-case scenario and expected scenario. Realistic benefits indicates the actual losses sustained in the attack. The realistic benefits considered may not exactly reflect the actual ones, due to the limited amount of technical information available. On the other hand, worst-case benefits are the consequences sustained in the worst-case scenario that is a domino accident in the tank farm, with several casualties and injuries and severe damage and production loss. Indeed, expected benefits are the benefits derived from a hypothetical scenario, which considers the average benefits, weighted by probabilities of occurrence, of four possible outcomes (i.e., indicated as T1, T2, T3 and T4), as described in Section 4.2.5. Illustrative probabilities were defined for each category of scenario, together with a detailed description of all the scenarios analyzed in the case study, and reported in Table 6. 16. It was assumed that, for each scenario considered, benefits are independent from the security countermeasure that can be implemented.

The benefit categories, subcategories and formula to assess the overall annual benefits (i.e., avoided losses) derived from the occurrence of a generic accidental scenario *j* are calculated according to Module 3 of EM-PICTURES version of the economic model; further information on benefit assessment is reported in Section 4.2.5.

In the calculation of Supply chain benefits, a realistic production rate for the facility has been estimated by assuming 1/10 of the overall national French oil derivatives production in 2013

that is $1.26 \cdot 10^6$ $barrel/day$ (OPEC, 2014); for the conversion into mass flow rate a reference density for naphtha has been considered (Engineering ToolBox, 2017). The estimated production rate for the facility has been $4.17 \cdot 10^5\, kg/h$, with a profit per unit sold that is the market price equal to $4.08 \cdot 10^{-4}$€ (Wang and Kim, 2015). For Schedule benefits, the fine for a cancelled contract has been assumed, based on expert judgment, $1.00 \cdot 10^5$ €$/contract$ and the fine for delay in deliveries per day, $1.00 \cdot 10^4$ €$/(delay \cdot day)$.

In the calculation of Damage benefits, illustrative commercial equipment costs for storage tanks have retrieved from vendors (Shanghai Iven Pharmatech Engineering Co. Ltd, 2016): a commercial value of $8.00 \cdot 10^4$ € for $40000\, m^3$ tank and of $3.0000 \cdot 10^4$ € for $10000\, m^3$ tank has been assumed throughout the case study. For the estimation of finished goods damages, the same market price has been assumed for both the products (i.e., naphtha and petrol).

In the calculation of Legal benefits and after, it should be noted that, as for costs calculations, many benefits subcategories consist of wages; the expression for converting annual salaries into hourly wages applied has been the same one reported in Section 6.4.3. Moreover, also the same values regarding conversion rate from U.S.A. dollars to € and location factor have been applied (Section 6.4.3). In the case of Legal benefits, the job profiles involved are junior lawyers and seniors lawyers, specialized lawyers, security manager, security engineer, security analyst and security consultant. The total security budget prior to the accident has been assumed, based on expert judgment, $8.00 \cdot 10^4$ €, but the percentage increase of the security budget after the accident is different for the three scenarios considered, depending on consequences severity.

In the calculation of Insurance benefits, the value of the current total premium cost of the facility has been considered, based on expert judgment, $5.00 \cdot 10^7$€, while the percentage increase of the premium due to the accident is scenario dependent. In the calculation of Human benefits, the value of a statistical life (VSL) has been retrieved from a previous study (Viscusi and Aldy, 2003) and converted from $U.S.A.$\$(2000) into €(2016) by the application of appropriate conversion rate (X-Rates, 2016) and inflation rate (Friedman, 2017); the final VSL is $7.07 \cdot 10^6$€. Following the same reference and approach, the monetary values for a light and a serious injury are respectively $1.41 \cdot 10^4$ € and $2.06 \cdot 10^5$ €. Hiring benefits are inserted in Human and environmental benefits category as they refer to the costs that should be sustained by the company when an employee is hospitalized or dead after the accident to hire additional personnel in substitution. Hiring and training costs have been assumed equivalent to a monthly salary each for the employee category, based on previous studies (Gavious et al., 2009; Reniers and Brijs, 2014b).

Table 6. 16 Description of the scenarios applied in the case study for benefit assessment: realistic scenario, worst-case scenario and expected scenario. Realistic benefits indicate the actual losses sustained in the terroristic attack. Expected benefits have been calculated as the average of four possible outcomes weighted by respective probabilities of occurrence. Worst-case and T1 benefits are coincident. Vulnerability probabilities are considered unitary.

SCENARIO ID	REALISTIC	WORST-CASE	EXPECTED			
			T1 Catastrophic accident	T2 Critical accident	T3 Marginal accident	T4 Negligible accident
			Probability of occurrence			
			5.00E-04	4.00E-01	5.55E-01	4.95E-02
BENEFITS	***Description***					
1. Overall supply chain benefits	No stop in production; 20% activity slowed for 13 hours (emergency intervention time); fines for delays in deliveries	Stop in production for 24 hours; 0% production rate at reactivation; 48 hours start-up; fines for delays in deliveries and 2 orders cancelled	Stop in production for few hours; delays in the supply chain	Production slowed for few hours; delays in the supply chain	Negligible	
2. Overall damage benefits	Two tanks completely destroyed, damage to piping	6 tanks destroyed with content; severe damage to piping; severe damages to other company's and public properties; severe damage to surrounding living areas	Two tanks completely destroyed and other assets damages.	Two tanks damaged (20%); minor other assets damages	Minor damages to 2 tanks (3%)	
3. Overall legal benefits	Civil liability fine for pollution; lawyers' wages; 50% increase of the Security budget; very improbable closing down (10^{-5}%)	Civil liability fine for pollution; lawyers' wages; 80% increase of the Security budget; possible closing down (10%)	Fines; salaries; 50% increase of Security budget	Fines; salaries; 30% increase of Security budget	Fines; salaries; 8% increase of Security budget	
4. Overall insurance benefits	0.1% premium increase	10% premium increase	0.1% premium increase.	10^{-2}%premium increase	10^{-3}% premium increase	
5. Overall human and environmental benefits	No casualties and injuries; content of the two tanks burnt	3 casualties; 4 serious injuries and 8 light injuries; several new recruitments; content of the six tanks burnt; severe environmental damages	2 serious injuries; 4 light injuries; environmental damages	1 light injury; marginal environmental damages	Negligible	
6. Overall intervention benefits	Significant emergency intervention	Massive Emergency intervention, with special units	Critical	Marginal	Negligible	
7. Overall reputation benefits	10^{-4}% expected drop in the share-price	1% expected drop in the share-price	10^{-4}% share price drop	$5 \cdot 10^{-5}$%share price drop	10^{-5}% share price drop	
8. Other benefits	Manager work-time benefits and cleaning benefits	Significant manager work-time benefits and cleaning benefits	Critical	Marginal	Negligible	
9. Overall specific benefits	Airport and traffic delays; limited immaterial consequences	Severe airport and traffic delays; relevant immaterial consequences	Critical	Marginal	Negligible	

In the calculation of Intervention benefits, a different flat rate has been assumed for the three scenarios. In the calculation of Reputation benefits, a current total market price for the

company of $3.84 \cdot 10^{10}$€ has been accounted, but the expected percentage drop is scenario dependent. In the calculation of Other benefits, wages for security manager and cleaning employees have been accounted, while in the estimation of Specific benefits, transportation delays costs and psychological counselling for accident witnesses have been considered.

Eventually, all the benefit numerical values have been determined accordingly to the pertinent 9 categories of EM-PICTURES, up to Overall benefits $(C_{Loss,j})$, for each of the three scenarios considered, which are respectively realistic scenario, worst-case scenario and expected scenario. The results of benefits calculations are summarized in Figure 6. 11, Figure 6. 12 and Table 6. 17.

The comparison among benefits percentage compositions forming the expected scenario, reported in Figure 6. 11, highlights that benefits distributions depend on the scenario severity: for catastrophic (i.e., T1) and critical scenarios (i.e., T2), the costs due to casualties and injuries are prevailing, while for marginal (i.e., T3) and negligible (i.e., T4) accidents, the prevailing losses are related to legal issues and assets damages. Indeed, as stated in previous studies referred to benefit assessment for major accidents within the chemical industry domain (Gavious et al., 2009; Reniers and Brijs, 2014b), the value of indirect losses, which include for instance reputational losses, human and environmental losses, legal and insurance losses, is generally superior to direct losses. The gap between direct and indirect benefits tends to increase with the increasing severity of the accident (Gavious et al., 2009). The Overall expected benefit value is $6.459 \cdot 10^5$€; the expected benefits apportionment is reported in Figure 6. 11 and shows that human and environmental benefits are prevailing, followed by reputational benefits and assets damages.

The comparison among percentage compositions, obtained for the three scenarios by using the respective Overall benefits as reference and reported in Figure 6. 12, shows that, from a general point of view, Human and environmental benefits, Overall reputational benefits, Overall damage benefits, Overall insurance benefits are the most relevant categories. Both for worst-case scenario and for expected scenario Human and environmental benefits are relevant, due to the high monetary value attributed to injuries and casualties, in comparison with damages to assets; however, especially in worst-case scenario, the reputation loss is prevailing. On the other hand, for realistic scenario, benefits distribution among categories is the most uniform one, but Overall damage benefits are slightly prevailing, due to the relevant damages to company assets and to the absence of human losses. As visible from Figure 6. 12, the values of Overall benefits belong to the same order of magnitude (i.e., 10^5 €) for realistic scenario and expected scenario, while the Overall benefits referred to worst-case scenario are three orders of magnitude higher; details on benefit calculations for the three scenarios are available in Table 6. 17.

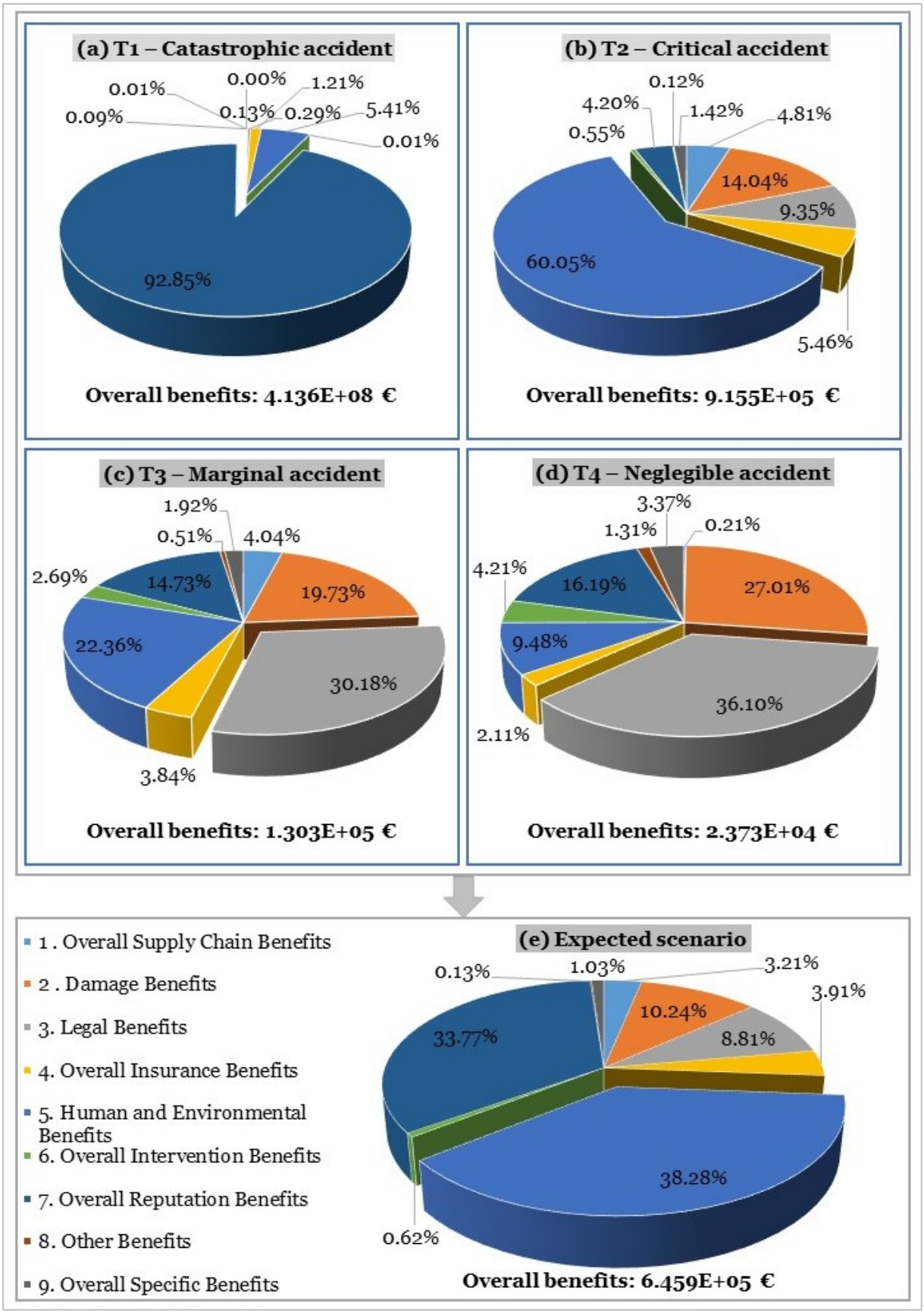


Figure 6. 11 Percentage composition of Overall benefits for four different scenarios: (a) T1, (b) T2, (c) T3 and (d) T4, composing the expected scenario (e), calculated according to the categories of the model. Overall benefits values are reported for each scenario.

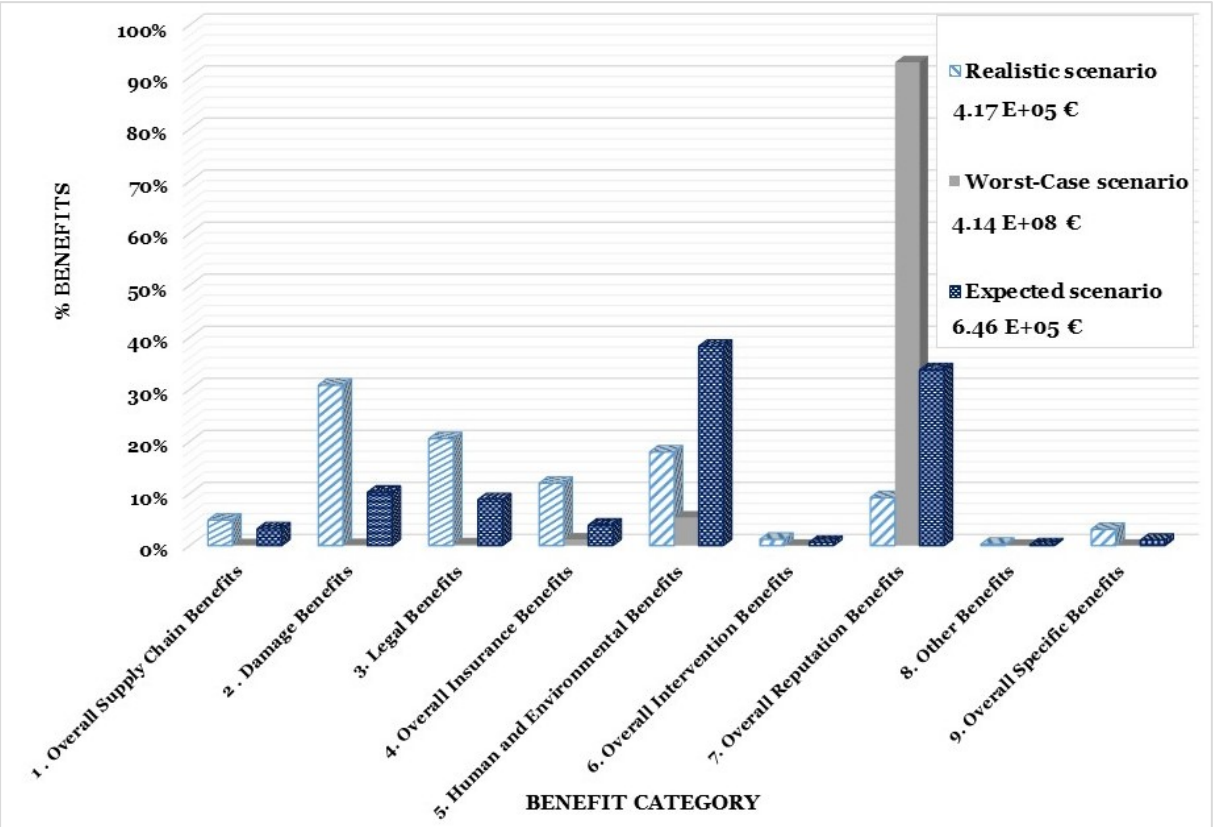


Figure 6. 12 Percentage composition of Overall benefits for three different scenarios. For each benefit category, from the left to the right: realistic scenario, worst-case scenario and expected scenario. Overall benefits are reported in the box on the right for each scenario.

Table 6. 17 Overall annual benefits results for different scenarios: realistic benefits, worst-case benefits and expected benefits. The calculation of Overall benefits has been carried out as the sum of nine main categories: (1) Overall supply chain benefits, (2) Overall damage benefits, (3) Overall legal benefits, (4) Overall insurance benefits, (5) Overall human and environmental benefits, (6) Overall intervention benefits, (7) Overall reputation benefits, (8) Other benefits, (9) Overall specific benefits.

CALCULATION OF OVERALL BENEFITS ($C_{Loss,j}$)			REALISTIC SCENARIO	WORST - CASE SCENARIO	EXPECTED SCENARIO
Symbol	***Description***	***Unit***	***Value***	***Value***	***Value***
$B_{SUPC,OV}$	***1 . Overall supply chain benefits***	€	2.04E+04	3.87E+05	2.07E+04
$B_{DAMAGE,OV}$	***2. Overall damage benefits***	€	1.29E+05	5.23E+05	6.61E+04
$B_{LEGAL,OV}$	***3. Overall legal benefits***	€	8.56E+04	1.18E+06	5.69E+04
$B_{INS,OV}$	***4. Overall insurance benefits***	€	5.00E+04	5.00E+06	2.53E+04
$B_{H\&E,OV}$	***5. Overall human and environmental benefits***	€	7.50E+04	2.24E+07	2.47E+05
$B_{INTV,OV}$	***6. Overall intervention benefits***	€	5.00E+03	3.00E+04	3.99E+03
$B_{REPT,OV}$	***7. Overall reputation benefits***	€	3.84E+04	3.84E+08	2.18E+05
$B_{OTH,OV}$	***8. Other benefits***	€	1.06E+03	9.94E+03	8.12E+02
$B_{SPEC,OV}$	***9. Overall specific benefits***	€	1.30E+04	5.50E+04	6.64E+03
$C_{Loss,j}$	***Overall benefits***	€	**4.17E+05**	**4.14E+08**	**6.46E+05**

6.4.5 Results and discussion

6.4.5.1 Results of the case study

The results of the assessment of the case study consist in cost-benefit and cost-effectiveness analyses results, obtained according to the deterministic approach presented in EM-PICTURES version of the model. The first are the values of actualized Net benefits, for five PPS upgrades and for three scenarios. The latter are the most profitable combinations of security upgrades for each scenario, within the constraint of the security budget. Further information on the equations to be applied is available in Sections 4.2.7.1 and 4.2.8.1.

Overall costs for each security measure and Overall benefits for each scenario have been made comparable by applying appropriate discount rates (i.e., 3.5% and 1.5% respectively (HSE - Health and Safety Executive, 2016)) over a 10 year time-span, according to equation (4.19). The latter is a conventional number of operational years for a security measure.

Certain costs (e.g., initial and installation costs) occurs only in the present and thus do not have to be actualized, whereas other costs (e.g., operating costs, maintenance, inspection and sustainability costs, other running costs) refer to the whole remaining lifetime of the facility and therefore they should be discounted to the present. The benefit categories should be all actualized, as they represent positive cash flows, occurring throughout the remaining lifetime of the facility. The actualized values of Overall Benefits are respectively $2.70 \cdot 10^5$ € for realistic scenario, $2.76 \cdot 10^8$ € for worst-case scenario and $4.31 \cdot 10^5$ € for expected scenario.

Table 6. 18 Cost-benefit analysis results, in term of Net Benefits, for five different PPS upgrades and three possible scenarios.

SECURITY UPGRADES		*NET BENEFITS*		
		REALISTIC SCENARIO	**WORST - CASE SCENARIO**	**EXPECTED SCENARIO**
Upgrade ID	**DESCRIPTION/UNIT**	€	€	€
A	**External infrared fence sensors as perimeter detection system (at fence level)**	**6.80E+04**	**9.76E+07**	**1.22E+05**
B	**Construction of an external reinforced concrete wall (instead. of the fence)**	**-2.21E+04**	**-2.21E+04**	**-2.21E+04**
C	**Addition of detection elements (i.e., cameras) at sabotage targets**	**-4.69E+04**	**1.44E+06**	**-4.60E+04**
D	**Addition of delay elements at sabotage targets**	**-2.06E+04**	**4.90E+07**	**6.59E+03**
E	**Reduction of response force time (by creating a closer guard dispatch)**	**4.86E+04**	**9.63E+07**	**1.02E+05**

Considering the threat and vulnerability probabilities unitary, the value of Net Benefit, also named Net Present Value (*NPV*), has been calculated for each of the five PPS upgrades, according to the three scenarios, by applying equation (4.20). The final results of cost-benefit analyses, reported in Table 6. 18, prove the coherency of the model, highlighting that security upgrades A and E are economically feasible for all the scenarios considered. Upgrade D is acceptable only with reference to expected scenario and worst-case scenario; upgrade C is acceptable only with reference to worst-case scenario. Therefore, according to the multi-scenario acceptability criteria expressed by equation (4.21), upgrades B, C and D are not economically profitable.

Cost-effectiveness analysis has been applied in order to determine the most profitable combination of security upgrades within the security budget constraint for each scenario, according to the deterministic approach. For each scenario, all the possible 30 combinations of PPS upgrades have been considered, starting from each single security measure, to couples, triplets, quartets and eventually group of five. Actualized Overall costs have been calculated for each combination by applying a 3.5% discount rate to the pertinent cost categories of each option taken and by summing the actualized costs (HSE - Health and Safety Executive, 2016), then Overall costs have been compared with the actualized security budget. It should be noted that the security budget is different among the three scenarios, due to different percentage increases of security budget after the accident, depending on consequence severity. For each scenario, only the combinations respecting the budget criteria have been selected and their Net Benefits have been calculated and compared, according to equation (4.27), proposed in EM-PICTURES version of the model. The actualized values of Overall benefits applied in the calculation have been the ones reported in this section.

Table 6. 19 Cost-effectiveness analysis results, regarding all possible combinations of security measures, for each of the three scenario. From the left to the right: first-most profitable combination, second-most profitable combination and security budget.

SCENARIO REFERENCE	***FIRST COST-EFFECTIVE COMBINATION***			***SECOND COST-EFFECTIVE COMBINATION***			***Security Budget***
	Combination ID	***Net Benefit*** (€)	***Total Cost of Combination*** (€)	***Combination ID***	***Net Benefit*** (€)	***Total Cost of Combination*** (€)	***Value*** (€)
REALISTIC	**A+E**	**1.17E+05**	7.90E+04	**A+B+E**	**9.46E+04**	1.01E+05	**1.20E+05**
WORST - CASE	**A+C+E**	**1.95E+08**	1.27E+05	**A+E**	**1.94E+08**	7.90E+04	**1.44E+05**
EXPECTED	**A+E**	**2.24E+05**	7.90E+04	**A+B+E**	**1.01E+05**	2.02E+05	**1.10E+05**

The results of cost-effectiveness analyses, reported in Table 6. 19, show that the combination of security measures A and E (i.e., application of detection system at external fence level and relocation of security guards) is the one with the maximum Net Benefit for realistic and expected scenario. Nevertheless, the most profitable combination for worst-case scenario includes, besides upgrades A and E, also upgrade C, which refers to additional detection system at sabotage targets. The second most profitable combination includes upgrades A and E for the three scenarios; indeed, for realistic and expected scenarios also the application of upgrade B (i.e., additional delay element at external level) is suggested.

Figure 6. 13 shows the complete ranking of all possible combinations of security measures, according to cost-effectiveness analysis, for each of the three scenarios. The results confirm that several profitable combinations offer an integration of different security functions (i.e., detection, delay and response), providing therefore a more complete security protection. Nevertheless, none of the combinations respecting the budget constraints includes more than three security upgrades. Moreover, in the top ten most profitable combinations for the three scenarios are often present security measures whose single performance increases are very limited, due to the relatively low costs of implementation (e.g., upgrade B).

Therefore, the consistent results of cost-benefit and cost-effectiveness analyses highlight that upgrade A and upgrade E are the suggested security measures to be implemented together.

This option offers improved detection at perimeter level and improved response of security guards. However, the implementation of a triplet of security upgrades (e.g., upgrades A+B+E), might be convenient with reference to a worst-case scenario. According to all these options, an integration of different security functions is carried out, providing therefore a more complete security protection, according to the Organizational-Physical-Electronics-Reporting principle (OPER) principle (Reniers et al., 2015).

These results may offer sound indications for the stakeholders to rationally select and allocate security measures, providing a range of economically profitable options, which should be eventually compared with company-specific acceptance criteria and information.

