NARSIS

New Approach to Reactor Safety ImprovmentS

WP3: Integration and Safety Analysis

Del 3.1 – Risk integration methods for high risk industries

This project has received funding from the Euratom research and training programme 2014-2018 under Grant Agreement No. 755439.

Project Acronym: NARSIS

Project Title: New Approach to Reactor Safety Improvements

Deliverable:

Month due: 12 **Month delivered:** 12

Leading Partner: Delft University of Technology

Version: V1

Primary Authors: Varenya Kumar D MOHAN, Philip VARDON (Delft University of Technology), Milorad DUSIC (NUCCON)

Other contributors:

- Delft University of Technology: Pieter VAN GELDER, Michael HICKS
- ENEA Luciano BURGAZZI

Deliverable Review:

- **Reviewer #1:** James DANIELL, Karlsruhe Institute of Technology **Date:** 10/08/2018
- **Reviewer #2:** Andrija Volkanovski, Jožef Stefan Institute **Date:** 10/08/2018

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of contents

List of Figures

List of Tables

List of Abbreviations

AEB	Accident Evaluation and Barrier analyses
AIRS	Advanced Investigation Reporting System
AIT	Augmented Inspection Team
AHP	Analytic Hierarchy Processing
ALARA	As Low As Reasonably Achievable
ARAMIS	Accidental Risk Assessment Methodology for IndustrieS
ARMONIA project	Applied multi Risk Mapping Of Natural hazards for Impact Assessment (EU project)
ASCOT	Assessment of Safety Culture in Organizations Team
ASP	Accident Sequence Precursor Programme
ASRM	Aviation System Risk Model
ASSET	Assessment of Safety Significant Events Team
ATC	Air Traffic Control
ATHEANA	A Technique for Human Error ANAlysis
AVN	Association Vinçotte Nuclear
BDBA	Beyond Design Basis Accidents
BE	Best Estimate
BEPU	Best Estimate Plus Uncertainties
BORA	Barrier and Operational Risk Analysis
BWR	Boiling Water Reactor
BN	Bayesian Network
CANL	Complex Adaptive Non-Linear model
CAPRA platform	Central American Probabilistic Risk Assessment platform
CATS	Causal Model for Air Transport Safety
CCA	Common Cause Analysis
CCDP	Conditional Core Damage Probability
CEPREDENAC	Central American Coordination Centre for Disaster Prevention
CLUVA	Climate Change and Urban Vulnerability in Africa
CMA	Common Mode Analysis
CNS	Convention on Nuclear Safety
CREAM	Cognitive Reliability and Error Analysis Method
CSN	Consejo De Seguridad Nuclear
DBA	Design Basis Accident
DBN	Dynamic Bayesian Network
DD	Dependence Diagrams
DEC	Design Extension Conditions

DID	Defence-In-Depth
EASA	European Aviation Safety Agency
EDF	Électricité de France
ESD	Event Sequence Diagrams
ESWS	Essential Service Water System
ET	Event Tree
EU	European Union
E-BEPU	Extended Best Estimate Plus Uncertainties
E&CFC	Event and Causal Factor Charting
FAA	Federal Aviation Administration
FCM	Fuzzy Cognitive Maps
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effect Analysis
FOE	Feedback of Operating Experience
FORM	First-Order Reliability Method
FT	Fault Tree
GRS	Global Research for Safety/ Gesellschaft für Anlagen- und Reaktorsicherheit
GSR	General Safety Requirements
HAEA	Hungarian Atomic Energy Authority
HAZAN	Hazard Analysis
HAZOP	Hazard and Operability
HBN	Hybrid Bayesian Network
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HET	Human Error Template
HOF	Human and Organisational Factors
HPES	Human Performance Enhancement System
HPIP	Human Performance Investigation Process
HPM	Human Performance Models
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
ICCP	Impressed Current Cathodic Protection
IDAC	Information, Decision and Action in Crew context
IDEA	Investigate, Discuss, Estimate and Aggregate
IE	Initiating Event
IIT	Incident Investigation Team
INES	International Nuclear Event Scale

INSAG	International Nuclear Safety Group
IRBE	Integration Risk-Based Engineering
IRSN	Institut de Radioprotection et de Sûreté Nucléaire
I-RISK	Integrated (technical and management) Risk
IRS	International Reporting System
ISDR	(United Nation's) International Strategy for Disaster Reduction
JPD	Joint Probability Distribution
LCO	Limiting Conditions for Operation
LER	Licensee Event Reports
LOCA	Loss of Coolant Accident
MACHINE	Model of Accident Causation using Hierarchical Influence NEtwork
MA	Markov Analysis
MATRIX project	New Multi-HAzard and MulTi-RIsK Assessment MethodS for Europe (EU project)
MAUD	Multi-Attribute Utility Decomposition
MC	Monte Carlo
MCMC	Markov Chain Monte Carlo
MIC	Methyl Isocyanate
MLD	Master Logic Diagrams
MORT	Management Oversight and Risk Tree
MoTBFs	Mixture of Truncated Basis Functions
MOVE project	Methods for the improvement of Vulnerability Assessment in Europe (EU project)
MTE	Mixture of Truncated Exponential
MTO	Man, Technology, Organisation
NASA	National Aeronautics and Space Administration
NEA	Nuclear Energy Agency
NPBN	Non-Parametric Bayesian Network
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NUPEC	Nuclear Power Engineering Center
OECD	Organisation for Economic Co-operation and Development
ORIM	Organizational Risk Influence Model
PORV	Power Operated Relief Valve
PROSPER	Peer Review of the effectiveness of the Operational Safety Performance Experience Review
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor

PSSA	Preliminary System Safety Assessment
PWR	Pressurised Water Reactor
RAIN project	Risk Analysis of Infrastructure Networks in response to extreme weather (EU project)
RAW	Risk Assessment Worth
RCA	Root Cause Analyses
RCS	Reactor Coolant System
RIRIP	Risk-Informed Regulation Implementation Plan
RPP	Risk-informed and Performance-based Plan
RPV	Reactor Pressure Vessel
RRW	Risk Rejection Worth
SAM	System Action Management
SD	System Dynamics
SDP	Significance Determination Process
SIT	Special Investigation Team
SLIM	Success Likelihood Index Method
SoTeRiA	Socio-Technical Risk Analysis
SPDS	Safety Parameter Display Systems
SSG	Specific Safety Guide
STUK	Säteilyturvakeskus (Radiation and Nuclear Safety Authority – Finland)
SUJB	Státního úřadu pro jadernou bezpečnost (State Office for Nuclear Safety – Czech Republic)
SWOT	Strengths, Weaknesses, Opportunities and Threats
THERP	Technique for Human Error-Rate Prediction
TRACEr	Technique for the Retrospective and predictive Analysis of Cognitive Error in air traffic management
TMI	Three Mile Island
UCIL	Union Carbide India Limited
UNISDR	United Nations International Strategy for Disaster Reduction
WB-IRS	Web-Based Incident Reporting System
WENRA	Western European Nuclear Regulators Association
WPAM	Work Process Analysis Model
ZSA	Zonal Safety Analysis

1 Executive Summary

Nuclear power plants are exposed to a variety of hazards, which may result in risks (the product of the likelihood of the hazard and resulting consequence). One of the key objectives of the NARSIS project is to improve the integration of external hazards and their consequences with existing state-of-the-art risk assessment methodologies in the industry. Accordingly, the main goals of this deliverable are to:

- Review the various aspects of risk integration and associated methodologies;
- Review case histories of accidents in complex industrial set-ups, both nuclear and non-nuclear, and highlight prevalent 'latent weaknesses' that eventually led to these accidents;
- Review deterministic and probabilistic methods to identify latent weaknesses;
- Review risk integration methods currently used in high-risk industries such as nuclear, chemical and aviation;
- Review accident investigation procedures and international initiatives associated with major nuclear accidents;
- Discuss specific risk integration method(s) that are relevant to the NARSIS project.

The variety of hazards threatening a NPP and associated consequences that could arise implies that a multi-risk approach is essential. NPPs have a very high safety level and therefore it is the combination of several hazards and low probability events which must be assessed. These hazards affect several sub-systems which interact at various levels and therefore, nuclear power plants are considered to be complex systems. The maintenance and decision making which occurs also means that human aspects should be considered to gain a full picture of the risks. There are very few cases of significant events in the nuclear industry, which precludes conventional statistical analysis to predict future risks. The scarcity of data can often be addressed with input from experts, although appropriate care must be taken. Due to the aspects considered above, and inherent variability of parameters affecting risk, uncertainties exist. Methods to deal with such uncertainties have been reviewed, and they are either based on deterministic analysis with a consideration of the uncertainties or a probabilistic analysis where the uncertainties are inherent in the analysis. Methods in the literature, for integrating each of the above mentioned aspects into risk assessments, are reviewed in this deliverable. In general, multi-risk frameworks that allow for integration of multi-hazard and multi-vulnerability aspects are suited for NPP risk assessment. Bayesian Networks (BN) were found to have a wide variety of applications including integrating probabilistic multi-hazard/vulnerability aspects, analysing complex systems, handling expert opinion, and tracking and modelling uncertainty.

A series of case-histories of events in industries which are typically considered high-reliability are examined to understand the causes of the events. In most cases aspects of safety culture were major contributing factors. In addition, the methods currently applied in industry have been outlined. Following adverse events, an incident investigation is usually carried out. A brief review into the goals and practices is given. International initiatives in response to major events have been outlined, highlighting the benefits in acting internationally to minimising the likelihood of another accident.

A wide number of methods have been established for understanding risks, and to investigate causes of events. These can be fit into different groups based on the objective:

- Root Cause Analyses are designed for incident evaluation;
- Precursor analyses are used to determine the safety significance of events;
- Deterministic Transient Analyses are used to understand the physical behaviour of a plant, typically during quickly occurring events or design basis accidents;
- Probabilistic methods, such as Bayesian Networks are able to capture highly complex integrated situations and can be used to identify weaknesses.

All methods complement each other and therefore each has its place in practice. Probabilistic Safety Analysis (PSA) is standard of practice across nuclear, chemical and

aviation industries involving integration tools such as the Fault Trees (FT) and Event Trees (ET). The chemical industry employs unique methods such as the Hazard and Operability Study (HAZOP) and Hazard Analysis (HAZAN) approaches, while the Failure Hazard Analysis (FHA) and Failure Mode Effect Analysis (FMEA) are tools that are often applied in the aviation industry to complement PSAs. These methods are not alien to the nuclear industry and can be integrated easily into standard practice. The Causal Model for Air Transport Safety (CATS) is a unique approach from the aviation industry that is of interest in the NARSIS context and provides a means to combine advantages of Event Sequence Diagrams (ESD), FTs, and BNs. In general, a combination of deterministic and probabilistic approaches is concluded to yield best results in high-risk industries, where, for example, deterministic methods can be used to identify high-risk scenarios and probabilistic methods can be used to integrate the risks from different hazards and cascading events.

The Extended-Best Estimate Plus Uncertainty (E-BEPU) analysis offers considerable promise in terms of a methodology that allows for integration of probabilistic and deterministic methods, and has been recognised by the International Atomic Energy Agency (IAEA) as an option for safety analyses. BNs have been used to analyse various risk integration aspects and their application in scientific literature spans high-risk industries such as nuclear, chemical, aviation and offshore. BNs offer advantages over other methods, e.g. fault/event trees, including diagnostic in addition to causal analysis, which can be used for identifying weaknesses. Nevertheless, BNs are yet to be part of standardized industry practice for safety analyses. Hence, both the E-BEPU and BN methods allow for the integration of probabilistic and deterministic tools/aspects and have not been extensively applied in the nuclear industry. These methods can be developed offering further benefits in quantifying the risks.

2 Introduction

One of the key objectives of the NARSIS project is to improve the integration of external hazards and their consequences with existing state-of-the-art risk assessment methodologies in the industry. The main goal of this deliverable (D3.1 of WP 3) is reviewing the gamut of risk integration methodologies currently under use in high-risk industries such as the nuclear, aviation or chemical industries. Further, case histories of accidents in complex industrial set-ups, both nuclear and non-nuclear, are reviewed to highlight prevalent 'latent weaknesses' that eventually led to these accidents.

Section 3 discusses the various aspects of risk integration that are of interest to this project including low probability/high risk events, multi-risk considerations, integration of human, social and organisational aspects, challenges with complex systems, the role and handling of uncertainty, and the inclusion of expert opinion within the risk assessment. The importance of each of these aspects is highlighted and existing literature regarding integrating these aspects into risk assessments are summarised. Section 4 looks at case histories in various industries that highlight the importance of identifying latent weaknesses and Section 5 details the importance of safety culture in avoiding accidents within industrial settings. Section 6 delves into the various state-of-the-art methods available for both root-cause-analysis (RCA) in the case of accidents or near-misses, and methods currently used for risk integration. Risk integration methods are summarised under deterministic and probabilistic classifications. Overall common methodologies in high-risk industries such as nuclear, chemical and aviation industries are discussed in Section 7. Between Section 6 and 7, the majority of risk assessment and integration methods are outlined. Section 8 discusses procedures and personnel involved with on-site investigations and corrective actions within a complex industrial setting, particularly in a nuclear power plant. Section 9 discusses the various international initiatives and schemes that were installed following major nuclear accidents of the past. Finally, Section 10 provides a summary and discussion of the various methods discussed, the potential to combine them, and associated challenges in implementation.

3 Risk integration – aspects of interest

Nuclear power plants (NPPs) are exposed to risks from a variety of natural hazards including geological, hydrogeological and hydrometeorological events that impact technical and socio-organisational aspects of the NPP. The varied sources of risk create the need for an integrated risk assessment framework that jointly considers the hazards and consequences from different sources, while also modelling their interaction.

Within the NARSIS project, the risks to the NPP from external events (hazards) of low probability are of primary interest. NPPs are complex systems that involve extensive technical areas that are intertwined with human, social and organisational aspects contributing to overall risk. Quantifying and integrating the risks from a diverse set of components with complex interdependencies is challenging. By the nature of the problem historic examples, and thereby available data, are scarce. For this reason, risk assessments for NPPs require considerable input from experts to fill knowledge gaps left by available data. In turn, since, the risk assessment concerns events of low probability that affect a complex system and requires integration of expert judgement, significant uncertainty stems from each step. The quantification and tracking of uncertainty becomes crucial to the risk assessment process to allow for well-educated decision making.

3.1 Multi-risk approach

Historically, natural disasters have caused numerous fatalities and extensive property damage. The impact of these disasters has often been amplified by the multi-hazard and multi-risk nature of these events – i.e. different hazards occurs concurrently or one natural disaster triggers a cascade of other natural or man-made hazards at varying spatial and temporal scales. Examples of such events include the Messina earthquake and tsunami of 1908, the Kobe earthquake and cyclone of 1995, hurricane Katrina, USA of 2005; the Haiti earthquake and tropical cyclone of 2010, the 2011 Tohoku earthquake and tsunami in Japan, etc. (Komendantova et al., 2013). These events highlight the need for a multi-risk perspective to risk integration. The multi-risk concept has evolved from the consideration of individual risks within the same framework, to an assessment that accounts for the interdependencies between natural hazards, and their interactions with socio-economic/political and techno-hazards (Mignan et al., 2014; van Erp et al., 2017).

The multi-risk concept has also been split to isolate multi-hazard and multi-vulnerability perspectives. The multi-hazard component is generally associated with two aspects:

(i) component(s) or area(s) under risk from multiple hazards at the same or at different times, or
(ii) cascading effects from one hazard that leads to other hazards.

Multi-vulnerability relates to:

(i) the exposure of different targets (buildings, infrastructure systems, people etc.) with varying responses to each of the different hazards, or
(ii) a temporal variation in the vulnerability of exposed elements (Garcia-Aristizabal and Marzocchi, 2012 and Marzocchi et al., 2012 from the MATRIX project; Gallina et al., 2016).

Figure 1 shows a schematic representation of the below listed steps for the implementation of a multi-risk approach (Marzocchi et al., 2012):

(a) Define the spatial and temporal window for the assessment, along with the final risk metric quantifying loss;
(b) Identify the various hazard sources and corresponding intensities for the study area, while assessing possible interactions and cascading effects;

(c) Assess hazards as a function of the stochastic characteristics of the hazard source, intensity and the diffusion process – the pathway between the source and exposed elements;
(d) Assess vulnerability of hazards as a function of hazard intensity while also accounting for vulnerability interactions and cascading effects;
(e) Estimate expected loss per chosen metric for the set of all considered scenarios.

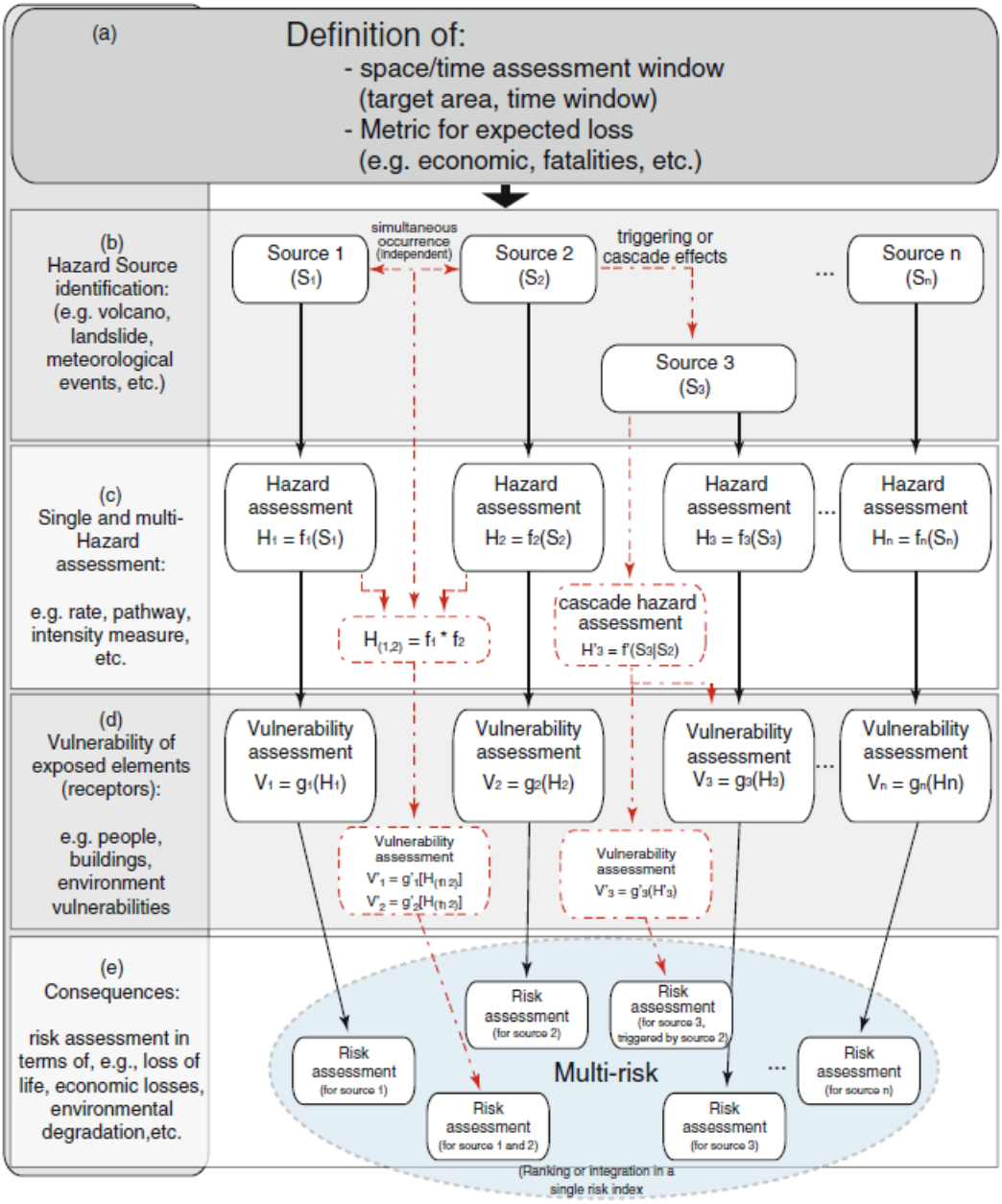

Figure 1: Schematic for multi-risk assessment methodology (Marzocchi et al. 2012)

3.1.1 Multi-hazard

The multi-hazard concept, as mentioned above, is associated with evaluation of relevant hazards, their interactions, triggering and cascading effects that endanger specific elements or areas, either simultaneously or at different times. The nature of the multi-hazard problem will be examined from two angles (discussed below) and later in Section 3.7, state-of-the-art methods that quantify multi-hazards along with other aspects of multi-risk will be discussed.

Multiple disparate hazards affecting target element(s) or area(s)

Literature that examines this interpretation of multi-hazard typically identifies the spatial distribution of various hazards across a range of relevant intensities to estimate a probability of exceedance for a required return period. The focus is on the quantification of individual hazards and the integration of their models and outputs which, among other objectives, specifically allows for: (i) identification of dominant risks across timescales (Grunthal et al., 2006), and (ii) identification of spatial patterns for various hazards and their consequences (Del Monaco et al. 2007 – ARMONIA project; Kappes et al., 2010, 2011; Bernal et al., 2017). The results from such consideration of multiple hazards include presentation of area-wide hazard curves and maps from which the probability of exceedance of an intensity measure can be obtained (Carpignano et al., 2009; Schmidt et al. 2011). Naturally, efforts have been aligned towards homogenisation of the single hazard assessments to make risks from different hazards comparable, and several approaches have been adopted in this regard (Grunthal et al., 2006; Kleist et al., 2006; Del Monaco et al. 2007 – ARMONIA project; Marzocchi et al., 2009; Merz and Thieken, 2009; Munich Re, 2011).

Interdependent hazards with cascading effects

The occurrence of a single hazard may trigger cascading effects through other interdependent hazards. The total risk from such events is not a simple summation of the risk from individual hazards, and can be much higher than such a sum. The occurrence of one event alters the probability of occurrence of other dependent events, and in turn alters the risk posed by the dependent impacts, i.e. cascading. With respect to the interaction of interdependent hazards, the relevant factors of interest are (Liu et al., 2015):

(i) the physical mechanisms associated with the triggering and the triggered events;
(ii) the intensity measures of the triggering event and its effect on the intensity of the triggered events – this is inherently linked with the physical mechanisms behind these hazards, and
(iii) random effects that affect the chain of events.

Due to the tree-like structure of events that characterise such cascading effects, the resulting interdependencies, and the uncertainty associated with physical mechanisms and random effects, modelling of cascading events is best tackled using a probabilistic approach (Nadim and Liu, 2013; Zhang, 2014; Gasparini and Garcia-Aristizabal, 2014; Garcia-Aristizabal et al., 2015). Interactions between interdependent events in a cascade scenario can occur at two levels – at the hazard level and at the vulnerability level (Marzocchi et al., 2012; Selva, 2013). As mentioned earlier, at the hazard level the probability of occurrence of one event impacts the probability of interdependent events. At the vulnerability level, the focus is on assessing the response of an exposed element to the sequentially triggered events down the cascading chain, given that the triggering event has already impacted the damage state of the element (Garcia-Aristizabal et al. 2013; Selva, 2013). Multi-vulnerability aspects within the multi-risk approach are discussed next.

3.1.2 Multi-vulnerability

As discussed earlier, the multi-vulnerability perspective concerns both the response to hazards of various exposed elements as well as the temporal variation of the response. While hazards from various sources impact vulnerability considerations, the point of interest within interactions at the multi-vulnerability level narrows down to the cumulative response of exposed elements over time. In this section, multi-vulnerability from this time-variant standpoint is discussed and in Section 3.7, multi-risk studies that have implemented these multi-vulnerability considerations are summarized.

Temporal Variation in Vulnerability

Temporal variation in vulnerability is typically of interest due to functionality/response degradation of elements over time. However, the multi-vulnerability viewpoint within a multi-

risk framework is particularly related to cumulative effects on vulnerability when hazard events occur consecutively over time. For instance, the response of a building to earthquake shaking to one event degrades compared to the previous event and therefore vulnerability changes over a period where consecutive events occur (seismic aging) (Dong et al. 2013; Iervolino et al., 2015; Iervolino et al., 2014; Karapetrou et al., 2017; Jalayer and Ebrahimian, 2017). Asprone et al. (2010) examined the progressive deterioration of reinforced concrete structures under the effect of both earthquakes as well as loads from blasting. Time-variant vulnerability interactions between different hazard events have also been studied. Akiyama and Frangopol (2013) evaluated the combined effects of earthquakes and tsunamis, and resulting continuous degradation, on the reliability of bridges. Liu et al. (2015) consider multi-vulnerability within a Bayesian network-based multi-risk framework, while evaluating multi-hazard scenarios involving earthquakes and debris flows. The time-variant vulnerability of bridges to flood-scour and earthquakes is quantified in Guo and Chen (2016). Marasco et al. (2017) conducted a cascading hazard analysis while accounting for the effects of from a series of events – earthquake, blast and a fire - affecting the considered structure. Bonacho and Oliveira (2018) studied the interaction of tsunami and earthquake related damages and developed an additive function to estimate the aggregate damage from the two hazards. Similarly, often these studies (see Goda and Risi, 2017 etc) have not just looked at additive function but often have additive functions with an overlapping portion which is removed or classed as effects from both hazards.

While it is common to associate vulnerability with physical characteristics of elements as in the above studies, socio-economic, political and environmental vulnerability are also an important consideration under the threat of hazards. Figure 2 shows the Climate Change and Urban Vulnerability in Africa (CLUVA) framework for assessing vulnerability and a multi-risk framework should be able to consider these facets of vulnerability as well as their temporal variation. Zhang et al. (2013) presented a methodology to estimate vulnerability factors for the loss of life due to slides, rockfalls and debris flows that could occur either simultaneously or consecutively. A combination of physical and social vulnerability perspectives is adopted in Karagiorgos et al. (2016) as part of risk management for flash floods. Ciurean et al. (2013) presented a conceptual framework to account for the various facets of multi-vulnerability for reducing the impact from natural disasters. These methods present approaches and considerations that need to be applied while integrating multi-vulnerability aspects within the NPP risk assessment.

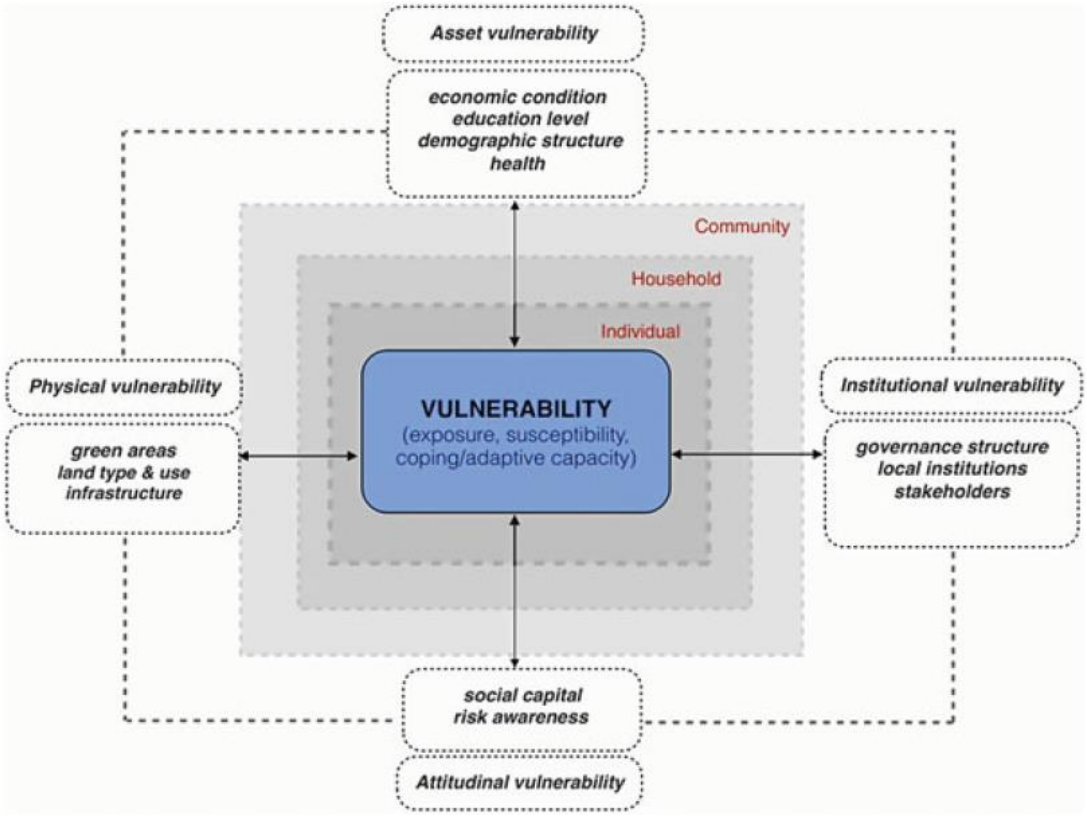

Figure 2: CLUVA framework for assessing social vulnerability (Jean-Baptiste et al., 2013)

3.2 Low probability events

One of the core objectives of the NARSIS project lies in better characterizing natural external hazards, considering external natural events, either simultaneous-yet-independent hazards or cascading events, and the correlation in intra-event intensity parameters. Such hazards, even individually, occur infrequently while their concomitance and the cascading of their effects are further rare. However, the effects of such low probability, high-impact events have occurred and have significant consequences. While the high consequences of these events warrant their quantification in risk assessments, the key challenge in characterising low probability events is the dearth of historical information that precludes the use of classical statistical techniques for predicting occurrence. These are also often termed as 'extreme events' in the literature, though not all extreme events are necessarily catastrophic in nature. Extreme events not only often have rarity and severity in common, but also tend to share characteristics such as high level of fear and uncertainty, and a notion of being involuntary (Slovic et al., 1979). Characterising low probability/extreme events presents the following challenges (Bier et al. 1999):

(i) Identifying potential extreme events: in many cases, extreme event scenarios that are being modelled are unknown. Systematic approaches such as the ones prescribed in Haimes (1981), Fiering and Kindler (1984), or Kumamoto and Henley (2000) are useful in determining all possible scenarios to minimise the changes of neglecting a possible extreme event;

(ii) Identifying the distribution of the parameter of interest: the parameter of interest may be: (a) part of the tail of a distribution of events – e.g. extreme river discharge is at the tail of distribution of river discharges; or (b) the entire distribution may be of interest – e.g. financial loss as a result of varying levels of flooding;

(iii) Specifying the probability distribution: in some cases a probabilistic approach may even be impractical given an extreme scarcity of data.

The following are some methods by which the data gap that exists due to the lack of knowledge and rare occurrences of these events is offset:

(i) Using a high safety factor in system design. However, this often adds complexity to the system, and makes it expensive.
(ii) Eliciting expert judgements in a structured manner (discussed later in Section 3.5)
(iii) Uncertainty analyses (discussed later in Section 3.6) including Monte Carlo (MC) simulations, use of evidence theory and imprecise probabilities, fuzzy logic approaches, and Bayesian theory applications.
(iv) Entropy maximisation based on information theory. The maximum entropy distribution is the least informative distribution that satisfies the specified constraints (Jaynes, 1996; Levine and Tribus, 1979). In other words, the least amount of information as possible is assumed over and above what is available. This distribution could be used, for instance, in a Bayesian approach as a prior distribution.
(v) Application of extreme value theory in cases where maximum values dominate the anticipated effects (Kinnison, 1983; Castillo, 2012). For example, flood risk can be well-handled using extreme value theory (e.g. Todorovic and Zelenhasic, 1970; Lamb et al. 2010).

Aven (2015) highlighted the need for current risk analysis methodologies to be extended to include black swan events, which are particularly relevant for NPP risk assessments that need to consider very low probability events. Pate-Cornell (2012) examined the issue of 'black swan' or 'perfect storm' events and emphasises that precursors often exists for such events. Monitoring of signals, identification of precursors and near-misses, and reinforcement of the system are prescribed to counter the threat from such low probability events. Au and Wang (2014) present simulation techniques for identifying small failure probabilities and Mignan et al. (2014) present a generic framework for assessing probabilistic risk using a sequential MC method (described in Section 3.7). They key advantage of the method is that it allows for identification of extreme, low probability scenarios that may result in catastrophic consequences. Khakzad et al. (2015) highlight techniques to focus on event precursors in pre-posterior analysis. Turati et al. (2017) propose an adaptive simulation framework to identify extreme, unexpected events within dynamic engineering systems. The approach uses a guided MC simulation within a semi-automatic framework such that prior user knowledge can be incorporated. A signal processing-based framework approach for identifying signs of critical slowdown in a system, which often leads to unforeseen events, is discussed in Damnjanovic and Aven (2017). Similar approaches could be considered for assessing NPP systems to identify black swan events.

In the NARSIS project, the identification of low probability events driven by external hazards and methods for modelling them are discussed in detail in Deliverable 1.1 (Daniell et al., 2018).

3.3 Complex systems

A complex system is defined by Guckenheimer and Ottino (2008), as a system with, besides interacting components, "a network that describes which components of the system interact, multiple scales of space and/or time, and symmetry. The components of many complex systems are heterogeneous and form a hierarchy of subsystems." Further, pervading uncertainty is a characteristic of complex systems, and its quantification and tracking are crucial in predicting and controlling the system (Guckenheimer and Ottino, 2008). Nuclear power plants are complex systems with several technical (sub-systems, structures, components), organisational and human aspects that interact within themselves and amidst each other. Such complex systems present a multitude of risks and their simultaneous modelling within a unified risk framework is at the least, a challenging task.

The consideration of the concept of complex systems is important because the understanding of system constituents does not imply an understanding of system behaviour (Heylighen, 2008). From just a purely physical point of view, system complexity arises from factors such as the variety of engineering materials used, their deterioration rates, compatibility and interaction between the various materials etc. (Garcia et al., 1996). If the functionality of the components, responses to external events, their interactions, organisational, social and human factors are added the complexity becomes immense. Majority of available risk assessment tools were developed for simple systems with several assumptions that complex systems would never meet.

Probabilistic Safety Assessments (PSA) have become standard of practice for complex engineering systems, but the success of the PSA will depend on the ability of the risk framework to capture the mathematical complexity of the system being modelled (Huh and Haldar, 2011). Garcia et al. (1996) introduced an integrated approach for risk management of complex engineering systems threatened by aging effects. They integrate PSA methodologies from the nuclear industry, with surveillance techniques, constitutive model development for aging of materials, and computational code modelling to manage risks of aging. In addition, life-cycle of complex systems is predicted and coupled with decision analysis concepts to manage risks. Ottino (2003) reviewed three major tools used for quantitative modelling of complex systems – nonlinear dynamics, agent-based models, and network theory. Amaral and Ottino (2004) highlight the need to use network theory to augment frameworks for assessing complex systems. Huh and Haldar (2011) present a hybrid seismic risk assessment framework for complex structural systems excited by dynamic seismic loading under a time domain. Borgonovo and Smith (2011) identify that most quantitative models used in risk-informed operation decision models for complex engineering systems are multilinear in nature, and hence, examine the potential for interactions amidst components by assessing interactions in multilinear functions. Their results are applied to space PSA efforts. Zio and Sansavini (2011) model cascading failures in critical infrastructure using simulations that account for physical characteristics of components and their interdependencies. Torres-Toledano and Sucar (1998) introduced the use of Bayesian networks for reliability modelling of complex systems. The advantages of using Bayesian Networks for risk assessments and decision making in complex systems are discussed in Weber and Simon (2016). Liu et al. (2016) present an extended object-oriented Bayesian Network approach for risk assessment of large scale complex, dynamic systems. Fuzzy Cognitive Maps (FCM) is used to develop an integrated decision support tool for dynamic risk assessment of complex systems in Jamshidi et al. (2018). This FCM-based approach prioritises various risk factors, isolates their contribution to overall risk and their influence on other risk factors, while also capturing the interdependencies between risk factors. Haimes (2018) summarises the theory and implementations of risk modelling for complex system of systems.

3.4 Human and organisational aspects

The literature contains several definitions of ‘human and organisational factors’. From a risk and safety assessment purview ‘human and organisational factors’ can be defined as ““environmental, organizational and job factors, and human and individual characteristics that influence behaviour at work in a way that can affect health and safety” (HSE 1999). People have a significant impact in accident causation and system safety (Saleh et al., 2010). During the Fukushima-Daiichi accident in 2011, ‘human error’ was identified to play a crucial part in the development of adverse situations (Hollnagel and Fujita, 2013). According to Nivalianitou et al. (2006), well over a third of petrochemical industrial accidents and equipment failures occur due to human factors. It has also long been acknowledged that human factors play a key role in response to extreme situations in complex facilities. It was in recognition of this fact that methods such as THERP (Swain and Guttman, 1983), HEART (Williams, 1986), SLIM-MAUD (Embrey et al., 1984), ATHEANA (Cooper et al. 1996), CREAM (Hollnagel, 1998), TRACEr (Shorrock and Kirwan, 2002), HET (Marshall et al., 2003) and IDAC (Chang and Mosleh, 2007 a, b & c) have been developed to analyse and predict human error. Such

methods are often based on Human Reliability Analysis (HRA) concepts and have been widely applied in industrial environments. Another angle that has been notably explored has been the effect on human error/reliability due to introduction of changes, particularly digital updates from improving technology (O'Hara et al., 1996; Sarter et al., 1997; Lee and Seong, 2005; Niwa and Hollnagel, 2002; Sarter et al. 2007; Lee et al. 2011, Li et al., 2018). It is mostly insufficient, however, to look at human error exclusive of management structures that surround personnel in complex industrial facilities.

A directly linked subject to human factors has been organisational factors that contribute to overall risk. A host of methodologies have been prescribed for quantifying organisational factors such as Manager (Pitbaldo, 1990), MACHINE (Embrey, 1992), SAM (Paté-Cornell & Murphy, 1996), WPAM (Davoudian et al., 1994 a&b), I-RISK (Bellamy et al, 1999), Omega Factor Model (Mosleh and Golfeiz, 1999), ORIM (Øien, 2001), ARAMIS (Hourtolou and Salvi, 2003), ASRM (Luxhoj, 2004), BORA (Sklet et al., 2005). Most or all of these methods tend to focus on "deviation from normative performance" rather than realistically modelling organisational and human behaviours (Rasmussen, 1997). Within the NARSIS framework, any of the above listed methods may be of use in modelling human error, but the impact of organisational factors needs to be coupled with the consideration of human error. Also, more recent methods, reviewed below, focus on underlying functions and mechanism in an organisation that impact accident scenarios and modelling of human behaviour under these conditions.

Biondi (1998) examined the organisational factors that affect the reliability of offshore systems and proposed a qualitative framework based on the Complex Adaptive Non-Linear (CANL) model. Cook (2004) and Leveson (2004) both used System Dynamics (SD) concepts to model organisational factors that impact safety of engineering systems. Leveson (2011) uses system theory and control theory to establish a model for jointly assessing social and technical aspects while accounting for their interactions. Performance shaping factors (PSFs) have been identified and developed for use in Human Reliability Analysis or within risk frameworks for NPPs (Groth and Mosleh, 2009; Liu et al., 2017).

While the above listed methods all look to analyse human error and organisational factors, their integration into PSAs is a challenge either because the tools/results do not allow for direct integration into other risk frameworks or a clear integration methodology does not exist. In this regard, Mohaghegh and Mosleh (2009) present the SoTeRiA framework for merging the system risk model with organisational root causes. Mohaghegh et al. (2009) provide a framework for choosing from available techniques, both probabilistic and deterministic, and merging their uses in a hybrid approach. They provide an example that fuses SD, Bayesian Networks (BN), Event Sequence Diagrams (ESD) and Fault Tree (FT) methods, and can be used to incorporate organisational factors into PSAs of complex facilities. Along similar lines, Kazemi et al. (2017) describe a two-level methodology first using SD, followed by BN to model risks of adverse events in health-care facilities. The model captures the feedback of organisational factors, their non-linearity and the impact of decisions over time. Perhaps, one of the most relevant studies to the NARSIS context is the Causal Model for Air Transport Safety (CATS) method that models human and organisational factors within a BN framework using PSFs. The CATS model integrates deterministic techniques with the BN, including human performance models (HPM) to calculate overall accident probability. Wang et al. (2011) performed a probabilistic study for offshore fire accidents using a fault tree approach that is converted to a BN to incorporate human and organisational factors. Garcia-Herrero et al. (2013) performed a BN analysis for evaluating the safety and organisational culture in a NPP. Mkrtchyan et al. (2015) summarise the advantages and applications of BNs in HRA for risk analysis. However, the gaps in application and the need for better integration of human aspects (cognitive models, empirical data and expert judgement) within the risk framework are also highlighted. Musharraf et al. (2013) model the dependency between human factors using BNs. The Bayesian approach for evaluating HEP is compared with results from the analytical SLIM approach. Grozdanovic (2015) further demonstrates the use of SLIM for human reliability quantification.

Hence, the above listed methods or their modifications/combinations are relevant for use in the NARSIS project provided the modelling of human error considers the impact of organisational factors and underlying mechanisms influencing human behaviour. The method must also be integrable with the overall risk framework used for multi-risk modelling.

3.5 Expert judgement

As discussed earlier, risk analyses that try to model extreme events of low probability are handicapped by the fact that there is not enough data regarding these events to perform a Classical Statistics-based evaluation of risk. Simulating experiments to reflect any such scenarios can be either too impractical, complex, dangerous or prohibitively expensive. This leaves a large uncertainty with our risk models and the succeeding decision making. One widely accepted way to offset this data gap is to rationally quantify and manage this uncertainty by including expert judgement.

An expert is "a person who has a background in the subject matter at the desired level of detail and who is recognised by his/her peers or those conducting the study as being qualified to solve the questions" (Meyer and Booker, 1991). Another definition reads: "a person with substantive knowledge about the events whose uncertainty is to be addressed" (Ferrel, 1994). O'Hagan et al. (2006) issue a caveat – "A simple conception is that an expert is someone who has great knowledge of the subject matter. However, expertise also involves how the person organises and uses that knowledge." It is also common to use the opinions of multiple experts to improve accuracy and reduce the impact of specific skewed opinions or biases in selection of experts. The critical factor in expert elicitation though, comes with structured collection of information that allows it to be used as scientific data while ensuring accountability, neutrality, fairness, and the ability for empirical control (Cooke, 1991).

Morgan and Henrion (1990), Cooke (1991) and O'Hagan et al. (2006) provide the most detail with respect to expert elicitation. Clemen and Winkler (1999) reviewed various methods – 'behavioural' and 'mathematical' - to convert expert judgements into probability distributions needed for risk assessments. "Behavioural" techniques, like the Delphi method, Nominal Group Technique, and an aggregation method by Kaplan (1992), typically require interactions within the group of experts where they may agree on an output probability distribution or merely exchange ideas. "Mathematical" techniques attempt to integrate expert opinions into a probability distribution through either axiomatic approaches like the Linear Opinion Pool, the Logarithmic Opinion Pool, a combination of these two methods (Cooke, 1991); or Bayesian approaches. Cooke et al. (1988) proposed a mathematical methodology of rating experts based on the performance of their opinions compared to empirical data. Such an approach has been termed as the "Classical Model" where experts answer 'target questions' for which insufficient data is available, along with 'calibration questions' for which the analyst has data, typically inaccessible to the experts (Cooke, 1991). The performance of the experts on the calibration questions and all their assessments are weighted accordingly while combining them. The combination is scored based on the calibration questions as well, thus validating both individual opinions but also that of the group. While Cooke (1991) originally prescribed using a linear opinion pool for combining opinions and weighting them based on performance ratings, other combining and weighting methods have been considered (Cooke et al., 2008; Burgman et al., 2011; Aspinall and Cooke, 2013, Hora et al., 2013). Cooke and Goosens (2008) publicly released forty-five applications of the Classical model. This public dataset was later used to assess the effects of overconfidence on the accuracy of expert judgement (Lin and Bier, 2008; Lin and Huang, 2012). Clemen (2008) examines the Classical Model and assesses if the weighting scheme used impacts the honesty of experts, and also evaluates its performance out-of-sample. Colson and Cooke (2017) present a case study of the use of the Classical Model for risk management of invasive species in the U.S. Great Lakes along with thirty-three applications of the model, reviewing both expert performance and methods used to combine and validate their judgements.

Apart from the Classical Model, other methods have been suggested for expert elicitation. The Expected Relative Frequency model is prescribed that is based on the proximity of central values from expert opinion and known information as part of the calibration dataset (Flandoli et al., 2011). The IDEA protocol is a more recent structured expert elicitation method shown in Figure 3 that attempts to combine mathematical and behavioural approaches to estimating probability distributions from expert opinion (Burgman, 2015; Hemming et al., 2018; Hanea et al., 2018).

Dubois and Guyonnet (2011) focus on recommendations of elicitation methods and steps have been examined for specific risk assessment tools like the BNs, particularly for obtaining expert judgement on node dependencies (Wang 2006; Dalton et al., 2012; Zhang and Marsh, 2016; Gerstenberger and Christophersen, 2016; Renooij, 2001; de Waal et al., 2016).