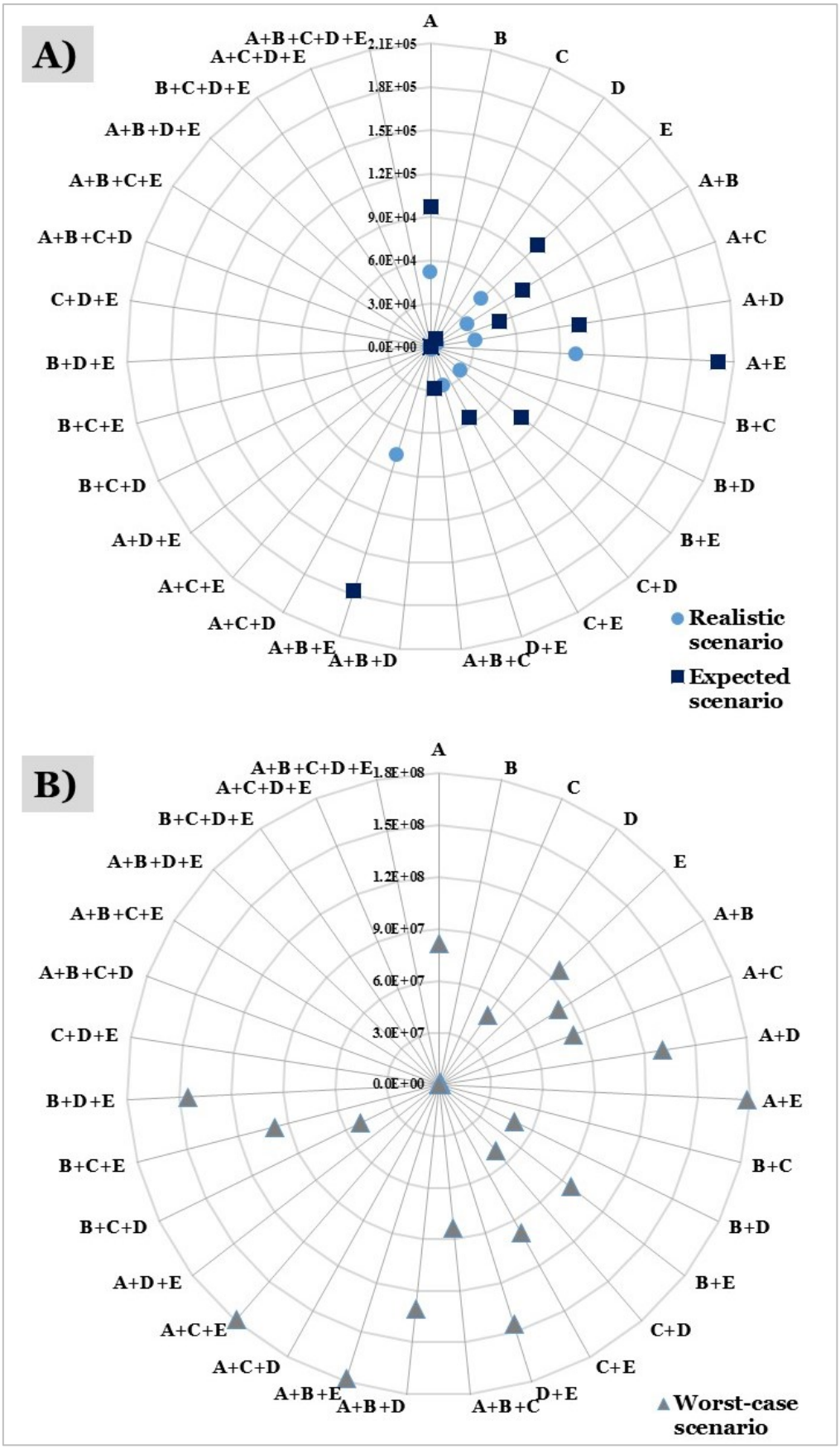


Figure 6. 13 Cost-effectiveness analysis results, showing the ranking in terms of Net Benefit respecting budget (expressed in €(2016)) for all possible combinations of security measures, with reference to the three scenarios: A) realistic scenario and expected scenario; B) worst-case scenario.

6.4.5.2 Uncertainty analysis

As discussed in the methodology section (see Section 4.3), the application of EM-PICTURES version of the model requires to perform an uncertainty analysis on threat and vulnerability probabilities, in purpose to evaluate the effect of their variations on economic analyses results.

According to the equations and concepts expounded in Section 4.2.6, the uncertainty analysis regarding case study results focuses on:

1) The effect of threat probability $\left(P(T)_{ij}\right)$, here named also $P(T)$, as it assumes an uniform value for all security measures and scenarios, and conditional loss probability $\left(P(L|H)\right)$ variations on cost-benefit analysis and cost-effectiveness analysis results. The two terms, which are related, depend on the typologies of adversaries and malicious acts. The values considered in the uncertainty analysis are reported in Table 6. 20.

2) The effect of conditional hazard probability $\left(P(H|T)\right)$ variations on economic analysis results. This term depends on the complexity of the explosive device applied in the terroristic attack. The values considered in the uncertainty analysis are reported in Table 6. 20.

Table 6. 20 Values applied for uncertainty analysis on the threat and vulnerabilities values of the case study.

Threat severity	**Example of adversaries and malicious act**		$P(T)$	$P(L \mid H)$
Medium	Organized criminals/ terrorists stealing assets/ weak sabotage action		0.3	0.80
High	Terrorists aimed at causing a major accident		0.1	1
Conditional threat	Terrorists aimed at causing cascading effects		1	1
$P(H \mid T)$				
	Reliability of Improvised Explosives Devices		***Global Performance Shaping Factors***	$P(H \mid T)$
Device complexity	**Representative IED design**	R_{IED}	PSF **for a terroristic organization**	
Simple	Pipe bomb	0.931	0.981	0.913
Medium	Mobile phone initiated VBIED (Vehicle Borne Improvised Explosive Device)	0.920	0.980	0.902
Complex	Improvised mortar	0.910	0.905	0.824
Conservative assumption	No information available	1	1	1

According to point 1), the value of conditional hazard probability was kept unitary and unchanged; the uncertainty analysis dealt on only with the variation of $P(T)$ and $P(L|H)$.

The value of Net Benefit, also named Net Present Value (NPV), has been recalculated for each of the five PPS upgrades, according to the three scenarios, by applying equation (4.20), with the mentioned different values of $P(T)$ and $P(L|H)$; the recalculated cost-benefit analysis results are reported in Figure 6. 14. For instance, according to realistic scenario, the only upgrades profitable with $P(T) = 1$ and $P(L|H) = 1$ that are security measures A and E, become not profitable with lower values of the threat probability and $P(L|H)$. According to worst-case scenario, all the single security measures are still profitable, after the decrease of $P(T)$ and $P(L|H)$ values, with the exception of upgrade B. According to the expected scenario, security measures A, D and E are profitable with $P(T) = 1$ and $P(L|H) = 1$; only security measure A is profitable with $P(T) = 0.3$ and $P(L|H) = 0.8$ and none of the security measures is still profitable with $P(T) = 0.1$.

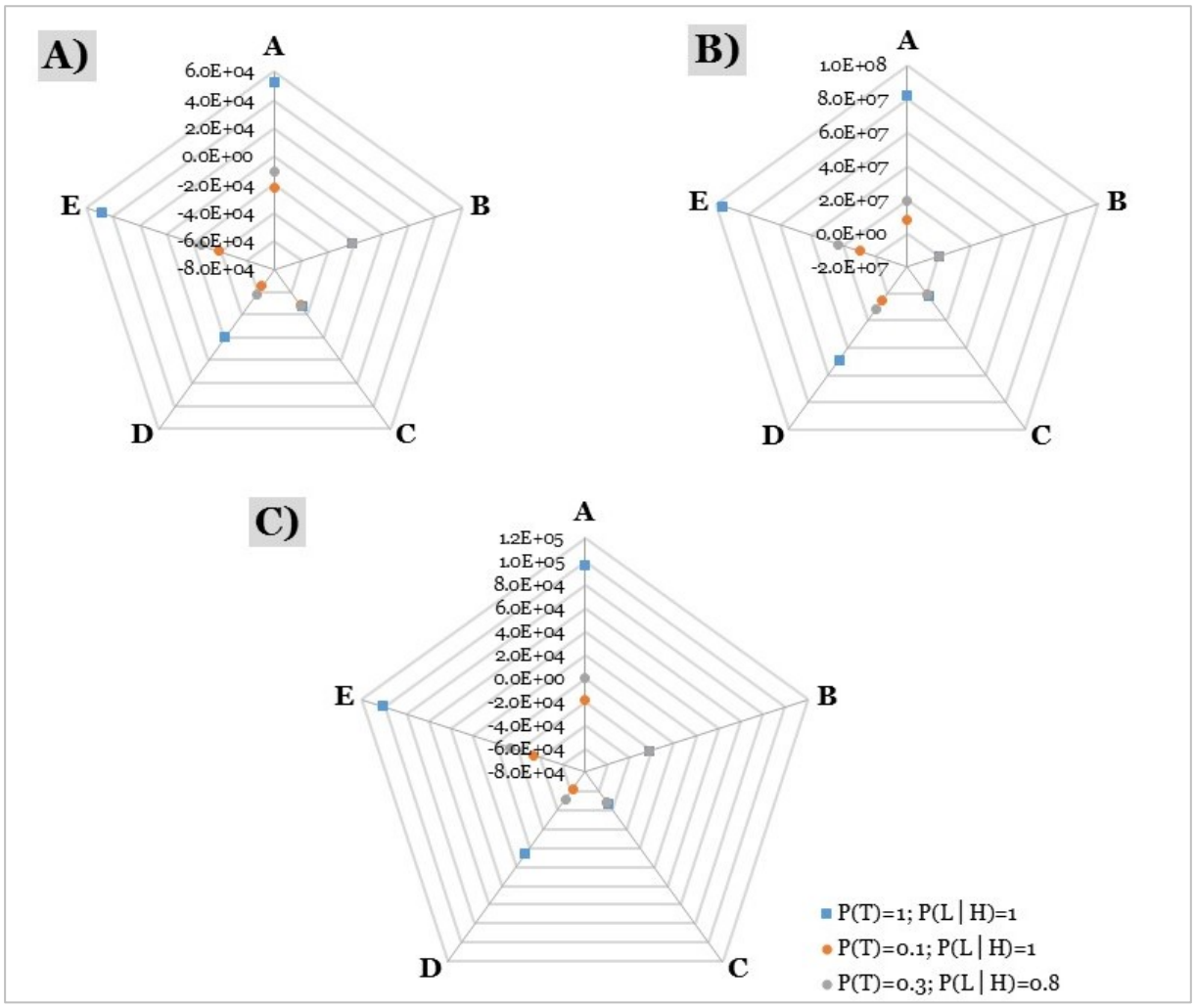


Figure 6. 14 Results of cost-benefit analysis as a function of threat probability $P(T)$ and conditional loss probability $(P(L|H))$ values, for the five PPS upgrades and three scenarios: A) realistic scenario; B) worst-case scenario; C) expected scenario. Monetary values are expressed in (€, 2016).

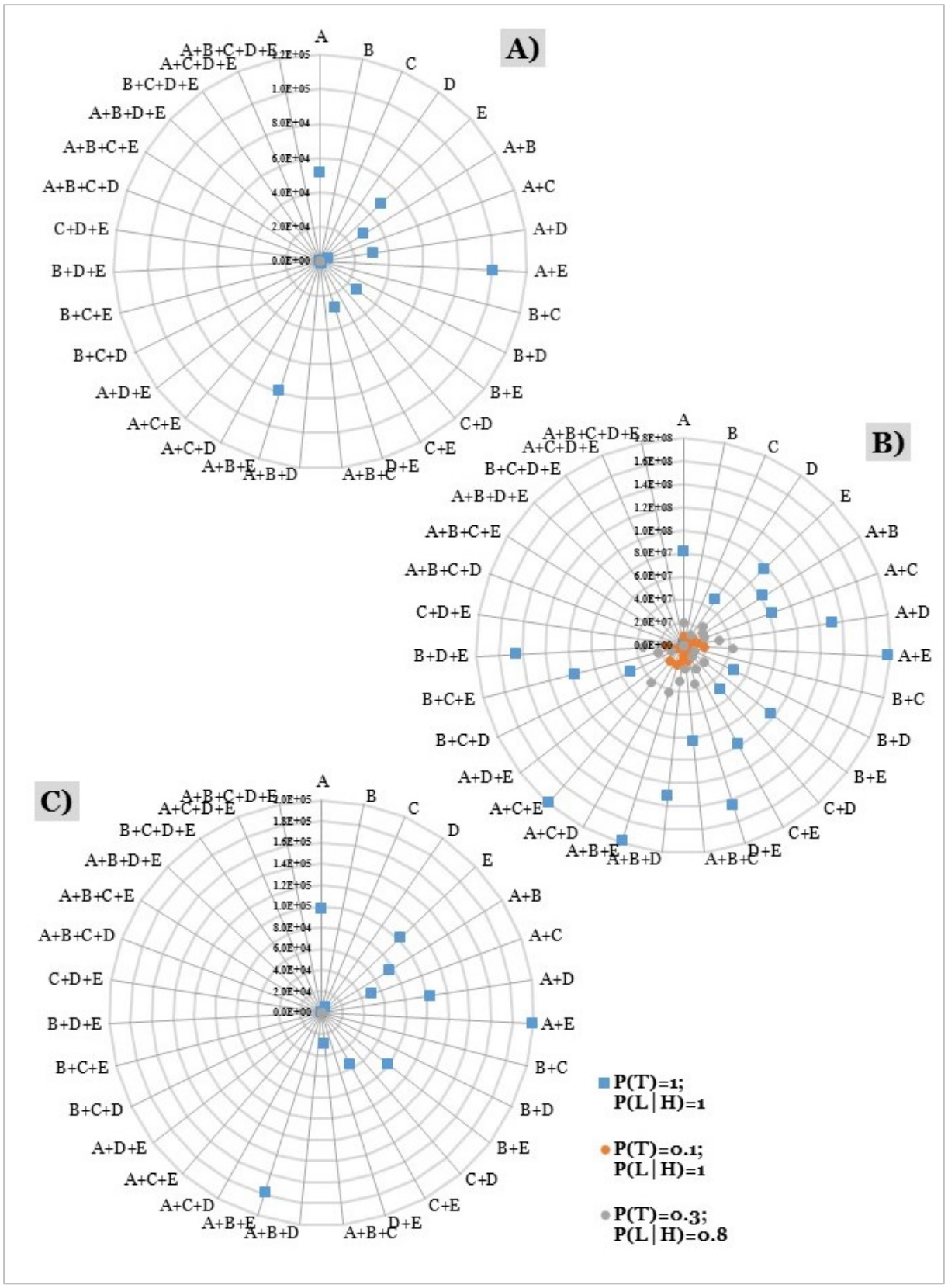


Figure 6. 15 Results of cost-effectiveness analysis as a function of threat probability ($P(T)$) and conditional loss probability ($P(L|H)$) values, for the five PPS upgrades and three scenarios: A) realistic scenario; B) worst-case scenario; C) expected scenario. Monetary values are expressed in (€, 2016).

Indeed, the effects of uncertainties regarding $P(T)$ and $P(L|H)$ values on cost-effectiveness analysis results were evaluated by inserting the modified inputs in equation (4.27); the results are available in Figure 6. 15. Values not respecting the security budget threshold have not been reported in Figure 6. 15. According to realistic and expected scenario, none of security measures combination is profitable with lower values of the threat probability and $P(L|H)$. According to worst-case scenario, the reduction of $P(T)$ and $P(L|H)$ values turn into a reduction of $Net\ Benefit_{vj}$, but the number of combinations respecting the threshold criteria is unchanged, as well as the most profitable combination, which remains A+C+E.

In conclusion, Figure 6. 14 and Figure 6. 15 show that the modified values of $P(T)$ and $P(L|H)$ have a linear effect on cost-benefit analysis and cost-effectiveness analysis results. In a general perspective, removing the over-conservative assumptions of $P(T) = 1$ and $P(L|H) = 1$ lead to a significant reduction of the profitability, both for a single security upgrade and for a combination of them, with an analogous trend for cost-benefit and cost-effectiveness analyses. This difference is scenario-dependent, and becomes even more remarkable with decreasing scenario severity (i.e., lower $C_{Loss,j}$) , as arguable from the equations applied (see Sections 4.2.7.1 and 4.2.8.1).

According to point 2), the values of conditional loss probability and $P(T)$ were kept unitary and unchanged; the uncertainty analysis dealt only with the variation of the conditional hazard probability (i.e., $P(H|T)$), proportionally increasing with the decreasing explosive device complexity, according to the values reported in Table 6. 20. The effects of uncertainties regarding $P(H|T)$ values on cost-benefit analysis results were evaluated by inserting the modified inputs in equation (4.20); the results are available in Figure 6. 16, for the five PPS upgrades and the three scenarios considered in the case study. According to realistic scenario, the only upgrades profitable with $P(H|T) = 1$ are security measures A and E, and they are still profitable, with lower values of Net Benefits, with lower values of $P(H|T)$. Also according to worst-case scenario, the reduction of $P(H|T)$ lead only to a reduction of Net Benefits for all the security upgrades, but all of them, with the exception of upgrades B, remain feasible. According to the expected scenario, the upgrades profitable with $P(H|T) = 1$ are A, D and E; upgrade D becomes not feasible removing the conservative assumption of $P(H|T) = 1$, regardless the complexity of the explosive device.

Indeed, the effects of uncertainties regarding $P(H|T)$ values on cost-effectiveness analysis results were evaluated by inserting the modified inputs in equation (4.27); the results are available in Figure 6. 17. Values not respecting the security budget threshold have not been reported in Figure 6. 17. According to realistic, worst-case and expected scenario, the reduction of $P(H|T)$ lead to a limited reduction of the Net Benefit for a generic combination of security measures; the most profitable combination for each scenario is unchanged.

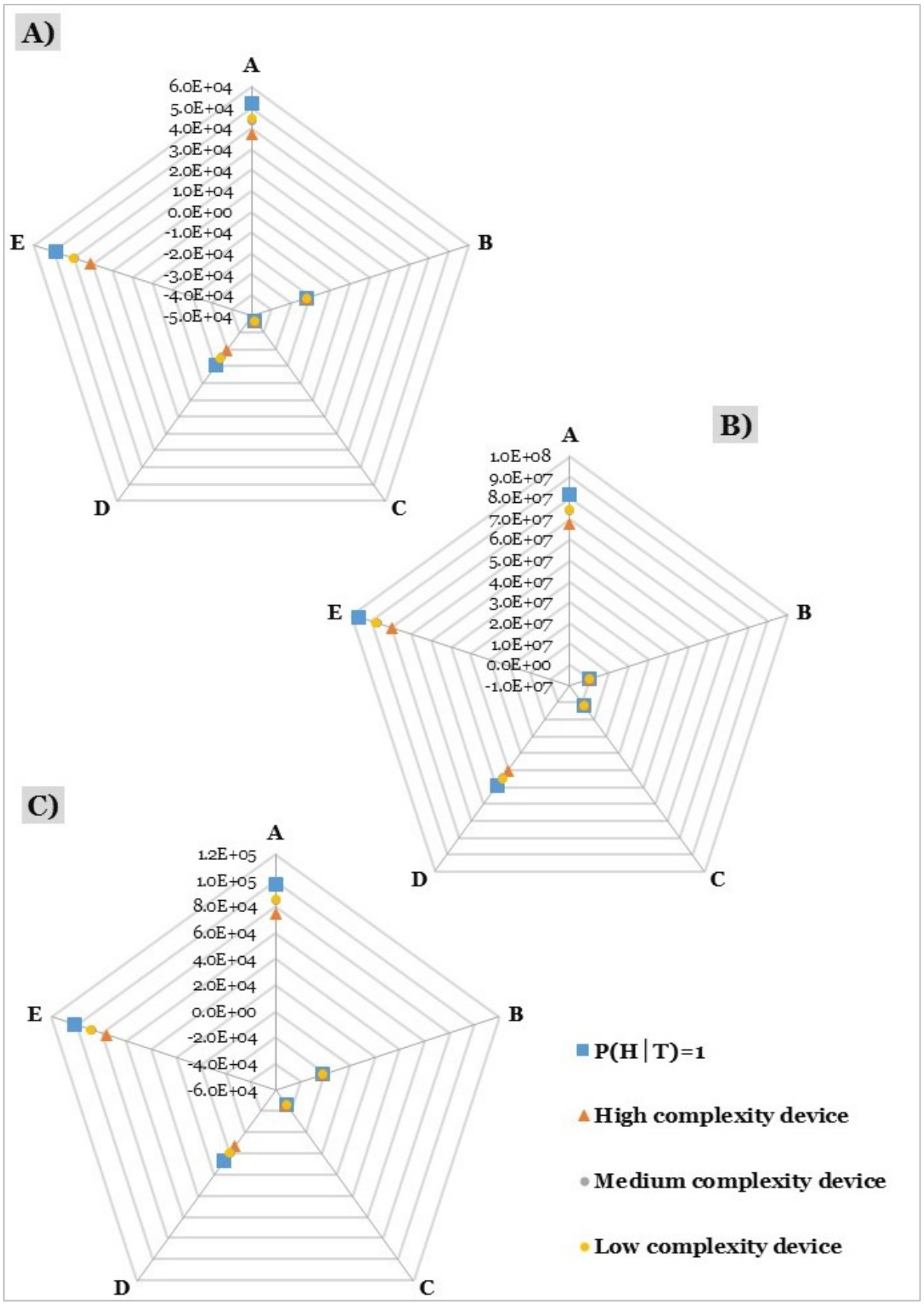


Figure 6. 16 Results of cost-benefit analysis as a function of conditional hazard probability values $(P(H|T))$, which express device complexity, for the five PPS upgrades and three scenarios: A) realistic scenario; B) worst-case scenario; C) expected scenario. Monetary values are expressed in (€, 2016).

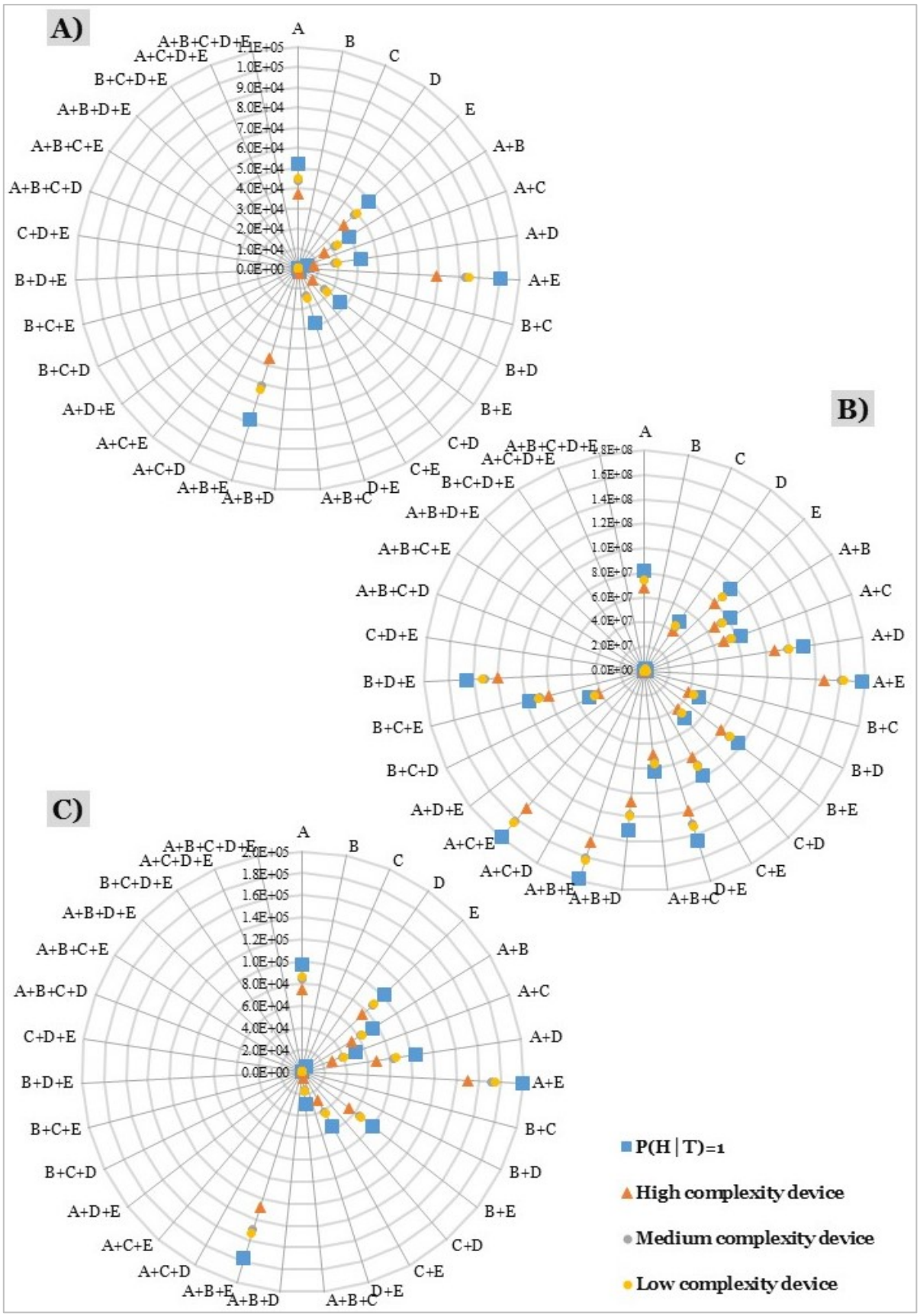


Figure 6. 17 Results of cost-effectiveness analysis as a function of conditional hazard probability $(P(H|T))$ values, for the five PPS upgrades and three scenarios: A) realistic scenario; B) worst-case scenario; C) expected scenario. Monetary values are expressed in (€, 2016).