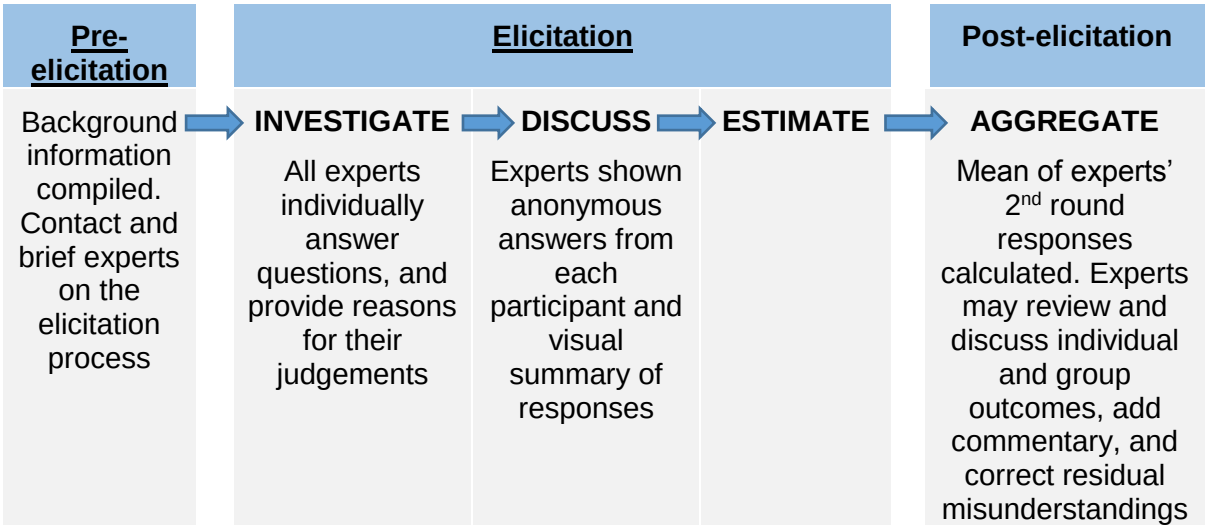

Figure 3: IDEA protocol overview (Hemming et al., 2018)

Prior to applying any of the above methods, or even eliciting expert opinion it is mandatory to assess the need for expert judgement. If sufficient data and consensus on the subject are available or if outcomes are highly behaviour-dependent, expert elicitation should likely be avoided (Hora, 2007; Morgan, 2014). This is because the key objective of using expert opinion is to manage uncertainty in the risk assessment, but not add to it. Nevertheless, the uncertainty analyses applied to other parts of the PSA need to be considered for expert judgements as well.

3.6 Uncertainty

The literature contains several definitions for uncertainty. One of the simpler definitions is provided by Walker et al. (2003) – "incomplete information about a particular subject." Some of the more specific definitions tend to be relatively narrowly applicable to particular situations or fields of study. From the perspective of NPP risk, uncertainty analysis forms a crucial part of probabilistic safety or risk assessments (PRA) for the power plant. ASME defines uncertainty as "representation of the confidence in the state of knowledge about the parameter values and models used in constructing the PRA" (ASME, 2009). Uncertainty within an NPP risk assessment, applies to qualitative and quantitative aspects. Similarly, it pertains to probabilistic and deterministic features of all hazards and vulnerabilities considered.

3.6.1 Taxonomy of uncertainty

Several approaches exist for uncertainty analysis, but a common first step is to classify uncertainties based on the nature of its source. The most widespread classification is the distinction of aleatory and epistemic uncertainties. Aleatory uncertainty is associated with the

inherent randomness within the data used in the risk model, while epistemic uncertainty stems from incompleteness or imprecision in data or inadequacy of model. A classification of sources of uncertainty is given in Table 1.

Table 1: Taxonomy of sources of uncertainty (Rohmer et al., 2012)

Type of uncertainty	Main underlying causes
Aleatory uncertainty	Inherent variability (temporal or/and spatial)
Epistemic uncertainty - data	Measurement errors, representativeness of the samples, bias in the measurement process.
Epistemic uncertainty - parameter	Incompleteness and imprecision of observations, experts' judgments (vagueness, conflicting views).
Epistemic uncertainty - model	Structure, several choices of "good" models.
Epistemic uncertainty - scientific	Ignorance, indeterminacy, immeasurability, conflicting evidence.

In addition to the above classifications of uncertainty sources, Varde and Pecht (2018) present what they refer to as subjective/cognitive uncertainties, within their Integration Risk-Based Engineering (IRBE) approach. Figure 4 shows their proposed taxonomy for uncertainty. The moral component of subjective uncertainty stems from the deterioration in ethical or moral provisions such as guidelines and pledges, or the development of unethical situations. The judgement/rule driven uncertainty arises from imprecise knowledge of rules, ambiguous or blurred guidelines that leads to the use of intuition or interpretation.

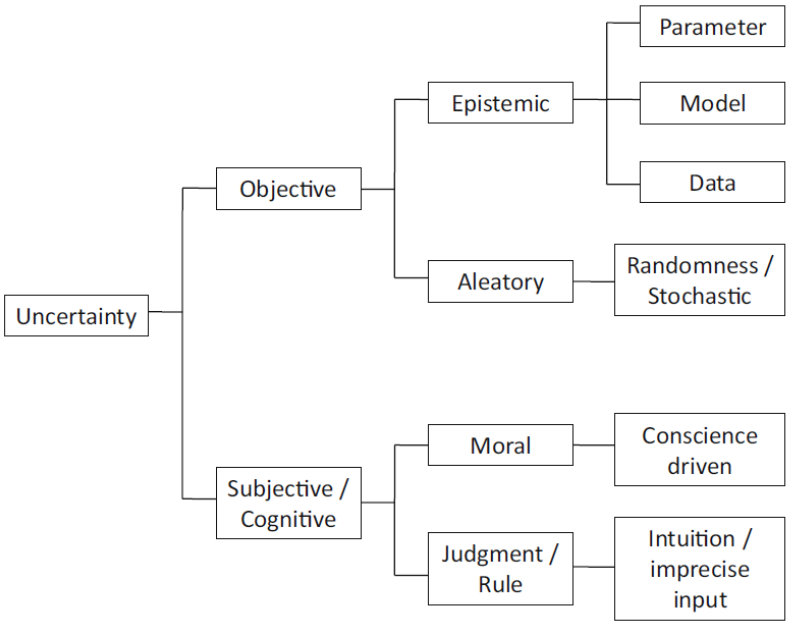

Figure 4: Taxonomy of uncertainty adopted for IRBE (Varde and Pecht, 2018)

3.6.2 Uncertainty within risk assessments

Within the PSA framework for NPPs, relatively more data is typically available for internal physical components while significant uncertainty stems from the characterisation of external events and social/organisation aspects. Every step within a risk assessment contains its sources of uncertainty that affect the overall uncertainty of the risk assessment results. At the hazard level, uncertainty assessments for single hazards have been studied extensively (e.g. Abrahamson, 2000; Merz and Thieken, 2005, 2009; Straub and Schubert, 2008; Marzocchi et al., 2004). For single hazards, uncertainties are associated typically with their source, propagation, and the estimation of hazard within spatial limits of interest. Further uncertainty comes at the vulnerability level with respect to the characterisation of elements under risk,

their damage types and extent, and finally, with the estimation of loss from damages. Under a multi-risk framework, further uncertainties arise at the hazard level due to the consideration of cascading effects where there is uncertainty in both the extent of interaction and impact between hazards. At the vulnerability level, there is uncertainty in element response to one hazard due to the accumulated effects from another. Uncertainty sources for various cascading scenarios and interactions at the vulnerability level are summarised in Vangelsten et al. (2013). Volkanovski (2015) analysed the introduction of probability distributions for component unavailability and its impact on the overall unavailability of the system being analysed within the PSA framework. A fault tree analysis was used to track the propagation of uncertainty, and results showed that the probability distribution of the top event depends on the unavailability characteristics of basic events and the importance of chosen events.

3.6.3 Quantification and propagation of uncertainty for a multi-risk approach

Methods are prescribed in the literature that are suited to modelling uncertainty within a risk analysis, particularly suited to multi-risk approaches. The most prevalent method is of course, to use a probabilistic approach – either frequentist or Bayesian (Pate-Cornell, 1986; Nilsen and Aven, 2003) – where distributions are assigned to model the occurrence of events. The frequentist approach relies on the presence of data for the hazard or element under consideration, whereas the Bayesian approach uses a subjective probability where the 'prior belief' in an event can be updated based on posterior evidence (Sui and Kelly, 1998). MC simulations are widely used to model uncertainty as they allow for consistent tracking of uncertainties with input parameters and transformation models. Latin Hypercube methods are as well widely used for uncertainty propagation along with MC simulations (Helton and Davis, 2003). Another approach is the use of 'imprecise probabilities' under evidence theory for uncertainty modelling (Dempster, 1967; Shafer, 1976; Caselton and Luo, 1992, Limbourg and Rocquigny, 2010). Structural reliability modelling has often used the response surface method or the first-order reliability method (FORM) (Cizelj et al., 1994). Where prior assumptions of distributions cannot be made (nonparametric tests), bootstrap approach or Wilk's method may be used. When variables tend to comprise imprecise ideas or semantic notions, a fuzzy logic approach is often adopted (Zadeh, 1965).The MOVE (2010) EU project recommends a set of approaches for uncertainty propagation based on available input data and quantification methods used (Figure 5). Within the NARSIS project expert judgement, MC simulation and Bayesian theory-based approaches to handling uncertainty are likely to be most applicable.

			Type of Input data		
		Column	A	B	C
	Row		Qualitative	Semi-Quantitative	Quantitative
Method	1	Implicit	Expert judgement Qualitative scenario analysis	Fuzzy logic Bayesian theory/networks NUSAP (Numerical, Unit, Spread, Assessment and Pedigree)	Fuzzy logic Bayesian theory/networks
	2	Explicit	Appropriate input data ranking procedure Monte-Carlo simulation Fuzzy logic NUSAP (Numerical, Unit, Spread, Assessment and Pedigree) Expert judgement	Monte-Carlo simulation Fuzzy logic NUSAP (Numerical, Unit, Spread, Assessment and Pedigree) Expert judgement Possibility theory and hybrid methods	Monte-Carlo simulation First-order second moment First-order reliability method NUSAP (Numerical, Unit, Spread, Assessment and Pedigree) Expert judgement

Figure 5: Recommended approaches for uncertainty propagation (MOVE, 2010)

3.7 Multi-risk frameworks – state-of-the-art

An important feature of multi-risk frameworks is the harmonisation of various hazards in time, space and in terms of a common loss metric (Garcia-Aristizabal et al., 2015). Harmonisation over time is achieved typically by defining a common time interval that is used in hazard estimation. Over space, the hazards are harmonised by the consideration of both the spatial resolution of hazards as well as the spatial distribution of vulnerable elements. Finally, by using a common loss metric determined by the problem at hand, the risk from various sources is harmonised to provide common grounds for comparison. Some state-of-the-art implementations of multi-risk approaches that have integrated the previously discussed multi-hazard, multi-vulnerability, and other risk assessment perspectives to varying degrees, and have harmonised risks from various sources with a focus on external natural events, are summarized below. As part of the discussion of these multi-risk frameworks, software packages implementing multi-hazard risk analysis have been mentioned – HAZUS, CAPRA, RiskScape, and CLIMADA. The details of implementation of these programs are beyond the scope this report. However, some of these programs have been evaluated and their scopes and methodologies have been detailed in the literature (e.g. Daniel et al., 2014).

The Central American Coordination Centre for Disaster Prevention (CEPREDENAC), in collaboration with Central American Governments, the United Nation's International Strategy for Disaster Reduction (ISDR), the Inter-American Development Bank and the World Bank together developed CAPRA, a GIS-based tool for probabilistic risk analysis. CAPRA allows for some consideration of multi-hazards and dependency in the fact that it considers primary events (earthquakes, rainfall and hurricanes) which could lead to cascading hazards (tsunami, landslides, and floods) (Bernal, 2010).

HAZUS, a GIS-based tool was developed by the Federal Emergency Management Agency to estimate losses – damages to buildings, economic losses and social impacts – from individual hazards, particularly, floods, hurricanes and earthquakes (FEMA, 2011). This method does not account for dependencies and cascading effects between hazards and does not consider multi-vulnerability.

Schmidt et al. (2011) developed a quantitative framework for modelling multi-risk through the software package RiskScape. The framework functions are not dependent on the nature of hazards and vulnerabilities of elements, but instead standardise the hazards, exposed elements and their fragility functions to evaluate the risk. Figure 6 shows the four main modules within the framework - hazard, asset (elements), loss (vulnerability), and aggregation – and the methodology adopted in RiskScape for calculation of overall risk. The steps include: (i) overlaying assets and hazards to evaluate the affected assets, (ii) using fragility functions to calculate relative asset losses, (iii) applying asset evaluations to calculate absolute value of losses, (iv) probabilistic calculation of time-averaged losses, (v) averaging risk spatially using the aggregation module. This framework considers multi-hazard multi-risk quantitatively, but does not account for cascading effects or multi-vulnerability interactions.

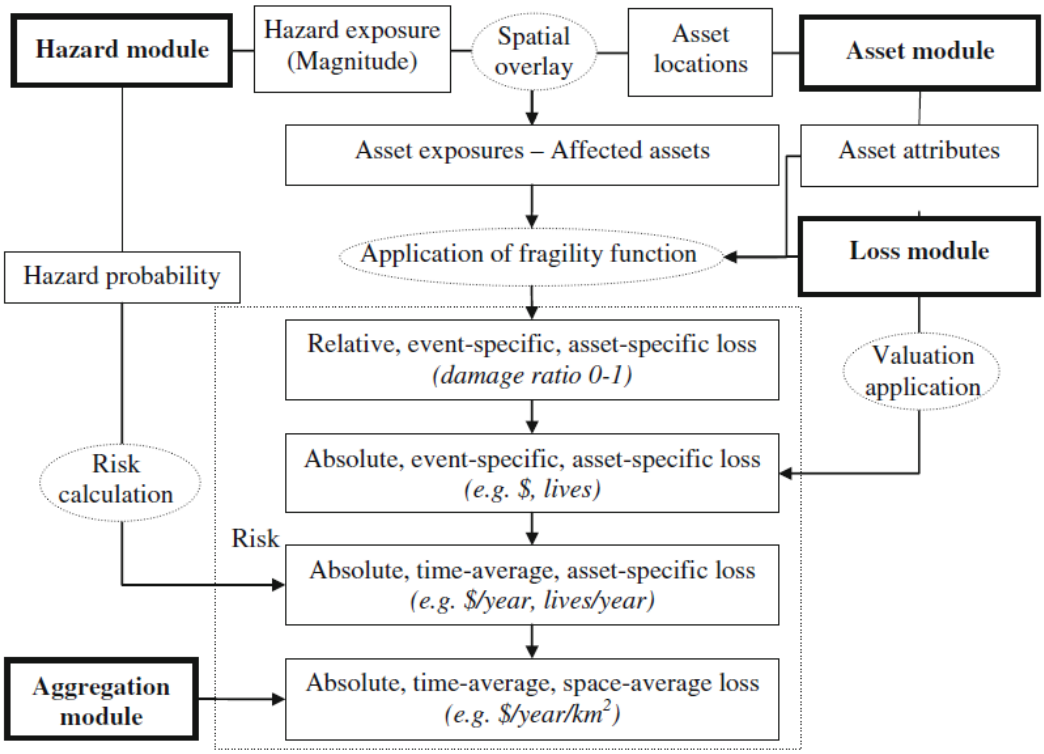

Figure 6: Generic risk calculation framework in RiskScape (Schmidt et al. 2011)

Important concepts and principles of multi-risk assessment are introduced in Marzocchi et al. (2012), where hazard interaction and cascading effects are considered. The multi-risk schematic introduced in this study was presented earlier in Figure 1. A case study of the Casulnuovo municipality in Italy (based on Marzocchi et al., 2009) is considered with special focus on harmonisation of individual risks from various hazards along with the quantification of their interaction. For example, a specific case is considered where volcanic ash accumulation, triggering a pipe-bridge collapse inside an industrial area that further triggers an explosion, which in turn contaminates air and water. The overall risk estimation showed that not considering the cascading impacts of even a relatively minor volcanic risk, can significantly underestimate the industrial risks in the region. Other hydrogeologic risks such as flooding and landslides are also considered for the Casulnuovo municipality area.

Nadim et al. (2013) developed a three-level theoretical framework as part of the MATRIX project, for multi-risk analysis while accounting for interactions between the hazards. Figure 7 shows the outline of the multi-risk framework. The first level (Figure 8) comprises a quantitative flowchart that the end-user can use to decide if a multi-risk approach, involving considerations for cascading hazards and dynamic vulnerability in reference to conjoint or cascading hazards, is required. This is followed by a semi-quantitative second level (Figure 9) of analysis to examine further the need for a detailed multi-risk approach. Finally, at the third level, a quantitative multi-risk analysis is carried out using BNs (this is discussed further in Section 6.4.1). The key aspect of this three-level framework is that it allows for quantification of cascading effects and multi-vulnerability aspects discussed earlier. Case studies of (i) debris flow triggered by earthquakes and rainfall and (ii) volcanic eruption or tectonic seismic activity are also carried out. Further details on the harmonisations of hazards, vulnerability interactions and implementation of the risk assessment can be found in Nadim et al. (2013) and Liu et al. (2015). Multi-risk analyses using BNs are explored further in this deliverable and will be used in NARSIS project.

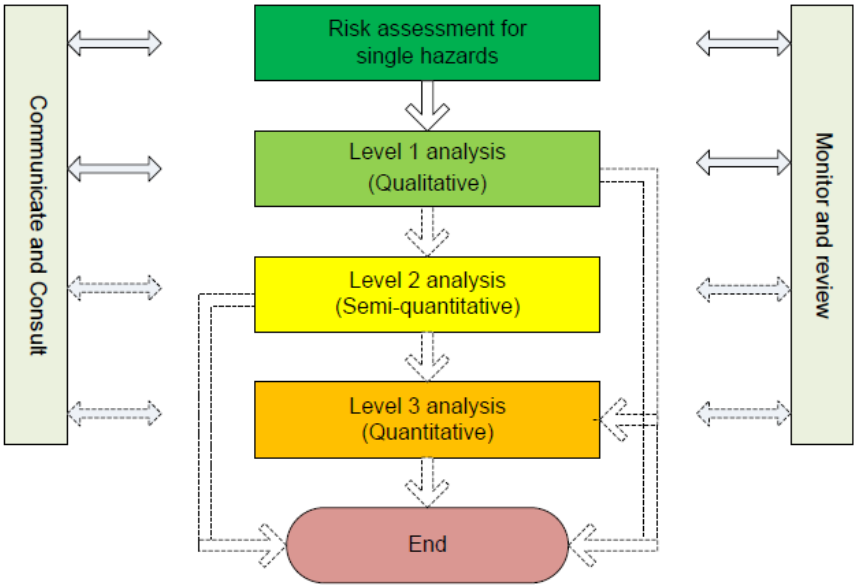

Figure 7: MATRIX multi-risk assessment framework (Nadim et al. 2013)

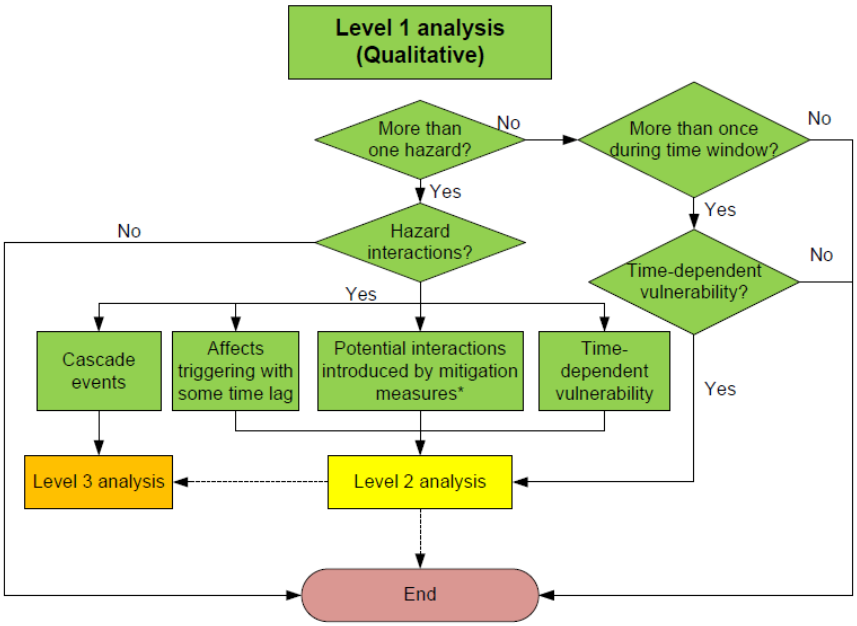

Figure 8: Level 1 of three-level multi-risk framework (Nadim et al., 2013)

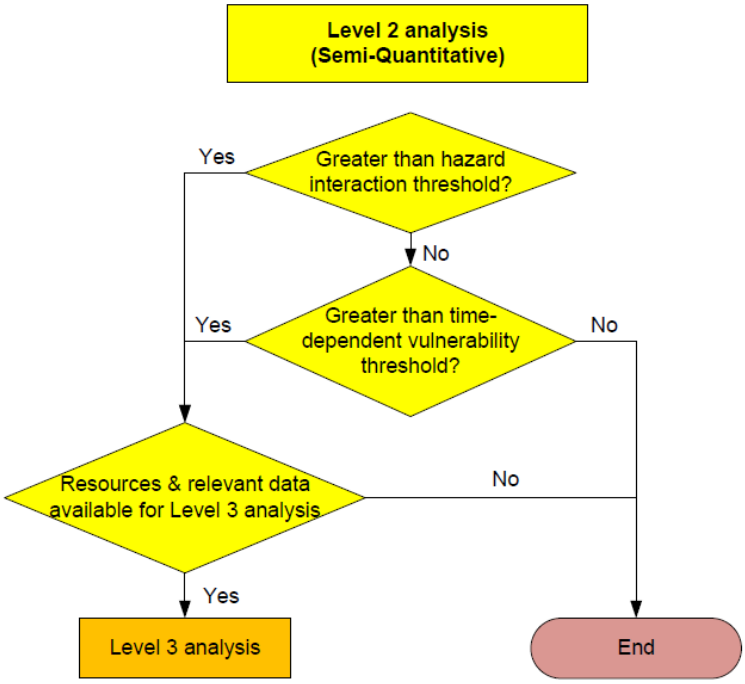

Figure 9: Level 2 of three-level multi-risk framework (Nadim et al., 2013)

As discussed above, multi-hazard and multi-vulnerability are linked to quantifying hazard interactions and cascading effects. For this purpose, Mignan et al. (2014) present a generic framework for assessing probabilistic risk using a sequential MC method. The objective of this study was to create a framework to model hazard interactions and time-dependent vulnerabilities, independent of the problem type. This is achieved by firstly generating N_{sim} time series by sampling events from a Poisson distribution, and one risk scenario is assigned to each time series. Probabilistic analyses of these scenarios aid in identifying likely risk paths. The stochastic events within the MC method correspond to hazard events with an occurrence rate (λ) and estimated loss parameter (Λ)(related to hazard intensity), while each event also corresponds to a given source. Event identifiers and occurrence times (say, ranging from t_0 to t_{max}) are added to the simulated dataset to capture hazard interactions. This is done by tracking the characteristics of an event j that occurs at a given time, t. Relevant events k are resampled between times t to t_{max} provided the conditional probability $P(k|j)$ exists. The concept of hazard correlation matrix also is introduced in this study, in which these conditional probabilities are stored. The process is iteratively repeated until t reaches t_{max}. Thus, interacting hazard events within the multi-hazard framework are accounted for in this manner (Figure 10). As for multi-risk, the simulation sets are now appended with loss values for each event. Time-variant vulnerability is accounted for using the following equation (Mignan et al., 2014):

$$E_i = E_0 - \sum_{i=1}^{i} \delta_i E_{i-1} + e_i \qquad \text{Equation 1}$$

where E_0 is the original exposure, E_i is the exposure of the system immediately after event i, δ_i is the damage ratio associated with event i, and e_i is a function giving exposure reconstruction until event i occurs. In general, the loss from a risk scenario, $\Lambda = \delta E$. Hence, since exposure now varies with time, the loss risk scenarios also vary temporally. Edge-case scenarios for Equation 1 are instantaneous reconstruction ($e_i = \Sigma\Lambda i$) with $E_i = E_0$ and no reconstruction ($e_i = 0$) with $0 \leq E_i \leq E_0$. A conditional mean damage ratio $\delta_{j|i}$ is suggested for the impact of event clustering on vulnerability. The study does not consider the temporal variation of vulnerability itself in the form of time variant damage ratios.