In conclusion, Figure 6. 16 and Figure 6. 17 show that the modified values of $P(H|T)$ have a linear effect on cost-benefit and cost-effectiveness analyses results. In a general perspective, removing the conservative assumptions of $P(H|T) = 1$ and decreasing $P(H|T)$ lead to a limited reduction of the profitability, both for a single security upgrade and for a combination of them, with similar trend for cost-benefit and cost-effectiveness analyses. Indeed, this difference is not particularly significant, as arguable from the values applied and reported in Table 6. 20, which are all close to 1; in particular, the results obtained for a medium complexity and a low complexity device almost overlap.

Therefore, the results of uncertainty analysis highlighted that it is important to consider adequate values of the threat probability within EM-PICTURES application, because they deeply affect economic analyses results. On the other hand, the effect of explosive device complexity on economic analyses results is generally limited and therefore may be neglected, especially in case of limited information available.

6.4.5.3 Scenario analysis validation

The application of EM-PICTURES highlighted a significant similarity, in terms of benefit category results between realistic scenario and expected scenario (see Figure 6. 12).

As explained in Section 6.4.4, the initial probabilities of occurrence for four different outcomes that compose expected benefits have been chosen arbitrarily, for illustrative purposes (Table 6. 16). Indeed, a validation of scenario analysis through the re-calculation of probabilities for four different outcomes has been carried out, imposing for each category, as well as for Overall values, the equality of expected benefits with realistic benefits, by means of Excel Solver® (version 2013).

The comparison has been made among non-actualized benefit values, but it should be remarked that this element does not affect the comparison results, as long as the discount rate applied is the same. The results of probability revision, reported in Table 6. 21, show that the severity of consequences in the real accident is between category T2 (critical accident) and category T3 (marginal accident), accordingly to the severity ranking considered in the case study.

Therefore, EM-PICTURES may be effectively applied also retrospectively, in purpose to validate the probability of occurrence for security-based accidental scenarios.

The present application might be useful in the security domain, due to the lack of quantitative information regarding accidents occurrence in this domain.

Table 6. 21 Scenario validation (i.e., sv) results.

EXPECTED BENEFITS RECALCULATION RESULTS		***EXPECTED SCENARIO***		***RATIO*** $(C_{Loss,Expected} - C_{Loss,Realistic})/C_{Loss,Realistic}$	
		After scenario validation		***Before scenario validation***	***After scenario validation***
Symbol	***Description***	***Unit***	***Value***	***Value (%)***	***Value (%)***
$B_{SUPC,OV}$	***1 . Overall supply chain benefits***	€	2.04E+04	1.39%	0
$B_{DAMAGE,OV}$	***2 . Overall damage benefits***	€	6.59E+04	-48.55%	-48.74%
$B_{LEGAL,OV}$	***3. Overall legal benefits***	€	5.75E+04	-33.55%	-32.91%
$B_{INS,OV}$	***4. Overall insurance benefits***	€	2.27E+04	-49.45%	-54.54%
$B_{H\&E,OV}$	***5. Overall human and environmental benefits***	€	2.33E+05	229.67%	210.93%
$B_{INTV,OV}$	***6. Overall intervention benefits***	€	4.09E+03	-20.21%	-18.27%
$B_{REPT,OV}$	***7. Overall reputation benefits***	€	3.84E+04	468.00%	0
$B_{OTH,OV}$	***8. Other benefits***	€	8.22E+02	-23.24%	-22.32%
$B_{SPEC,OV}$	***9. Overall specific benefits***	€	6.60E+03	-48.91%	-49.21%
C_{Loss}	***Overall benefits***	€	**4.50E+05**	**54.85%**	**7.80%**
PROBABILITY OF OCCURENCE RECALCULATION RESULTS		**EXPECTED SCENARIO**		**RATIO** $(P_{after\ sv} - P_{before\ sv})/P_{before\ sv}$	
		After scenario validation			
Category	***Descriptive word***	***Value***		***Value (%)***	
T1	**Catastrophic accident**	**3.05E-05**		**-93.91%**	
T2	**Critical accident**	**3.91E-01**		**-2.35%**	
T3	**Marginal accident**	**6.09E-01**		**10.79%**	
T4	**Negligible accident**	**0**		**-100.00%**	

6.4.5.4 Discussion

The current Section has been aimed at applying the EM-PICTURES version of the economic model to an original case study, regarding a terroristic attack to a storage tank farm. The case study, freely adapted from a real event, considered a multi-targets terroristic attack on a realistic chemical installation, including site-specific and accident-specific information in the calculations. The application of EM-PICTURES version of the economic model to the present case study definitely demonstrate that this version of the model provides a useful insight on the profitable security measures to be adopted in a chemical and process facility and therefore it validates the EM-PICTURES version of the methodology, described in Section 4.

The application highlighted that the model provides site-specific answers to security analysts, because it allows evaluating the performance of physical security measures present on a real chemical installation, composing the physical protection system, in relation with the specific adversary sequence of actions. The case study proved the ability of the model to represent a

complex multi-targets terroristic attack and to include adversary mode of action in the effectiveness assessment, which is site-specific and accident-specific, as it depends on the possible adversary path of actions. Indeed, several possible security upgrades were proposed, according to the security functions of detection, delay and response; the pool of security options has been enlarged in comparison with the previous simplified case study (see Section 6.3), in purpose to include more than one detection and delay upgrades, considering improvements at perimeter and at sabotage targets level. The use of a large pool of security options offer a broader pool of alternatives to be considered in the economic analyses, making their results more realistic, even if they add complexity to the calculations. The additional security measures have been compared in terms of overall effectiveness improvement, showing that, with reference to the realistic plant layout and the specific adversary action, it is suggested either to apply fence sensors at external level or to relocate guards in a closer dispatch. However, three options over five show relevant effectiveness improvement indexes results, making the final results of economic analyses application not obvious from the outset. Indeed, it should be noted that the effectiveness analysis results are site-specific and accident-specific and cannot be generalized beyond the current case study. Moreover, although the model is able to take into account possible additional terms that may affect the overall performance of the physical protection system (e.g., lag-time in detection by the security guards), it should be considered as a simplified representation of reality.

The cost assessment allows a precise definition of the most relevant cost terms due to the implementation of the five possible security upgrades, leaving at the same time enough space for the analyst to add site-specific costs. Cost calculations confirmed that the overall cost due to the implementation of a single security upgrade generally belongs to the same order of magnitude (i.e., 10^4€) and installation costs are generally prevailing; for detection upgrades operating costs are significant. Information regarding certain cost voices needs to be retrieved from vendors, other information are related to the plant layout (e.g., the number of detection devices in place); as visible in Section 6.4.3, it is necessary to present cost calculations clearly, as well as to discuss assumptions made and uncertainties arisen.

The potentiality of EM-PICTURES both in predictive and in posterior analysis has been evaluated by its application to several possible accidental scenarios, including a worst-case scenario, a realistic scenario and an expected scenario. The use of multiple scenarios allows providing a broader number of economic indicators and to apply multi-scenario economic criteria provided by the model. The precise categories and subcategories elaborated for benefit calculations allows preventing omissions and inaccuracies; nevertheless, its inputs are validated for the case study by a panel of security experts, in purpose to avoid misleading conclusions. Indeed, the case study proved that benefit assessment allows a detailed

description of the losses derived from either perspective or retrospective accidental scenarios. In particular, the retrospective application of EM-PICTURES (Section 6.4.5.3) may offer an additional tool to retrieve and validate quantitative information on security-based scenarios. Nevertheless, as all economic analyses, EM-PICTURES requires the monetization of all the losses derived from a major accident, which is not always free from complication. For instance, assigning monetary values to mortality and morbidity is a common practice in economic analyses, but it is still defined "a complicated situation" (Tappura et al., 2014), which might arise ethical concerns (Ale et al., 2015). Due to the high monetary value assigned to casualties, human losses are the prevailing category in case of a catastrophic accident (i.e., worst-case scenario). Therefore, the variation of this term affects significantly final economic analyses results, at least for a catastrophic scenario.

Moreover, also the assumptions regarding discount rates for overall costs and benefits might be affected by subjectivity of the analyst; within the case study, standard assumptions referred to cost-benefit analysis for industrial facilities have been considered. Indeed, also the definition of adequate threat and vulnerability probabilities requires carefulness of the security analyst, as they depend on many variables (e.g., typology of terroristic organization and device used in the attack). The deterministic approach provided by EM-PICTURES version of the model is applied here by assuming conservatively unitary values for threat and vulnerabilities. This assumption is justified for the case study, as it refers to a terroristic attack, which may possibly cause a cascading event; it allows focusing on the role of security measures in the prevention of accidental scenarios. Therefore, whenever EM-PICTURES is applied, it is important to present the analysis in a fully transparent manner, specifying the assumptions made and discussing the uncertainties arisen, for example regarding threat and vulnerabilities, in purpose to avoid misleading conclusions.

The application of EM-PICTURES to an illustrative case study, based on a real accident, made clear that a distinctive feature of model application is the flexibility, given by its capability to perform both cost-benefit and cost-effectiveness analyses, offering as outputs a broad spectrum of economic analyses results, which can support the security decision-making process. Indeed, the interpretation of the economic analyses results derived from EM-PICTURES application to the case study is a crucial point. Within this specific application, the results provided by cost-benefit and cost-effectiveness analyses are generally coherent; however, they show a strong dependency on the selection of pertinent security-based scenarios. For instance, cost-benefit analysis results suggest to apply either additional detection at perimeter level or to relocate guard; all the other security upgrades are feasible only with reference to certain scenarios and therefore they do not respect the multi-scenario acceptability criteria of the model. Indeed, the case study highlighted that security measures that are not feasible with reference to a marginal scenario might be appropriate with reference

to a catastrophic scenario. This issue makes the selection of an appropriate pool of credible scenarios even more important.

Cost-effectiveness analysis results confirm that the combination of improved detection at fence is the most profitable option for realistic and expected scenario; according to worst-case scenario it is suggested to adopt a triplet a measures, including, besides the mentioned upgrades, also detection measures at targets level. Nevertheless, the second most profitable combination of security measures diverge with the indications previously provided by cost-benefit analysis, for two scenarios over three, as it includes a measure (i.e., additional delay at perimeter level) singularly not feasible. Indeed, the final results may suggest adopting combinations of security measures that include also one or more security measures singularly not profitable. Indeed, a profitable combination of security measures may include one or more measures whose performances are not excellent, due to several factors standing between effectiveness assessment and final results (e.g., costs, budget threshold, selection of scenarios, etc.). In these situations, it is a management decision whether to revise the security expenditure, as well as to give priority either to cost-benefit or to cost-effectiveness analyses results. Moreover, the results of cost-effectiveness analysis depend on the security budget threshold, which is generally defined yearly by security management; the increase of security budget after the accident is in turn scenario dependent. In comparison with the simplified case study presented in Section 6.3, for the current case study cost-effectiveness analyses results are more significant than cost-benefit ones, due to the extended pool of possible combinations (i.e., 30), to the use of multiple scenarios and to the strict security budget threshold, which excludes several possible combinations of security upgrades. From a general perspective, within the case study, it might be profitable to apply a combination of security measures, which includes upgrades belonging to all the security functions (e.g., additional detection and delay at fence, joined with relocation of security guards), as it provide a more complete security protection.

The uncertainty analysis performed on cost-benefit and cost-effectiveness analyses highlighted that the variation of threat and vulnerability probabilities values has a linear effect on model results, tending to reduce the Net Benefits for all security upgrades and scenarios. The effect of removing the conservative assumptions regarding threat and vulnerabilities is relevant for what concerns the threat and conditional loss probability, but it is limited regarding the conditional hazard probability. The most profitable combination of security measures for all the scenarios is unchanged; therefore, within the present case study, the uncertainty analysis do not offer significantly different results in comparison with the ones previously obtained.

In conclusion, the application of EM-PICTURES version of the economic model to the present case study demonstrated definitely that model outputs may be applied in risk-informed

security decision-making both at company and at regulatory level, to increase the awareness of management or regulators toward security issues by means rather user-friendly outputs, given by cost-benefit and cost-effectiveness analyses results. Moreover, the case study proved that model application gives accurate results, due to its precise checklists and classifications, but it is not over-complicated, even with reference to a complex terroristic attack for a realistic chemical installation.

Therefore, the present case study proved the applicability of EM-PICTURES version of the model in industrial practice, within chemical facilities or related regulatory bodies. However, it is necessary to validate also the other version of the economic model (i.e., ECO-SECURE), specifically referred to environmental security-based accidents, by means of a benchmark case study, referred to a realistic accident.

6.4.6 Conclusions on the case study

EM-PICTURES version of novel economic model for cost-benefit and cost-effectiveness analyses of process-industry related counter-terrorism measures was applied to an illustrative case study, based on a real accident.

Model application started from baseline physical protection system effectiveness assessment for a specific process facility, then it included the evaluation and comparison of the costs derived from the introduction of a security upgrade with the losses derived from either perspective or retrospective accidental events, named benefits, accounting also effectiveness improvement. The application of cost-benefit analysis allows defining single profitable security measures. Cost-effectiveness analysis output is the ranking of security measures combinations, in order of decreasing profitability, for each scenario and according to budget threshold. The uncertainties related to threat and vulnerabilities probabilities are considered, within case study application.

Therefore, the case study definitely demonstrated that EM-PICTURES model version enables to define a more rational selection and allocation of process industry related physical security measures, by means of its outputs, which are a set of economic security-related indicators. EM-PICTURES outputs provide a sound support to managers and regulators involved in the security decision-making process, and its application in industrial practice may eventually contribute to the reduction of chemical plants vulnerability towards intentional malevolent acts.

6.5 ALLOCATION OF PREVENTIVE SECURITY MEASURES AGAINST ENVIRONMENTAL AND ECOLOGICAL TERRORISM IN CHEMICAL FACILITIES (ECO-SECURE APPLICATION)

In this Section, the economic model for the selection and allocation of preventive physical security measures against terroristic attacks in chemical facilities, presented in Section 4, is tested to an original case study, according to ECO-SECURE version, specifically referred to environmental security-related accidents. This benchmark application is aimed at understanding the full potential and possible outcomes of the approach developed, by means of an illustrative case study, freely inspired by a possible security-related event that took place in a chemical facility in Italy.

6.5.1 Definition of the case study

The ECO-SECURE model was applied to an illustrative case study, consisting in the terroristic sabotage of four storage tanks in a fuel storage facility, aimed at causing environmental damages by releasing water pollutants.

The oil depot considered in the case study includes 37 storage tanks containing various liquid hydrocarbons, as diesel and heating oil. The accident scenario consisted of a sequential sabotage of four storage tanks, named after respectively Target 1, Target 2, Target 3 and Target 4, as shown in Figure 6. 18. Target 1 and Target 2 are two heating oil tanks, containing in total 800,000 kg of product; while Target 3 and Target 4 are two diesel tanks, containing in total 1,800,000 kg of product. The distances among the targets have been reported in Table 6. 22, Part B. The damages, as well as the plant layout, are freely adapted from a real security-based accident that took place during the night between 22nd and 23rd February 2010 in Villasanta, Monza-Brianza province, Italy (Alpas et al., 2011; Associated Press in Rome, 2010; EMARS - Major accidents reporting system, 2010; Winfield, 2010a). However, the case study is fictional and its aim is the validation and the further implementation of ECO-SECURE version of the model, addressing the selection and allocation of physical security measures against environmental and eco-terroristic attacks in a chemical facility. Therefore, the causes of the security-based accident here-in considered (i.e., an external environmental terroristic attack) are not related to the causes of the real accident (Berni, 2016; La Repubblica, 2016).

The starting point for the adversary was chosen in correspondence of a railway route just outside the border of the facility, at about 50 m distance from the first target. The adversary was supposed to carry out the sabotage action by foot. The sabotage sequence of actions consisted in opening a valve and switching on a pump in correspondence of each target, leading

to the spill of the entire contents of the four tanks, for a total amount of 2,600,000 kg of hydrocarbon liquid products (ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010). The spill substance, from the pipes of the loading docks and the repayment of the product, overfilled the tanks of the oil-water separator tank coming indirectly from the sewage system inside the plant and directly passed to curb protection, likely due to saturation of the sewer system itself; part of the spill was also poured into the containment basins. Then, the spill was drained from the oil-water tank through the main valve, always kept open to allow the discharge of wastewater from a hydraulic barrier aimed at remediation, to the sewer outside the plant, which flows into the main collector. Indeed, the spill reached the treatment plant of the nearby city through the main sewer. Consequently, the spill has been poured into the nearby river and caused a significant pollution of river water and rive sides downstream of the filter for about 100 km, with involvement of a second river in the stretch downstream from the mouth of the first river. Contaminated waters of the second river affected the second river delta and the coastal area of the sea.

In the actual event, the Lambro river (i.e., first river in the case study) and the Po river (i.e., second river in the case study) were polluted for about 350 km. The realistic damages, derived from the actual event, consisted in severe environmental losses to the ecosystem, requiring therefore emergency actions to contain pollution that lasted several days after the accident. Furthermore, intense monitoring and in-site and off-site remediation actions were required during the subsequent months. The company had to sustain legal costs due to prosecution, as well as the payment of fines. The accident resulted in no human losses but in severe damages to the environment, in economic damages to the company, and in collateral damages to surrounding activities and public infrastructures (e.g., the treatment plant was off for about one month) in the nearby densely populated area (EMARS - Major accidents reporting system, 2010).

The determination of PPS in place was carried out using available information and comparing the description of PPS usually present in chemical facilities (Reniers et al., 2015) with photos and maps of the layout of the reference installation, reported in Figure 6. 18. The screening allowed the identification of key protection elements and key distances, which are data necessary to calculate the baseline physical protection system effectiveness. Further information on the PPS in place is reported in Section 6.5.2.

The application was carried out in Excel® modelling environment, using 7 different datasheets, corresponding to ECO-SECURE modules, as explained in Section 4.2.1.

Figure 6. 18 Layout of the reference installation considered in the case study, with adversary starting point and path of actions, the latter indicated by the numbers. The ending point is target 4. Further information on adversary tasks is available in Table 6. 22. The layout has been retrieved from Google Earth®.

6.5.2 Development of adversary sequence diagram and effectiveness calculation

6.5.2.1 Definition of site-specific adversary sequence diagrams and calculation of the baseline system effectiveness

A possible critical site-specific adversary sequence path, in relation with physical protection elements present on the reference site, was defined and is described in Table 6. 22, Part A and shown in Figure 6. 18. The calculation of baseline system effectiveness was carried out according to the approach described in Section 4.2.2 for ECO-SECURE version of the model, with the aim to determine the probability of interruption (i.e., P_{I,p^*} indicated also as $P_I{}^*$) of the critical adversary path.

The solely detection elements present are cameras on the wall delimiting the two storage areas, with $P_{AD,9} = 0.9$. The probability of assessed detection $(P_{AD,i})$ expresses the likelihood of detecting an adversary within the zone covered by cameras or intrusion detection sensors. In addition, the location of detection elements was included in the analysis, according to the EASI model, considering a standard B location, indicating detection before delay. For all delay elements with the exception of running times, specific data have been retrieved (Garcia, 2007) and reported in Table 6. 22, Part A, jointly with all the data inherent to the detection function for the path considered in the case study. For the calculation of running times, the standard adversary velocity of $10\ ft/s = 3.048\ m/s$ has been assumed, considering a reduction factor

due to additional weights carried by the adversary unitary (i.e., no additional weight carried by the adversary).

Table 6. 22 Input for the calculation of baseline PPS effectiveness referred to the critical path. Part A) Adversary sequence and inputs for the calculation of detection and delay elements referred to the identified adversary path; Part B) Additional data for the calculation of running delay times; Part C) Inputs for the calculation of the response function. Standard deviation was assumed 3/10 of the mean value. Values retrieved from data repository (Garcia, 2007) and site-specific plant layout.

Part A) Adversary Sequence Diagrams and Inputs for Detection and Delay elements				
ADVERSARY TASKS		***DETECTION***	***DELAY***	
Task number	***Task Description***	***Detection elements and assessed detection probabilities*** $P_{AD,i}$	***Delay elements***	***Mean delays*** $t_{D,i}$ ***(s)***
1	**Starting point**	-	-	-
2	**Climb external wall**	None	Height of the wall	10.0
3	**Run to first tank (Target 1)**	None	Running time	14.8
4	**Open first valve**	None	Time required to open first valve	30.0
5	**Activate first pump**	None	Time required to activate first pump	60.0
6	**Run to second tank (Target 2)**	None	Running time	16.4
7	**Open second valve**	None	Time required to open second valve	30.0
8	**Activate second pump**	None	Time required to activate second pump	60.0
9	**Run to third tank (Target 3)**	Camera on wall delimiting two areas ($P_{AD,9} = 0.9$)	Running time	26.9
10	**Open third valve**	None	Time required to open third valve	30.0
11	**Activate third pump**	None	Time required to activate third pump	60.0
12	**Run to fourth tank (Target 4)**	None	Running time	43.6
13	**Open fourth valve**	None	Time required to open fourth valve	30.0
14	**Activate fourth pump**	None	Time required to activate fourth pump	60.0
15	**Ending point**	-	-	-

Part B) Data for Calculation of running delay times							
Description of the action	***Symbol***	***Value***	***Unit***	***Description of the action***	***Symbol***	***Value***	***Unit***
Adversary velocity during running	v	3.048	m/s	**Distance external wall/ target 1 (Task 3)**	d_3	45	m
Distance target 1/ target 2 (Task 6)	d_6	50	m	**Distance target 2/ target 3 (Task 9)**	d_9	82	m
Distance target 3/ target 4 (Task 12)	d_{12}	133	m	**Reduction factor due to additional weight carried by adversary**	φ	1	*Adim.*

Part C) Data for the calculation of Response function			
Probability of guard communication P_C	0.95	***Mean Response Force Time*** t_G ***(s)***	480

Distances among delay elements were retrieved from the reference map and reported in Table 6. 22, Part B. Standard deviation for the delay parameter of each security element and for the response force time parameter was assumed as 3/10 of the mean value throughout the case

study, according to the conservative assumption on data dispersion reported in the EASI model (Garcia, 2007). This assumption allows considering that guards will not always respond exactly after the same time, and that adversaries may take more or less time to penetrate barriers with respect to average values. Inputs for the calculation of response element have been reported in Table 6. 22, Part C; for the probability of guard communication (P_C) a conventional value for industrial facilities was assumed (Garcia, 2007), with a response force time (t_G) of 8 minutes, considering that security guards are not present on site during the night shift, with the exception of the facility caretaker.

The critical probability of interruption (P_I^*) has been calculated according to equation (4.1) and its value is 0.0425. P_I^*will be considered in the development of the case study and represents the value of the baseline PPS effectiveness (i.e., $\eta_{PPS,old}$). The value was obtained by inserting in the EASI model datasheet (Garcia, 2007) the inputs listed in Table 6. 22, according to the approach described in Section 4.2.2 for ECO-SECURE version of the model. Therefore, the calculation of baseline system effectiveness highlights security weaknesses, which may be tackled by the introduction of pertinent security upgrades.

The baseline effectiveness calculations can be performed in other case studies, according to the same approach proposed in ECO-SECURE version of the model; however, the results are site-specific as they require data regarding distances on site and security measures in place. Therefore the value of baseline effectiveness obtained (i.e., 0.0425) cannot be extended beyond the current case study.

6.5.2.2 Security upgrades identification and calculation of upgraded system effectiveness

Starting from the value of baseline PPS effectiveness ($\eta_{PPS,old} = 0.0425$), six PPS upgrades have been proposed, according to technical references (Garcia, 2007; Reniers et al., 2015):

A) Adding surveillance cameras as perimeter detection system;

B) Construction or additional height to concrete-reinforced external perimeter wall as perimeter delay element;

C) Adding detection elements (i.e., surveillance cameras) at sabotage targets level;

D) Adding delay elements at sabotage targets level;

E) Adding alarm for unauthorized manual valve opening and cages to hinder unplanned switching on/off pumps at sabotage targets level;

F) Reducing response force time by building a closer and 24h active guard dispatch.

It should be noted that upgrades A and C refer to the detection function, upgrades B and D refer to the delay function, upgrade E refers to the combination of detection and delay functions and upgrade F refers to the response function. Moreover, upgrades A and B refer to the external perimeter of the facility, while upgrades C, D, E and F refer to the proximity to the sabotage targets. All the tanks of the storage facility have been considered possible targets.

Table 6. 23 Effectiveness results for six different possible PPS upgrades. From the left to the right, in column order: Upgrade identity, description of the upgrade, Physical protection function modification, reference number of adversary sequence diagram modified tasks, modified inputs for the effectiveness calculations, upgraded PPS effectiveness ($\eta_{PPS,new\ i}$) and effectiveness improvement index ($\overline{\Delta\eta_i}$). (*) Reduction of response force time does not affect a single task. A data repository regarding modified inputs values for security upgrades is available in Garcia (Garcia, 2007).

Upgrade ID	*Description*	*PPS - function modification*	*N° of modified tasks*	*Modified inputs*	$\eta_{PPS,\ new\ i}$	$\overline{\Delta\eta_i}$
A	**Addition of cameras at external perimeter wall level**	Detection; exterior cameras	2	$P_{AD,2} = 0.9$	0.3904	**0.3479**
B	**Construction/ additional height to external concrete-reinforced perimeter wall (3m high)**	Delay; wall hardness	2	$t_{D,2} = 180\ s$	0.0425	**0**
C	**Addition of detection elements at sabotage targets (cameras on each tank)**	Detection; exterior cameras	3; 6; 9; 12	$P_{AD,3} = P_{AD,6} = P_{AD,12} = 0.9$ $P_{AD,9} = 0.99$ for existing cameras	0.3685	**0.3260**
D	**Addition of delay elements at sabotage targets**	Delay; additional wall with doors	3; 6; 9; 12	$t_{D,3} = t_{D,6} = t_{D,9} = t_{D,12} = 30\ s$ additional delay with running time	0.0783	**0.0358**
E	**Addition of alarms for unauthorized manual valves opening and cages for pumps at sabotage targets**	Detection (alarms); Delay (cages)	4; 7; 10; 13 5; 8; 11; 14	$P_{AD,4} = P_{AD,7} = P_{AD,10} = P_{AD,13} = 0.9$ for alarms $t_{D,5} = t_{D,8} = t_{D,11} = t_{D,14} = 30\ s$ for pumps cages	0.5215	**0.4790**
F	**Reduction of response force time (by creating a closer and 24h active guard dispatch)**	Response; relocation of guards closer to storage area	- (*)	$t_G = 240\ s$	0.5771	**0.5346**

The upgraded values of effectiveness, indicated as $\eta_{PPS,new\ i}$, for each of the six options have been calculated by inserting the modified input items, listed in Table 6. 23 (i.e., third to last column), in the effectiveness model previously applied to calculate baseline PPS effectiveness (i.e., the EASI model), according to the approach presented in Section 4.2.3 for ECO-SECURE version of the model. The modified inputs regarding each security upgrade, with the exception of upgrade F, affect only specific tasks of the adversary sequence diagram; for all the remaining tasks, the values reported in Table 6. 22 have been applied.

The results regarding upgraded effectiveness (i.e., $\eta_{PPS,new\ i}$) and effectiveness improvement index (i.e., $\overline{\Delta\eta_i}$, named sometimes also risk reduction, as discussed in Section 4.2.7.1),

corresponding to each of these upgrades, have also been reported in Table 6. 23. Effectiveness improvement values have been obtained for each security upgrade according to equation (4.8), using the baseline effectiveness value (i.e., $\eta_{PPS,old} = 0.0425$) and the upgraded effectiveness value (i.e., $\eta_{PPS,new\ i}$).

The results in Table 6. 23 clearly show that, from the effectiveness point of view, the best option is the reduction of response force time (upgrade F), followed by the application of alarms for valves and cages for pumps at sabotage targets level (upgrade E). On the other hand, the presence of additional delay elements, represented by options B and D, proved to be ineffective in increasing PPS effectiveness. The addition of detection elements (i.e, cameras), both at external and sabotage targets level, represented respectively by upgrade A and C, shows an intermediate performance in terms of risk reduction. However, even if upgrades F and E are the best ones from the effectiveness intermediate calculation, it does not mean automatically that they are the best options in the end of the application, due to additional terms that are still to be considered in the analysis (e.g., costs, benefits, budget threshold, etc.). The approach presented in Section 4.2.3, here applied, can be used analogously in other case studies. However, the results of effectiveness calculations are site-specific and accident-specific; consequently they cannot be generalized beyond the current case study.

6.5.3 Cost calculation for security upgrades

Cost calculations were carried out for each of the six PPS upgrades proposed in the case study, according to the six main categories, 22 subcategories and formula presented in the model (Section 4.2.4), considering the time span of one year and the implementation of a single security upgrade. It should be noted that many subcategories consist of wages, so realistic annual salaries have been retrieved from a specific database (PayScale, 2016) and converted into hourly wages considering 1920 $hours/year$.

Several data regarding cost calculation have been retrieved in US dollars of year 2016. A conversion rate from US dollars to Euro of 0.9019 $€/U.S.A.$ \$ was assumed (X-Rates, 2016). Moreover, a location factor of 1.20 (Richardson Products & Cost Data On Line Inc., 2008) was applied in order to adjust US prices and salaries to those of Italy, the location of the case study. The use of location factor throughout the analysis allowed a site-specific cost calculation. In the estimation of wages, several professional profiles, which are typically involved in the selection, design, installation and maintenance of a security system in a chemical facility, were considered. According to their different job tasks, the following security-related jobs have been accounted for the calculation of appropriate cost subcategories: purchasing office staff and manager, security manager, security engineer, security guards and officers, training expert (i.e., security consultant), masons, installation and maintenance technicians.

In the calculation of initial costs for each security upgrade, wages for the job profiles involved, costs of auxiliary materials and publications of leaflets for internal use have been considered.

In the calculation of Installation costs, with particular reference to equipment costs, specific information of market prices for each security upgrade have been retrieved from vendor websites and reported in Table 6. 24.

In the calculation of operating costs, utility costs consist of the costs of annual electric power consumption, which are significant only for upgrades A, C and E. For the three mentioned upgrades the power has been calculated through the standard power law, retrieving data on intensity and voltage from products datasheets (Alibi, 2016; Shenzhen An Ying Technology Co. Ltd., 2016) and accounting the number of devices in place, which have been assumed to be working continuously all year long. The estimated annual electric power consumption has been $5.78 \cdot 10^2$ kWh for upgrade A, $3.89 \cdot 10^3$ kWh for upgrade C and $7.78 \cdot 10^3$ kWh for upgrade E. Considering an average industrial electric energy market price in Italy of 0.175 €/kWh (Eurostat, 2016), utilities costs have been finally calculated. Human resources operating costs have been calculated by considering the manpower, in terms of security officers and guards wages for each security upgrade, which is not negligible for upgrade A, C and E. It should be noted that for security upgrades B and D, which are walls in different positions, this subcategory is equal to zero. For upgrade F, the hiring of four additional security guards, aiming to extend the security surveillance during the night shift, has been accounted. Therefore, operating costs, prevailing over other cost categories for upgrade F, consist of security guards annual wages, hiring and training costs.

In the calculation of Maintenance, inspection and sustainability costs, the following assumptions have been made for each security upgrade: material costs were estimated assuming an annual substitution rate for equipment and other materials in the range between 3% and 5%, 2 scheduled maintenances, 1 unscheduled maintenance and 2 scheduled inspections per year have been accounted. License and renewal costs appeared to be negligible for all the six upgrades.

Other running costs have been calculated for each security upgrade; only for upgrade F this cost category has a significant role, provided that the construction of a new building for security guards requires additional office furniture and utilities.

In the calculation of Specific costs, the contribution offered by false-positive costs should be considered only for detection elements (i.e., upgrade A, C and E). For these upgrades, a single false-alarm cost has been assumed, based on expert judgement, $2.80 \cdot 10^3$ € (Toronto Municipality, 2016) and $P(alarm \mid no\ attack) = 0.143$ (Garcia, 2007). According to the considerations expressed in Section 4.2.4, false-positive costs depend on the assumption regarding the probability of the attack. Assuming the probability of the attack equal to one

turns false-positive costs to zero, leading to the minimum value of specific costs value. Consequently, assuming the probability of the attack equal to zero, leads to the maximum value of specific costs. Site-specific costs, as revisions of safety measures and procedures, have been accounted in particular for delay elements, whose implementation might require a revision of emergency routes, as well as entrance doors and exit doors. Therefore, specific costs are represented by a range of values only for detection elements (i.e., upgrades A, C and E), in turn determining a range of values for Overall costs. Nevertheless, in case of a narrow range of values for overall costs, as in the case study, this dependence might be neglected.

Table 6. 24 Data for the calculation of Equipment costs for six different PPS upgrades.

UPGRADE ID	***DATA FOR THE CALCULATION OF EQUIPMENT COSTS***			
	Description	***Unit***	***Value***	***Reference/Notes***
A	Number of surveillance cameras at perimeter level	$n°units$	11	8% of spare items not included
	Cost of an outdoor surveillance camera	$€/unit$	195.9	Vendor website (Alibi, 2016)
B	Length and height of the concrete wall, with footings	m	1382; 3	Layout of the facility
	Cost of the wall (according to these specifications)	€	3251.76	Vendor website (Get A Quote, 2016)
C	Number of cameras for each tank	$n°units/tank$	2	-
	Cost of an outdoor camera	$€/unit$	195.9	Vendor website (Alibi, 2016)
	Total number of cameras in place	$n°units$	74	8% of spare items not included
D	Number of tanks group	$n°units$	9	Layout of the facility
	Average length and height of the concrete wall around each unit	m	800; 3	Layout of the facility
	Cost of the wall for each unit (according to these specifications)	$€/unit$	1900	Vendor website (Get A Quote, 2016)
	Cost of security doors to be applied on each unit	$€/unit$	1082	Vendor website (Grainger, 2016)
E	Number of alarm per valve	$n°units/valve$	1	-
	Cost of an industrial alarm	$€/unit$	117.4	Vendor website (Shenzhen An Ying Technology Co. Ltd., 2016)
	Number of alarms	$n°units$	37	8% of spare items not included
	Number of cages per pump	$n°units/pump$	1	-
	Cost of a metallic cage for pump with lock	$€/unit$	18.4	-
	Number of pumps	$n°units$	37	-
F	Unit cost for the new building (standard warehouse with concrete floor and metal clad)	$€/m^2$	582.3	Vendor website (BMT, 2016)
	Area of the building	m^2	70	Layout of the facility

For each of the six security upgrades, the main results obtained from cost calculations, according to the six cost categories of the model, as well as the Overall costs ($C_{Security,i}$) have been illustrated in Table 6. 25.

Table 6. 25 Calculation of Overall costs for six security upgrades, as the sum of six main categories: 1) Overall initial costs, 2) Overall installation costs, 3) Overall operating costs, 4) Overall maintenance, inspection & sustainability costs, 5) Other running costs, 6) Overall specific cost. For detection upgrades (i.e., upgrades A, C, E) Overall specific costs, and consequently Overall costs, depend on the assumption regarding the probability of the attack. Setting $P(T)_{ij} = 1$ leads to the minimum value of specific costs and consequently to the minimum value of Overall costs for a generic security measure. Setting $P(T)_{ij} = 0$ leads to the maximum value of specific costs and consequently to the maximum value of Overall costs for a generic security measure.

CALCULATION OF OVERALL COSTS $(C_{Security,i})$			UPGRADE A	UPGRADE B	UPGRADE C	UPGRADE D	UPGRADE E	UPGRADE F
Symbol	***Description***	***Unit***	***Value***	***Value***	***Value***	***Value***	***Value***	***Value***
$C_{INITIAL,OV}$	***1. Overall initial costs***	**€**	**3.53E+03**	**1.57E+03**	**3.53E+03**	**1.57E+03**	**4.41E+03**	**4.49E+03**
C_{INV}	Investigation costs	€	4.75E+02	4.75E+02	4.75E+02	4.75E+02	4.75E+02	4.75E+02
$C_{S\&D}$	Selection and design costs	€	5.73E+02	6.79E+02	5.73E+02	6.79E+02	6.79E+02	5.73E+02
$C_{MAT,I}$	Material costs	€	1.50E+03	0	1.50E+03	0	1.50E+03	2.00E+03
C_T	Training costs (start-up/in service)	€	6.87E+02	1.14E+02	6.87E+02	1.14E+02	1.45E+03	1.14E+03
$C_{G\&I}$	Changing of guidelines and informing costs	€	3.00E+02	3.00E+02	3.00E+02	3.00E+02	3.00E+02	3.00E+02
$C_{INSTALL,OV}$	***2. Overall installation costs***	**€**	**4.17E+03**	**7.10E+03**	**1.92E+04**	**3.11E+04**	**7.87E+03**	**5.71E+04**
C_{START}	Start-up costs	€	7.42E+02	1.16E+03	7.42E+02	9.57E+02	9.13E+02	9.57E+02
C_E	Equipment costs	€	2.95E+03	3.95E+03	1.77E+04	2.78E+04	5.89E+03	4.57E+04
$C_{INSTALL}$	Installing costs	€	4.77E+02	1.99E+03	7.34E+02	2.37E+03	1.06E+03	1.04E+04
$C_{OPERATION,OV}$	***3. Overall operating costs***	**€**	**1.01E+03**	**0**	**7.99E+03**	**0**	**5.01E+03**	**1.70E+05**
$C_{U,OP}$	Utilities costs	€	1.01E+02	0	6.81E+02	0	1.36E+03	0
C_{HRO}	Human resources operating costs		9.13E+02	0	7.30E+03	0	3.65E+03	1.70E+05
$C_{MIS,OV}$	***4. Overall maintenance, inspection & sustainability costs***	**€**	**1.98E+03**	**1.05E+03**	**2.69E+03**	**2.18E+03**	**2.62E+03**	**2.79E+03**
$C_{MAT,M}$	Material costs	€	8.05E+01	9.76E+01	2.75E+02	8.05E+02	4.10E+02	1.32E+03
C_{MNT}	Maintenance team costs	€	1.36E+03	6.78E+02	1.87E+03	1.11E+03	1.67E+03	9.27E+02
C_{INSP}	Inspection team costs	€	5.42E+02	2.71E+02	5.42E+02	2.71E+02	5.42E+02	5.42E+02
C_{LIC}	License and rental renewal	€	0	0	0	0	0	0
$C_{OR,OV}$	***5. Other running costs***	**€**	**1.80E+02**	**2.80E+02**	**1.80E+02**	**2.80E+02**	**2.80E+02**	**2.43E+04**
C_{OF}	Office furniture costs	€	0	0	0	0	0	1.81E+04
C_T	Transport costs	€	1.00E+02	2.00E+02	1.00E+02	2.00E+02	2.00E+02	3.00E+02
C_{COMM}	Additional communication costs	€	6.00E+01	6.00E+01	6.00E+01	6.00E+01	6.00E+01	6.00E+01
C_I	Insurance costs	€	0	0	0	0	0	0
C_{OU}	Office utilities costs	€	2.00E+01	2.00E+01	2.00E+01	2.00E+01	2.00E+01	5.60E+03
C_{OS}	Office supplies costs	€	0	0	0	0	0	2.00E+02
$C_{SPEC,OV}$	***6. Overall specific costs***	**€**	**3.00÷ E+02 7.00 E+02**	**1.00E+03**	**4.00E+02 ÷8.00 E+02**	**8.00E+02**	**8.00E+02 ÷ 1.20 E+03**	**1.00E+03**
C_{FP}	False-positive case costs	€	0÷4.00E+02	0	0÷4.00E+02	0	0÷4.00E+02	0
C_{SITE_SP}	Site-specific costs	€	3.00E+02	1.00E+03	4.00E+02	8.00E+02	8.00E+02	1.00E+03
$C_{Security,\ i}$	***Overall costs***	**€**	**1.12E+04 ÷1.16E+04**	**1.10E+04**	**3.39E+04 ÷3.43E+04**	**3.60E+04**	**2.10E+04 ÷2.14E+04**	**2.60E+05**

Figure 6. 19 summarizes the results obtained from cost calculations. The values of Overall costs belong to the same order of magnitude (i.e., 10^4 €) for all the security upgrades, with the exception of upgrade F that is one order of magnitude higher. The comparison among percentage compositions, also reported in Figure 4, shows that for detection and delay elements (i.e., upgrades A, B, C, D and E) installation costs are the prevailing ones. For upgrades regarding the detection function (i.e., upgrades A, C and E), initial costs and operational costs are also relevant items.

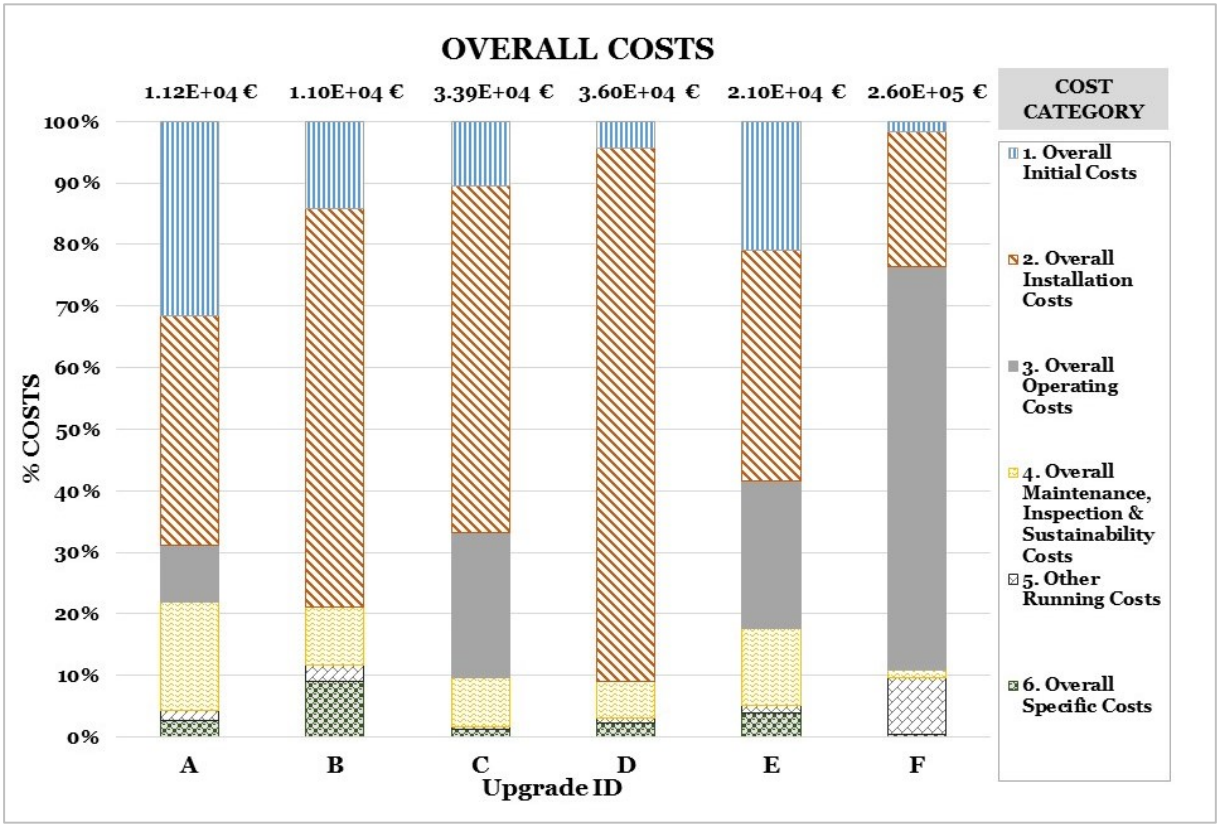


Figure 6. 19 Percentage composition of Overall costs for each upgrade of the PPS, according to the six cost categories considered, under the assumption of $P(T)_{ij} = 1$. On x-axis, from the left to the right, the six PPS upgrades are represented: A) Adding surveillance cameras as perimeter detection system; B) Construction or additional height to concrete-reinforced external perimeter wall as perimeter delay element; C) Adding detection elements (i.e., surveillance cameras) at sabotage targets level; D) Adding delay elements at sabotage targets level; E) Adding alarms for unauthorized manual valves opening and cages to hinder unplanned switching on/off of pumps at sabotage targets level; F) Reducing response force time by building a closer and 24h active guard dispatch. Overall cost of each security upgrade is reported on the top of the corresponding column.

6.5.4 Benefit calculation for the actual scenario

The losses derived from a successful attack should include the environmental damages and other damages, both direct and indirect, which will accrue because of a successful attack, taking into account the value and vulnerability of environment, people and infrastructures, as described in Section 4.2.5 for ECO-SECURE version of the model. Consequently, benefits calculations are dependent on the choice of an appropriate accidental scenario. In case of

economic analyses based on a real event it is common practice to account the retrospective losses, named also realistic benefits, which indicate the actual losses sustained in the accident. Therefore, the realistic benefits were considered in the case study. These may not exactly reflect the actual ones, due to the limited amount of technical and site-specific information available. It was assumed that benefits are independent from the security measure that can be implemented.

Benefit calculations have been carried with respect to the actual scenario considered in the case study, according to the categories, subcategories and formula proposed in Section 4.2.5 for ECO-SECURE version of the model, which specifically refers to environmental consequences.

In the calculation of Supply chain benefits, production losses and start-up losses have been neglected because the facility is an oil depot, not a production facility (e.g., a refinery). A flat rate for Schedule benefits has been retrieved (Galvani, 2015); details are available in Table 6. 27.

In the calculation of Damage benefits, illustrative commercial equipment costs for the pumps damaged have been retrieved from vendors; details on the calculations are reported in Table 6. 26. The values of damages to company infrastructures, surrounding living area (e.g., canals, private properties) have been reported in Table 6. 27. The estimation of damages to public infrastructures, as the water treatment system of the nearby city is presented in the same table. Regarding the evaluation of finished goods damages, average market prices have been assumed for both the products (i.e., diesel and heating oil); details on calculations are reported in Table 6. 26.

In the calculation of Legal & insurance benefits and after, it should be noted that, as for costs calculations, many benefits subcategories consist of wages. The same data displayed in Section 6.5.3, regarding the conversion rate from US dollars to € and the location factor have been applied. In the case of Legal & insurance benefits, the job profiles involved are junior lawyers and seniors lawyers, specialized lawyers, security manager, security engineer, security analyst and security consultant. Details on the data applied for the calculation of Legal & insurance benefit subcategories are available in Table 6. 26.

No human losses and injuries have been sustained in the actual accident; however, data regarding the calculation of Human benefits, as the value of a statistical life (VSL) and compensation costs for injuries might have been retrieved from previous studies (Nicola Paltrinieri et al., 2012; Viscusi and Aldy, 2003).

Table 6. 26 Data for the calculation of benefit subcategories with respect to the actual scenario.

BENEFIT CATEGORY	**BENEFIT SUBCATEGORY SYMBOL**	***DATA FOR THE CALCULATION OF BENEFIT SUBCATEGORIES***				
		Symbol	***Description***	***Unit***	***Value***	***Reference/Notes***
DAMAGE BENEFITS	$B_{D,OM\&P}$	A	*Damage to the company equipment and machines*	€	1.19E+04	Damage to 4 pumps; average unit cost for a pump assumed 2.98E+03 € from vendors and validated by expert judgement
		B	*Damage to the company buildings and other infrastructures*	€	5.00E+03	Limited damages to piping/surrounding infrastructures (EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement
		C	*Damage to the company raw materials and finished goods*	€	6.52E+05	Spill of diesel and heavy oil. Inventories of spilled diesel and heavy oil available in Section 6.5.1. Average market prices assumed for diesel and heavy oil (i.e., respectively 280 $€/m^3$ and 95 $€/m^3$)
LEGAL & INSURANCE BENEFITS	B_{ILAW}	K	*Civil liability fines*	€	6.89E+06	Civil liability fines as expressed by prosecutors (Totaro, 2014)
		M	*Administrative liability fines*	€	8.90E+05	Taxation on spilled products (Galvani, 2015)
	B_{LEG}	S_B	*Total security budget of the facility*	€	1.00E+04	Severe security deficiencies highlighted by accident report (EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement
		I_{SB}	*Increase of the security budget for the facility after accident occurrence*	%	17.00	Scenario dependent value, based on expert judgement, to reach usual budget values reported by (Reniers and Van Erp, 2016)
	$B_{P\&LIC}$	C_{CD}	*Cost due to facility close-down*	€	1.20E+08	Data retrieved from (Berni and Rosa, 2015)
		L_P	*Likelihood of losing operating permit* (%)	%	10.00	Likely closing-down of the facility after the accident (Berni and Rosa, 2015) – quantification based on expert judgement
	B_{INS}	P_F	*Current total premium cost of the facility*	€	5.00E+07	Premium based on possible value of the facility after partial sale, as declared by company owner (Pecorella, 2011)
		I_{PF}	*Expected increase of the premium*	%	1.00	Expert judgement
ENVIRONMENTAL BENEFITS	B_{REM}	$m_{SP,i}$	*Amount of product spilled* (kg) *or* (m^3)	kg	2.60E+06	Inventory of spilled hydrocarbons products available in Section 6.5.1
		$C_{SP,i}$	*Cost per unit of product i spilled* $\left(\frac{€}{kg}\right)$ *or* $\left(\frac{€}{m^3}\right)$	€	1.44	Unit remediation cost for liquid hydrocarbon spills retrieved from a previous study (Etkin, 1999), converted and actualized to (€(2016))
		$C_{REM,LT}$	*Long-term remediation costs*	€	2.00E+07	Long-term remediation costs for the site retrieved from (Berni and Rosa, 2015)
REPUTATION BENEFITS	B_{SP}	M_{REP}	*Current total market value of the company*	€	6.00E+07	Current total market price for the company based on (Pecorella, 2011)
		D_{REP}	*Expected drop in the share price*	%	31	Expected long-time percentage drop of market price regarding a major oil spill (Goossens, 2012)

Hiring benefits are inserted in Human benefits category as they refer to the costs that should be sustained by the company when an employee is hospitalized or dead after the accident to hire additional personnel in substitution. Therefore, no hiring benefits have been sustained in the actual accident. Data regarding their calculation may be retrieved from previous studies (Gavious et al., 2009; Reniers and Brijs, 2014b); it is suggested to consider hiring and training costs equivalent to a monthly salary each for the employee category.