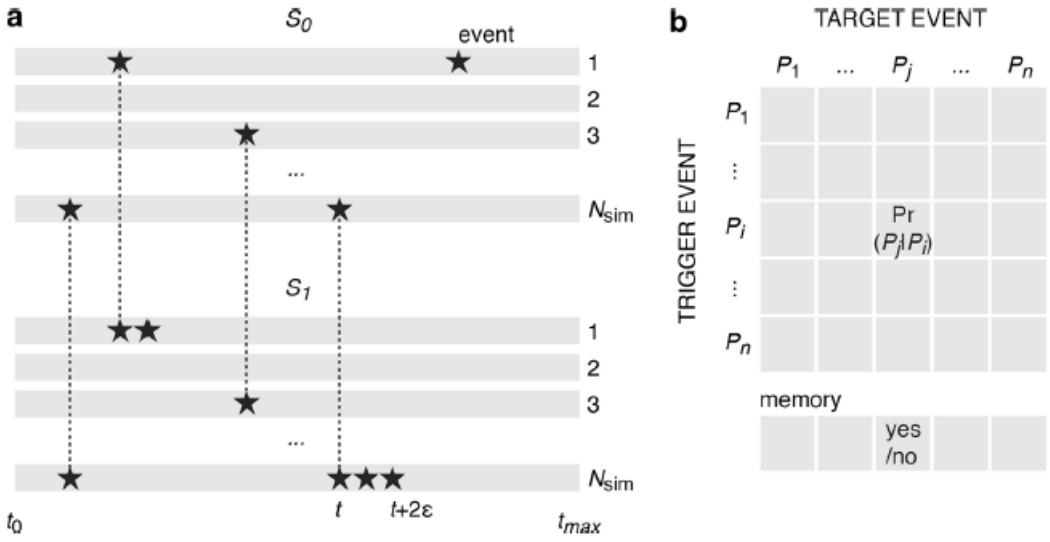

Figure 10: Generic multi-risk framework (multi-hazard part).

"a. Sequential MC [method]: the simulation set S_0 represents the null hypothesis H_0 of having no interaction in the system, while set S_1 represents any multi-risk hypothesis. Grey rectangles represent different simulated time series. b. Concept of hazard correlation matrix: trigger events are represented in rows *i* and target/triggered events in columns *j*. A given peril *P* consists of *n* events P_i with $1 \leq i \leq n$. Each cell of the square matrix indicates the 1-to-1 conditional probability of occurrence $P_r(P_j \mid P_i)$ over Δt, which is used as input in the MC [method]. The n-to-1 conditional probability is considered by incorporating a memory element to the correlation matrix. The proposed approach can be seen as a variant of a Markov chain" (Mignan et al., 2014).

Garcia-Aristizabal et al. (2015) present a refined three-level-analysis methodology, in agreement with the MATRIX project framework, for harmonizing risks from various sources, quantifying the combined risk and translating it to information used for decision-making under uncertainty. Figure 11 shows the proposed three-level analysis. The potential physical damages are evaluated within level 1. The expected losses from the physical risk are calculated from the quantitative form for a single risk (Cornell and Krawinkler, 2000 - Equation 2) and correspondingly for *i*th hazard (Equation 3):

$$\lambda(l) = \int_D \int_{I_m} F(l|D) dG(D|I_m) d\lambda(I_m, \Delta t) \qquad \textit{Equation 2}$$

$$L_p^i \equiv \lambda(l) = \int_D \int_{I_m} F(l|D) dG\left(D\middle|I_m^i\right) d\lambda(I_m^i, \Delta t) \qquad \textit{Equation 3}$$

where L_p^i is the loss assessment considering the i^{th} hazard and integration of contributions from all exposed elements (consideration of multi-vulnerability), $\lambda(l)$ is a measure of exceedance rate of a given amount of loss, D is a damage state, $F(l|D)$ is the conditional probability that the considered loss level occurs given that the damage state has been reached, $\left(D\middle|I_m^i\right)$ is the measure of fragility (or vulnerability) given that a certain intensity measure is reached for the i^{th} hazard, and $\lambda(I_m^i, \Delta t)$ measures the rate of exceedance of the hazard above a given intensity measure within the considered time interval, Δt. The approach in Equation 3 can be applied in NPPs, for example, to quantify the losses from various systems, structures and components exposed to say, flooding risks. Within level 1, the hazards are spatially (resolution of both hazard assessment and inventory of exposed elements) and temporally (through time period in hazard assessment for estimating rate of occurrence) harmonised. Also, a common loss metric is chosen that allows for comparison and integration of risks from different exposed elements. This is followed by an assessment of the hazard interactions, particularly identification of the most critical interaction scenarios which are likely to accentuate the losses. This could be done for instance, using a fault tree

or an event tree or a combination. The possible interactions of interest are those which provide a higher cumulative effect than a mere sum of losses from individual risks. As discussed earlier in Sections 3.1.1 and 3.1.2, interactions can happen both at the hazard and vulnerability levels. At the hazard level, the probability of occurrence of a triggered event (event 2) conditional on the triggering event (event 1) is given by (Gasparini and Garcia-Aristizabal, 2014):

$$p\left(\geq IM_2^i\right) = \sum_j p(\geq IM_2^i \left| IM_1^j \right) p(IM_1^j) \qquad \textit{Equation 4}$$

for *j* = 1, 2, 3…, *n*, where *n* is the number of mutually exclusive classes of intensity measure *IM* for the triggering event. The interactions accounted for at the vulnerability level are aligned with the multi-vulnerability viewpoint - they are associated with the quantification of changes to damage levels of elements already exposed to a given hazard, in the case that another hazard(s) occurs simultaneously or shortly after. Assuming events 1 and 2 have occurred at intensity measure values of *i* and *j*, the probability that a given damage state (D_k) is exceeded is (Garcia-Aristizabal et al., 2013; Gasparini and Garcia-Aristizabal, 2014):

$$P(D_k) = \sum_i \sum_j [p(D_k | \, IM_1^i \cap IM_2^j) p(IM_1^i \cap IM_2^j) \qquad \textit{Equation 5}$$

using which all events, dependent or independent, can be accounted for.

Indirect losses due to various socio-economic contexts are considered in level 2. The key aspect of this step is that the losses from these non-physical contexts, once identified, are directly estimated in the same metric as in the first level using the intensity footprint of hazards in the target area. This allows for easier integration with level 1 results.

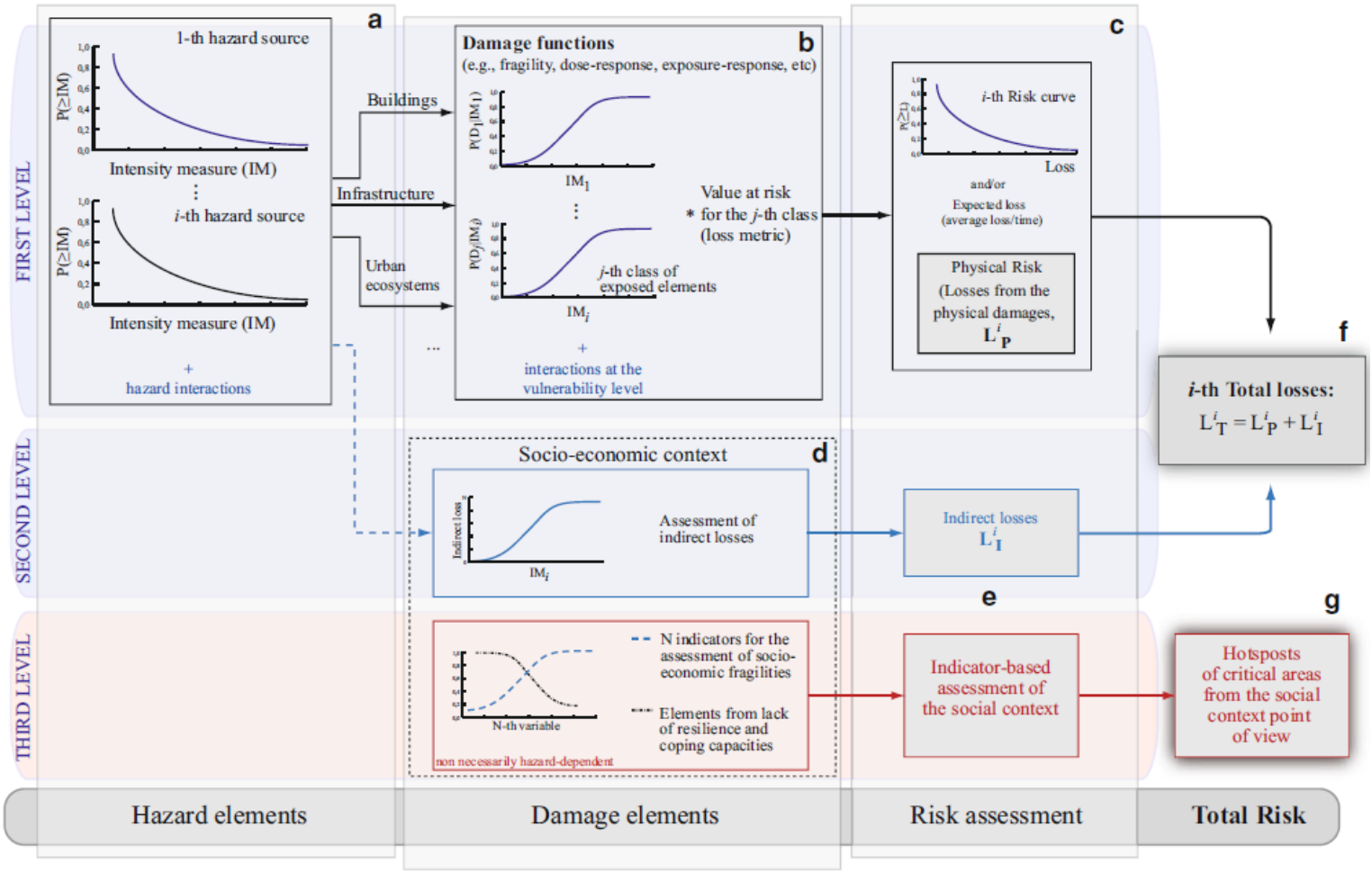

Figure 11: Schematic representation of three-level multi-risk from Garcia-Aristizabal (2015)

"Level 1 (a, b, c) is related to physical risks. Level 2 (d, e) is associated with the evaluation of relevant socio-economic contexts and their contribution to total indirect losses, and integration with level 1 results (f). In level 3, relevant socio-economic contexts are considered using an indicator-based approach".

Finally, in level 3, socio-economic contexts are applied in an indicator-based approach, i.e. estimation of an ad hoc index using a predefined set of indicators that characterise the context. The chosen indicator typically reflects intrinsic parameters that curb adverse responses during an event or limit worsening of the situation. Typically, information integrated at this level is subjective and hence, the quantification of the indicators or formulation of the index is not standardised. A specific strategy needs to be implemented for the quantification and normalisation of this index. Nevertheless, such indices (e.g. social fragility index) can be useful in characterizing the relevant socio-economic context. For example, the percentage of very young and very old people within the total population can be an indicator, and the spatial distribution of the resulting index can highlight areas where the impact from an event are likely to be magnified or the recovery afterwards may be more complex. Finally, the authors implement the three-level framework in a pilot case study for the city of Dar es Salaam, Tanzania.

Chen et al. (2016) examine the specific problem of multi-hazard risk assessment for rainfall-induced slope failures and debris flows. Rather than using a generic multi-risk framework, the authors develop a physical-based model for assessing the risk from these two hazards for a highway near Wenchuan, China. A grid system composed of a large number of cells is formulated for the study area. Relevant physical properties within each cell and the inter-cell movements of material are analysed. Figure 12 presents the framework used for multi-risk assessment. There are five main steps in the implementation of this risk model (Chen et al., 2016):

(i) The terrain of the study area, in digital form, is divided into cells of optimal size. Each cell is associated with the relevant physical properties chosen in the study – geology, topography, soil properties, hydrological properties and groundwater table.
(ii) The initial pore-water pressure profile is developed using an antecedent rainfall rate (prior to the rainfall event) after the rainfall model is assigned specially to each cell.
(iii) The spatial rainfall distribution is used to develop pore-water pressure profiles for each cell across time. This allows for stability calculation at each cell along with estimation of material movement and deposition.
(iv) The debris flow simulation module is used to estimate the probability of debris flow, its volume, area of impact, and impact on vehicles.
(v) The multi-risk quantitative module estimates the contribution of rainfall-induced slope failures to debris flow and estimates the consequences of such scenarios to the study area, including risks to travellers on the adjacent highway.

Hence, this framework models multi-hazard for a pair of hazards by estimating the cascading effect of one hazard on the other, using a physical-based model.

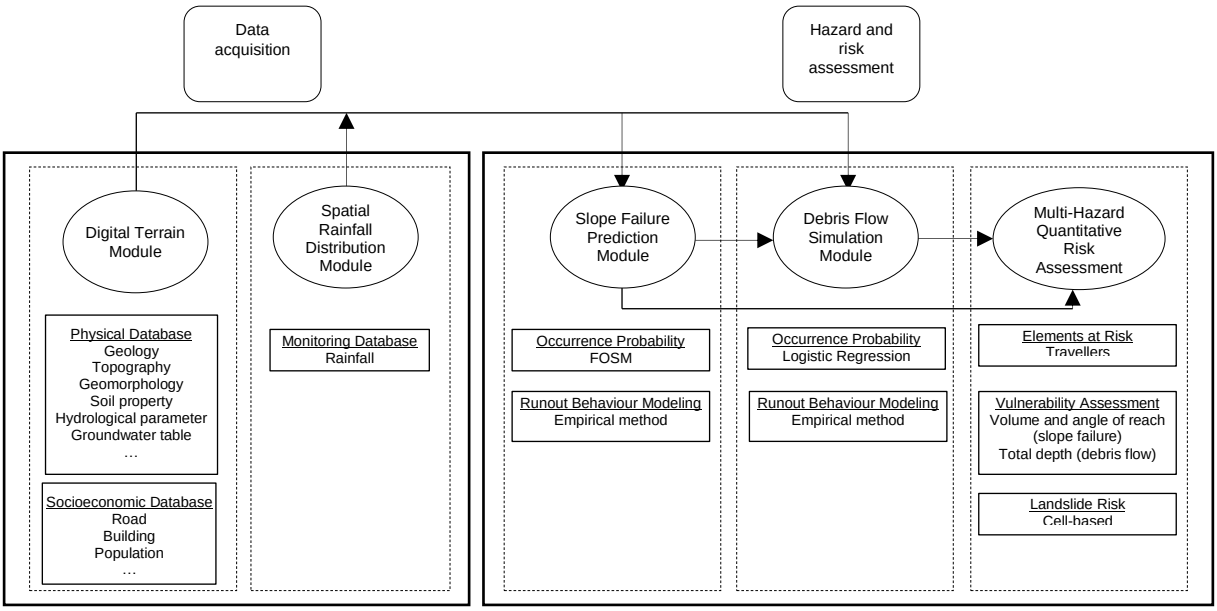

Figure 12: Multi-risk framework for rainfall-induced slope failures and debris flows for a given region (Chen et al., 2016)

Van Erp et al. (2017) focused on the modelling of cascading effects in large-scale infrastructure networks. Existing methods such as Markov chain and Dynamic Bayesian Network (DBN) were compared and found to provide similar results for the test case considered. A new method was developed as part of the RAIN project – the use of Bayesian probability theory and a probability sort algorithm to model time-dependent, inhomogeneous and cascading effects over time and space. Human intervention, to reduce risk, can also be modelled within this method. The probability sort algorithm gives a list of most possible damage states, beginning with the most probably damage state. This probability sort algorithm allows for exact computation of even exponentially large event trees, provided the system entropy of the tree is sufficiently low. The detailed implementation of the method is provided in van Erp et al. (2017).

4 Case histories of pre-existent latent weaknesses in industrial accidents

Incidents are an inevitable part of operational life of any complex industrial facility. It is very hard to predict the way that various contributing factors combine to cause the undesired outcome, but it is possible to detect the existence of latent weaknesses that together with the triggering failure(s) result in abnormal events.

Such latent weaknesses are poor management practices, deficiencies in design, gaps in supervision, maintenance faults, inadequate procedures, shortfalls in training, etc. they by themselves are not events or incidents, they by themselves do not harm the system, they are for the most of the time invisible, they just “sit” in the system and wait for a triggering event to manifest themselves in a small incident or a major accident.

In order to prevent as many incidents and accidents as possible, at complex industrial facilities, it is necessary to try to detect and eliminate as many as possible such latent weaknesses. The key to latent weaknesses detection is a good surveillance program. A good surveillance program should be able to detect the most apparent latent weaknesses and eliminate them before they have a chance to develop into incidents or accidents.

Surveillance of design, i.e. re-evaluation of a design, being periodic within a periodic safety review or at the time of any design modification or on special occasions as it was the case after the Fukushima-Daiichi accident during the stress tests at European Utilities, will detect latent weaknesses in design which might be present from the start of operation of the facility. Periodic surveillance of procedures to verify and validate their intended use will detect inadequate procedures. Surveillance of the training programmes will reveal any potential gaps in operator knowledge. Periodic surveillance of the maintenance programmes will identify potential flaws. The same applies also to other operational activities in any complex industrial facility.

The root causes of incident and accidents should therefore be looked at as the management of the surveillance programmes which were not able to eliminate the latent weaknesses that were responsible for the undesired event.

Examples of large industrial accidents (non-nuclear as well as nuclear), well described in open literature will be used to demonstrate the pre-existence of such latent weaknesses and in most cases how easy it would have been to identify and eliminate them with a good surveillance programme.

4.1 Non-nuclear accidents

In this section, examples of large non-nuclear industrial accidents (nuclear in Section 4.2) will be used to demonstrate the pre-existence of such latent weaknesses. It will be demonstrated that in most cases it would have been easy to identify and eliminate them with a good surveillance programme. All described incidents and accidents will be only briefly described as information on what happened is very well described in openly available literature. The emphasis will therefore be on demonstration of the pre-existing latent weaknesses as identified in investigations following the incidents or accidents.

4.1.1 Case 1: Piper Alpha North Sea platform

Figure 13: Piper Alpha North Sea platform (PA Images, 2018)

Piper Alpha was a North Sea oil and gas platform (Cullen, 1990). It had two compressors and the utility procedure required the crew to have one of them in operation at all times as stopping the production would result in big financial losses due to the long time required to bring the production back to full capacity after stoppage.

On the day of the accident, compressor A was under maintenance and a safety valve was taken out as a routine procedure. In its place, a bank plate was installed in order to keep the system closed. The maintenance work could not be finished before the shift turnover, but there was no verbal communication between outgoing and incoming shifts. Shift turnover procedures as are standard today were not part of their normal operation.

During the next shift, compressor B stopped working and could not be restarted. The shift supervisor looked into the main control room logbook and concluded that it was safe to restart compressor A as per the utility procedure that demanded one compressor in operation at all times. The reason that the shift supervisor did not recognise that compressor A was out of service and under maintenance was because it was common practice to have documentation stored locally, close to the equipment in question and not centrally in the main control room. The logic was that documentation was readily available close to the equipment but missed the importance of having all relevant information in one place.

Once the shift supervisor started the compressor A, the blank plate that was installed in the place of a safety valve could not withstand the pressure and a large explosion swept throughout the platform. Fire walls were not effective due to their design specification. The Piper Alpha platform was initially designed as only an oil platform and as such had fire walls designed only against fire hazard and not against explosion. Once it became also a gas platform, explosion was an additional hazard, but fire walls were not redesigned accordingly. As a consequence the fire spread very rapidly throughout the platform.

The fire would have died out were it not been fed with new oil from other two platforms. Even though, it could be seen from the distance that Piper Alpha was burning, two platforms further down the line kept pumping oil and delivering it to the Piper Alpha as the utility procedure prohibited stopping the production.

Eventually, the platform slipped into the sea.

Latent weaknesses

Without going into the fine details of the Piper Alpha accident, a number of latent weaknesses can easily be identified when analysing this accident, most of them associated with safety culture. All of them could have been identified and eliminated through a thorough surveillance program:

- Shift turnover procedures and practices were non-existent. It is clear that in any complex industrial facility the shift turnover must be formalised and carried out in

order to familiarise the incoming shift with the status and activities at the facility. The periodic review of practices could have easily identified such shortcomings.

- Maintenance logbooks were stored locally and no information was available in the main control room. Surveillance of practices could have easily identified the shortcomings of such practice in spite of benefits that information stored in the vicinity of the equipment brings.
- When moving from being only oil platform to becoming an oil and gas platform, the safety provisions should have been revisited. It is a major modification and as such requires a renewed safety analysis report with all hazards being reassessed for new conditions.
- The utility procedure, which stipulated not to stop the production as large cost would incur in restarting the operation, clearly indicated that production had priority over safety and that poor safety culture was in place within the organisation, particularly at corporate level.

4.1.2 Case 2: Challenger space shuttle 1986 accident

On January 28th, 1986 the space shuttle Challenger carrying 7 crew members exploded 73 seconds after being launched from the NASA space centre Cape Canaveral in Florida, USA (Rogers Commission, 1986). The reason for explosion was the failure of Challenger's right solid rocket booster caused by the failure of the O-ring seal, allowing pressurised burning gas to reach the external fuel tank. The O-ring seal was designed to contain the pressurised burning gas produced by the burning solid propellant and to force the gas to exit through the nozzle at the end of each rocket.

Morton Thiokol was a contractor responsible for the design of solid rocket boosters. The experimental test in 1977 using pressurised water to simulate the effects of booster combustion showed that the pressure would force metal parts to bend away from each other thus opening a gap for the gas leakage. This would allow the combustion gases to erode the O-ring, which would have catastrophic consequences.