In the calculation of Environmental benefits, flat rates for external and internal intervention costs have been reported in Table 6. 27. Environmental remediation costs have been estimated according to the data reported in Table 6. 26. A flat rate for other environmental damages to the surrounding ecosystem (i.e., plants and animals) is available Table 6. 27.

The data for the calculation of Reputation benefits are available in Table 6. 26. The expected percentage drop of market price regarding a major oil spill has been assumed, with a value of 31% (Goossens, 2012). This data was confirmed in a long-term time perspective, which is the time span required for benefit calculations, by a recent study (Neilan, 2016). In the calculation of Specific benefits, collateral damages, due to voluntary spills in the river from nearby facilities subsequent to the major accident (Querzé, 2010), have been reported in Table 6. 27.

The data reported in Table 6. 26 and Table 6. 27, applied for the calculation of benefit categories and subcategories, were retrieved from a collection of references and validated by a panel of security managers and academic security experts. Eventually, all the benefit numerical values have been determined accordingly to the pertinent categories and subcategories of ECO-SECURE version of the model, allowing the calculation of the Overall benefits $(C_{Loss,j})$, for the actual scenario (Table 6. 27).

Table 6. 27 Overall benefits results for realistic scenario. The calculation of Overall benefits ha been carried out as the sum of seven main categories: (1) Overall supply chain benefits, (2) Overall damage benefits, (3) Overall legal & insurance benefits, (4) Overall human benefits, (5) Overall environmental benefits, (6) Overall reputation benefits, (7) Overall specific benefits. Intermediate calculations regarding benefit subcategories are reported, with assumptions made.

CALCULATION OF OVERALL BENEFITS ($C_{Loss,j}$)				
Symbol	***Category/ subcategory description***	***Unit***	***Value***	***Assumptions***
$B_{SUPC,OV}$	***1. Overall supply chain benefits***	**€**	**1.70E+06**	**See assumptions for subcategories**
B_{PL}	*Production loss benefits*	€	0	No stop in production, it is an oil depot
B_{START}	*Start-up benefits*	€	0	No start-up benefits, it is not a production facility
B_{SCH}	*Schedule benefits*	€	1.70E+06	Costumers refunding – flat rate retrieved from reference (Galvani, 2015)
$B_{DMG,OV}$	***2. Overall damage benefits***	**€**	**2.29E+06**	**See assumptions for subcategories**
$B_{D,OM\&P}$	*Damage to own material/property*	€	6.69E+05	Limited damages to equipment and machines – calculated according to data in Table 6. 26; limited damages to piping/surrounding infrastructures – calculated according to data in Table 6. 26; damage to finished goods (e.g., diesel and heavy oil) - calculated according to data in Table 6. 26
$B_{D,OCM\&P}$	*Damage to other companies material/property*	€	2.00E+04	Very limited damages to other companies materials/properties (EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement, assuming 1.00E+04 € of damages each for 2 boundary facilities
$B_{D,SA}$	*Damage to surrounding living area*	€	1.00E+05	Damage to private properties/canals (ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010; EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement, assuming 5.00E+03 € of damages for 20 householders in the surrounding densely inhabited area
$B_{D,PM\&P}$	*Damage to public material/property*	€	1.50E+06	Damages to the water treatment system of the nearby city (Pecorella, 2011)
$B_{LGL\&INS,OV}$	***3. Overall legal & insurance benefits***	**€**	**2.05E+07**	**See assumptions for subcategories**
B_{FINES}	*Fines-related benefits*	€	7.78E+06	Civil liability fines and taxation of spilled products – calculated according to data in Table 6. 26; no criminal liability fines – based on expert judgement
B_{ILAW}	*Interim lawyers benefits*	€	1.31E+04	Senior and junior lawyers' wages – calculated according to (PayScale, 2016)
B_{SLAW}	*Specialized lawyer benefits*	€	6.28E+02	Specialized lawyers' wages – calculated according to (PayScale, 2016)
B_{IREST}	*Internal research team benefits*	€	2.91E+03	Security manager, security engineer and security analysts' wages – calculated according to (PayScale, 2016)
B_{EH}	*Expert at hearings benefits*	€	6.14E+02	Security consultant's wage – calculated according to (PayScale, 2016)
B_{LEG}	*Legislation benefits*	€	1.70E+05	Increase of security budget after the accident – calculated according to data in Table 6. 26
$B_{P\&LIC}$	*Permit and license benefits*	€	1.20E+07	Calculated according to data in Table 6. 26
B_{INS}	*Insurance premium benefits*	€	5.00E+05	Calculated according to data in Table 6. 26
$B_{H,OV}$	***4. Overall human benefits***	**€**	**0**	**No human losses and injuries** (EMARS - Major accidents reporting system, 2010)**, no recruit benefits**
$B_{ENV,OV}$	***5. Overall environmental benefits***	**€**	**3.80E+07**	**See assumptions for subcategories**
$B_{E,INTV}$	*External intervention benefits (salaries related to emergency interventions / materials / post-accident monitoring / others)*	€	1.20E+07	Overall external intervention benefits – flat rate retrieved from bulletin released by Italian environmental protection agency (ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010)
$B_{I,INTV}$	*Internal intervention benefits (manager work-time benefits/ cleaning benefits)*	€	1.55E+06	Overall internal intervention benefits – flat rate based on an interview to the company owner (Galvani, 2015)
B_{REM}	*Environmental remediation benefits (short-term / long-term)*	€	2.37E+07	Environmental remediation for hydrocarbons spill and cost of requalification project for the site – calculated according to data in Table 6. 26
$B_{OTH,ENV}$	*Other environmental benefits*	€	7.00E+05	Damages to the ecosystem close to the river (Franceschi, 2010)
$B_{REPT,OV}$	***6. Overall reputation benefits***	**€**	**1.86E+07**	**Expected long-term drop in market price - calculated according to data in Table 6. 26**
$B_{SPEC,OV}$	***7. Overall specific benefits***	**€**	**5.01E+05**	**See assumptions for subcategories**
B_{SITE_SP}	*Site-specific benefits*	€	5.00E+05	Collateral damages, due to voluntary spills in the river from nearby facilities subsequent to the major accident (Querzé, 2010) – quantification based on expert judgement, considering 1% of overall environmental benefits
B_{IMM}	*Immaterial benefits*	€	5.00E+02	Post-accident psychological meeting for employees (12 hours) – Salary of psychologist retrieved from (PayScale, 2016).
$C_{Loss,j}$	***Overall benefits***	**€**	**8.16E+07**	**-**

The results of benefit calculations are summarized in Figure 6. 20, expressing losses apportionment. The overall benefits were estimated of $8.16 \cdot 10^7$ €, justifying therefore the definition of the accident as an "ecological disaster" (Winfield, 2010b). As shown in Figure 6. 20, environmental benefits are strongly prevailing (i.e., about 47% of Overall benefits), with a particular relevance of the environmental remediation benefits subcategory. Moreover, reputational benefits and legal and insurance benefits are relevant (i.e., about 23% and 25% of Overall benefits respectively), due to the high media coverage give to the accident and to the legal procedures. The calculated benefit apportionment is typical of a major accident. Indeed, as stated in previous studies referred to the chemical industry domain (Gavious et al., 2009; Reniers and Brijs, 2014b), the value of indirect losses, which include for instance reputational losses, human and environmental losses, legal and insurance losses, is generally superior to direct losses. The gap tends to increase with the increasing severity of the accident (Gavious et al., 2009). Moreover, the comparison with a previous work, regarding the estimation of reputational losses derived from notorious accidents within the same domain (Kyaw and Paltrinieri, 2015), confirmed the gravity of reputational losses with respect to Overall benefits. In the present case study, damage benefits represent only 2% of Overall benefits derived from an environmental disaster. This low percentage value is confirmed by a previous application referred to a less severe accident scenario (Gavious et al., 2009) that estimated damage benefits around 10% of Overall benefits (i.e., $3.56 \cdot 10^5$ €).

The application of a possible global approach toward benefit calculations, including human and assets damages, has no relevance on the present case study, as human benefits value is zero, due to the absence of casualties and morbidities.

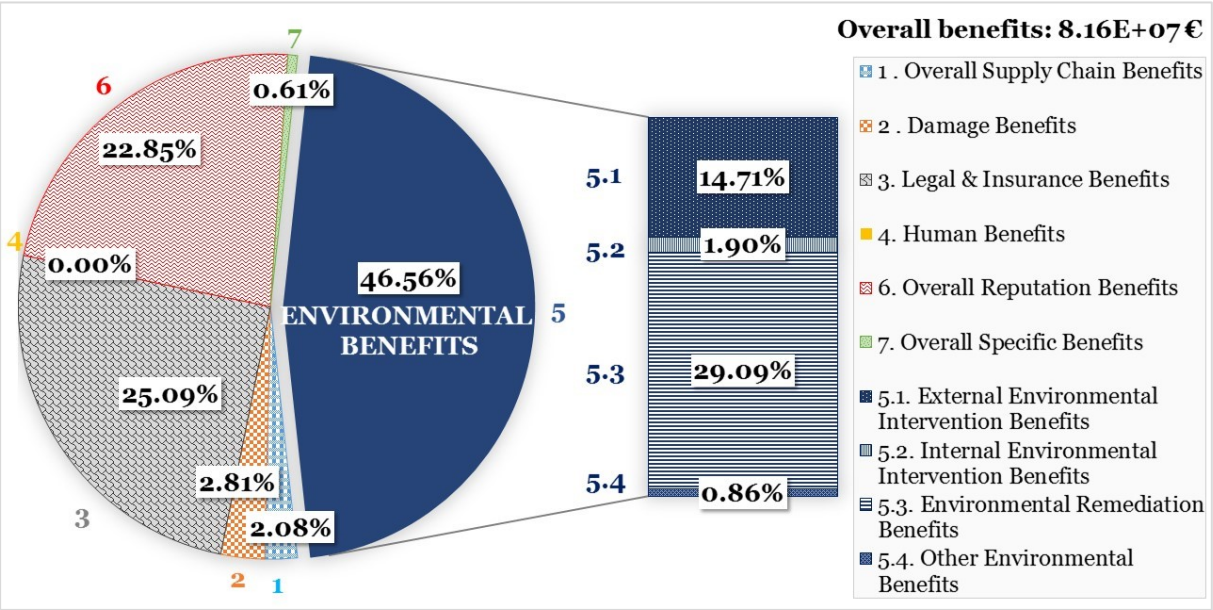


Figure 6. 20 Percentage composition of Overall benefits for the actual scenario, according to seven benefits categories.

6.5.5 Results

The results of the assessment of the case study consist in cost-benefit analysis results, cost-effectiveness analysis results and final results based on the application of an original scoring system to cost-effectiveness analysis, according to ECO-SECURE version of the model, which couples deterministic and break-even approaches toward threat probability estimation and economic analyses. Cost-benefit analysis results are the values of actualized Net benefits, according to deterministic approach and the values of break-even probabilities for six upgrades, with reference to the actual scenario. Cost-benefit analysis results have been calculated according to the equations presented in Section 4.2.7, for ECO-SECURE version of the model. Cost-effectiveness analysis results are the most profitable combinations of security upgrades for the actual scenario, within the constraint of the security budget, for both deterministic and break-even approaches. Further information on the equations to be applied within ECO-SECURE version of the model is available in Sections 4.2.7 and 4.2.8. The specific scoring system that allow the integration of results is presented in Section 4.2.8.3.

Overall costs for each security measure and Overall benefits for each scenario have been made comparable by applying appropriate discount rates (i.e., 3.5% and 1.5% respectively (HSE - Health and Safety Executive, 2016)) over a 10 year time-span, according to equation (4.19). The latter is a conventional number of operational years for a security measure. With regards to the deterministic approach, the conservative conditional threat probability assumption of $P(T)_{ij} = 1$ has been taken (Garcia, 2007), because the scenario analysis is retrospective and refers to an environmental disaster. Regarding the break-even approach, the threat probability is the output of the economic analysis. Vulnerability probabilities (i.e., $P(H|T)$ and $P(L|H)$) have been assumed unitary throughout the case study, due to the lack of information on these terms.

Cost-benefit analysis results, reported in Table 6. 28, for both the deterministic and break-even approaches, are coherent. Indeed, the security measures A, C, D, E and F may be applied according to the actual scenario. Therefore, the simple application of a conventional cost-benefit analysis does not offer precise indication on which single measure is the most useful with respect to the case study.

Cost-effectiveness analysis was thus applied to determine the most profitable combination of security upgrades within the security budget constraint, according to a deterministic approach and a break-even approach. All the possible 63 combinations of PPS upgrades have been considered. Actualized Overall costs were calculated for each combination summing the Overall costs of each option and applying a 3.5% discount rate (HSE - Health and Safety Executive, 2016). Overall costs were then compared with the actualized security budget. Actualized security budget value considered is of 51.4 k€. The results, reported in Table 6. 29,

show that the most profitable combinations of security measures are different between deterministic and break-even approaches. Nevertheless, upgrades A (i.e., addition of cameras at external perimeter wall level) and/or upgrade E (i.e., installing alarms for unauthorized manual valves opening and cages for pumps at sabotage targets) are present within all the most profitable combinations, regardless the approach.

Table 6. 28 Cost-benefit analysis results according to a deterministic and a break-even approach, in term of Net Benefits and $P(T)_{ij}^{*}$ respectively, for six different PPS upgrades with respect to the actual scenario.

PPS UPGRADE		DETERMINISTIC APPROACH		BREAK-EVEN APPROACH	
		Net Benefit	**Upgrade economic feasibility**	$P(T)_{ij}^{*}$	**Upgrade economic feasibility**
Upgrade ID	**DESCRIPTION/UNIT**	**€**	**-**	***adim.***	**-**
A	Addition of cameras at external perimeter wall level	1.89E+07	accept	1.75E-04	accept
B	Additional height to external perimeter wall (3m instead of 1.5m)	-3.14E+03	refuse	1.00E+00	refuse
C	Addition of a detection element at the sabotage targets (cameras on each tank)	1.77E+07	accept	5.53E-04	accept
D	Addition of a delay element at the sabotage targets (concrete wall + security door)	1.94E+06	accept	3.95E-04	accept
E	Putting alarms for unauthorized manual valves opening and cages for pumps at sabotage targets	2.60E+07	accept	2.35E-04	accept
F	Reduction of response force time (by creating a closer and 24h active guard dispatch)	2.90E+07	accept	2.56E-03	accept

The complete rankings of security measures combinations, obtained according to deterministic and break-even approaches to cost-effectiveness analysis, are available in Figure 6. 21. Combinations not respecting the security budget have not been reported.

Table 6. 29 Cost-effectiveness analysis results according to deterministic and break-even approaches. From the top to the bottom: first-most profitable combination, second-most profitable combination and third-most profitable combination. Combinations of security measures are indicated by the acronym *Comb. ID*.

COST-EFFECTIVENESS RANKING	*DETERMINISTIC APPROACH*				*BREAK-EVEN APPROACH*			
	Comb. ID	***Net Benefit*** (€)	***Total Cost of Combination*** (€)	KPI_1	***Comb. ID***	$P(T)_{vj}^{*}$ *(adim)*	***Total Cost of Combination*** (€)	KPI_2
FIRST	**A+C+D+E**	**6.46E+07**	2.91E+04	10	**A**	**1.75E-04**	3.31E+03	10
SECOND	**A+B+C+D+E**	**6.46E+07**	3.23E+04	9.9995	**A+E**	**2.09E-04**	9.42E+03	9.9997
THIRD	**A+C+E**	**6.27E+07**	1.89E+04	9.7003	**E**	**2.35E-04**	6.11E+03	9.9994

In order to allow a comparison of the results obtained from the two approaches, indicators KPI_1 and KPI_2, expressing deterministic and break-even cost-effectiveness analysis results, were calculated, according to the scoring system developed within ECO-SECURE version of the model, applying equation (4.29) and equation (4.30), respectively. The results for the most profitable combinations are reported in Table 6. 29.

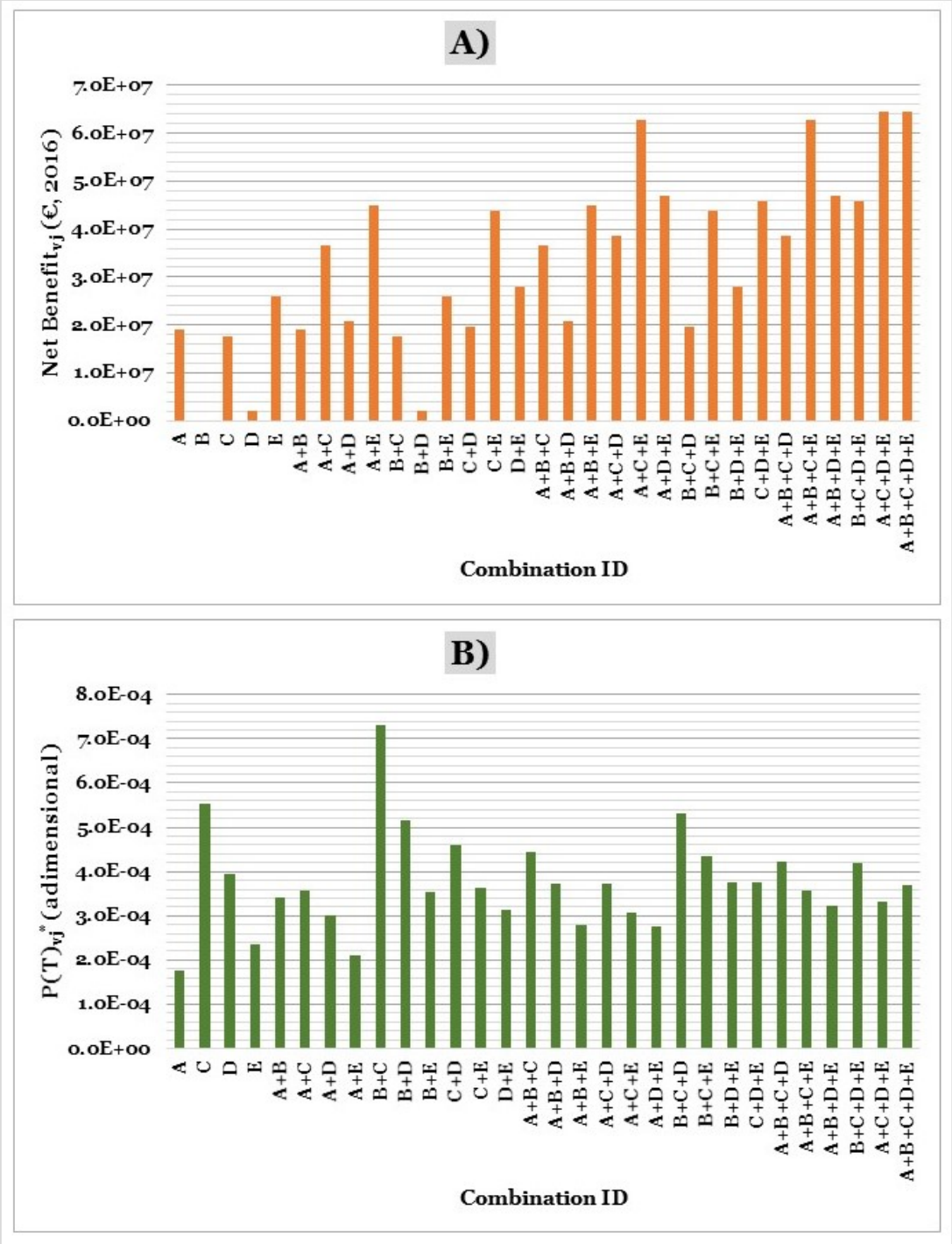


Figure 6. 21 Cost-effectiveness analysis results, showing the ranking of security measures combinations respecting budget, for the actual scenario, according to: A) deterministic approach; B) break-even approach.

Figure 6. 22 shows the values calculated for the overall cost-effectiveness indicator, ECS, obtained combining KPI_1 and KPI_2, according to equation (4.31) and setting both the threshold values in the equation, α and β, equal to 3, according to the guideline provided in Table 4. 6. All the combinations not complying with threshold values were not reported in Figure 6. 22.

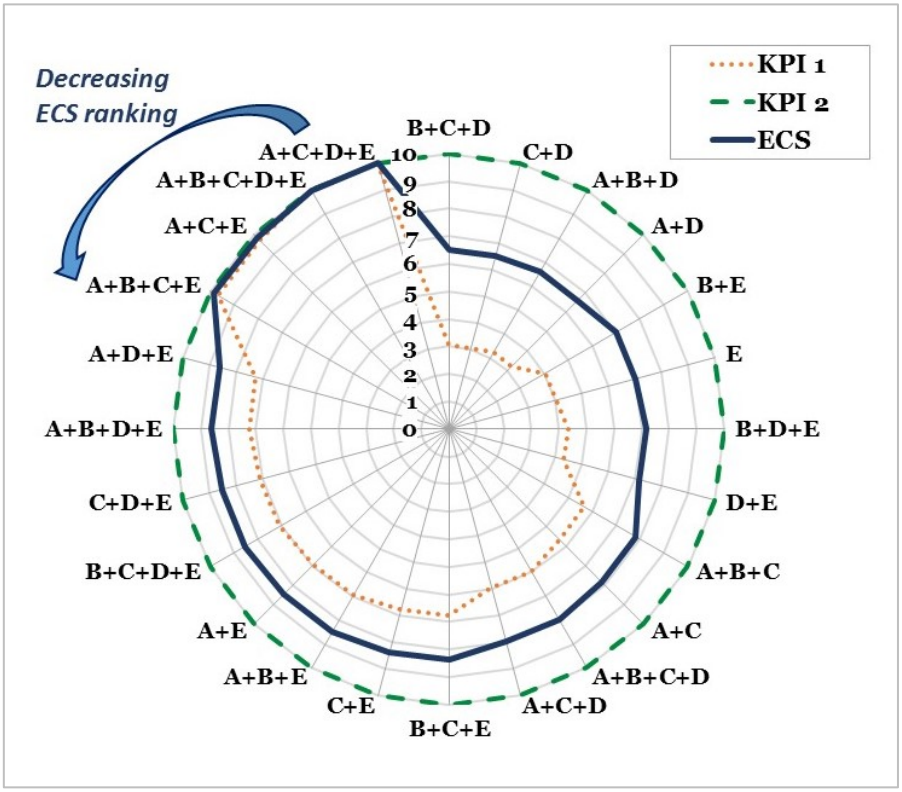


Figure 6. 22 Values calculated for the deterministic performance indicators (KPI_1), break-even performance indicator (KPI_2) and overall cost-effectiveness indicator (ECS). Only combinations with threshold values α and β higher than 3 are reported.

As shown in the figure, the combinations with the highest values of ECS always include at least three measures. All the ten top combinations offer an integration of different security functions (i.e., detection, delay and response), providing therefore a more complete security protection. It should be noted that none of the combinations reported in Figure 6. 22 include the security upgrade F, because its overall cost does not respect the security budget, even if its effectiveness improvement is the highest one.

6.5.6 Discussion

The current Section has been aimed at applying the ECO-SECURE version of the economic model to an original case study, regarding a terroristic attack an oil depot. The case study, which is illustrative but freely adapted from a possible security-related event, considered a terroristic attack on a chemical installation, aimed at causing environmental damages.

The application of ECO-SECURE version of the economic model to the present case study demonstrate that this version of the model suggests some answers to practical challenges that

a security manager may face within a chemical facility, and therefore it validates the ECO-SECURE methodology, described in Section 4.

For instance, the application demonstrates that ECO-SECURE offers a complete framework for economic analysis, aimed at the selection and allocation of security measures w.r.t. environmental accidents, within the specific chemical industry context. Model application starts from the site-specific evaluation of physical security measures performance present on a real chemical installation, which in the case study highlighted security weaknesses. ECO-SECURE effectiveness assessment provides site-specific answers to the security analyst, as it represents a complex terroristic attack, including site-specific and accident-specific adversary sequence of actions, but with fewer inputs required in comparison with EM-PICTURES version of the model (for application of the latter, see for example Section 6. 4). Therefore, the global approach to effectiveness assessment provided by ECO-SECURE is suggested to be applied whenever the information regarding adversary mode of action in case of multiple targets are scarce.

Six possible security upgrades were proposed in the case study, according to the security functions of detection, delay and response. The choice of an appropriate pool of security upgrades is particularly important, as it influences all the following results; in the current case study, the pool of security options has been enlarged in comparison with the previous application (see Section 6. 4), in purpose to obtain a broader set of economic indicators. The additional security measures have been compared in terms of overall effectiveness improvement, showing that, with reference to the realistic plant layout and the specific adversary action, four options over six show relevant and comparable effectiveness improvement indexes results, making the final results of economic analyses application not obvious from the outset. Indeed, the effectiveness analysis results are site-specific and accident-specific and cannot be generalized beyond the current case study. Moreover, although the model is able to take into account uncertainties that may decrease the overall performance of the PPS (e.g., possible lag-time in detection by security guards), it offers just a simplified description of a possible real accident.

The main advantage that emerged from ECO-SECURE application to the current case study is its completeness with respect to cost and performance of security measures, as well as to losses, and the consequent accuracy of results. The cost assessment allows a precise definition of the most relevant cost terms due to the implementation of the six possible security upgrades, including also information from vendors and site-specific data. The overall costs due to the implementation of a single security upgrade belong to the same order of magnitude (i.e., 10^4€), for five over six upgrades; however, cost distributions are different and related to the security function (i.e., detection, delay and response).