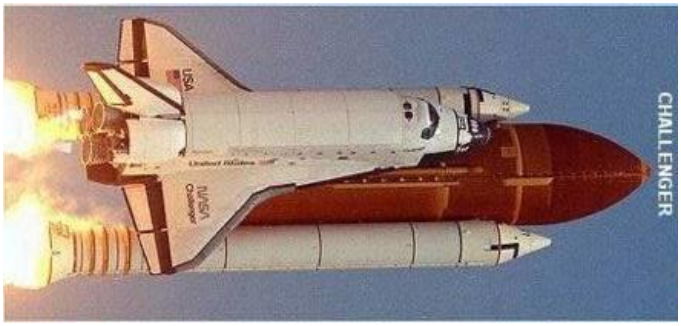

Figure 14: Challenger space shuttle (Wikipedia, 2018a)

NASA's research centre in Alabama, the Marshall Space Flight Centre wrote to the manager of the Solid Rocket Booster project several times warning that the design was unacceptable due to such deficiencies. This correspondence however was not forwarded to Morton Thiokol and the design was accepted for subsequent flights in 1980s.

Since 1981 there was evidence of O-seal erosion and the O-ring were re-classified as "Criticality-1", which meant that their failure would result in the destruction of the Space Shuttle. Nevertheless, the Marshall Centre did not report these findings to the senior managers at NASA as required by the NASA regulations but decided to keep the problem within their reporting channels with the design contractor Morton Thiokol. In addition, no one at Marshall Centre suggested that the Shuttles be grounded until the problem is being resolved.

In 1984, the first incident of hot gas escape was diagnosed on one of their flights. In the post flight analysis by Thiokol, it was determined that the amount of the escaped gas was relatively small and they concluded that such damage was an acceptable risk.

In 1985, seven of nine flights exhibited the O-ring erosion. By now, both the Marshall Centre and Thiokol realised that they were dealing with a potentially catastrophic problem. They started to re-design the system with addition of 3-inch of steel to reinforce the grip. They did not call for a halt of Shuttle flights until the re-design was completed but rather treated the problem as an acceptable risk.

In the morning of the launch, January 28th, 1986 the weather was exceptionally cold, with temperatures below freezing. In a teleconference NASA, Marshall Centre and Thiokol discussed the weather conditions. Some engineers expressed their concerns about the resilience of the rubber O-rings at such low temperatures and recommended the launch postponement. They argued that the O-rings were never tested for temperatures below 12 °C. NASA, however, ignored their warnings, and asked them to prove that O-rings would fail at such low temperatures. In addition they argued that even if the primary O-ring failed, there was still the secondary O-ring that would not. Such arguments, however, should not have applied for “Criticality-1” components. For those components it was forbidden to rely on back-up provisions. Later, NASA defended their decision on not following the recommendation by saying that they were not aware of Morton Thiokol’s prior concerns about the effects of cold temperatures on the O-rings.

After the accident, the NASA Space Shuttle program was halted for 32 months and the then US President Ronald Reagan appointed the “Rogers Commission” to investigate the accident.

Latent weaknesses

The commission, chaired by William P. Rogers with 12 vice-chairmen, among whom were Neil Armstrong and Richard Feynman, concluded that the cause of the accident was the failure of the O-ring sealing a joint on the right solid rocket booster, allowing hot gases and eventually flames to escape past the O-ring and destroy the adjacent external tank. The failure of the O-ring was attributed to a faulty design.

Apart from this major finding, also a number of contributing causes can be identified and all of them can be viewed as latent weaknesses in a sense that they could have been eliminated through a thorough surveillance program and that they were related to aspects of safety culture:

- All involved failed to respond adequately to the danger posed by the deficient joint design even after it became apparent that it could have catastrophic consequences. NASA’s safety culture shifted into risk-taking; not suddenly but gradually over the years.
- Instead of stopping the subsequent flights, they came to define the problems as an acceptable risk.
- Managers at Marshall Centre had known about the problem since 1977 but failed to discuss it with NASA. It was discussed only within their reporting channels with Thiokol which was a violation of NASA regulations – failures in communication.
- Morton Thiokol engineers warned about the effect of cold weather on the O-rings and that O-rings were never tested for such low temperatures. They were however asked to prove that it was unsafe to launch the Shuttle.

4.1.3 Case 3: Columbia space shuttle 2003 accident

Almost 17 years after the Challenger space shuttle accident, another catastrophic accident occurred when space shuttle Columbia disintegrated upon re-entry into the Earth's atmosphere (Gehman et al., 2003).

82 seconds after the launch of Columbia's 28th mission, a piece of insulation foam from the external tank broke free and struck the shuttle's left wing, damaging the protective carbon heat shielding panels. This damage allowed the super-heated gases to enter the wing structure during re-entry into the Earth atmosphere.

The problem of debris shedding from the external tank was well known. It caused damage on almost every prior shuttle flight. The damage was usually, but not always, minor. On at least 6 occasions in the previous 20 years the damage was significant.

The NASA management had become accustomed to these phenomena when no serious consequences had resulted from earlier episodes and gained confidence that it was an acceptable risk. Again, this was reflective of issues associated with the safety culture.

Figure 15: Columbia space shuttle (Wikipedia, 2018b)

Latent weaknesses

- NASA management failed to respond to the requests of engineers for installation of imaging devices to inspect possible damage.
- Engineers made three separate requests to the Department of Defence for imaging of the shuttle in orbit to determine damage more precisely. NASA did not honour the requests and in some cases intervened to stop the Department of Defence from assisting.
- NASA managers were influenced by their belief that nothing could be done even if damage were detected.
- NASA's decision-making and risk-assessment process were criticised by the investigation commission led by Admiral Harold W. Gehman, Jr. The commission made recommendations for significant changes in processes and organisational culture.

4.1.4 Case 4: Bhopal chemical accident

The Bhopal accident was a leak of 40 tons of toxic gas at the Union Carbide India Limited (UCIL) pesticide plant in Bhopal, India (Eckerman, 2005). It is considered to be one of the world's worst industrial disasters that ever happened. Over half a million people were exposed to methyl isocyanate (MIC) gas causing over 3700 immediate deaths and over 8000 deaths within the following 2 weeks.

UCIL factory was producing pesticide using MIC as an intermediate. Other manufacturers produced the same product without the involvement of MIC, though at a greater manufacturing costs. The liquid MIC was stored in three underground tanks. The regulation

specified that the tanks be filled only 50% and pressurised using inert nitrogen gas. This enabled the MIC to be pumped out as needed and kept impurities out of the tanks.

At the time of accident, extensive maintenance was being carried out at the plant. A clogged pipe adjacent to the MIC storage tank was being water cleaned but no isolation plate was inserted between two tanks. Even though the exact reason and path of water ingression into the MIC tank has never been clearly established, the fact is that water reaction with the liquid MIC caused the temperature increase and enormous increase in the volume and subsequent pressure in the MIC tank by a runaway exothermic reaction, which was accelerated by the high ambient temperature and presence of impurities in the form of iron particles from corroding non-stainless steel pipes.

Figure 16: Bhopal chemical plant (Anderson, 2018)

The emergency relief valve opened but the pressure continued to increase in spite of the atmospheric venting. Direct atmospheric venting could have been prevented by at least three safety devices had they been operational:

- A refrigerator system used to cool the tanks containing liquid MIC had been shut down for two years and temperature alarms disconnected.
- A flare tower intended to burn the MIC gas if it escaped, was improperly sized but also the connecting pipe was removed for maintenance.
- A vent gas scrubber which was also improperly sized for the magnitude of the release had been turned off.

As a consequence, 30 metric tons of gas was released within the first 30 – 45 minutes and this amount increased to 40 metric tons within the next 2 hours. The plant had two alarm systems; one for inside the plant and the second one to alarm the public. The first alarm sounded and the workers evacuated the plant but the second alarm was turned off so the public was not aware of the leak in the plant. Only an hour and a half later the public siren had been activated.

Latent weaknesses

- The most prevailing case of the accident is seen as corporate negligence – an aspect of safety culture. The disaster was caused by a combination of an under-maintained and decaying facility, a weak attitude towards safety, and an insufficiently trained workforce, which culminated in workers actions that enabled water to penetrate the MIC tank in the absence of proper safeguards.

- Workers claimed that they were not told to isolate the tank with a pipe slip-blind plate while water cleaning the clogged pipe 100 m away.
- Other factors identified by the governmental enquiries pointed out the lack of skilled operators, reduction in safety management, insufficient maintenance, and inadequate emergency action plans.
- As the demand for pesticide had fallen, low morale and rapid turnover had been seen at the plant.

4.2 Nuclear accidents

4.2.1 Case 5: Davis-Besse reactor pressure vessel corrosion – a major event

Figure 17: Davis-Besse RPV head (US NRC, 2002)

In 2002, an inspection of the control rod drive mechanism nozzle cracking on the head of the Davis-Besse NPP reactor pressure vessel was performed (US NRC, 2002). After the nozzle crack repair by welding, the nozzle was observed to tip sideways. This was obviously strange as the nozzle was penetrating the reactor vessel head and would normally have no room to tilt to such angle. After removing the control rod drive mechanism nozzle and cleaning the deposited boric acid from the top of the reactor pressure vessel head, a large cavity was discovered (see Figure 17). Ultrasonic testing measured 3/8 inch (0.95 cm) of the remaining thickness of the reactor pressure vessel head, which corresponded exactly to the thickness of the stainless steel cladding. The ultimate barrier of the primary circuit was reduced to 3/8 inch (0.95 cm) of the stainless steel cladding.

The corrosive effects of the boric acid were known for a long time. It was first reported in 1987 at Turkey Point and Salem nuclear power plants and in 1988 Nuclear Regulatory Commission (NRC) issued the NRC Generic Letter 88-05 addressing the corrosive effects of the boric acid and informing all utilities about the possible consequences. From 1996 onwards, the boric acid deposits were found on the top of the reactor pressure vessel also at Davis-Besse nuclear power plant. The amount of boric acid was so large, that it also clogged filters inside the containment. At the beginning, they were entering the containment every few months in order to clean filters; towards the end they were entering the containment on a two-weekly basis. Nobody, including the NRC resident inspector, has asked the question why was it necessary to enter the containment during normal operation and why so often.

The utility believed that the boric acid was leaking through the control rod drive mechanism flange and that elevated temperatures at that location would prevent corrosion.

Latent weaknesses

For several years warning signs were ignored, e.g. industry reports, coolant leakage, boron on filters, and amount of boric acid on the reactor pressure vessel head, all were indications of poor safety culture. The impact of safety culture in organisations on their safety performance is more thoroughly described in subsequent sections of this report.

4.2.2 Case 6: Reduced operability of safety and isolation valves for one year at a nuclear power plant

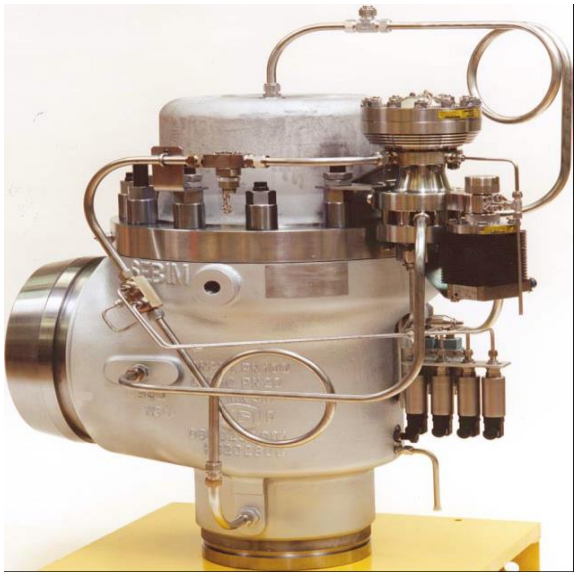

Figure 18: Tandem valve (IAEA, limited distribution a)

At this nuclear power plant, pressuriser safety and isolation valves consist of three tandem valves (IAEA, limited distribution a). Both safety and isolation functions were controlled by the internal pressure of the system and therefore an unobstructed path, from the system through the valves, must be ensured in order for the hydraulic pressure to perform its function. Three set-points are specified for the relief function, p > 165, 169, 171 bar (16,500; 16,900; 17,100 kPa) and the isolation is initiated at p < 139 bar (13,900 kPa).

In order to ensure the unobstructed path for the hydraulic pressure, hollow bolts were used to connect the valves to the primary system. Initially, for the purpose of outages, a system was designed to replace the hollow bolts with the solid ones in order to maintain the integrity of the primary system. The size of the head of solid bolts was deliberately made bigger to make sure that solid and hollow bolts were not mixed up by mistake. Solid bolts had a head of 30 mm and the hollow bolts of 27 mm. As it was somehow a cumbersome operation, another solution for blocking the openings during outages was later designed and solid bolts were no longer needed to close the system. However, the solid bolts, even though not needed remained in the tool box used for decoupling the valves from the system. Having in mind, that the primary system would be opened only at a time of outages, the procedure was written which specified, that after every outage, the set points of the safety and isolation valves should be verified.

During an unscheduled shutdown, there was a need to open the primary system and hence decouple the safety and isolation valves. Work was performed by two technicians in decoupling the valves and another two in assembling them back after the necessary work has been completed. However, only one out of four technicians had a special training by the valve manufacturer. In the process of assembling the system, solid bolts were installed instead of the hollow once. In order to assemble the solid bolts, a 30 mm wrench was

needed which was not in the tool kit as the solid bolts were no longer needed and had been left in the tool box by mistake. The technician had to go and find the 30 mm wrench elsewhere and had written it down in his work order. The work order was later on endorsed by his supervisor, who could have questioned the need for the 30 mm wrench which was not supplied in the working tool kit. As this was not a scheduled outage, the valves set points were not verified as the procedure clearly stipulated that the set point verification should be performed after the scheduled outages. The plant went into operation and stayed on line until the next outage in approximately a year's time. The solid bolts were discovered at set point verification at that outage in accordance with the established procedure. For that time period, the operability of the safety and isolation valves was greatly diminished but never challenged. The tests performed later at the manufacturer's premises showed that the valves would have functioned but at a different pressure values.

Latent weaknesses

The important latent weaknesses found were in training, procedures and work practices:

- Only one out of four technicians was trained by the valve manufacturer for the job performed.
- The procedure should have been revised and written along the lines that the set point verification should be performed each time when the system is reassembled and not only after yearly scheduled outages.
- Work order processing practices should have been revisited to assure that the approvals and assignments of responsibility are not performed routinely without close consideration of their content.

As will be elaborated later on in this report, the extent of cause can be applied very widely to other training programmes, other procedures and other practices to assure that similar causes are not present also elsewhere.

4.2.3 Case 7: Essential service water system train B inoperability due to pipe break

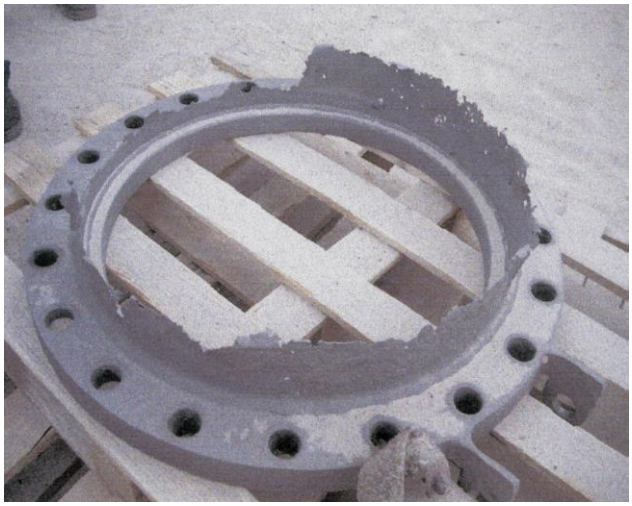

Figure 19: Break within the ESWS (IAEA, limited distribution b)

During this case, the NPP in question was operating at 100% power (IAEA, limited distribution b). The Essential Service Water System (ESWS) has two 100% trains: A and B, with Train A in operation. At 5:10 am, the pump of Train B was started for a maintenance check and soon after, it was noticed that the system (Train B) has lost pressure. The field operator was dispatched to identify the problem in the field and he found that one of the manholes in the train B was full of water. The fire brigade was asked to pump out the water and a leak in the system was identified. Leakage in the ESWS Train B was discussed on the morning daily meeting and it was decided to continue operation and monitor daily for

increased leakage. In subsequent days no increased leakage was observed as the mortar served as a barrier. It was believed that there was no need for immediate action and the design team started working on a temporary modification that would be implemented later in the year using the 72 hours Limiting Conditions for Operation (LCO). Two months later, before the design was completed a circumferential break at the same place occurred after a start-up of the pump which was aligned to Train B.

As the plant is located at the sea coast with high humidity and salty atmospheric conditions in which equipment is prone to rust, the initial design of the ESWS was modified based on operating experience from other nuclear power plants which were also situated in coastal areas, to include certain provisions that would minimise the potential for rust. Those provisions included the following:

- cathodic protection against rust;
- manholes within collection boxes to enable inspection of piping integrity and cathodic protection;
- manholes were covered by concrete slabs but without water seals;
- no drain, no humidity measurement, no ventilation, no water level indication;
- there was a provision to examine and drain boxes every 4 months.

Cathodic protection is a technique used to control the corrosion of a metal surface by making it the cathode of an electrochemical cell (see Figure 20). A more easily corroded “sacrificial metal” is used as the anode.

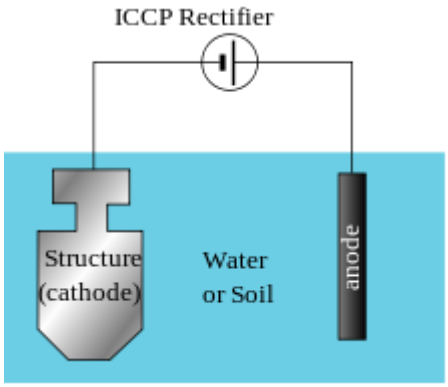

Figure 20: Cathodic protection (Wikipedia, 2018c)

To fully understand the event it is necessary to know the operating history of the ESWS. For the first 13 years the system was inspected by a contractor on both trains every year during the outage. After 13 years a new contractor was engaged and at the same time the frequency of inspections was reduced first to every 18 months and later to even every 36 months. The plant specification for inspection never specifically required the examination of external surfaces but only internal surfaces.

The first cases of corrosion were reported already in the first year of plant operation and the corrosion was the most severe in the boxes close to the sea, as was expected. The corrosion problems were dealt with by brushing and painting the surface. On two occasions, the contractor recommended the measurement of the thickness of the pipe as frequent brushing was diminishing the pipe thickness but the utility did not act on those recommendations, even though the recommendations were in written form on the related work orders.

Latent weaknesses

- The ESWS initial design was inadequate to prevent formation of external corrosion.

In spite of corrosion difficulties lasting for more than 10 years, the plant did not consider making design modifications. From the open literature it can be found that the preferences for safety solutions are normally ranked as follows:

- Design,

- Safety devices,
- Warning devices,
- Human factors review,
- Procedures,
- Personnel,
- Acceptance of residual risk.

The plant relied completely on procedures and personnel to control the hazard of external corrosion; these two being the least reliable solutions.

The plant was recommended to develop and implement design changes to reduce the potential for corrosion by installing automatic or passive design features (seals, drainage, humidity measurement, ventilation, water level indication, etc.).

- Plant inspection and maintenance specifications for cathodic protection did not include external surfaces.

In spite of the increased severity of external corrosion, the inspection intervals were reduced from 12 months to 18 months and later on even to 36 months. For more than 10 years corrosion was dealt with by brushing and painting the pipes. Twice the recommendation was given to measure the thickness of the pipe but the action was never performed. The plant was recommended to modify the inspection and maintenance specifications for the cathodic protection system to include search for external corrosion and provide specific guidance for its remediation.

- Inadequate policies for root cause analysis and trending of failures failed to identify repetitive corrosion.

The plant did not have a policy in place for systematic root cause analysis and trending for the first ten years. The plant did not identify the trend of corrosion on the neck of the pipe, even though the corrosion was reported on every inspection report for more than ten years. The plant was recommended to improve the existing programme of root cause analysis and trending to reflect the state-of-the-art in the nuclear industry. It should further consult the feedback of operating experience (FOE) from plants with similar operational environment i.e. sea costal area.

- Inadequate policies for change management existed to control contractor changes in inspection frequencies.

Changes in subcontractor after 13 years did not bring improvements but rather the opposite. The frequency of inspection changed from 12 to 18 months initially and later to 36 months. The first contractor was reporting to the plant maintenance department and the second to the engineering department. There was no feedback to the requestor when maintenance rejected the request for pipe wall thickness measurement.

The plant was recommended to develop a comprehensive change management program for making changes in the equipment, processes, procedures, contractors, personnel or organisation. When changing the inspection frequency on safety systems, the plant should perform a safety impact assessment.

- Inadequate maintenance process failed to implement the recommendations of the contractor inspection reports.

Individuals decided not to complete the requested measure of wall thickness and requestors did not follow-up with the group to which the request has been made.

The plant was recommended to modify the relevant procedures to require notice with explanation to all parties whenever it is decided not to implement recommended corrective actions. A review process should be required whenever recommendation is not followed.

- Decisions made by the plant management at the time of the first leak were inconsistent with conservative decision making in operation and contributed to the later guillotine pipe break.

The plant recognised the seriousness of the leak by increasing the frequency of surveillance to daily and by starting the temporary design modification to be implemented using 72 hours LCO. Nevertheless, in the morning meeting on the day of a leak, they decided to continue operation in spite of the procedure describing the treatment of degraded and non-conforming condition, which required an assessment before continuing operation. The plant was recommended to review the implementation of the policy on procedure compliance and emphasise the commitment of plant management to conservative actions.

With the situation of such corrosion impact, the extent of condition was necessary to be performed. The plant conducted an extensive survey of all other collection boxes in order to determine if similar conditions existed also there. There was also a potential for external corrosion to exist in all other systems apart from the ESWS, exposed to similar weather conditions at the plant.

4.3 Overview

In all of the seven case studies, from non-nuclear and nuclear fields, a number of pre-existing and long lasting latent weaknesses existed. Deficiencies vary from case to case but most of them relate to deficiencies in management, design verification, procedures and work practices. In all cases it was found that procedures and practices were centred on productivity, and in all cases the surveillance programmes were not in place or capable of detecting and eliminating those latent weaknesses. For all of them deficiencies in safety culture could be identified.

5 Safety culture and its influence on the safety performance of complex industrial facilities – a focus on key hazards

As could be seen from the presented case studies in the previous section of this report, deficiencies in safety culture could be identified in all described events, being non-nuclear or nuclear related. The term 'safety culture' first appeared in industrial parlance after the Chernobyl accident in 1986. The first internationally recognised definition of safety culture came with the publication of the International Atomic Energy Agency's (IAEA) INSAG-4 document in 1991 (IAEA, 1991). Very soon, almost all countries operating nuclear power plants accepted this concept and started making efforts towards evaluation and enhancement of safety culture in their organisations. The IAEA created a new service ASCOT (Assessment of Safety Culture in Organizations Team) with the objective of promoting this concept. The ASCOT Guidelines (IAEA, 1994) were published in 1994 which gave guidance to the IAEA Member States on evaluation of safety culture, recognizing the fact that safety culture is not tangible but manifests itself in tangible evidence. While it has been stated that the US NRC has recognised safety culture as an important aspect of operations (e.g. US NRC, 1989a), it did not give it substantial attention for a long time, claiming that its effects could be captured by other tangible means and that intangible effects could not be regulated (personal communication Dusic, 2018). This attitude changed after the Davis-Besse accident which clearly pointed out the deficiencies in safety culture.

The safety culture definition from INSAG-4 is still the definition most widely used throughout the nuclear community. It states that:

> "Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear safety issues receive the attention warranted by their significance" (IAEA, 1994).

The above definition stipulates that safety culture in attitudinal and structural, meaning that it has a structure, set up by the management and covers also the attitudes of individuals which work within this framework and benefit from its structure. Very often safety culture is perceived only as the attitude of individuals, forgetting, that the framework that must be created by the management is an equal part of the sound safety culture. Policy level commitment and managers' commitment form the framework within which individuals respond. All three together, policy level commitment, managers' commitment and individuals' commitment form the concept of safety culture.

The above definition further stipulates that safety culture is a characteristic of organisations and individuals. Very often safety culture is perceived only as a characteristic of individuals, but the root causes of events reveal that it is most often deficiency of an organisational safety culture which let to undesired outcomes.

Similar definition of safety culture was later on published by the US NRC (2014) in NUREG-2165:

> "Core values and behaviours resulting from a collective commitment by leaders and individuals to emphasise safety over competing goals to ensure protection of people and the environment".

The latent weaknesses presented in six case studies relate also to deficiencies in safety culture. Often it is seen that production pressure overrides the safety concerns. In some ways it is expected if one is not careful as production (if tangible) – is an event, and safety is intangible – and hence, a non-event. However, identified latent weaknesses relate to basic organisational processes, such as design, operation, maintenance, training, supervision, management etc. production and safety depend upon the same organisational principles and safety therefore should not be treated as a separate issue but as part of the everyday activity within an organisation.

The IAEA publication Safety Report Series #11 (IAEA, 2001) identifies three types of organisations depending on the level of safety culture development within the organisation:

- Rule based behaviour,
- Goal based behaviour,
- Improvement based behaviour.

Within a rule based behaviour organisation, safety is based on rules and regulations. Safety is seen as an external requirement. As such, safety is accomplished through compliance with rules and regulations. Problems are not anticipated and people making mistakes are blamed for not complying with the rules. At the organisation, reactive incident investigation is undertaken instead of proactive incident prevention.

Within a goal based behaviour organisation, a good safety performance is an organisational goal. Safety is dealt with through procedural solutions and retraining. Potential problems are identified and prevention measures are taken through procedures, rules and hardware solutions. Management response to mistakes is to put more controls in place via procedures and retraining. Safety is however still thought to imply higher costs.

Within an improvement based behaviour organisation, there is a belief that safety performance can always be further improved. It is clear that the organisational culture exists. Such organisations act strategically and focus on long term. They anticipate problems and latent weaknesses and deal with them proactively. In these organisations, safety and production are seen as interdependent. People within the organisation are respected and valued for their contribution.

Each organisation can perform a self-assessment and determine in which of the above three categories they belong. The IAEA Safety Report Series #11 (IAEA, 2001) offers three questions that would help organisations to find out where they belong:

- To what extend is safety being achieved primarily by high standards of engineering control?
- Has the organisation developed clear safety goals and a comprehensive system for the management of safety?
- Are most people, at all levels in the organisation, actively and routinely involved in enhancing safety?

Most organisations will answer positively to the first two questions but probably very few to the third one, the reason being that the positive answer to the third question requires the involvement and dedication to a high safety culture standards of all employees within the organisation.

Achieving a strong safety culture within an organisation is one thing, maintaining it at a high level for longer periods of time might be another challenge. The IAEA's International Nuclear Safety Group (INSAG) has for that reason developed a document INSAG-15 (IAEA, 2002) which among other issues defines also typical patterns of declining safety performance. In this document, 5 steps are identified that would be indicative of the declining safety performance (taken from INSAG-15):

Step1: Overconfidence

This is brought about as a result of good past performance, praise from independent evaluations and unjustified self-satisfaction.

Step 2: Complacency

In this phase, minor events begin to occur and self-assessments that are inadequate are performed to understand their significance. Self-satisfaction leads to delay or cancellation of some improvement programmes.

Step 3: Denial

Denial is often visible when the number of minor events increases and more significant events begin to occur. However there is a prevailing belief that those are still isolated cases. Negative findings by internal audit or self-assessments tend to be rejected as invalid and the programmes of RCA are not applied or are weakened. Corrective actions are not systematically carried out; implementation programmes are incomplete or terminated early.

Step 4: Danger

Danger sets in when a few potentially severe events occur but management and staffs tends consistently to reject criticism coming from internal audits, regulators or other external organisations. The belief develops that the results are biased and that there is unjust criticism of the plant. As a consequence, the oversight organisations are often silent and afraid to make negative assessments and/or to confront the management.

Step 5: Collapse

Collapse can be recognised most easily. This is the phase where problems have become clear to all parties and the regulator and other external organisations need to make special diagnostic and augmented evaluations. Management usually needs to be replaced. A major and very costly improvement programme usually has to be implemented.

The next few sections of this report will address the analytical methods that are being used for incident investigation. Latent weaknesses are just the starting point for such investigations; root cause analysis, probabilistic precursor analysis and deterministic transient analysis are the logical next steps in incident investigations for any complex industrial facility.

More recently, the revision of the IAEA Safety Standards brought new insights on safety culture issues, as reflected in General Safety Requirements (GSR) Part 2, which introduces the concept of an Integrated Management System (IAEA, 2016). Such system provides a single framework for the arrangements and processes necessary to address all the goals of the organization. These goals include safety, health, environment, security, quality and economic elements, and other considerations such as social responsibility.

New element in GSR Part 2 (IAEA, 2016) is also the introduction of the concept of “culture for safety” in addition to already established concept of “safety culture”. It is argued that by moving towards “culture for safety” we acknowledge that “safety culture” is not a separate entity that can be installed or removed from an organizational culture. It is rather an outcome of the organizational culture as it influences every aspect of how the organization’s members behave, from how the management system is developed to how defence-in-depth principles are manifested. Therefore the goal of any organization is to create an organizational culture that is working to achieve safety day by day – that is a culture for safety. Another hey principle introduced in GSR Part 2 is the influence of leadership on safety. It states that the safety performance of an organization starts with leadership. Leaders establish values and further align those values throughout the organization. Leaders set expectations and ensure accountability for their safety programmes. Therefore, leaders set standards for safe behaviour which in turn encourages and motivates workers to effectively engage in safe behaviour. Also noteworthy is the EU project ‘Training Schemes on Nuclear Safety Culture’ (TRASNUSAFE) developed training schemes to provide managers with the necessary knowledge and understanding about safety culture. The goal of the project was to avoid human errors or organizational factors leading to accidents and highlight the emphasis on safety culture within the EU (https://cordis.europa.eu/result/rcn/164237_en.html).

6 State-of-the-art root cause analysis and risk integration methodologies applicable to complex industrial facilities

6.1 Basic concepts and definitions

There are many definitions being used in the field of the feedback of operating experience but in this report, we will use those that are most commonly used throughout the nuclear industry.

Root cause:

Root cause is the most fundamental reason for an incident or condition, which if removed will prevent recurrence of such or similar incidents or conditions.

It is important to emphasise that in order to be considered a root cause, the factor must be under the management's control. While initiators and other factors may exist outside the organisation, the responsibility for effective barriers lies within the organisation. For example, an earthquake cannot be selected as a root cause as the fact if it happens or not is outside the management's control. But not having in place barriers for a potential earthquake is within the management's responsibilities and if inadequate it can be selected as a root cause.

Direct/Immediate/Observed/Apparent cause:

Direct cause is the simplest action(s) or conditions that directly resulted in a problem, and which require(s) immediate attention.

Many different names are used to describe the direct cause as indicated in the title above, but they all have the same meaning or definition. In reading the root cause analysis reports one will come across all of the above mentioned titles.

Contributing cause:

Contributing causes are actions or conditions not directly responsible for the problem but whose existence contributed to the problem or made the consequences more severe.

Barrier:

Barriers can be physical or administrative and are applied to inhibit inappropriate human actions or undesirable equipment performance.

Together with the definitions of the **extent of condition** and the **extent of cause**, which will be given later on, the above definitions are thought to be sufficient for the performance of root cause analysis in any complex industrial facility.

Root cause analysis of events in complex industrial facilities are performed with the aim to better understand what has happened and to develop corrective actions that will mitigate the consequences of the event and prevent possible occurrence of the same or similar events or conditions. It is therefore of utmost importance to identify the real root causes as only then we can develop appropriate corrective actions. Wrongly identified root causes will also result in inadequate corrective actions.

To obtain a full benefit of the feedback of operating experience, root cause analyses should not be limited to major events. Organisations with a sound safety culture will analyse:

- Significant events and experience,
- Low level events,
- Near misses/near hits/close calls,
- Deteriorating performance.

While most organisations will have a program in place to analyse the first three (and even that to various degrees of intensity), the last one, analysis of deteriorating performance is

rarely undertaken as was demonstrated in the case of NASA with regard to Challenger and Columbia space shuttle accidents.

There are numerous benefits of root cause analysis. Root causes rarely appear alone, especially for complex systems. They always stem from latent weaknesses and those need to be identified and eliminated before having a chance to develop into incidents or even accidents. Root cause should be sought to maximise lessons learned and not to "meet the requirements". It is beneficial to identify all root causes already during the initial analysis as it's cheaper, less painful, and more efficient than discovering only one root cause per problem. Root causes performed on near misses, sometimes referred to as near hits or close calls can be just as productive as when analysing major events. Normally root causes for near misses are the same as those for major incidents, just the consequences or outcomes are different, and usually they are only the result of chance.

Systematic root cause analysis requires methods as will be discussed in the next section of this report. Methods or "analytical techniques" should always be well documented, standardised approaches. Methods may vary in many ways, length, depth, comprehensives or complexity, appropriateness, time requirements, scope, power and appeal. Different analytical techniques will be detailed in the next section with identified advantages and shortcomings of each individual method. It will be also shown that the application of multiple methods can increase confidence in determination of root causes.

In order to have an effective root cause analysis programme in an organisation, several conditions need to be fulfilled. The root cause analysis programme must have:

- Full and sincere management support,
- Utility culture must be such that there is a common desire for its improvement,
- Voluntary reporting scheme,
- Personnel trained in investigation techniques,
- Prompt investigation as information tend to be lost exponentially with time,
- Effective learning from operating experience.

The established root cause analysis programme should in an organisation be governed by philosophy that emphasises:

Thoroughness:

This includes the thorough historical review inside and outside industry within which the organisation operates. It must encompass the extent of case and the extent of condition review for all identified problems and causes and should encourage a broad view of the problem – programmatic and managerial.

Fairness:

The reviewer when preforming interviews in the course of their investigation should listen sincerely and avoid jumping to conclusions. They should see themselves serving as a consultant and not as a policeman. They should emphasise the organisational learning and not the individual shortcomings.

Efficiency:

The resources for root cause analysis are usually limited. It is therefore advisable to "scale" the resources to significance.

As indicated above, all levels and types of incidents deserve appropriate attention. It is not absolutely necessary to categorise events as each of them can serve as a good source for learning lessons. Nevertheless we can find in an open literature several attempts to classify incidents, mostly in terms of their safety significance or risk that they may be associated with. One such classification can be found in reference MIL STD 882c (US Military, 1993) where they developed the so-called Qualitative Risk Matrix – this is now widely used and is standard per ISO 9001:2015, clause 6.1 (ISO, 2015). Risk, being defined as the product of

probability and consequences, is in this matrix represented by the probability of the event on one axis and its consequences on the other.

The ***probability of the event*** is categorised as follows (US Military, 1993):

- FREQUENT – likely to occur often during the life of an individual item or system or very often in operation of a large number of similar items.
- PROBABLE – likely to occur several times in the life of an individual item or system or often in operation of a large number of similar items.
- OCCASIONAL – likely to occur sometime in the life of an individual item or system, or will occur several times in the life of a large number of similar components.
- REMOTE – unlikely, but possible to occur sometime in the life of an individual item or system, or can reasonably be expected to occur in the life of a large number of similar components.
- IMPROBABLE – so unlikely to occur in the life of an individual item or system that it may be assumed not to be experienced, or it may be possible, but unlikely, to occur in the life of a large number of similar components.

On the other axis, the consequences of the event are categorised as follows (US Military, 1993):

- CATASTROPHIC – death, loss of system or plant, such that significant loss of production, significant public interest or regulatory intervention occurs or reasonably could occur.
- CRITICAL – severe injury, major system damage or other event, which causes some loss of production, effects more than one department, or could have resulted in catastrophic consequences under different circumstances.
- MARGINAL – minor injury, minor system damage, or other event generally confined to one department.
- NEGLIGIBLE – no potential to affect safety.

Both, probabilities versus consequences are then combined into the **Risk Matrix**

Table 2: Risk matrix (after US Military, 1993)

PROBABILITY/ CONSEQUENCES	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
Frequent	1	1	1	4
Probable	1	1	2	4
Occasional	1	2	3	4
Remote	2	2	3	4
Improbable	3	3	3	4

The events are classified according to this matrix in four categories, with the category 1 bearing the highest risk and the category 4 carrying the smallest risk. Placing of four categories in the above matrix is somehow arbitrary and can be also distributed differently, depending on the objective of categorisation.

Extent of cause and extent of condition

After completing the root cause analysis of an event it is necessary to perform also the extent of cause and the extent of condition for that particular event. That will reveal if the same cause could have affected also other systems or components and if the same condition could be found in other systems or components.

The ***extent of condition*** is defined as**:**

The extent of condition is the extent to which the actual condition exists or may exist with other plant processes, equipment or human performance.

The ***extent of cause*** is defined as the extent to which the root causes of an identified problem have impacted or may have impacted other plant processes, equipment or human performance.

The extent of condition review generally differs from the extent of cause review in that the extent of condition review focuses on the actual condition and its existence in other places.

The extent of cause review should on the other hand focus more on the actual root causes of the condition and on the degree that these root causes have resulted in additional weaknesses.

Having in mind the above, the timing is determined when should we review the extent of cause and when the extent of condition. The extent of condition review can be performed as soon as the condition is identified. The extent of cause however can only be done once the root causes are determined.

It is important to remember that once the root cause analysis is complete, the extent of the condition review should be revisited.

Flaws in the extent of condition and the extent of cause are usually common. They occur for at least reasons:

- First, due to the database weaknesses. Access to all records is usually not easy or feasible.
- Second, analysts are not as persistent in the extent of condition or the extent of cause reviews as they are in other aspects of evaluation. In most cases the reason lies in the fact, that the importance of reviews of the extent of cause and the extent of conditions are not strongly emphasised in most root cause analysis training courses.
- The third reason for flawed reviews is normally in inadequate definition of what should be actually covered by the root cause analyses.

Not all events are alike and therefore different techniques are required for their investigation and analysis, depending on the type of the event and the objective of the analysis.

The three main methods are being used worldwide for the event analysis, all three complementing each other:

- classical root cause analysis,
- probabilistic precursor analysis,
- deterministic transient analysis.

Not all events are alike in their nature and it is very important to be able to determine which methods to apply in the event analysis depending on the type of the event and the answers we are looking for.

For most unusual events a traditional **root cause analysis** techniques are being used. There is the whole spectrum of techniques being used, depending on the depth of analysis that should be achieved, the nature of the event and other factors such as event being a hardware failure, human error or the combination of both as in most cases. They are used to determine a root cause which is in most cases defined as the most fundamental reason for an incident or condition, which if removed will prevent recurrence of incident or condition.

In cases when our aim is to determine the safety significance of the event the best method to be used is the **probabilistic precursor analysis**. Probabilistic precursor analysis gives a quantitative estimation of safety significance of the event that happened. It uses the concept of Conditional Core Damage Probability (CCDP) to determine the safety significance of the event. It is basically a measure, in a PSA model, how far is the event which is being analysed from the core damage scenario. This method is far more detailed and fine in comparison with the event rating given by the International Nuclear Event Scale (INES), where the vast majority of the events fall into the category 0 or 1.

The tried type of the event analysis is known as **deterministic transient analysis**. As the name already indicates it is a method mostly suitable for analysing transients in nuclear power plants. It is therefore used mostly to analyse the fast developing events. It is the best method to be used for better understanding the phenomena, occurring during a specific event. As is it a simulation method, it is suitable for identification of the impact of different contributing factors and conditions by running different scenarios (for example modelling operator action vs. automated action) and determining their impact on the final results. It is the only method, which can give us the quantitative estimation of the remaining safety margins throughout the event.

6.2 Root cause analysis methods

Root cause analysis methods are the most commonly used methods for incident evaluation. Several techniques exist but all of them have the primary objective to identify root causes of the event. As already mentioned earlier, the root cause is defined as the underlying cause that if properly addressed would prevent recurrence of the same or similar event. Root causes have to be directly correctable, i.e. are within the influence of the organisation.

The following root cause analysis techniques will be described in more detail, giving descriptions, strengths and weaknesses of each individual technique (IAEA, 2014):

- Task analysis,
- Change analysis,
- Barrier analysis,
- E&CFC - Event and causal factor charting,
- ASSET/PROSPER,
- HPES – Human performance enhancement system,
- MTO – Man, technology, organisation,
- MORT – Management oversight and risk tree analysis,
- HPIP – Human performance investigation process,
- AEB – Accident Evaluation and Barrier analysis,
- Fault Tree analysis.

For each RCA methodology, a brief description will be given, together with the main strengths and weaknesses in comparison to other methods.

6.2.1 Task analysis

Description

Determine as much as possible about activities that were performed prior, during and after the event.

How is it done?

- Review work documents, logs, manuals etc. (learn how the task should be done);
- Review the task in question by direct observation or by interview.

Strengths

- Makes the investigator familiar with the actual task performance;
- Identifies possible contributors to the event;
- Helps to identify deviations from normal way of doing the task;
- Helps to identify barriers.

Limitations

- Can be time consuming;
- Most effective when performed with staff responsible for the task;
- Rarely used independently.

6.2.2 Change analysis

Description

Change analysis compares the previous trouble free activity with the event to identify differences.

Basic questions:

- What is different?
- What is the effect of the change?

Strengths

- Good starting point;
- Generates questions;
- Simple to use;
- Useful in evaluating equipment failures.

Limitations

- Usually produces more questions than answers;
- Gradual changes can be overlooked;
- Must be used in conjunction with other techniques.

When performing the Change analysis it is useful to create so-called Condensed Worksheets. On these sheets four columns are created;

A B CHANGES IMPACT

List in column A all features of trouble-free activity.

List in column B all features of the event.

Under Changes list all differences between column A and column B.

Under Impact list for each difference the real and potential impact.

Consider possible interactions (combined effects) of changes taken together.

Include source reference for all factual information.

6.2.3 Barrier analysis

Description

Barriers are devices employed to protect equipment and people, and can be physical or administrative in form:

- Physical: system interlocks, locked doors and valves, automatic fire systems (reliable but expensive);
- Administrative: permits, authorisation procedures, license (not so reliable, relatively cheap).

A single barrier is rarely relied upon. Barrier analysis identifies such barriers and determines those which either failed or were absent.

Strengths

- Helps to identify probable causal factors;
- Can be used independently or within an integrated E&CFC.

Limitations

- Danger of not recognising all failed barriers;
- Danger of having too restrictive concept of a barrier without addressing its quality and depth.

Below is schematically depicted the idea of different barriers preventing performance from evolving into an incident. If flaws in several barriers, which are normally present, align in a way to allow such propagation, the event occurs.

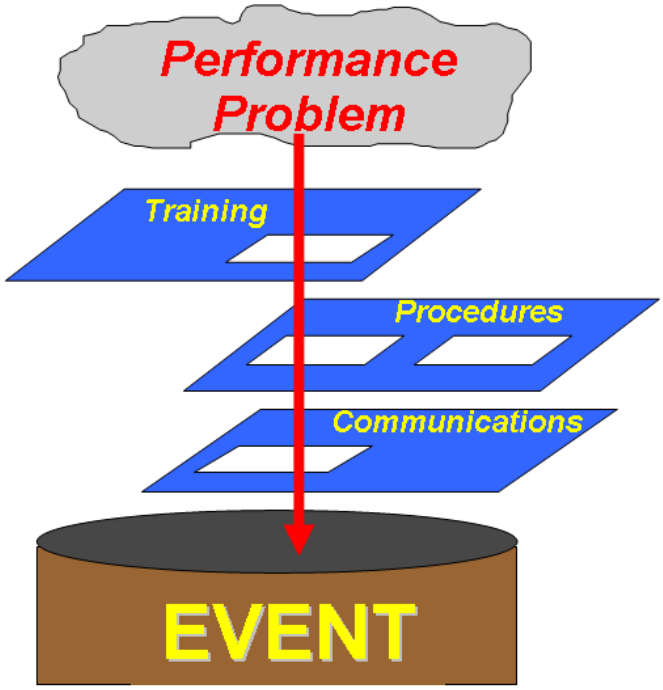

Figure 21: Barrier analysis (JRC, 2018)

6.2.4 Event and Causal Factor Charting

Description

An Event and Casual Factor Chart is a graphically displayed flowchart of an entire event plotted on a time line.

It is probably the most useful tool for recording and understanding the event progression.

As an event line is established, additional features such as related conditions, secondary events and presumptions are added.

Strengths

- An excellent opportunity to graphically display barriers, changes, causes and effects and human performance interactions;
- Organises data and provides a broad picture;
- Easy to understand and communicate with those not familiar with the techniques (management, operators).

Limitations

- Can be time consuming;
- Rarely stands alone and greatly enhanced by superimposed barrier and change analyses.