Within the case study, the original losses classification developed for environmental accidents was applied to the actual scenario, due to the retrospective analysis carried out. The classification allows focusing on environmental damages, providing a detailed description of losses sustained in the accident. The precise categories and subcategories elaborated for benefit calculations allows preventing omissions and inaccuracies; nevertheless, its inputs are validated for the case study by a panel of security experts, in purpose to avoid misleading conclusions. ECO-SECURE version of the model may be applied also in predictive analysis, as well as to different accident scenarios, in order to obtain scenario-specific economic indicators to be compared.

However, as all economic analyses, the results may reflect the subjectivity of the analyst, concerning the monetization of intangible costs and damages (e.g., assigning monetary values to casualties and morbidities) and the choice of discount rates, whose inaccuracies may lead to misleading results. For this reason, whenever ECO-SECURE is applied, it is important to present the analysis in a fully transparent manner, specifying the assumptions made and discussing the uncertainties arisen, as in the current application.

A distinctive feature of the ECO-SECURE application, in comparison with the other version of the model (i.e., EM-PICTURES), is the presence of two complementary approaches to the likelihood of the attack (i.e., threat probability), named deterministic and break-even, leading to two different economic analysis approaches. For instance, the results of the case study are a broad spectrum of outputs, including cost-benefit results, cost-effectiveness results and final results obtained from the application of a specific scoring system, which can eventually support the security decision-making process. As visible from Section 6.5.5, the application of solely cost-benefit analysis might not provide significant screening criteria, in particular with reference to very severe environmental accidents. Costs of security measures are several orders of magnitude inferior to overall losses, as in the case study, resulting therefore in the feasibility of almost all the single security measures.

Instead, with reference to the case study, cost-effectiveness analysis may offer sound indications for the stakeholders to rationally select and allocate security measures, providing a range of economically profitable options that consider also security measures combinations within the budget constraints, among 63 possible ones. The deterministic approach offers to the security manager insight on the optimal revision of the physical protection system, within the constraint of the annual security budget, after a variation regarding the likelihood of the attack. The deterministic results proposes the integration of several security measures, from triplets to groups of five.

The break-even approach, starting from a range of security options, allows defining the minimum likelihood of the attack that makes each option economically profitable, within the

constraint of the annual security budget. The combinations proposed by the break-even approach are different ones; nevertheless, additional detection measures at perimeter and additional detection and delay elements at sabotage targets level are shared between the two approaches. It should be noted that cost-effectiveness analyses results obtained from the case study may vary depending on the threshold of the security budget, which is generally defined yearly by security management.

The combined application of deterministic and break-even approaches to cost-benefit and cost-effectiveness analysis allows inserting directly the uncertainties related to the estimation of the likelihood of the attack in the application, avoiding the necessity to perform an additional sensitivity analysis on the results, which instead was required in EM-PICTURES application, as visible in Section 6.4.5.2.

Another original feature of ECO-SECURE is the use of a specific scoring system, made necessary to compare the cost-effectiveness results obtained from the two approaches and to eventually combine them into an overall cost-effectiveness indicator (i.e., ECS). Eventual company-specific criteria and additional information should be considered, in particular to define the additional acceptability thresholds for scoring system application (i.e., α and β). The results of scoring system application, available in Section 6.5.5, provide a complete ranking of security measures combinations; the combinations with the highest values for the specific case study offer an integration of different security functions (i.e., detection, delay and response), providing therefore a more complete security protection, by means of at least three additional security measures. For instance, the final output of ECO-SECURE is constituted by solely one typology of indicator (i.e., ECS), which can be easily understood also by decision-makers and stakeholders with non-technical background, increasing the possibility of ECO-SECURE to be applied in industrial practice. Therefore, the case study demonstrated that application of an original scoring system allows comparing a limited pool of final combinations, and consequently to allocate the dedicated budget on security upgrades according to a rational criteria.

In conclusion, the case study demonstrated that the outputs of ECO-SECURE might be applied in risk-informed security decision-making at company level with different purposes: to increase the awareness of management towards environmental security issues by means of non-technical and rather user-friendly outputs, to tackle security vulnerabilities in chemical facilities and to allocate the budget on profitable physical protection alternatives w.r.t. environmental accidents. Eventually, ECO-SECURE version of the model, as demonstrated by the case study, may be a systematic useful tool to cope with environmental-security based incidents in chemical facilities.

6.5.7 Conclusions on the case study

ECO-SECURE version of novel model for the selection and allocation of process-industry related security measures against environmental accidents was applied to an illustrative case study, based on a real accident, to show the model capabilities.

Model application highlighted that ECO-SECURE provides to security managers indications on the most profitable single security upgrades and combinations of them needed to prevent security-based accident scenarios, with a specific focus on environmental losses. Starting from the site-specific analysis of the baseline physical security system performance, the comparison of costs for different security upgrades with the benefits related to the actual losses was carried out. The uncertainties regarding the threat probability are included in model application by means of two complementary approaches (i.e., deterministic and break-even). Results of deterministic analysis allow upgrading the physical protection system, according to possible variations in the likelihood of the attack. Break-even analysis provides the optimal allocation of the security budget, defined yearly by security management. The application of a specific scoring system allows comparing the two set of results, obtaining overall indicators.

Thus, the case study definitely demonstrated that ECO-SECURE model version enables to define rational criteria for the selection and allocation of physical security measures and its outputs provide a sound support to managers within security risk assessment and related decision-making process. Its application may eventually contribute to the reduction of chemical plants vulnerability toward environmental and ecological terroristic attacks.

6.6 CONCLUSIONS

In this section, applications of an original economic model for the selection and allocation of preventive physical security measures against security-based accidents, with particular reference to terroristic attacks, within the chemical industry domain are presented. The two versions of the model, which are named EM-PICTURES and ECO-SECURE, are definitely validated by means of two illustrative case studies based on real accidents, presented in Section 6.4 and Section 6.5 respectively, which demonstrated model capabilities.

Model applications start from site-specific analysis of the baseline security system; then, they allow proposing security upgrades and accounting both the performance improvement and the costs of their implementation. The differences that emerged from applications of the two versions of the model mainly refer to the benefit assessment and to different approaches toward the definition of the threat probability, affecting economic analyses results. These differences make the model suitable to cope with a wide range of security-based accidents, from rather simple sabotage to complex and realistic terroristic attacks, from perspective to retrospective analysis of losses. In particular, EM-PICTURES application is a useful and

straightforward tool, generically applicable to all typologies of terroristic attacks within chemical facilities to upgrade the security system after a variation of the likelihood of the attack, but it requires to perform additional sensitivity analysis on threat probability. On the other hand, ECO-SECURE application is relatively more elaborated and focused on a specific typology of security-based accident (i.e., environmental accidents), but it couples with the deterministic analysis provided by EM-PICTURES, a break-even analysis that provides the optimal allocation of the security budget, avoiding the necessity to perform an additional sensitivity analysis on results. Moreover, ECO-SECURE application demonstrated the easiness to use of a specific scoring system for the presentation of results.

Therefore, model applications demonstrate that it enables including security hazards within risk assessment and related decision-making process. Indeed, it allows defining rational criteria for the selection and allocation of physical security measures and its outputs provide a sound support to managers and regulators involved in the security decision-making process. The case studies confirm that model application in industrial practice contributes to the reduction of chemical plants vulnerability towards intentional malevolent acts.

Extension of Quantitative Risk Assessment to the Analysis of External Hazard Factors in the Chemical and Process Industry

Section 7.
Conclusions

External hazard factors are capable to trigger cascading events, which have a catastrophic disruptive potential toward workers and population in the nearby of a chemical process facility, as well as assets and environment. The concepts and issues regarding the inclusion of external hazard factors within quantitative risk assessment, aimed at the prevention of major accidents and cascading events, have been deeply discussed in the current PhD research thesis, with a specific focus on the topics of domino effects accidents and security-based accidents.

State of the art approaches to Risk Assessment for chemical and process facilities have been analysed and classified, following novel criteria. The classification highlighted how the application of Risk Assessment have usefully supported the process industry business by enabling risk management. Despite the obvious fact that it is not an exact description of reality, QRA proved to be the best available, analytic, predictive tool to assess the risks of complex chemical process installations. However, the overview pointed out that better refinement of Risk Assessment tools is required to achieve its full potential of applicability. The main development pathway is given by the application of dynamic approaches, in particular Bayesian analysis and Bayesian Networks, which are capable to integrate emerging risk notions and potentially disregarded information. Indeed, risk assessment techniques should be constantly improved and evolve in parallel with the increasing complexity of the systems where they are applied.

State of the art regarding approaches and techniques aimed at including external hazard factors within Risk Assessment and related decision-making have been presented, considering both safety-based accidents (i.e., domino accidents) and security-based accidents (i.e., terroristick attacks and sabotage). The research field proved to be very active, due to the increasing concern toward the possible occurrence of these catastrophic events in chemical facilities, fostering the necessity to implement a unified framework for safety and security Risk Assessment, including external hazard factors.

The overview made clear that the risk evaluation step, including identification and evaluation of possible risk reducing measures (or barriers) is the most critical phase, to whom research efforts should be posed. Indeed, it emerged that the effectiveness of safety and security risk management mainly relies on an accurate technical and economic performance assessment of risk reducing measures. Then, the analysis of Risk Assessment techniques made clear the

paramount important role of safety and security measures (or barriers) within cascading events prevention, control and mitigation. For instance, safety measures are applied with respect to unintentional accidents (i.e., domino effects), while security measures refer to intentional accidents (i.e., security-based accidents).

Different typologies of risk reducing measures applied within chemical and process installations were described, together with methodologies to evaluate their performances, from economic and technical point of views. A parallelism among the three existing classes of safety and security measures (i.e., active-detection measures; passive-delay measures; procedural-response measures) has been highlighted, but methodologies needed to address performance assessment have demonstrated to be very different between safety and security measures.

About the inclusion of safety and security measures performance within Risk Assessment of external hazard factors, two main research gaps have been found.

Concerning measures technical performance, the overview made clear the superiority of dynamic techinques for safety barriers performance assessment, by means of Bayesian Networks, within major accident prevention, with respect to the conventional Event-Tree based technique, and the usefuleness to apply tailored safety performance gates, depending on barriers states and classification. On other hand, a significant research gap was pointed out: few applications of safety measures performance assessment, by means of Bayesian Networks exist, with regards to major accidents prevention in the chemical and process industry domain. Moreover, none of existing applications of domino accident analysis, by means of dynamic techniques (e.g., Bayesian Networks), included safety measures performance assessment in the modelling phase.

Concerning measures economic performance, the overview pointed out that, despite the existence of economic models for supporting decision-making processes in general, for instance cost-benefit and cost-effectiveness analyses, and ongoing research regarding economic models to support operational safety, no specific economic models are available in the domain of operational security (including counter-terrorism decision-making) to be applied within the chemical and process industry context.

Therefore, the research activities were aimed at filling these two gaps, by means of original methodologies and applications.

Concerning barriers technical performance, the research activity was devoted to the application of dynamic risk assessent techniques, to safety barriers performance assessment in the prevention of major accidents and cascading events (i.e., domino accidents), by means of Bayesian techniques and Bayesian Networks.

Preliminary applications and tutorials have been carried out to illustrate the potentialities of dynamic approaches. An original application has been focused on the implementation of Bayesian Networks to safety measures performance assessment, starting from a conventional approach, in the prevention of a major accident. Then, the Bayesian approach is extended to an original case study regarding the prevention of fire escalation. The case study proved the feasibility of Bayesian Networks application to safety barriers performance assessment with respect to accident escalation into a cascading event, as it is able to dynamically revise occurrence probabilities over time. Therefore, Bayesian Networks have been applied to cascading events prevention, for instance to domino accident analysis, in purpose to assess the effect of safety measures inclusion in the modelling phase. Two original case studies, the first regarding a simplified tank farm and the second regarding a realistic tank farm, have been carried out. Despite the increasing level of complexity of the realistic tank farm case study, the results of the two case studies were analogous: they showed a reduction of domino escalation probabilities of several orders of magnitude, due to safety barriers introduction within modelling phase.

Eventually domino accident analysis by means of Bayesian Networks, joined with safety barriers performance assessment, has proved to be an effective approach to represent severe accidental scenarios, and its application may offer a realistic risk picture of cascading events. Therefore, the case studies have demonstrated that the application of an advanced technique for safety barriers performance assessment, as Bayesian Networks, allows providing a very accurate identification of risk reducing measures within the risk evaluation phase of QRA, with reference to external hazard factors driven accidents (i.e., domino effects), offering a sound tool to support safety analysts.

Concerning measures economic performance, the research activity was devoted to the development and application of an original economic model for the prevention of security-based cascading events and for related decision-making support.

Starting from the baseline performance of the physical security system, the model allows proposing site-specific security upgrades and accounting both the performance improvement and the costs of their implementation. The model includes also the evaluation of benefits, considering avoided losses for several pertinent hypothetical scenarios. Moreover, it allows defining threat and vulnerability probabilities for a chemical installation, in relation with possible typologies of malicious acts. The application of economic techniques, by means of cost-benefit and cost-effectiveness analyses, enables the comparison among different security upgrades and the choice of economically feasible ones, as well as the determination of the combination with the maximum profit, with budgets constraints. The model is developed in

two-fold versions, which allows a realistic representation of different typologies and specificities of security-based accidents within chemical and process installations. EM-PICTURES (i.e., Economic Model for the selection of Process-Industry related Counter-Terrorism MeasURES) refers to the prevention of possible terroristic attacks in chemical facilities selection, by means of a rational selection and allocation of security measures; the approach toward economic analyses is solely deterministic and model application requires sensitivity analysis on the most variable parameters (e.g., threat and vulnerabilities probabilities). ECO-SECURE (ECOnomic model for the selection of SECurity measUREs) is specifically aimed at preventing potential environmental security-based accidents in chemical facilities by means of a rational allocation of security resources. Indeed, a specific classification for environmental losses is developed. A coupled approach toward the estimation of the threat probability and to economic analyses (i.e., deterministic and break-even) allows defining a broad set of economic indicators. Results of deterministic analysis allow upgrading the physical protection system, according to possible variations in the likelihood of the attack. Break-even analysis provides the optimal allocation of the security budget, defined yearly by security management. The application of a specific scoring system allows comparing the two set of results, obtaining overall indicators.

Model capabilities have been demonstrated by application to relevant case studies. For instance, EM-PICTURES version of the model was tested to an illustrative case study, dealing with the prevention of a possible sabotage to a storage tank farm in a process facility, whose occurrence may lead to a major accident, proving that model application provides an economic aid or criterion for selecting additional security measures in a simplified chemical installation. Then, EM-PICTURES was definitely validated by the application to a illustrative case study, based on a possible security-related event that took place in France, within a storage tank farm. ECO-SECURE version of the economic model, specifically aimed at the allocation of preventive security measures against environmental and ecological terroristic attacks within chemical installations, was validated by the application to an illustrative case study, freely adapted from a possible security-related environmental disaster that took place in Italy, which showed the capabilities and specific features of this economic model version. The complexity of the case studies and the use of realistic site-specific information for chemical installations provided a sound benchmark for the application of both versions of the original economic model within a real industrial context.

Indeed, applications to case studies confirmed that the original economic model developed in the PhD research project enables defining rational criteria for the selection and allocation of physical security measures (or barriers) and its outputs provide a sound support to managers within the security decision-making process. Therefore, the model may support the inclusion

of security hazards within quantitative risk assessment, and related delated decision-making, with particular mention to the risk evaluation phase, and its application may eventually contribute to the reduction of chemical and process plants vulnerability towards intentional malevolent acts.

The research work carried out provided a framework to approach for the inclusion of external hazard factors, being either domino or security hazards, within Risk Assessment for the chemical and process industry domain. Neverthless, the research work carried out still needs to be further refined and widened, with the aim to assist the progress toward a universal methodology for the prevention and assessment of cascading events triggered by external hazard factors, whose application may enhance safety, security and sustainability in the chemical and process industry.

Extension of Quantitative Risk Assessment to the Analysis of External Hazard Factors in the Chemical and Process Industry

Section 8.
References

Abimbola, M., Khan, F., Khakzad, N., 2014. Dynamic safety risk analysis of offshore drilling. Journal of Loss Prevention in the Process Industries 30, 74–85. doi:10.1016/j.jlp.2014.05.002

Ackerman, F., Heinzerling, L., 2002. Pricing the Priceless: Cost-Benefit Analysis of Environmental Protection. University of Pennsylvania Law Review 150, 1553. doi:10.2307/3312947

Al-Shanini, A., Ahmad, A., Khan, F., 2014. Accident Modelling and Analysis in Process Industries. Journal of Loss Prevention in the Process Industries 32, 319–334. doi:10.1016/j.jlp.2014.09.016

Ale, B., Van Gulijk, C., Hanea, A., Hanea, D., Hudson, P., Lin, P.-H., Sillem, S., 2014. Towards BBN based risk modelling of process plants. Safety Science 69, 48–56. doi:10.1016/j.ssci.2013.12.007

Ale, B.J.M., Hartford, D.N.D., Slater, D., 2015. ALARP and CBA all in the same game. Safety Science 76, 90–100. doi:10.1016/j.ssci.2015.02.012

Alibi, 2016. 3.0 Megapixel 100' IR IP Outdoor Bullet Security Camera - Technical and commercial datasheet [WWW Document]. Super Circuits Website. URL http://www.supercircuits.com/alibi-megapixel-day-night-ir-ip-outdoor-security-camera-ali-ipu3130r (accessed 3.20.17).

Alpas, H., Berkowicz, S.M., Ermakova, I., 2011. Environmental Security and Ecoterrorism, NATO Science for Peace and Security Series C: Environmental Security. Springer Netherlands, Dordrecht, The Netherlands. doi:10.1007/978-94-007-1235-5

Antonioni, G., Spadoni, G., Cozzani, V., 2009. Application of domino effect quantitative risk assessment to an extended industrial area. Journal of Loss Prevention in the Process Industries 22, 614–624. doi:10.1016/j.jlp.2009.02.012

Apeland, S., Aven, T., 2000. Risk based maintenance optimization: foundational issues. Reliability Engineering & System Safety 67, 285–292. doi:10.1016/S0951-8320(99)00068-X

Apostolakis, G.E., 2004. How useful is quantitative risk assessment? Risk Analysis 24, 515–20. doi:10.1111/j.0272-4332.2004.00455.x

Argenti, F., Landucci, G., Spadoni, G., Cozzani, V., 2015. The assessment of the attractiveness

of process facilities to terrorist attacks. Safety Science 77, 169–181. doi:10.1016/j.ssci.2015.02.013

ARIA, 2015. Accident study findings on malicious acts perpetrated in industrial facilities [WWW Document]. The ARIA database. URL http://www.aria.developpement-durable.gouv.fr/wp-content/uploads/2015/10/2015-10_01_SY_accidentologie_Malveillance_PA_FINAL_EN.pdf (accessed 3.20.17).

ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010. Ecoscienza. Emergenze ambientali, dal petrolio i rischi e i danni più gravi (in Italian). Bullettin of Environmental Protection Agency - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna 100.

Arunraj, N.S., Maiti, J., 2009. A methodology for overall consequence modeling in chemical industry. Journal of Hazardous Materials 169, 556–74. doi:10.1016/j.jhazmat.2009.03.133

Arunraj, N.S., Maiti, J., 2007. Risk-based maintenance - techniques and applications. Journal of hazardous materials 142, 653–61. doi:10.1016/j.jhazmat.2006.06.069

Associated Press, 2015. French minister says double plant blast was criminal act [WWW Document]. AP - Associated Press Website. URL http://bigstory.ap.org/article/1f9382f079764ac0a68b72d94bab4968/french-minister-says-double-plant-blast-was-criminal-act (accessed 3.20.16).

Associated Press in Rome, 2010. Environmental disaster warning as oil spill reaches the Po, Italy's biggest riverest river [WWW Document]. The Guardian. URL http://www.theguardian.com/world/2010/feb/24/oil-spill-po-italy-river (accessed 3.20.16).

Aven, T., 2012. The risk concept - historical and recent development trends. Reliability Engineering & System Safety 99, 33–44. doi:10.1016/j.ress.2011.11.006

Aven, T., 2007. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering & System Safety 92, 745–754. doi:10.1016/j.ress.2006.03.008

Aven, T., Renn, O., 2010. Response to Professor Eugene Rosa's viewpoint to our paper. Journal of Risk Research 13, 255–259. doi:10.1080/13669870903484369

Aven, T., Renn, O., 2009. On risk defined as an event where the outcome is uncertain. Journal of Risk Research 12, 1–11. doi:10.1080/13669870802488883

Aven, T., Vinnem, J.E., 2005. On the use of risk acceptance criteria in the offshore oil and gas industry. Reliability Engineering & System Safety 90, 15–24. doi:10.1016/j.ress.2004.10.009

Aven, T., Zio, E., 2011. Some considerations on the treatment of uncertainties in risk

assessment for practical decision making. Reliability Engineering & System Safety 96, 64–74. doi:10.1016/j.ress.2010.06.001

Bagster, D.F., Pitblado, R.M., 1991. Estimation of domino incident frequencies - an approach. Process Safety and Environmental Protection 69.

Bajpai, S., Gupta, J.P., 2007. Terror-Proofing Chemical Process Industries. Process Safety and Environmental Protection 85, 559–565. doi:10.1205/psep06046

Ball, D., Floyd, P., 1998. Societal Risk. London, UK.

BBC News, 2015a. France attack: as it happened [WWW Document]. BBC News Website. URL http://www.bbc.com/news/live/world-europe-33287095 (accessed 3.20.17).

BBC News, 2015b. France explosions: Devices found near Berre l'Étang plant [WWW Document]. BBC News Website. URL http://www.bbc.com/news/world-europe-33537345 (accessed 3.20.17).

Bearfield, G., Marsh, W., Rail, A., Tower, E., Road, E., 2005. Generalising Event Trees Using Bayesian Networks with a Case Study of Train Derailment George. Lecture Notes in Computer Science 3688, 52–66.

Beerens, H.I., Post, J.G., Uijt de Haag, P.A.M., 2006. The use of generic failure frequencies in QRA: the quality and use of failure frequencies and how to bring them up-to-date. Journal of Hazardous Materials 130, 265–70. doi:10.1016/j.jhazmat.2005.07.013

Berni, F., 2016. Lombarda Petroli: le motivazioni della sentenza che ha ribaltato il processo (in Italian) [WWW Document]. Il Cittadino MB - Il Quotidiano Online di Monza e Brianza. URL http://www.ilcittadinomb.it/stories/Cronaca/lombarda-petroli-le-motivazioni-della-sentenza-che-ha-ribaltato-il-processo_1180628_11/ (accessed 3.20.17).

Berni, F., Rosa, R., 2015. Lambro, il disastro Lombarda Petroli. Dopo 5 anni la bonifica è cancellata (in Italian) [WWW Document]. Corriere della Sera. URL http://milano.corriere.it/notizie/cronaca/15_febbraio_23/lambro-disastro-lombarda-petroli-5-anni-bonifica-cancellata-23d229c4-bb52-11e4-aa19-1dc436785f83.shtml (accessed 3.20.17).

BMT, 2016. Average cost of construction in Australia - Technical and commercial datasheet [WWW Document]. BMT Website. URL http://www.bmtqs.com.au/construction-cost-table (accessed 3.20.17).

Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E., 2001. Improving the analysis of dependable systems by mapping Fault Trees into Bayesian Networks. Reliability Engineering and System Safety 71, 249–260. doi:10.1016/S0951-8320(00)00077-6

Bohnenblust, H., Slovic, P., 1998. Integrating technical analysis and public values in risk-based decision making. Reliability Engineering & System Safety 59, 151–159. doi:10.1016/S0951-8320(97)00136-1

Boudali, H., Dugan, J.B., 2005. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering & System Safety 87, 337–349. doi:10.1016/j.ress.2004.06.004

Broder, J.F., Tucker, E., 2012. Risk analysis and the Security Survey, Fourth. ed. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C., Wood, T., 2008. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. Reliability Engineering & System Safety 93, 1616–1627. doi:10.1016/j.ress.2008.01.008

Buncefield Major Investigation Board, 2008. The Buncefield Incident 11 December 2005. Bootle, United Kingdom.

Cabinet Office, 2002. Risk: Improving government's capability to handle risk and uncertainty. Strategy Unit Report, Cabinet Office, London.

Campbell, H.F., Brown, R.P.C., 2003. Benefit-Cost Analysis: Financial and Economic Appraisal using Spreadsheets. Cambridge University Press, Cambridge, UK.

Campbell, S., 2005. Determining overall risk. Journal of Risk Research 8, 569–581. doi:10.1080/13669870500118329

CCPS - Center for Chemical Process Safety, 2008a. Guidelines for Hazard Evaluation Procedures. American Institute of Chemical Engineers (AIChE), New York, USA.

CCPS - Center for Chemical Process Safety, 2008b. Guidelines for Chemical Transportation Safety, Security, and Risk Management. American Institute of Chemical Engineers (AIChE), New York, USA.

CCPS - Center for Chemical Process Safety, 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers (AIChE), New York, USA.

CCPS - Center for Chemical Process Safety, 2000. Guidelines for Chemical Process Quantitative Risk Analysis. American Institute of Chemical Engineers (AIChE), New York, USA.

CCPS - Center for Chemical Process Safety, 1995. Guidelines for Consequence Analysis of Chemical Releases. American Institute of Chemical Engineers (AIChE), New York, USA.