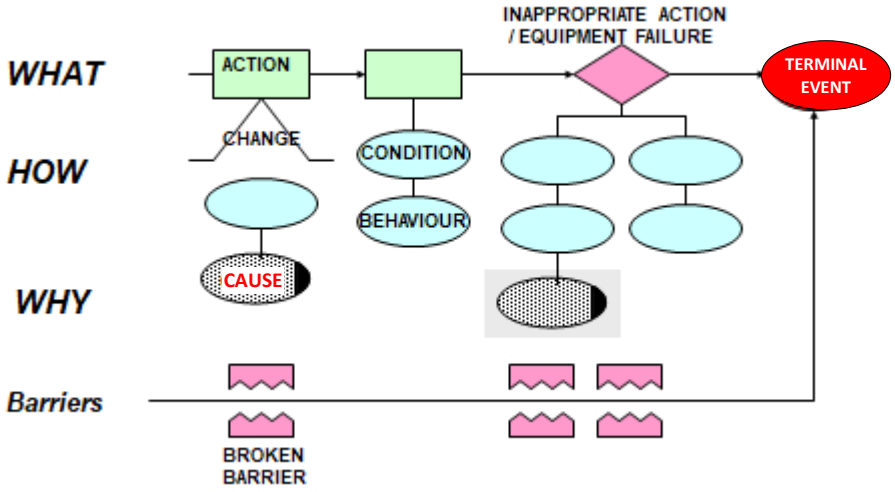

Figure 22: Event and causal factor charting (JRC, 2018)

An E&CF Chart should be started at the very beginning of the investigation. Even if **not complete at the beginning**, it will serve to:

- Organise and guide the investigation;
- Develop with new facts;
- Validate and confirm the sequence;
- Illustrate the sequence.

An E&CF Chart can be used for:

- Keeping "score" - show what you know;
- Showing the "big picture" - build a context;
- Evaluating corrective actions - they should break the main event line early and often answering Who? What? When? Where? How? Why?

The skeleton will need to be upgraded as additional facts are gathered.

It is extremely useful to:

- Explain to colleagues and management; exit meeting;
- Guide the preparation of reporting.

Below Figure 23 demonstrates the basic symbols that should be used when constructing the E&CF Chart. In rectangles which specify events it is needed to enter the following basic information:

- Date and time: when?
- Subject: who and what?
- Verb: Action – did what?
- Location: where?
- Source: document, interview, observation.

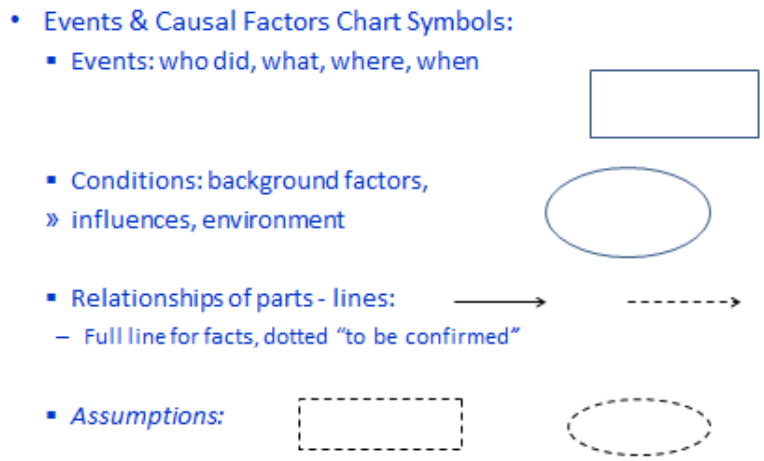

Figure 23: Symbols used in E&CF Charting (DOE, 2012)

6.2.5 ASSET/PROSPER

Description

The root cause methodology developed to support the IAEA ASSET/PROSPER services programme.

Root causes are clearly defined as the answer to the question: why was it not prevented through a comprehensive surveillance programme?

Strengths

- Freely available to use;
- Used numerous times on ASSET/PROSPER Missions;
- Output is directed at NPP management;
- Training available by the IAEA.

Limitations

- Has a different definition of root cause as other techniques;
- Identifies deficiencies in management and policy, therefore requires knowledgeable senior staff to do the analyses.

6.2.6 Human Performance Enhancement System (HPES)

Description

The techniques encompassed within the HPES package include:

- Task analysis, Change analysis, Barrier analysis, E&CFC;
- Behavioural analysis, Situational analysis;
- Interviewing techniques.

Strengths

- Provides a toolbox of techniques;
- Proven methodology used worldwide;
- Training courses and handbooks available.

Limitations

- Requires experience and training to apply effectively;
- The process does not specifically identify organisational issues.

6.2.7 Man, Technology, Organisation (MTO)

Description

MTO is a general concept which stresses the importance of interaction among man, technology and the organisation.

It is a modified version of HPES.

Strengths

- Describes the context of event analysis in terms of necessary organisational structure;
- Has a strong connection to human factors.

Limitations

- Being a modified version of HPES the same limitation of required experience and training to be applied effectively exist.

6.2.8 Management Oversight And Risk Tree (MORT)

Description

The method consists of a Fault Tree together with a long series of interrelated questions.

Strengths

- Comprehensive manual and training available;
- Uses detailed Fault Trees;
- Flexible (can use parts of Fault Tree for small events);
- Uses barrier analysis;
- Computerised version is available.

Limitations

- Requires experience to use;
- Time consuming due to extensive task analysis.

6.2.9 Human Performance Investigation Process (HPIP)

Description

HPIP is a method developed for the US NRC in NUREG/CR-5455 (US NRC, 1993).

Strengths

- Similar to HPES;
- Simplified Fault Trees are easy to use;
- Training on HPIP is minimal if users are experienced in other techniques.

Limitations

- It is a process and being a simplified version of HPES does not produce any better results or added value.

6.2.10 Accident Evaluation And Barrier Analysis (AEB)

Description

The AEB method models the failures and errors in the interaction between human and technical systems leading to an incident.

Strengths

- Formalises the link between human performance and technology;
- Uses barrier function analysis in a more graphical way.

Limitations

- Not widely used;
- Does not present all the data in the AEB main flowchart and hence runs the risk of missing potential relevant contributing factors.

6.2.11 Fault Tree analysis

Description

Systematic approach, used when the problem is known but the causes are not clear. It uses a set of questions to help direct the investigator to the causes.

The Qualitative Fault tree emphasises the relationship among events. It however does not include probability statements, but has more of an explanatory emphasis. The Quantitative Fault tree emphasises the probability of event occurrence. It often has a predictive emphasis.

Strengths

- Can be used with limited training;
- Gives structure to an event;
- Pin-points logical connections.

Limitations

- Potentially superficial;
- Can cause tunnel vision and limit the identification of other contributors.

The method uses Boolean logic with “and” and “or” gates as schematically presented below. There are always minimum 2 inputs per output and all events must be connected by gates. For clarity, there are no gate-gate connections. It is extremely useful in determining the critical path(s). For the top event it is useful to define it “negatively” i.e. in a failure mode. Once the top event is defined, it is worked top-down and left-right in each branch of the Fault tree. It is necessary to make sure that all possible inputs are represented. It is then continued down on each input – which now becomes an output. This way, branches are created. For large trees, it is possible to transfer from one branch to another by inserting adequate symbols at the transfer points. After all branches are developed, a research begins to eliminate some possibilities which will make the Fault tree easier to manage. For every piece of information on the tree, source references need to be provided. Once the full fault tree is constructed, the critical path that actually happened can be identified and by doing so, the answer on “how did it happen” has been answered.

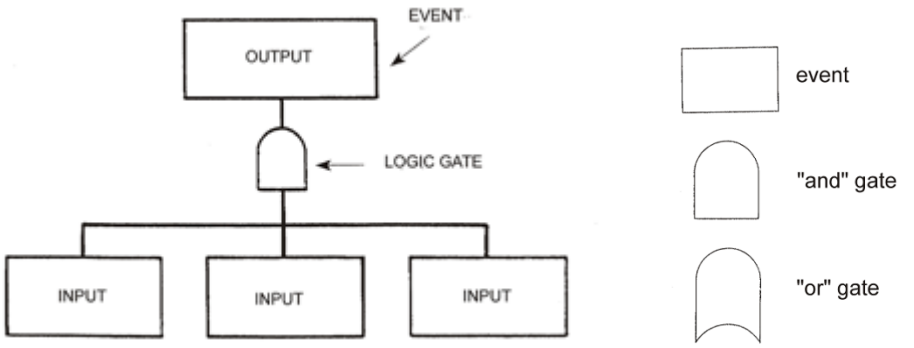

Figure 24: Symbols used in Fault Tree analysis (JRC, 2018)

This method originated in the aerospace industry and was initially used primarily for hardware issues. Today its use has been expanded also to procedural and human problems.

6.2.12 Probabilistic precursor analysis

CCDP is probably the only method that provides **quantitative estimation of safety significance of an event** (IAEA, 2004).

Precursor analysis uses the concept of CCDP to determine the safety significance of an event. It is a measure in the PSA model of how far an event which is being analysed is from the core damage scenario.

International Nuclear and Radiological Scale (INES) has also been designed to provide information about the safety significance of an event, but only for the purposes of communicating with the public. The Precursor analysis is however much more detailed and does not measure only the real consequences of the event but can also address “near missis”, when there were no actual consequences but large potential for a serious event.

CCDP is defined as the probability of core damage given that either:

- an initiating event has happened at the plant, or
- safety related equipment was out of service for prolonged time duration.

In some cases both can happen simultaneously, which would also be classified as a precursor.

Figure 25 schematically represents a precursor with the initiating event and the prolonged safety system unavailability.

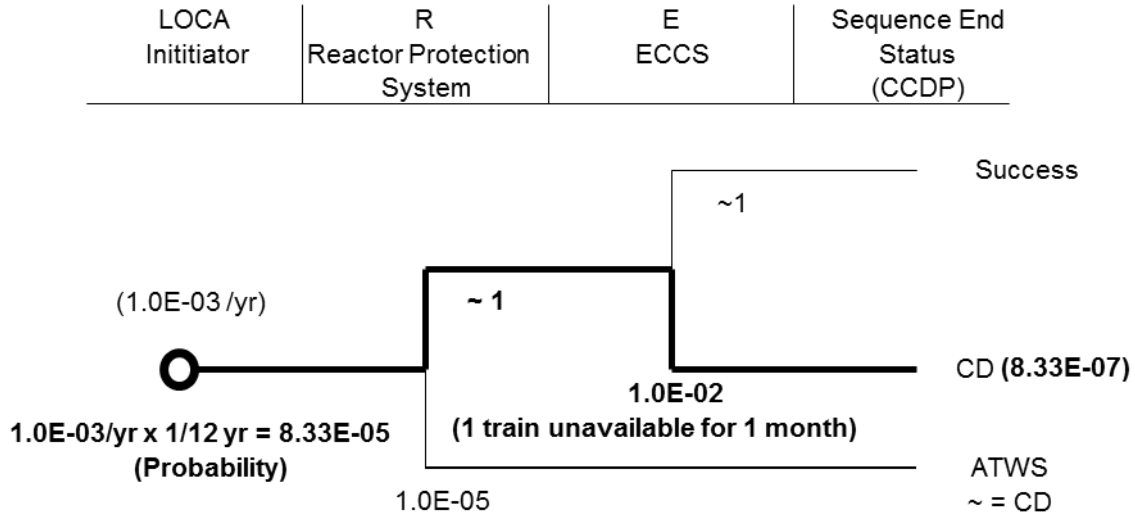

Figure 25: Conditional Core Damage Probability (CCDP)

In accordance with the above definition, there are two types of precursors:

- a transient which interrupts normal operation;
- unavailability or a degradation of equipment/systems for a longer time period.

In the first case when we are dealing with the transient that interrupts normal operation, we see a real effect on plant operation. In this case it is easy to relate the event to an initiating event in the PSA. Scenarios or sequences in PSA that are affected by this event are all those developing from that particular initiating event.

In the second case, when we are dealing with longer unavailability of safety systems, there is no immediate impact on plant operation. It is therefore harder to associate the event with any particular initiating event in the PSA study. The precursor affects several safety functions and all sequences which involve the affected safety systems/functions for all initiating events need to be considered.

The process of precursor analysis involves therefore the following steps:

Step 1: Understanding the event

In this step, thorough analysis of what has happened needs to be performed in order to be fully familiar with the development of the event.

Step 2: Mapping of the precursor on the PSA

Mapping of the precursor involves relating what has happened and the implications on the PSA model. In most cases it will be found that the precise same sequence that has happened during the event is not fully modelled in the PSA. It is therefore necessary to revise and expand the PSA model in such a way as to include also such sequence.

Step 3: Quantification of sequences

In this step, PSA reliability model is adopted and failure probabilities have been estimated.

Step 4: Initial evaluation

After having all necessary input data, the CCDPs are calculated for all affected sequences.

Step 5: Recovery actions

During this step, potential recovery actions are determined and adequately modelled.

Step 6: Evaluation

Evaluation is performed as the last step of this part of the precursor study with recalculation of importance measures (Risk Achievement Worth – RAW and Risk Reduction Worth – RRW) and performance of sensitivity and uncertainty analysis.

Step 7: Extension

In many cases, an additional "What-If" analysis is performed to evaluate what could have happened under different conditions. This part of the analysis can give us very useful insights about the potential consequences of such events.

Step 8: Reporting

In this final step, interpretation, conclusions, insights and corrective measures are documented.

The usual terminology used in precursor analysis to distinguish the importance of calculated precursors is the following:

CCDP < 10^{-6} not considered to be a precursor

10^{-4}> CCDP > 10^{-6} **Precursors**

10^{-4}> CCDP > 10^{-3} **Important Precursors**

CCDP > 10^{-3} **Significant Precursors**

The precursor analyses are performed in many countries worldwide, by utilities, regulatory bodies or technical support organisations. In the following section, the selected experiences from several countries will be described, descriptions coming from a number of annual meetings organised by Electrabel (Belgium) on the subject of Precursor analyses with the aim of the exchange of experience with the performance of such analyses (Electrabel, 2010):

United States of America (IAEA, 2012)

The US Nuclear Regulatory Commission uses precursor analyses for several programmes:

1. **Accident Sequence Precursor programme (ASP)**

All events reported under LER (Licensee Event Reports) are screened and the precursor analysis performed on those that are seen as suitable (not all events can be modelled by PSA, as will also be seen in later section on deterministic transient analyses). From the start of the accident sequence precursor programme until 2010 almost 65,000 LERs have been

reviewed. After 2011, the results of precursor analysis are no longer in the public domain as they are a perfect tool for identification of plant vulnerabilities and as such have been removed for the obvious security reasons.

The NRC rule stipulates that all significant precursors (CCDP > 10^{-3}) must be reported to the US Congress. During the past 30 years, significant precursors occurred once every 5 years, the last one being the Davis-Besse vessel head corrosion event in 2002, which had the CCDP of 6.0×10^{-3}.

The accident precursor programme also analysed the August 14, 2003 US Grid event when 9 NPPs lost off-site power for 1 – 6 hours. The events drew significant public attention but precursors were not very significant. CCDPs for affected plants ranged from 4.0×10^{-6} to 3.0×10^{-5}.

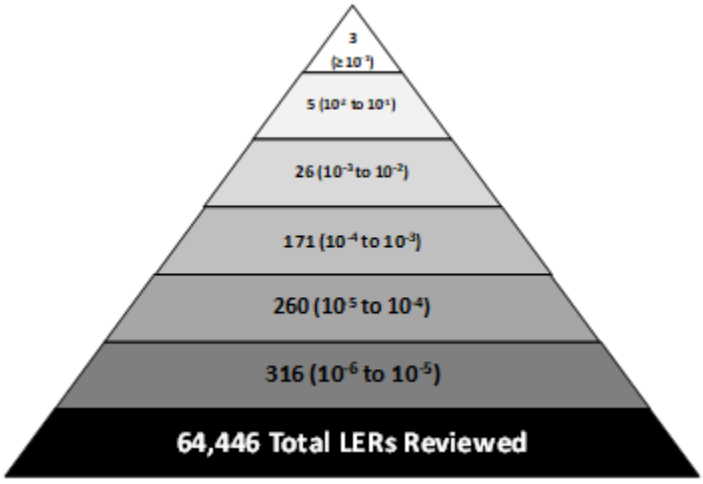

Figure 26: Accident Sequence Precursor Programme findings (IAEA, 2012)

The three events among the LERs with CCDP > 10^{-1} were the following:

- Three Mile Island on March 28, 1979 with CCDP = 1.0 when the operator misinterpreted plant conditions, including the reactor coolant system (RCS) inventory, during a transient triggered by a loss of feedwater flow and a stuck open power operated relief valve (PORV). As a result, the operator prematurely shut off high pressure safety injection, turned off the reactor coolant pumps, and failed to diagnose and isolate a stuck-open PORV. With no RCS inventory makeup, the core became uncovered and fuel damage occurred.
- Rancho Seco on March 20, 1978 with CCDP = 1.0×10^{-1} when, with the reactor at power, a loss of main feedwater caused a reactor trip. The instrumentation drift falsely indicated that the steam generators contained enough water and the operator did not take prompt action to open the auxiliary feedwater flow control valves to establish the secondary heat removal. As a consequence, it resulted in the steam generators drying out.
- Browns Ferry fire on March 22, 1975 with CCDP = 2.0×10^{-1} when the fire was started by an engineer, who was using a candle to check for air leaks through a penetration seal to the reactor building. The fire resulted in significant damage to cables related to the control of Units 1 and 2. All Unit 1 emergency core cooling systems were lost, as was the capability to monitor core power. Unit 1 was manually shut down and cooled using remote manual relief valve operation. Unit 2 was also shut down.

2. Significance determination process (SDP)

Significance determination process is used to characterise the significance of inspection findings. It provides the framework for discussing and communicating the risk significance of inspection findings. It also provides a basis for the assessment of the licensee performance

and enforcement actions associated with those findings. The inspection findings are categorised into four levels, marked with different colours, green, white, yellow and red in increasing safety significance. The precursor values for each level are depicted in Figure 27.

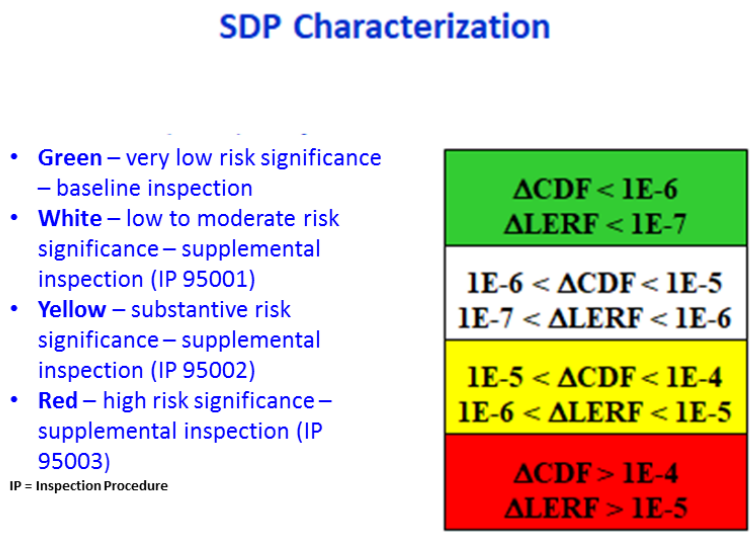

Figure 27: Significance determination process (IAEA, 2012)

3. Event response/ Incident investigation

On certain safety significant events, the NRC may decide to send an inspection team in addition to the investigation performed by resident inspectors. The composition of the team and its mandate is determined by the seriousness of the event, which is determined by the precursor analyses. It can be a special inspection team, augmented inspection team (AIT) or incident investigation team (IIT) in the increased order of importance. The corresponding precursor values are indicated in Figure 28.

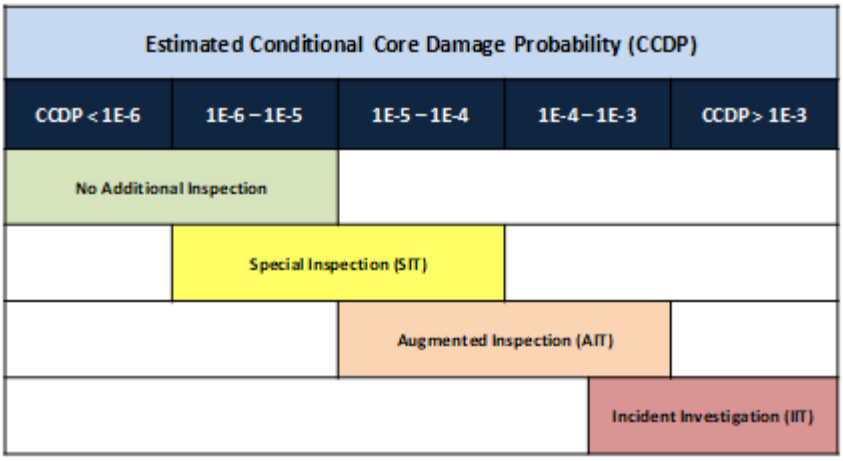

Figure 28: NRC Incident investigation teams

France (Electrabel, 2010)

In France, about 450 significant events are reported each year for the 900 MWe, 1300 MWe and 1450 MWe series NPPs. About 50% of those are selected for in-depth analysis each year and half of those are suitable for precursor analysis. The rest involves for example containment degradation, earthquake resistance weaknesses, exceedance of operational limits and conditions etc. About 15 events per year are identified as precursors i.e. with CCDP > 10^{-6} and normally no more than one as a significant precursor i.e. with CCDP > 10^{-4}.

The trend that EDF has observed in the past decade is that the number of precursors and their safety significance has been decreasing.

An interesting comparison was performed by IRSN (France), GRS (Germany) and NUPEC (Japan) as a blind exercise on the same event. The results were very different. The reasons were use of different PSA models, use of different hypothesis and presumed different duration of unavailability or the extent of degradation of equipment which has shown, how sensitive precursor analysis to input data is.

Spain (Electrabel, 2010)

At the Spanish regulatory body CSN, the precursor analysis is performed on the request of the feedback of operating experience group. On average 3 – 5 events are analysed each year. The CSN has established an internal rule that for each event with CCDP > 10^{-4} a special regulatory inspection is carried out at the utility.

In addition CSN has established internal safety indicators that there should be:

- no events with CCDP > 10^{-2},
- no more than one event with CCDP > 10^{-3} in 5 years,
- no more than 2 events with CCDP > 10^{-4} in 5 years,
- no more than 5 events with CCDP > 10^{-5} in 5 years, but no more than 1 in any single year and
- no more than 10 events with CCDP > 10^{-6} in 5 years, but no more than 2 in any single year.

Germany (Electrabel, 2010)

German precursor study started already in 1985 for Biblis NPP but it has been carried out more systematically since 1997 by their technical support organisation GRS. The general findings from their precursor analysis are that half of them are due to long system unavailability and half due to common cause failures.

The main benefits from those analyses are better determination of safety significance of events, identification of potential weak points in safety and safety-related systems and identification of events that resulted in safety margin degradation.

The results also show the approximately equal distribution of more important precursors between their PWR and BWR plants, but higher percentage of less important precursors (those with CCDP between 10^{-5} and 10^{-6}) in their BWR plants.

Belgium (Electrabel, 2010)

The Belgian precursor program was started in 1997 by AVN, the Belgian technical support organisation at that time also acting as the Belgian regulatory body.

Each year they have screened around 50 potentially interesting events that were suitable for precursor analysis. About 10% were selected for in-depth precursor analysis that was then also performed.

For each selected event, a CCDP for the real event has been evaluated and a CCDP for the “what-if” case. This has enabled them to identify potential safety issues for possible improvements.