Čepin, M., Mavko, B., 2002. A dynamic fault tree. Reliability Engineering & System Safety 75, 83–91. doi:10.1016/S0951-8320(01)00121-1

Charvet, C., Chambon, J.-L., Corenwinder, F., Taveau, J., 2011. Learning from the application of nuclear probabilistic safety assessment to the chemical industry. Journal of Loss Prevention in the Process Industries 24, 242–248. doi:10.1016/j.jlp.2010.09.007

Council Directive, 2008. Council Directive, 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union.

Council of the European Union, 2012. Council conclusions on the new CBRNE Agenda. Brussels, Belgium.

COVO Commission, 1981. Risk analysis of six potentially hazardous object in the Rijnmond area, a pilot study. Report to the Rijnmond Public Authority, Central Environmental Control Agency, Schiedam, the Netherlands.

Cox, L.A., 2009. Improving risk-based decision making for terrorism applications. Risk Analysis 29, 336–341. doi:10.1111/j.1539-6924.2009.01206.x

Cozzani, V., 2010. Towards the inclusion of external factors in quantitative risk assessment: the analysis of NaTech accident scenarios. Chemical Engineering Transactions 19, 1–6. doi:10.3303/CET1019001

Cozzani, V., Antonioni, G., Landucci, G., Tugnoli, A., Bonvicini, S., Spadoni, G., 2014. Quantitative assessment of domino and NaTech scenarios in complex industrial areas. Journal of Loss Prevention in the Process Industries 28, 10–22. doi:10.1016/j.jlp.2013.07.009

Cozzani, V., Antonioni, G., Spadoni, G., 2006. Quantitative assessment of domino scenarios by a GIS-based software tool. Journal of Loss Prevention in the Process Industries 19, 463–477. doi:10.1016/j.jlp.2005.11.007

Cozzani, V., Campedel, M., Renni, E., Krausmann, E., 2010. Industrial accidents triggered by flood events: analysis of past accidents. Journal of Hazardous Materials 175, 501–9. doi:10.1016/j.jhazmat.2009.10.033

Cozzani, V., Gubinelli, G., Antonioni, G., Spadoni, G., Zanelli, S., 2005. The assessment of risk caused by domino effect in quantitative area risk analysis. Journal of Hazardous Materials 127, 14–30. doi:10.1016/j.jhazmat.2005.07.003

Cozzani, V., Salzano, E., 2004a. The quantitative assessment of domino effects caused by overpressure. Part I. Probit models. Journal of Hazardous Materials 107, 67–80. doi:10.1016/j.jhazmat.2003.09.013

Cozzani, V., Salzano, E., 2004b. The quantitative assessment of domino effect caused by overpressure. Part II. Case studies. Journal of Hazardous Materials 107, 81–94. doi:10.1016/j.jhazmat.2003.09.014

Cozzani, V., Salzano, E., 2004c. Threshold values for domino effects caused by blast wave interaction with process equipment. Journal of Loss Prevention in the Process Industries 17, 437–447. doi:10.1016/j.jlp.2004.08.003

Cozzani, V., Tugnoli, A., Salzano, E., 2009. The development of an inherent safety approach to

the prevention of domino accidents. Accident analysis and prevention 41, 1216–1227. doi:10.1016/j.aap.2008.06.002

Cozzani, V., Tugnoli, A., Salzano, E., 2007. Prevention of domino effect: from active and passive strategies to inherently safer design. Journal of Hazardous Materials 139, 209–19. doi:10.1016/j.jhazmat.2006.06.041

Creedy, G.D., 2011. Quantitative risk assessment: How realistic are those frequency assumptions? Journal of Loss Prevention in the Process Industries 24, 203–207. doi:10.1016/j.jlp.2010.08.013

Cropper, M., Sahin, S., 2009. Valuing mortality and morbidity in the context of disaster risks. World Bank Policy Research Working Paper. doi:10.2139/ssrn.1344717

Crowl, D.A., Louvar, J.F., 2011. Chemical Process Safety: Fundamentals with Applications, Third. ed. Prentice Hall, Boston, MA, USA.

CSB, 2007a. Investigation Report Refinery Explosion and Fire BP Texas City. Washington, DC, USA. doi:REPORT No. 2005-04-I-TX

CSB, 2007b. Mixing and heating a flammable liquid in a open top tank. Washington, DC, USA.

Darbra, R.M., Palacios, A., Casal, J., 2010. Domino effect in chemical accidents: Main features and accident sequences. Journal of Hazardous Materials 183, 565–573. doi:10.1016/j.jhazmat.2010.07.061

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, 220–233. doi:10.1016/j.jhazmat.2005.07.010

Delvosalle, C., 1998. A methodology for the identification and evaluation of domino effects, Belgian Ministry of Employement and Labour. Brussels, Belgium.

Delvosalle, C., Fiévez, C., Pipart, A., 2006. ARAMIS Project: Reference Accident Scenarios Definition in SEVESO Establishment. Journal of Risk Research 9, 583–600. doi:10.1080/13669870500419529

Delvosalle, C., Fiévez, C., Pipart, A., Fabrega, J.C., Planas, E., Christou, M., Mushtaq, F., 2005. Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering & System Safety 90, 238–246. doi:10.1016/j.ress.2004.11.003

Demichela, M., Piccinini, N., 2004. Risk-Based Design of a Regenerative Thermal Oxidizer. Industrial & Engineering Chemistry Research 43, 5838–5845. doi:10.1021/ie0342208

DHS - US Department of Homeland Security, 2007. Chemical Facility Anti-Terrorism Standards (CFATS) - Risk-Based Performance Standards (RBPS). Washington, DC, USA.

Dillon, R.L., Liebe, R.M., Bestafka, T., 2009. Risk-Based Decision Making for Terrorism

Applications. Risk Analysis 29, 321–335. doi:10.1111/j.1539-6924.2008.01196.x

Egidi, D., Foraboschi, F.P., Spadoni, G., Amendola, A., 1995. The ARIPAR project: analysis of the major accident risks connected with industrial and transportation activities in the Ravenna area. Reliability Engineering & System Safety 49, 75–89. doi:10.1016/0951-8320(95)00026-X

EMARS - Major accidents reporting system, 2010. Release of liquid hydrocarbons from an oil depot in Villasanta (Monza province –Lombardia Region-Northern Italy) with environmental consequences in the rivers Po and Lambro [WWW Document]. URL https://emars.jrc.ec.europa.eu/fileadmin/eMARS_Site/PhpPages/ViewAccident/ViewAccidentPublic.php?accident_code=756 (accessed 3.20.17).

EMS, 2001. LUL QRA - London Underground Limited Quantified Risk Assessment. London, UK.

Engineering ToolBox, 2017. Liquid densities [WWW Document]. The Engineering ToolBox Website. URL http://www.engineeringtoolbox.com/liquids-densities-d_743.html (accessed 3.20.17).

Etkin, D.S., 1999. Estimating Cleanup Costs for Oil Spills, in: International Oil Spill Conference Proceedings. Arlington, MA, USA, pp. 35–39. doi:10.7901/2169-3358-1999-1-35

EU, 2012. SEVESO III. Directive 2012/18/EU Of The European Parliament And Of The Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.

European Commission, 2008. Sixth Framework Programme on Transnational Terrorism, Security and the Rule of Law, Deliverable 5, Workpackage 3, Concepts of Terrorism: Analysis of the Rise, Decline, Trends and Risk. Transnational Terrorism, Security & the Rule of Law.

European Commission - Environment Directorate, 2015. The Seveso Directive - Prevention, preparedness and response [WWW Document]. European Commission website. URL http://ec.europa.eu/environment/seveso/ (accessed 3.20.17).

Eurostat, 2016. Electric prices for industrial consumers, second half 2014 [WWW Document]. Eurostat - statistics explained Website. URL http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Electricity_prices_for_industrial_consumers,_second_half_2014_(¹)_(EUR_per_kWh)_YB15.png#file (accessed 3.20.17).

Fadier, E., De la Garza, C., 2006. Safety design: Towards a new philosophy. Safety Science 44, 55–73. doi:10.1016/j.ssci.2005.09.008

Falck, A., Flage, R., Aven, T., 2015. Risk assessment of oil and gas facilities during operational phase, in: Safety and Reliability of Complex Engineered Systems. Proceedings of the European Safety and Reliability Conference, ESREL 2015. Zurich, Switzerland, pp. 373–

380.

Falck, A., Skramstad, E., Berg, M., 2000. Use of QRA for decision support in the design of an offshore oil production installation. Journal of Hazardous Materials 71, 179–92. doi:10.1016/S0304-3894(99)00078-3

Ferdous, R., Khan, F., Sadiq, R., 2013. Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. Process Safety and Environmental Protection 91, 1–18. doi:10.1016/j.psep.2011.08.010

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., Veitch, B., 2012. Handling and updating uncertain information in bow-tie analysis. Journal of Loss Prevention in the Process Industries 25, 8–19. doi:10.1016/j.jlp.2011.06.018

Fountain, H., 2016. 30 Years After Chernobyl Disaster, Shelter Nears Completion [WWW Document]. The New York Times. URL https://www.nytimes.com/2016/04/27/science/30-years-after-chernobyl-disaster-shelter-nears-completion.html?_r=0 (accessed 3.20.17).

Franceschi, A., 2010. Che fine ha fatto l'emergenza petrolio nel fiume Lambro? (in Italian) [WWW Document]. Il Sole 24 Ore Website. URL http://www.ilsole24ore.com/art/SoleOnLine4/Italia/2010/05/intervista-responsabile-acque-wwf-fiume-lambro.shtml?uuid=79c5be10-579b-11df-b335-c4e158cb6808&DocRulesView=Libero&refresh_ce=1 (accessed 3.20.17).

Frewer, L.J., Howard, C., Hedderley, D., Shepherd, R., 1996. What determines trust in information about food-related risks? Underlying psychological constructs. Risk Analysis 16, 473–485. doi:10.1111/j.1539-6924.1996.tb01094.x

Friedman, S.M., 2017. The inflation calculator [WWW Document]. Westegg Website. URL http://www.westegg.com/inflation/ (accessed 3.20.17).

Galvani, M., 2015. Monza - Processo Lombarda Petroli. La verità di Tagliabue: volevano sabotare la cessione dell'area (in Italian) [WWW Document]. Il Giorno. URL http://www.infonodo.org/node/40075 (accessed 3.20.17).

Garcia, M.L., 2007. The Design and Evaluation of Physical Protection Systems, Second. ed. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Garcia, M.L., 2005. Vulnerability Assessment of Physical Protection Systems. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Gavious, A., Mizrahi, S., Shani, Y., Minchuk, Y., 2009. The costs of industrial accidents for the organization: Developing methods and tools for evaluation and cost-benefit analysis of investment in safety. Journal of Loss Prevention in the Process Industries 22, 434–438. doi:10.1016/j.jlp.2009.02.008

Get A Quote, 2016. Concrete wall and footing price estimation [WWW Document]. Get A Quote

Website. URL http://www.get-a-quote.net/quickcalc/concrete.htm (accessed 3.20.17).

Goossens, G.J.H., 2012. The Big Oil Spill: The Market Value Consequences of the Deepwater Horizon Disaster. Tilburg School of Economics and Management, Tilburg, Belgium.

Gorrens, B., De Clerck, W., De Jongh, K., Aerts, M., 2009. Domino effecten van en naar Seveso-inrichtingen, Rep. 07.0007.

Gowland, R., 2006. The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: a step forward towards convergent practices in risk assessment? Journal of Hazardous Materials 130, 307–10. doi:10.1016/j.jhazmat.2005.07.007

Grainger, 2016. Security doors and frames - Technical and commercial datasheet [WWW Document]. Grainger Website. URL http://www.grainger.com/category/security-doors/door-and-door-frames/security/ecatalog/N-b6c (accessed 3.20.17).

Greenberg, M., Haas, C., Cox, A., Lowrie, K., McComas, K., North, W., 2012. Ten most important accomplishments in risk analysis, 1980-2010. Risk Analysis 32, 771–781. doi:10.1111/j.1539-6924.2012.01817.x

Haimes, Y.Y., 2004. Risk Modelling, Assessment, and Management. Wiley, Hoboken, NJ, USA.

Hale, A.R., Heming, B.H.J., Smit, K., Rodenburg, F.G.T., van Leeuwen, N.D., 1998. Evaluating safety in the management of maintenance activities in the chemical process industry. Safety Science 28, 21–44. doi:10.1016/S0925-7535(97)00061-1

Hale, A.R., Kirwan, B., Kjellén, U., 2007. Safe by design: where are we now? Safety Science 45, 305–327. doi:10.1016/j.ssci.2006.08.007

Hansson, S.O., 2007. Philosophical Problems in Cost–Benefit Analysis. Economics and Philosophy 23, 163. doi:10.1017/S0266267107001356

Hashemi, S.J., Ahmed, S., Khan, F., 2014. Risk-based operational performance analysis using loss functions. Chemical Engineering Science 116, 99–108. doi:10.1016/j.ces.2014.04.042

Hauge, S., Kråknes, T., Håbrekke, S., Jin, H., 2013. Reliability prediction method for safety instrumented systems - PDS Method Handbook 2013 Edition. SINTEF Technology and Society, Trondheim, Norway.

Hauge, S., Okstad, E., Paltrinieri, N., Edwin, N., Vatn, J., Bodsberg, L., 2015. Handbook for monitoring of barrier status and associated risk in the operational phase, the risk barometer approach. SINTEF F27045. Trondheim, Norway.

Haugom, G.P., Friis-Hansen, P., 2011. Risk modelling of a hydrogen refuelling station using Bayesian network. International Journal of Hydrogen Energy 36, 2389–2397. doi:10.1016/j.ijhydene.2010.04.131

Hendershot, D., 2006. Implementing inherently safer design in an existing plant. Process

Safety Progress 25, 52–57. doi:10.1002/prs

Hester, P.T., Adams, K.M., Mahadevan, S., 2010. Examining metrics and methods for determining critical facility system effectiveness. International Journal of Critical Infrastructures 6, 211. doi:10.1504/IJCIS.2010.033337

Hirst, I.L., Carter, D.A., 2002. A ' worst case ' methodology for obtaining a rough but rapid indication of the societal risk from a major accident hazard installation. Journal of Hazardous Materials 92, 223–237. doi:10.1016/S0304-3894(02)00016-X

HSE - Health and Safety Commission, 1984. Control of major hazards: third report. Her Majesty's Stationery Office, London, UK.

HSE - Health and Safety Executive, 2016. Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions [WWW Document]. URL http://orr.gov.uk/__data/assets/pdf_file/0018/18009/revised-safety-cba-guidance-05022016.pdf (accessed 3.20.17).

HSE - Health and Safety Executive, 2012. The major accident failure rates project for the Health and Safety Executive 2012. RR915. The major accident failure rates project. Concept phase.

HSE - Health and Safety Executive, 2011. Buncefield: Why did it happen? [WWW Document]. URL www.hse.gov.uk/comah/buncefield/buncefield-report.pdf (accessed 3.20.17).

HSE - Health and Safety Executive, 2009. Failure Rate and Event Data for use within Land Use Planning Risk Assessments.

HSE - Health and Safety Executive, 1992. The Tolerability of Risk from Nuclear Power Stations.

Hugin, 2016. Hugin Expert software, Researcher Version 8.1.

IAEA, 1999. Living probabilistic safety assessment (LPSA). Wien, Austria.

IRGC - International Risk Governance Council, 2009. Risk Governance Deficits. An analysis and illustration of the most common deficits in risk governance. Geneva, Switzerland.

ISO, 2009. Risk Management - Vocabulary Guide. Geneva, Switzerland.

ISO, 2002. BS EN ISO 17776:2002. Petroleum and natural gas industries - Offshore production installations - Guidelines on tools and techniques for hazard identification and risk assessment. CEN, Brussels, Belgium.

ISO31000:2009, 2009. Risk management - Principles and Guidelines. Geneva, Switzerland.

Janssens, J., Talarico, L., Reniers, G.L.L., Sörensen, K., 2015. A decision model to allocate protective safety barriers and mitigate domino effects. Reliability Engineering & System Safety 143, 44–52. doi:10.1016/j.ress.2015.05.022

Jensen, F. V., Nielsen, T.D., 2007. Bayesian Networks and Decision Graphs, Second. ed. Springer, New York, USA.

Johansen, I.L., Rausand, M., 2014. Foundations and choice of risk metrics. Safety Science 62, 386–399. doi:10.1016/j.ssci.2013.09.011

Johansen, I.L., Rausand, M., 2012. Risk Metrics: Interpretation and Choice, in: IEEE International Conference on Industrial Engineering and Engineering Management. pp. 1914–1918. doi:10.1109/IEEM.2012.6838079

Jonkman, S.N., van Gelder, P.H.A.J.M., Vrijling, J.K., 2003. An overview of quantitative risk measures for loss of life and economic damage. Journal of Hazardous Materials 99, 1–30. doi:10.1016/S0304-3894(02)00283-2

Jorissen, R.E., Stallen, P.J.M., 1998. Quantified societal risk and Policy Making. Technology, Risk and Society 12.

Kalantarnia, M., Khan, F., Hawboldt, K., 2010. Modelling of BP Texas City refinery accident using dynamic risk assessment approach. Process Safety and Environmental Protection 88, 191–199. doi:10.1016/j.psep.2010.01.004

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. doi:10.1016/j.jlp.2009.04.006

Kaplan, S., 1997. The words of risk analysis. Risk Analysis 17, 407–417. doi:10.1111/j.1539-6924.1997.tb00881.x

Kaplan, S., Garrick, B.J., 1981. On The Quantitative Definition of Risk. Risk Analysis 1, 11–27. doi:10.1111/j.1539-6924.1981.tb01350.x

Kelman, S., 1981. Cost-benefit analysis: an ethical critique. Across the board 18, 74–82.

Khakzad, N., 2015. Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. Reliability Engineering & System Safety 138, 263–272. doi:10.1016/j.ress.2015.02.007

Khakzad, N., Khan, F., Amyotte, P., 2013a. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety science 57, 108–117. doi:10.1016/j.ssci.2013.01.022

Khakzad, N., Khan, F., Amyotte, P., 2013b. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection 91, 46–53. doi:10.1016/j.psep.2012.01.005

Khakzad, N., Khan, F., Amyotte, P., 2013c. Risk-based design of process systems using discrete-time Bayesian networks. Reliability Engineering & System Safety 109, 5–17. doi:10.1016/j.ress.2012.07.009

Khakzad, N., Khan, F., Amyotte, P., 2012. Dynamic risk analysis using bow-tie approach. Reliability Engineering & System Safety 104, 36–44. doi:10.1016/j.ress.2012.04.003

Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliability Engineering & System Safety 96, 925–932. doi:10.1016/j.ress.2011.03.012

Khakzad, N., Khan, F., Amyotte, P., Cozzani, V., 2013d. Domino effect analysis using Bayesian networks. Risk Analysis 33, 292–306. doi:10.1111/j.1539-6924.2012.01854.x

Khakzad, N., Khan, F., Amyotte, P., Cozzani, V., 2013e. Risk management of domino effects considering dynamic consequence analysis, Risk Analysis. doi:10.1111/risa.12158

Khakzad, N., Khan, F., Paltrinieri, N., 2014. On the application of near accident data to risk analysis of major accidents. Reliability Engineering & System Safety 126, 116–125. doi:10.1016/j.ress.2014.01.015

Khakzad, N., Reniers, G.L.L., 2015. Cost-effective allocation of safety measures in chemical plants w.r.t land-use planning. Safety Science 1–8. doi:10.1016/j.ssci.2015.10.010

Khan, F., Abbasi, S.A., 2002. A criterion for developing credible accident scenarios for risk assessment. Journal of Loss Prevention in the Process Industries 15, 467–475. doi:10.1016/S0950-4230(02)00050-5

Khan, F., Abbasi, S.A., 1998a. Techniques and methodologies for risk analysis in chemical process industries. Journal of Loss Prevention in the Process Industries 11, 261–277. doi:10.1016/S0950-4230(97)00051-X

Khan, F., Abbasi, S.A., 1998b. DOMIFFECT (DOMIno eFFECT): user-friendly software for domino effect analysis. Environmental Modelling and Software 13, 163–177. doi:10.1016/S1364-8152(98)00018-8

Khan, F., Abunada, H., 2010. Development of risk-based process safety indicators. Process Safety Progress 29, 133–143. doi:10.1002/prs

Khan, F., Haddara, M.R., 2004. Risk-based maintenance (RBM): A new approach for process plant inspection and maintenance. Process Safety Progress 23, 252–265. doi:10.1002/prs.10010

Khan, F., Husain, T., Abbasi, S.A., 2002a. Design and evaluation of safety measures using a newly proposed methodology 'SCAP'. Journal of Loss Prevention in the Process Industries 15, 129–146. doi:10.1016/S0950-4230(01)00026-2

Khan, F., Iqbal, A., Ramesh, N., Abbasi, S.A., 2001. SCAP: a new methodology for safety management based on feedback from credible accident-probabilistic fault tree analysis system. Journal of Hazardous Materials 87, 23–56. doi:10.1016/S0304-3894(01)00276-X

Khan, F., Sadiq, R., Husain, T., 2002b. Risk-based process safety assessment and control measures design for offshore process facilities. Journal of hazardous materials 94, 1–36. doi:S0304389402000043

Khan, F.I., Abbasi, S.A., 1999. The world's worst industrial accident of the 1990s: What happened and what might have been - A quantitative study. Process Safety Progress 18.

Kirchsteiger, C., 2002. Preface. International workshop on promotion of technical harmonisation on risk-based decision-making. Safety Science 40, 1–15.

Knight, F.H., 1921. Risk, Uncertainty, and Profit. Houghton Mifflin Co., Boston, MA, USA.

Kyaw, K., Paltrinieri, N., 2015. The cost of reputational damage when a major accident occurs, in: Safety and Reliability of Complex Engineered Systems. Proceedings of the European Safety and Reliability Conference, ESREL 2015. Zurich, Switzerland, pp. 4537–4544.

La Repubblica, 2016. Milano, petrolio nel Lambro: condannato in appello il titolare della ditta che scaricò i silos (in Italian) [WWW Document]. La Repubblica Milano Website. URL http://milano.repubblica.it/cronaca/2016/04/04/news/milano_petrolio_nel_lambro-136917367/ (accessed 3.20.17).

Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015a. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliability Engineering & System Safety 143, 30–43. doi:10.1016/j.ress.2015.03.023

Landucci, G., Reniers, G.L.L., Cozzani, V., Salzano, E., 2015b. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliability Engineering & System Safety 143, 53–62. doi:10.1016/j.ress.2015.03.004

Le Guernigou, Y., Revilla, F., 2015. Criminal intent seen in petrochemical fire on French Bastille Day [WWW Document]. Reuters Website - UK Edition. URL http://uk.reuters.com/article/2015/07/14/uk-france-fire-intent-idUKKCN0PO0S420150714 (accessed 3.20.17).

Le Huffington Post, 2015. Bouches-du-Rhône: incendie sur le site pétrochimique LyondellBasell à Berre-l'Étang [WWW Document]. Huffington Post Website - French Edition. URL http://www.huffingtonpost.fr/2015/07/14/incendie-bouches-du-rhone-berre-letang-petrochimie-plan-orsec_n_7790400.htm (accessed 3.20.17).

Le Sage, T., 2013. Scenario based risk assessment [WWW Document]. JDiBrief Series. URL www.jdibrief.com (accessed 3.20.17).

Lee, W., Fan, W., Miller, M., Stolfo, S., Zadok, E., 2002. Toward cost-sensitive modeling for intrusion detection and response. Journal of Computer Security 10, 5–22.

Lin, P.-H., Van Gulijk, C., 2015. Cost-benefit analysis of surveillance technologies, in: Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014. pp. 409–415.

Lin, P.-H., Van Gulijk, C., 2014. Surveille Deliverable 3.5.: Cost Model [WWW Document]. Surveille FP7 European Program. URL http://surveille.eui.eu/ (accessed 3.20.17).

Lowrance, W.W., 1976. Of Acceptable Risk—Science and the Determination of Safety., William Ka. ed. Los Altos, CA, USA.

Mannan, M.S., 2005. Lees's loss prevention in the process industries, ThirD. ed. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Marhavilas, P.K., Koulouriotis, D., Gemeni, V., 2011. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009. Journal of Loss Prevention in the Process Industries 24, 477–523. doi:10.1016/j.jlp.2011.03.004

Marshall, V.C., 1997. The social acceptability of the chemical and process industries: A proposal for an Integrated Approach. Chemical Engineering Research and Design 75, 145–155. doi:10.1016/S0263-8762(97)80012-3

Martinez, L.J., Lambert, J.H., 2012. Risk-benefit-cost prioritisation of independent protection layers for a liquefied natural gas terminal. International Journal of Critical Infrastructures 8, 306–325. doi:10.1504/IJCIS.2012.050106

Martins, M.R., Schleder, A.M., Droguett, E.L., 2014. A Methodology for Risk Analysis Based on Hybrid Bayesian Networks: Application to the Regasification System of Liquefied Natural Gas Onboard a Floating Storage and Regasification Unit. Risk Analysis 34, 2098–2120. doi:10.1111/risa.12245

Medina, H., Arnaldos, J., Casal, J., 2009. Process design optimization and risk analysis. Journal of Loss Prevention in the Process Industries 22, 566–573. doi:10.1016/j.jlp.2009.04.007

Meel, A., O'Neill, L., Levin, J., Seider, W., Oktem, U.G., Keren, N., 2007. Operational risk assessment of chemical industries by exploiting accident databases. Journal of Loss Prevention in the Process Industries 20, 113–127. doi:10.1016/j.jlp.2006.10.003

Meel, A., Seider, W., 2008. Real-time risk analysis of safety systems. Computers & Chemical Engineering 32, 827–840. doi:10.1016/j.compchemeng.2007.03.006

Meel, A., Seider, W., 2006. Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science 61, 7036–7056. doi:10.1016/j.ces.2006.07.007

Moteff, J., 2005. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Science And Technology. Washington, DC, USA.

Murphy, J., Conner, J., 2012. Beware of the black swan: The limitations of risk analysis for predicting the extreme impact of rare process safety incidents. Process Safety Progress 31, 326–330. doi:10.1002/prs

National Research Council, 1989. Improving Risk Communication. Washington, DC, USA. doi:10.17226/1189

Necci, A., Argenti, F., Landucci, G., Cozzani, V., 2014. Accident scenarios triggered by lightning strike on atmospheric storage tanks. Reliability Engineering & System Safety 127, 30–46. doi:10.1016/j.ress.2014.02.005

Necci, A., Cozzani, V., Spadoni, G., Khan, F., 2015. Assessment of domino effect: State of the art and research Needs. Reliability Engineering & System Safety 143, 3–18. doi:10.1016/j.ress.2015.05.017

Neilan, C., 2016. BP's share price falls to six-year low as energy giant reveals worse-than-expected $2.2bn fourth quarter loss on back of falling oil prices [WWW Document]. City A.M. URL http://www.cityam.com/233593/bp-to-cut-7000-jobs-as-it-suffers-22bn-q4-loss-on-back-of-falling-oil-prices (accessed 3.20.17).

Nolan, D.P., 2008. Safety and Security Review for the Process Industries, Second. ed. Elsevier, Amsterdam, The Netherlands.

NORSOK, 2010. Standard Z-013, Risk and Emergency Preparedness Analysis., Third. ed. Standards Norway, Lysaker, Norway.

NUREG - US Nuclear Regulatory Commission, 2016. Backgrounder on Probabilistic Risk Assessment [WWW Document]. US Nuclear Regulatory Commission website. URL http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/probabilistic-risk-asses.html (accessed 3.20.17).

NUREG - US Nuclear Regulatory Commission, 2003. Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making. CR-6813. Washington, DC, USA.

Øien, K., 2001a. A framework for the establishment of organizational risk indicators. Reliability Engineering & System Safety 74, 147–167. doi:10.1016/S0951-8320(01)00068-0

Øien, K., 2001b. Risk indicators as a tool for risk control. Reliability Engineering & System Safety 74, 129–145. doi:10.1016/S0951-8320(01)00067-9

Okoh, P., Hauge, S., 2013. Maintenance-related major accidents: Classification of causes and case study. Journal of Loss Prevention in the Process Industries 26, 1060–1070. doi:10.1016/j.jlp.2013.04.002

Okstad, E.H., Hauge, S., Tinmannsvik, R.K., 2013. Proactive indicators for managing major accident risk in integrated operations. SINTEF F24087. SINTEF Technology and Society, Trondheim, Norway. Trondheim, Norway.

OLF, 2007. Metode for Miljørettet Risikoanalyse. Høvik, Norway.

OPEC, 2014. Annual Statistical Bulletin of Oil and Gas 2014 - World Output of Refined Petroleum Products by Country [WWW Document]. OPEC Website. URL http://www.opec.org/library/Annual Statistical

Bulletin/interactive/current/FileZ/Main-Dateien/Section3.html (accessed 3.20.17).

Paltrinieri, N., Bonvicini, S., Spadoni, G., Cozzani, V., 2012. Cost-Benefit Analysis of Passive Fire Protections in Road LPG Transportation. Risk Analysis 32, 200–219. doi:10.1111/j.1539-6924.2011.01654.x

Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., Cozzani, V., 2012. Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. Risk Analysis 32, 1404–1419. doi:10.1111/j.1539-6924.2011.01749.x

Paltrinieri, N., Hauge, S., Dionisio, M., Nelson, W.R., 2014a. Towards a dynamic risk and barrier assessment in an IO context, in: Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, ESREL 2013. Amsterdam, Netherlands, pp. 1915–1923. doi:10.1201/b15938-293

Paltrinieri, N., Hauge, S., Nelson, W.R., 2015a. Dynamic barrier management: A case of sand erosion integrity, in: Safety and Reliability of Complex Engineered Systems. Proceedings of the European Safety and Reliability Conference, ESREL 2015. Zurich, Switzerland, pp. 523–531.

Paltrinieri, N., Hokstad, P., 2015. Dynamic risk assessment: Development of a basic structure, in: Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014. Wroclaw, Poland, pp. 1385–1392. doi:10.1201/b17399-191

Paltrinieri, N., Khan, F., 2016. Dynamic risk analysis in the chemical and petroleum industry evolution and interaction with parallel disciplines in the perspective of industrial application. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Paltrinieri, N., Khan, F., Amyotte, P., Cozzani, V., 2014b. Dynamic approach to risk management: Application to the Hoeganaes metal dust accidents. Process Safety and Environmental Protection 92, 669–679. doi:10.1016/j.psep.2013.11.008

Paltrinieri, N., Khan, F., Cozzani, V., 2014c. Coupling of advanced techniques for dynamic risk management. Journal of Risk Research 9877, 1–21. doi:10.1080/13669877.2014.919515

Paltrinieri, N., Scarponi, G., 2014. Addressing Dynamic Risk in the Petroleum Industry by Means of Innovative Analysis Solutions. Chemical Engineering Transactions 36, 451–456. doi:10.3303/CET1436076

Paltrinieri, N., Tugnoli, A., Bonvicini, S., Cozzani, V., 2011. Atypical Scenarios Identification by the DyPASI Procedure: Application to LNG. Chemical Engineering Transactions 24, 1171–1176. doi:10.3303/CET1124196

Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M., 2013a. DyPASI Methodology: from Information Retrieval to Integration of HAZID Process. Chemical Engineering

Transactions 32, 433–438. doi:10.3303/CET1332073

Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M., Cozzani, V., 2013b. Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. Journal of Loss Prevention in the Process Industries 26, 683–695. doi:10.1016/j.jlp.2013.01.006

Paltrinieri, N., Tugnoli, A., Cozzani, V., 2015b. Hazard identification for innovative LNG regasification technologies. Reliability Engineering & System Safety 137, 18–28. doi:10.1016/j.ress.2014.12.006

Paltrinieri, N., Wilday, J., Wardman, M., Cozzani, V., 2014d. Surface installations intended for Carbon Capture and Sequestration: Atypical accident scenarios and their identification. Process Safety and Environmental Protection 92, 93–107. doi:10.1016/j.psep.2013.08.004

Pardini, S., 2016. Berre l'Etang - Feux à LyondellBasell un homme écroué [WWW Document]. La Provence.com. URL http://www.laprovence.com/article/faits-divers-justice/4000586/feux-a-lyondellbasell-un-homme-ecroue.html (accessed 3.20.17).

Pariyani, A., Seider, W.D., Oktem, U.G., Soroush, M., 2012a. Dynamic risk analysis using alarm databases to improve process safety and product quality: Part I-Data compaction. AIChE Journal 58, 812–825. doi:10.1002/aic.12643

Pariyani, A., Seider, W.D., Oktem, U.G., Soroush, M., 2012b. Dynamic risk analysis using alarm databases to improve process safety and product quality: Part II-Bayesian analysis. AIChE Journal 58, 826–841. doi:10.1002/aic.12642

Pasman, H.J., 2015. Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals, Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals. Elsevier Butterworth-Heinemann, Burlington, MA, USA. doi:10.1016/B978-0-12-800057-1.00013-4

Pasman, H.J., 2011. History of Dutch process equipment failure frequencies and the Purple Book. Journal of Loss Prevention in the Process Industries 24, 208–213. doi:10.1016/j.jlp.2010.08.012

Pasman, H.J., Reniers, G.L.L., 2014. Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP). Journal of Loss Prevention in the Process Industries 28, 2–9. doi:10.1016/j.jlp.2013.03.004

Pasman, H.J., Rogers, W.J., 2013. Bayesian networks make LOPA more effective, QRA more transparent and flexible, and thus safety more definable! Journal of Loss Prevention in the Process Industries 26, 434–442. doi:10.1016/j.jlp.2012.07.016

Pasman, H.J., Rogers, W.J., 2012. Risk assessment by means of Bayesian networks: A comparative study of compressed and liquefied H2 transportation and tank station risks. International Journal of Hydrogen Energy 37, 17415–17425.

doi:10.1016/j.ijhydene.2012.04.051

PayScale, 2016. Salary Comparison, Salary Survey, Search Wages [WWW Document]. PayScale - Human Capital Website. URL http://www.payscale.com/ (accessed 3.20.17).

Pecorella, G., 2011. Sessione Bicamerale d'inchesta del Parlamento italiano - Missione in Lombardia riguardante il sabotaggio della Lombardia Petroli (in Italian) [WWW Document]. URL http://www.camera.it/_bicamerali/leg16/rifiuti/missioni/17Lombardia/Rif_20110208 - 10 LombardaP.pdf (accessed 3.20.17).

Peters, R.G., Covello, V.T., McCallum, D.B., 1997. The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study. Risk Analysis 17, 43–54. doi:10.1111/j.1539-6924.1997.tb00842.x

Planas, E., Arnaldos, J., Darbra, R.M., Muñoz, M., Pastor, E., Vílchez, J.A., 2014. Historical evolution of process safety and major-accident hazards prevention in Spain. Contribution of the pioneer Joaquim Casal. Journal of Loss Prevention in the Process Industries 28, 109–117. doi:10.1016/j.jlp.2013.04.005

Post, J.G., Bottelberghs, P.H., Vijgen, L.J., Matthijsen, A.J.C., 2003. Instrument Domino Effecten, RIVM.

Querzé, R., 2010. Scaricati altri veleni nel Lambro (in Italian) [WWW Document]. Corriere della Sera. URL http://milano.corriere.it/notizie/cronaca/10_febbraio_28/lambro-scaricati-altri-veleni-sciacalli-1602569139849.shtml (accessed 3.20.17).

Rathnayaka, S., Khan, F., Amyotte, P., 2012. Accident modeling approach for safety assessment in an LNG processing facility. Journal of Loss Prevention in the Process Industries 25, 414–423. doi:10.1016/j.jlp.2011.09.006

Rathnayaka, S., Khan, F., Amyotte, P., 2011. SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. Process Safety and Environmental Protection 89, 151–164. doi:10.1016/j.psep.2011.01.002

Rausand, M., 2011. Risk Assessment: Theory, Methods, and Applications. Wiley, Hoboken, NJ, USA. doi:10.1039/9781847551856

Reniers, G.L.L., 2014. Safety and Security Decisions in times of Economic Crisis: Establishing a Competitive Advantage. Chemical Engineering Transactions 36, 1–6. doi:10.3303/CET1436001

Reniers, G.L.L., 2010. Multi-Plant Safety and Security Management in the Chemical and Process Industries, First Ed. ed. WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim, Germany. doi:10.1002/9783527630356

Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Safety

and Environmental Protection 92, 583–589. doi:10.1016/j.psep.2013.04.002

Reniers, G.L.L., Brijs, T., 2014a. An Overview of Cost-benefit Models / Tools for Investigating Occupational Accidents. Chemical Engineering Transactions 36, 43–48. doi:10.3303/CET1436008

Reniers, G.L.L., Brijs, T., 2014b. Major accident management in the process industry: An expert tool called CESMA for intelligent allocation of prevention investments. Process Safety and Environmental Protection 92, 779–788. doi:10.1016/j.psep.2014.02.003

Reniers, G.L.L., Cozzani, V., 2013. Domino Effects in the Process Industries: Modelling, Prevention and Managing, Domino Effects in the Process Industries: Modelling, Prevention and Managing. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Reniers, G.L.L., Sörensen, K., 2013a. Optimal allocation of safety and security resources. Chemical Engineering Transactions 31, 397–402. doi:10.3303/CET1331067

Reniers, G.L.L., Sörensen, K., 2013b. An Approach for Optimal Allocation of Safety Resources: Using the Knapsack Problem to Take Aggregated Cost-Efficient Preventive Measures. Risk Analysis 33, 2056–2067. doi:10.1111/risa.12036

Reniers, G.L.L., Van Erp, H.R.N., 2016. Operational Safety Economics: A Practical Approach focused on the Chemical and Process Industries. Wiley, Hoboken, NJ, USA.

Reniers, G.L.L., Van Lerberghe, P., Van Gulijk, C., 2015. Security Risk Assessment and Protection in the Chemical and Process Industry. Process Safety Progress 34, 72–83. doi:10.1002/prs.11683

Renn, O., Klinke, A., 2004. Systemic risks: a new challenge for risk management. EMBO reports 5, 41–46. doi:10.1038/sj.embor.7400227

RFI News, 2015. French chemical plant blaze may have been deliberate [WWW Document]. RFI English News Website - French Edition. URL http://www.english.rfi.fr/americas/20150714-french-chemical-plant-blaze-may-have-been-deliberate (accessed 3.20.17).

Richardson Products & Cost Data On Line Inc., 2008. Richardson International Construction Factors Manual [WWW Document]. Richardson books. URL http://www.icoste.org/Book_Reviews/CFM-Info.pdf (accessed 3.20.17).

Røed, W., Mosleh, A., Vinnem, J.E., Aven, T., 2009. On the use of the hybrid causal logic method in offshore risk analysis. Reliability Engineering and System Safety 94, 445–455. doi:10.1016/j.ress.2008.04.003

Rosa, E.A., 2003. The logical structure of the social amplification of risk framework (SARF): Metatheoretical foundation and policy implications., in: Pidgeon, N., Kaspersen, R.E, Slovic, P. The Social Amplification of Risk. Cambridge University Press, Cambridge, UK, pp. 47–79.

Rosa, E.A., 1998. Metatheoretical foundations for post-normal risk. Journal of risk research 1, 15–44. doi:10.1080/136698798377303

Rowe, W.D., 1977. An Anatomy of Risk. John Wiley & Sons, New York, USA.

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, 187–99. doi:10.1016/j.jhazmat.2005.07.034

Sevcik, A., Gudmestad, O.T., 2014. A systematic approach to risk reduction measures in the Norwegian offshore oil and gas industry, in: WIT Transactions on Information and Communication Technologies. WIT Press, pp. 287–305. doi:10.2495/RISK140251

Shanghai Iven Pharmatech Engineering Co. Ltd, 2016. Fuel storage tank - Technical and commercial datasheet [WWW Document]. Alibaba Website. URL http://www.alibaba.com/product-detail/fuel-storage-tank_60260194681.html?spm=a2700.7724838.14.5.WWRDh0&s=p (accessed 3.20.17).

Shariff, A.M., Zaini, D., 2013. Inherent risk assessment methodology in preliminary design stage: A case study for toxic release. Journal of Loss Prevention in the Process Industries 26, 605–613. doi:10.1016/j.jlp.2012.12.003

Shenzhen An Ying Technology Co. Ltd., 2016. Industrial alarm system - Technical and commercial datasheet [WWW Document]. Alibaba Website. URL http://www.alibaba.com/product-detail/GSM-Industrial-Alarm-Systems-Quad-Band_1460101510.html?spm=a2700.7724838.0.0.1fwpoJ (accessed 3.20.17).

Shenzhen P&H Electronic Co. Ltd, 2016. Outdoor fence detector alarm sensor - Technical and commercial datasheet [WWW Document]. Alibaba Website. URL http://www.alibaba.com/product-detail/outdoor-fence-detector-alarm-sensor_60249507350.html?spm=a2700.7724857.35.1.vKQFA2 (accessed 3.20.17).

Siegrist, M., 2000. The Influence of Trust and Perceptions of Risks and Benefits on the Acceptance of Gene Technology. Risk Analysis 20, 195–204. doi:10.1111/0272-4332.202020

Siegrist, M., Cvetkovich, G., 2000. Perception of hazards: The role of social trust and knowledge. Risk Analysis 20, 713–719. doi:10.1111/0272-4332.205064

Slovic, P., 2000. Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. Risk Analysis 19, 390–412. doi:10.1111/j.1539-6924.1999.tb00439.x

Slovic, P., 1993. Perceived Risk, Trust, and Democracy. Risk Analysis 13, 675–682. doi:10.1111/j.1539-6924.1993.tb01329.x

Spadoni, G., Contini, S., Uguccioni, G., 2003. The new version of ARIPAR and the benefits given in assessing and managing major risks in industrialised areas. Process Safety and Environmental Protection 81, 19–30. doi:10.1205/095758203762851958

Spadoni, G., Egidi, D., Contini, S., 2000. Through ARIPAR-GIS the quantified area risk analysis supports land-use planning activities. Journal of hazardous materials 71, 423–37. doi:10.1016/S0304-3894(99)00091-6

Spash, C.L., 1997. Ethics and Environmental Attitudes With Implications for Economic Valuation. Journal of Environmental Management 50, 403–416. doi:10.1006/jema.1997.0017

Srivastava, A., Gupta, J.P., 2010. New methodologies for security risk assessment of oil and gas industry. Process Safety and Environmental Protection 88, 407–412. doi:10.1016/j.psep.2010.06.004

Stevenson, A., 2016. Oxford Dictionary of English.

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

Stewart, M.G., Mueller, J., 2012. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Critical Infrastructure Protection, in: 5th International Conference on Reliable Engineering Computing. pp. 513–534. doi:10.1080/03071847.2012.714212

Stewart, M.G., Mueller, J., 2011. Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening. Journal of Homeland Security and Emergency Management 8, 1–24. doi:10.2202/1547-7355.1837

Stewart, M.G., Mueller, J., 2008. A risk and cost-benefit assessment of United States aviation security measures. Journal of Transportation Security 1, 143–159. doi:10.1007/s12198-008-0013-0

Swaminathan, S., Smidts, C., 1999a. The Event Sequence Diagram framework for dynamic Probabilistic Risk Assessment. Reliability Engineering & System Safety 63, 73–90. doi:10.1016/S0951-8320(98)00027-1

Swaminathan, S., Smidts, C., 1999b. Identification of missing scenarios in ESDs using probabilistic dynamics. Reliability Engineering & System Safety 66, 275–279. doi:10.1016/S0951-8320(99)00024-1

Tappura, S., Sievänen, M., Heikkilä, J., Jussila, A., Nenonen, N., 2014. A management accounting perspective on safety. Safety Science 71, 151–159. doi:10.1016/j.ssci.2014.01.011

Tixier, J., Dusserre, G., Salvi, O., Gaston, D., 2002. Review of 62 risk analysis methodologies of industrial plants. Journal of Loss Prevention in the Process Industries 15, 291–303. doi:10.1016/S0950-4230(02)00008-6

TNO, 2005a. The 'Purple book' – Guidelines for quantitative risk assessment, CPR 18 E, Publication Series on Dangerous Substances (PGS 3). Commitee for the Prevention of Disasters, The Hague, Netherlands.

TNO, 2005b. The 'Yellow Book' - Methods for the calculation of Physical Effects - CPR 14E, in: Publication Series on Dangerous Substances (PGS 2). Commitee for the Prevention of Disasters, The Hague, Netherlands.

Toronto Municipality, 2016. False alarms fees for the city of Toronto [WWW Document]. Toronto City Website. URL http://www.toronto.ca/311/knowledgebase/88/101000045888.html (accessed 3.20.17).

Totaro, S., 2014. Disastro ambientale nel Lambro, paga solo il custode: disastro compiuto contro ignoti (in Italian) [WWW Document]. Il Giorno. URL http://www.ilgiorno.it/monza-brianza/cronaca/lambro-sentenza-1.329538 (accessed 3.20.17).

US Department of Defense, 2000. Standard Practice for System Safety. MIL-STD-882D. Wright-Patterson AFB, OH, USA.

Vallee, A., Bernuchon, E., Hourtolou, D., 2002. MICADO: Méthode pour l'identification et la caractérization des effets dominos, Rep. INERIS-DRA-2002-25472. Paris, France.

Vaurio, J.K., 1995. Optimization of test and maintenance intervals based on risk and cost. Reliability Engineering & System Safety 49, 23–36. doi:10.1016/0951-8320(95)00035-Z

Villa, V., Cozzani, V., 2016. Application of Bayesian Networks to quantitative assessment of safety barriers' performance in the prevention of major accidents. Chemical Engineering Transactions 53, 151–156. doi:10.3303/CET1653026

Villa, V., Reniers, G.L.L., Cozzani, V., 2016. Application of cost-benefit analysis for the selection of process-industry related security measures. Chemical Engineering Transactions 53, 103–108. doi:10.3303/CET1653018

Vinnem, J.E., Bye, R., Gran, B. a., Kongsvik, T., Nyheim, O.M., Okstad, E.H., Seljelid, J., Vatn, J., 2012. Risk modelling of maintenance work on major process equipment on offshore petroleum installations. Journal of Loss Prevention in the Process Industries 25, 274–292. doi:10.1016/j.jlp.2011.11.001

Viscusi, W.K., Aldy, J.E., 2003. The Value of a Statistical Life: A critical review of market estimates thoughout the world. Journal of Risk and Uncertainty 27, 5–76. doi:10.1023/A:1025598106257

Vose, M.D., Rowe, J.E., 2000. Random heuristic search: applications to GAs and functions of unitation. Computer Methods in Applied Mechanics and Engineering 186, 195–220. doi:10.1016/S0045-7825(99)00384-9

Vrijling, J.K., van Hengel, W., Houben, R.J., 1995. A framework for risk evaluation. Journal of Hazardous materials 43, 245–261. doi:10.1016/0304-3894(95)91197-V

Wang, D., Kim, J., 2015. Asia Naphtha & LPG Report [WWW Document]. OPIS - Oil Price Information Service Website. URL

http://www.opisnet.com/Images/ProductSamples/AsiaNaphtha-sample.pdf (accessed 3.20.17).

Weber, P., Medina-Oliva, G., Simon, C., Iung, B., 2012. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence 25, 671–682. doi:10.1016/j.engappai.2010.06.002

Willis, H.H., 2007. Guiding resource allocations based on terrorism risk. Risk Analysis 27, 597–606. doi:10.1111/j.1539-6924.2007.00909.x

Winfield, N., 2010a. Italy's longest river at risk after sabotage at oil depot [WWW Document]. The Independent. URL http://www.independent.co.uk/news/world/europe/italys-longest-river-at-risk-after-sabotage-at-oil-depot-1909934.html (accessed 3.20.17).

Winfield, N., 2010b. Lambro River Oil Spill May Create 'Ecological Disaster' In Italy [WWW Document]. The World Post. URL http://www.huffingtonpost.com/2010/02/24/lambro-river-oil-spill-ma_n_474642.html (accessed 3.20.17).

X-Rates, 2016. Currency Calculator (US Dollar, Euro) [WWW Document]. X-Rates Website. URL http://www.x-rates.com/calculator/ (accessed 3.20.17).

Yang, M., Khan, F., Lye, L., 2013. Precursor-based hierarchical Bayesian approach for rare event frequency estimation: A case of oil spill accidents. Process Safety and Environmental Protection 91, 333–342. doi:10.1016/j.psep.2012.07.006

Yang, X., Mannan, M.S., 2010a. The development and application of dynamic operational risk assessment in oil/gas and chemical process industry. Reliability Engineering & System Safety 95, 806–815. doi:10.1016/j.ress.2010.03.002

Yang, X., Mannan, M.S., 2010b. An uncertainty and sensitivity analysis of dynamic operational risk assessment model: A case study. Journal of Loss Prevention in the Process Industries 23, 300–307. doi:10.1016/j.jlp.2009.11.001

Yuan, Z., Khakzad, N., Khan, F., Amyotte, P., 2015. Risk Analysis of Dust Explosion Scenarios Using Bayesian Networks. Risk Analysis 35, 278–291. doi:10.1111/risa.12283

Yuan, Z., Khakzad, N., Khan, F., Amyotte, P., Reniers, G.L.L., 2013. Risk-Based Design of Safety Measures To Prevent and Mitigate Dust Explosion Hazards. Industrial & Engineering Chemistry Research 52, 18095–18108. doi:10.1021/ie4018989

Extension of Quantitative Risk Assessment to the Analysis of External Hazard Factors in the Chemical and Process Industry

Acknowledgments

The author gratefully acknowledges the following people for the fundamental support in the development of the present PhD Research Project:

- Prof. Valerio Cozzani (*Alma Mater Studiorum - University of Bologna,* Bologna, Italy), advisor of the PhD Research Project, for the useful support and supervision during these three years;
- Prof. Genserik L.L. Reniers (*TU Delft – Delft University of Technology*, Delft, Netherlands), supervisor during the research period abroad, for the useful support, supervision and scientific collaboration;
- Prof. Nicola Paltrinieri (*NTNU – Norwegian University of Science and Technology*, Trondheim, Norway) and Prof. Faisal I. Khan (*Memorial University of Newfoundland*, St. John's, Canada) for the scientific collaboration on Dynamic Risk Assessment;
- Prof. Gigliola Spadoni (*Alma Mater Studiorum - University of Bologna,* Bologna, Italy), co-supervisor to the PhD Research Project;
- Dr. Gabriele Landucci (*University of Pisa,* Pisa, Italy);
- Prof. Carlo Gostoli (*Alma Mater Studiorum - University of Bologna,* Bologna, Italy);
- All the members of *LISES* Research Group at *University of Bologna* and all the members of *Safety and Security Science* Research Group at *TU Delft*.