Finland (Electrabel, 2010)

All Finish NPPs have completed full PSA Level 1 for power operation as well as for shutdown and low power states, including internal and external hazards.

As such they are very well equipped for precursor analyses. Their precursor programme provides overall picture on safety significance of events and system availabilities. The results of their precursor programme serve their regulatory body STUK as means of prioritizing future inspection actions.

Czech Republic (Electrabel, 2010)

Precursor analyses are performed by the Czech technical support organisation Rez on behalf of their regulatory body SUJB. They have created an operational event history database and as in the case of other countries, the results are used to prioritise the regulatory inspection actions.

Hungary (Electrabel, 2010)

The precursor analyses in Hungary are performed by VEIKI, their technical support organisation in cooperation with the regulatory body HAEA. The events to be analysed are provided to VEIKI by HAEA. Their precursor program is based on the NRC ASP approach and is in operation since 1999. Domestic software has been developed for this purpose and their unit-specific PSA models are regularly updated.

6.3 Deterministic transient analysis

Deterministic transient analyses are used for fast developing events i.e. transients (IAEA, 2009). It is a simulation of the plant behaviour with a computer code. A NPP model is constructed by combination of smaller parts by the so-called nodalisation process. By applying initial and boundary conditions as input data, the behaviour or the response of the plant is then calculated by simulation.

Such analyses are essential for better understanding of the physical phenomena taking place during a specific event. It is the only method that can calculate the erosion of safety margins while an event is happening. As such, it can also be used for operator training and procedure validation and verification.

In performing deterministic analyses we can compare code predictions with actual failures which have occurred. Both code predictions and failures have uncertainties and therefore, are distribution functions (OECD 2007; OECD 2011) – see Figure 29 and Figure 30. The distribution of code predictions/results is a consequence of uncertainties in initial and boundary conditions data as well as in computer model. The distribution of failures is on the other hand a consequence of our limited knowledge of the precise phenomena that cause failures.

Figure 29 demonstrates the concept of safety margin. On the left hand side the calculation results are presented as the probability distribution and on the right hand side the probability distribution of failures. Both distributions are the consequence of above mentioned uncertainties. The difference between both distribution peaks can be termed an “apparent margin”. The term is not fixed and also not universally accepted, it can be termed also differently, it is only important that it is precisely defined.

The difference between the 95/95 value of the code calculation and the value of the negligible tail of the failure distribution is normally called “licensing margin” or “safety margin”. The name “licensing margin” indicates that this is the value which is normally required by the regulatory authority to be fulfilled in safety analyses for Design Basis Accidents (DBA).

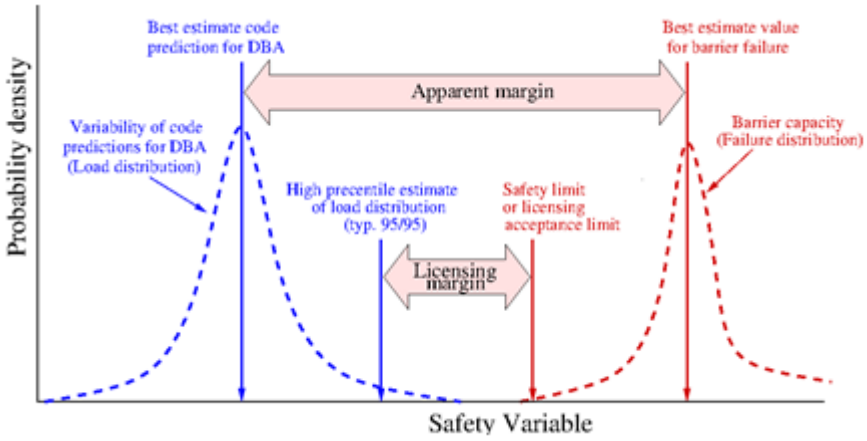

Figure 29: Distribution of code predictions and distribution of failures (OECD, 2007)

Historically, deterministic safety analyses, which generally consist of transient analyses and Loss of Coolant Accident (LOCA) analyses, were using strictly conservative approach due to the limitations in computer capabilities and lack of experimental data. With the rapid development in computer capabilities and increased number of experimental data, deterministic calculations evolved into more realistic scenarios.

The IAEA Specific Safety Guide SSG-2 on Deterministic Safety Analyses (IAEA, 2009) recognises 4 options.

- The first option is strictly conservative option which used conservative computer codes/models with conservative input data on initial and boundary conditions. It is known as the Conservative option.
- The second option uses Best Estimate (BE) codes i.e. more realistic codes but still utilises conservative initial and boundary conditions. It is termed as the BE option.
- The third option uses BE codes and realistic input data for initial and boundary conditions but requires the evaluation of uncertainties. This option is called Best Estimate Plus Uncertainty (BEPU) option.

All three above options have in common that the assumptions on the availability of safety systems are conservative.

- The fourth option is the extension of the BEPU where the assumptions on the availability of safety systems is based on the PSA or rather system reliability results. It is known as Extended BEPU analyses option or in short E-BEPU.

Table 3: Four options for deterministic safety analyses (after IAEA, 2009)

Applied codes	Input & BIC (boundary and initial conditions)	Assumptions on systems availability	Approach	Regulation
Conservative codes	Conservative input	Conservative assumptions	Deterministic*	10 CFR § 50.46 Appendix K
Best Estimate (realistic) codes	Conservative input	Conservative assumptions	Deterministic	SG NS-G-1.2 para 4.89
Best Estimate (realistic) codes	Realistic input + Uncertainty	Conservative assumptions	Deterministic	SG NS-G-1.2 para 4.90
Best Estimate (realistic) codes	Realistic input + Uncertainty	PSA-based assumptions	Deterministic + probabilistic	Risk informed

Each subsequent option from Table 3 requires more computational time and more effort from the analyst. The easiest calculation is the conservative calculation where a single run can demonstrate that under a certain conditions (transient, LOCA, etc.) the variable which is being calculated (temperature, pressure etc.) stays below the regulatory limit and sufficient safety margins are still present. However, in certain cases, where the results of calculations come very close to the regulatory limit it is necessary to perform a less conservative and more realistic calculation that would reveal greater available safety margin. It requires more computational time and effort but pays back in the demonstration of greater safety margin availability. Figure 30 illustrates how the available safety margins increase with the use of different computational options. Already option 2 reveals more safety margin than option 1. Also the upper uncertainty bound of option 3 reveals more safety margin i.e. greater distance to the acceptance limit than the option 2.

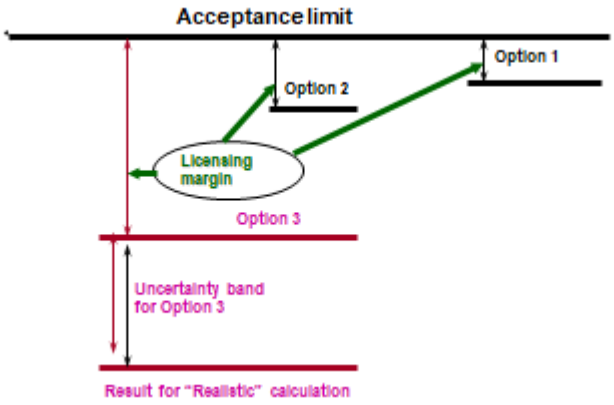

Figure 30: Safety margins as calculated by options 1, 2 and 3. (JRC, 2018)

6.4 Probabilistic risk integration using Bayesian Networks

Van Erp and van Gelder (2015) present a comparison of quantitative risk analysis frameworks for single and multiple hazards as part of the RAIN project. An objective ranking effort is carried out using Similarity Judgement, Analytic Hierarchy Process (AHP) and a Delphi-Panel, to order existing frameworks used to assess risks due to single hazards. Among the 22 different frameworks considered were BN, bow-tie analysis, cause and consequence analysis, checklist, event tree analysis, fault tree analysis, hazard and operability study, what if analysis, point method, SWOT analysis, decision matrix, common safety method, critical path method and program evaluation and review technique, method of optimal network connection, method of consuming activities, Gantt diagram, methods and measures lowering impacts, subsystem of technical security devices, Subsystem of organisational measures, Bayesian probabilities, and influence diagrams. Each of the above listed frameworks was evaluated under the following criteria:

i. Knowledge and Information – overall expertise within research consortium, availability of data, expert engineering knowledge;
ii. Framework – completeness, reliability, validity, transparency;
iii. Use of Framework – attractiveness, simplicity, extensibility;
iv. Innovativeness of Framework; and
v. Suitability for problem.

The weightage for each of the above criteria/sub-criteria were assigned using AHP. Finally, the Delphi panel scored each of the framework types based on the selected criteria with an outcome lying between 0 and 1. The conclusion of this effort in the RAIN project was that Influence diagrams (a specific case of BNs that includes decision variables), BNs and Bayesian probabilities-based methods ranked as the best frameworks for risk assessment of single and multiple hazards, and it is recommended that tools using Bayesian probability theory be implemented in the inference phase of the risk assessment. At the framework

level, no differentiation was made between single and multiple hazards; for both types of hazards, the inference phase is implemented with Bayesian probability theory and the decision phase through decision theory. The difference between single and multiple hazards occurs at the implementation level where interdependencies and cascading effects need to be accounted for in the case of multiple hazards. Further details can be found in van Erp and van Gelder (2015). In this section, BN methodology is discussed in detail and their applications are summarized. Importantly, in the NARSIS context, the suitability of BN to risk analysis applications is discussed. Other deterministic and probabilistic risk integration tools and methods used in high-risk industries are discussed in Section 7, and hence, are not detailed in this section. Advantages of BNs over widely used risk integration tools such as the FT are also discussed later in Section 7.4.

6.4.1 Bayesian Networks (BNs)

The risk assessment framework can be separated into two parts; (i) the inference phase, where the resultant probability distributions of each possible action under consideration are derived, and (ii) the decision-making phase, where the safest or most appropriate action is selected. While dealing with multi-hazard systems composed of uncertainties and evolving data, methodologies that apply Bayesian probability theory are assessed to be most appropriate for the inference phase and decision theory-based methods are mostly suited for the decision phase (van Erp and van Gelder, 2015).

A BN is a specific application of Bayesian probability theory. A BN is a directed acyclic graph which is composed of nodes that correspond to random variables, and arcs that link dependent variables. The direction of the arcs indicate the cause-effect relationships between the nodes (“directed”), and these arcs never cycle back to parent nodes (“acyclic”). Hence, a BN is a visually explicit representation (“graph”) of the mutual causal relationship between random variables, and represents the joint probability distribution (JPD) of all random variables within the model.

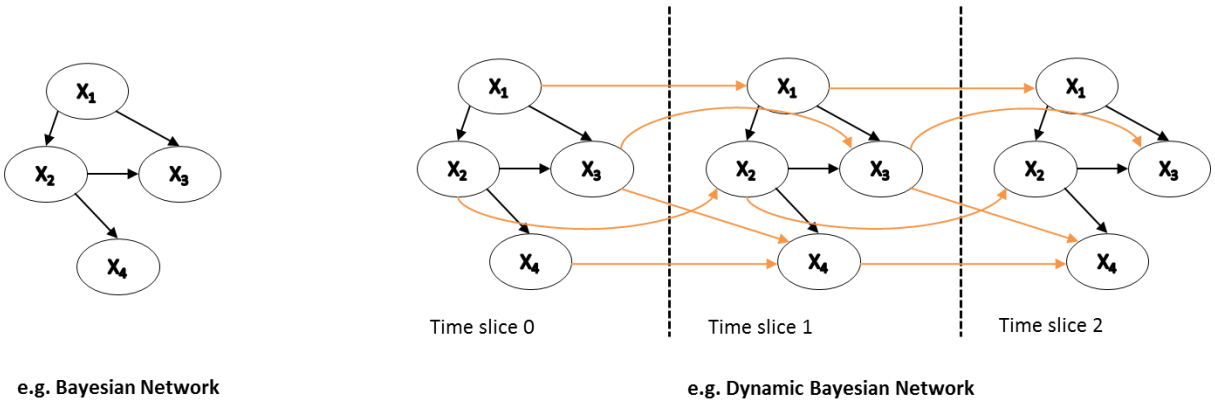

Figure 31: Examples of BN and DBN (after Jensen and Nielsen, 2007)

The dependencies between random variables are usually encapsulated within conditional probability tables (given by (P(Xi)|Parents(Xi))) at each node of the BN. The JPD is given by the chain rule of BNs:

$$P(X_1, X_2, \dots, X_n) = \prod_{i=1}^{n} P(X_i \,|Parents(X_i)) \qquad \textit{Equation 6}$$

The JPD of the static BN shown in Figure 31 is given by:

$$P(X_1, X_2, X_3, X_4) = P(X_1)P(X_2|\,X_1)P(X_3|X_1, X_2)P(X_4|\,X_2) \qquad \textit{Equation 7}$$

A DBN is a type of BN where the probability distributions of random variables vary over time. The DBN is composed of discretised time slices that allow for a random variable to have

conditional dependencies: (i) with its parents within a given time slice, (ii) with its parents within the previous time slice, and (iii) with itself within the previous time slice:

$$P\left(U^{t+\Delta t}\right) = \prod_{i=1}^{n} P(X_i^{t+\Delta t} | X_i^t, \pi\left(X_i^t\right), \pi\left(X_i^{t+\Delta t}\right)) \quad \textit{Equation 8}$$

Through Bayesian inference, the JPD can be queried to infer the state of a random variable given our beliefs regarding the other variables. In other words, BNs can be used to answer probabilistic queries when one or more variables have been observed. For example, for the static BN in Figure 31, assume we know that $X_2 = x_2$ and we want to find out the conditional probability $p(x_1 | x_2)$; the posterior distribution is obtained by marginalising the joint distribution given in Equation 7 as follows:

$$p(x_1, x_2) = \sum_{x_3, x_4} p(x_1, x_2, x_3, x_4) \quad \textit{Equation 9}$$

$$p(x_2) = \sum_{x_1, x_3, x_4} p(x_1, x_2, x_3, x_4) \quad \textit{Equation 10}$$

Now, $p(x_1 | x_2) = p(x_1, x_2)/p(x_2)$. This way, the BN can be queried and calculated for any required distribution. However, as the size of the BN gets beyond that of trivial cases such as the above, this method of inference becomes computationally inefficient. To allow for more efficient inference within BNs, several algorithms have been proposed – either exact or approximate inference algorithms. The most widely known exact inference algorithms are the 'variable elimination' method and the 'junction tree' algorithm. In exact inference, the conditional probability distribution over the variables of interest is analytically computed. Again, exact inference can get computationally tedious and hence, several approximate inference algorithms on statistical sampling (often random sampling) have been developed. Some of the more common choices for approximate inference algorithms are rejection or importance sampling. More advanced Markov Chain Monte Carlo (MCMC) schemes such as Gibb's sampling are also frequently used. Further details regarding these methods can be found in Korb and Nicholson (2010), Koller and Friedman (2009), and Robert and Casella (2009). Inference techniques for DBNs are based on similar principles and several algorithms exclusive to DBNs have been developed (Murphy and Russell (2002) provide a summary).

Along with inference, two other major functions for BNs are parameter and structure learning. The data-based estimation of unknown parameters within conditional probability distributions of random variables so as to maximise the probability of occurrence of the available data, is called parameter learning. The estimation of unknown network topology within the BN based on algorithms is called structure learning.

Discrete BNs are those where each node is represented by a discrete random variable. Continuous BNs, similarly, model continuous random variables at their nodes. BNs involving both continuous and discrete variables are often called Hybrid BNs (HBN). The nature of random variables is important in defining the conditional dependency relations between parents and children and solving the BN.

6.4.1.1 Discrete, continuous and hybrid Bayesian networks

As discussed earlier, discrete BNs are those with discrete random variables at their nodes. Discrete BNs have been widely used in several applications and algorithms have been developed for exact and approximate inference of discrete BNs (Pearl, 1988; Zhang, 1994 etc.). However, they are limited in that they often fail to model variables that are continuous in nature. Also, for complex problems building conditional probability tables becomes unwieldy (because networks can be large and discrete variables can have multiple states) leading to errors and offhand quantification.

Continuous BNs were originally developed for normal random variables (Gaussian BNs). A mean and a conditional variance are specified for each node and a regression coefficient is assigned to each arc in the BN. This greatly reduces the effort of mentioning large numbers

of conditional probabilities as in the case of discrete BNs. Nevertheless, continuous BNs are limited in their assumptions: (i) random variables being normally distributed and, (ii) their joint distribution being normally distributed. Both these assumptions, of course, need not be true in real-world problems. In addition, practical problems often tend to be composed of both discrete and continuous random variables, and this leads to the need for a hybrid approach.

Langseth et al. (2009) review inference approaches for HBNs including some mentioned below. One approach for a HBN is a modification of the continuous BN where discrete variables are allowed, but only as parents of continuous variables (Cowell and Dawid, 1999). This approach does not eliminate the assumption of normality in the variables. Another widely used method to tackle HBNs is through discretisation of continuous variables by division into intervals. For reasonable accuracy, a significantly large number of divisions need to be made, which leads to challenges of scarcity of data for each interval as well as excessively large conditional probability tables. Another approach, called the enhanced BN (or eBN), is based on structural reliability methods (Straub and Der Kiureghian, 2010). This approach involves transforming the BN into a reduced structure that contains only discrete variables, allowing for the use of established inference methods for discrete BNs. This approach helps in inference of large BNs with several random variables (Straub and Der Kiureghian, 2008; Straub and Der Kiureghian, 2009). Nevertheless, the method still requires some discretisation with respect to the outcome space of a continuous variable that is part of the inference (Hanea et al. 2015). Mixture of truncated basis functions (MoTBFs) method perform a type of discretisation where by densities are estimated within each region of the density function using Fourier series approximations (Langseth et al., 2009). Two methods that would fall under MoTBF framework are the mixture of truncated exponential (MTE) model and the mixture of polynomials model (Langseth et al., 2010, Shenoy and West, 2015). Computational efficiency within large BNs remains a challenge for these methods, and also the data requirement is relatively high for implementation (Hanea et al., 2015; Fernandez et al., 2013).

This leads to the method originally proposed by Kurowicka and Cooke (2004) and further developed by Hanea et al. (2010), called the Non-Parametric Bayesian Network (NPBN). In this method, the JPD is built using marginal distributions of the variables along with one-parameter copulae assigned to the arcs to define conditional dependence (Nelsen, 1999). The copulae are parametrised using Spearman's rank correlations. Hence, the NPBN can be quantified using just the marginal distributions of the random variables and conditional dependence relations equal in number as the number of arcs in the graph. The copulae are assigned to the arcs based on a non-unique ordering of parent nodes. A specific configuration of the graphical structure, the marginal distributions and the conditional copulae used provide a unique JPD of the variables. Hanea et al., (2015) provide more details of the NPBN approach and certain modifications to the original approach.

Inference is performed within the NPBN using sampling procedures. Hanea et al. (2006) detail a general sampling procedure for NPBNs using one-parameter copulae. Although any one-parameter copulae could be implemented, using anything but the Gaussian copula significantly multiplies the computation effort due to increased numerical computations of multiple integrals. The Gaussian copula allows for sampling from the joint distribution of original variables along with the dependence structure realised by the copula, and hence, significantly reduces computational effort. Hence, the most efficient inference method in NPBNs is to realise the rank correlations using a normal copula. Another option for inference is the use of fast discretisation algorithms typically used for discrete BNs. Once the JPD of the variables is defined in the NPBN approach, the JPD can be sampled extensively and this 'fake' dataset can then be used for discretisation. This approach is different from direct discretisation of continuous variables which necessitates lot of assessment of intervals and leads to offhand quantifications. Hence, inference algorithms for discrete BNs can now be used to perform inference on the JPD defined by the NPBN approach (Hanea et al., 2006).

While dealing with HBNs, the NPBN approach meets some challenges in handling discrete variables. Defining Spearman's rank correlations between discrete variables or between

discrete and continuous variables becomes tricky, though Hanea et al. (2007) provide theoretical solutions to this problem. Nevertheless, discrete BNs were preferred over NPBNs if discrete variables in the network outnumber continuous variables (Hanea et al., 2015).

Hence, the NPBN offers greater computational efficiency in the case of larger, complex networks, while moving away from cumbersome definitions of conditional probability tables, the loss of accuracy from discretisation and assumption of normal distribution of variables. However, the increased computational efficiency is mostly limited only to the assignment of the Gaussian Copula to the arcs. Moreover, NPBNs are not well suited for problems involving more discrete variables than continuous variables.

With the background of these basic BN concepts, we will now look at some applications of BNs in risk analysis. Specifically, we will review studies that have applied BNs for some or all of the multi-risk aspects discussed in Section 3.

6.4.2 Bayesian network applications to risk analysis

Among the various risk analysis tools reviewed in the literature as part of this report, Bayesian networks have been used extensively across various risk analysis applications that consider multi-risk, complex facilities, low probability-high consequence events, expert judgement and thorough uncertainty analysis. This fact is also reflected in publication trends indicating the increased use of BNs in risk analysis in engineering (Figure 32). BNs also show up in the most frequent keywords associated with “risk assessments” among engineering publications (Figure 33).

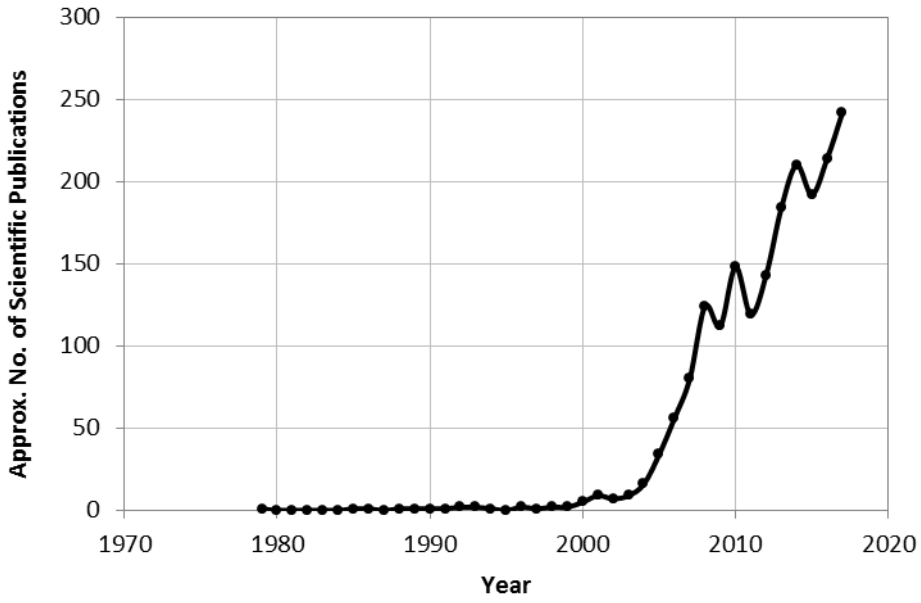

Figure 32: Approximate trend of publications of Bayesian networks used in engineering risk analysis contexts (based on data from the website www.scopus.com)

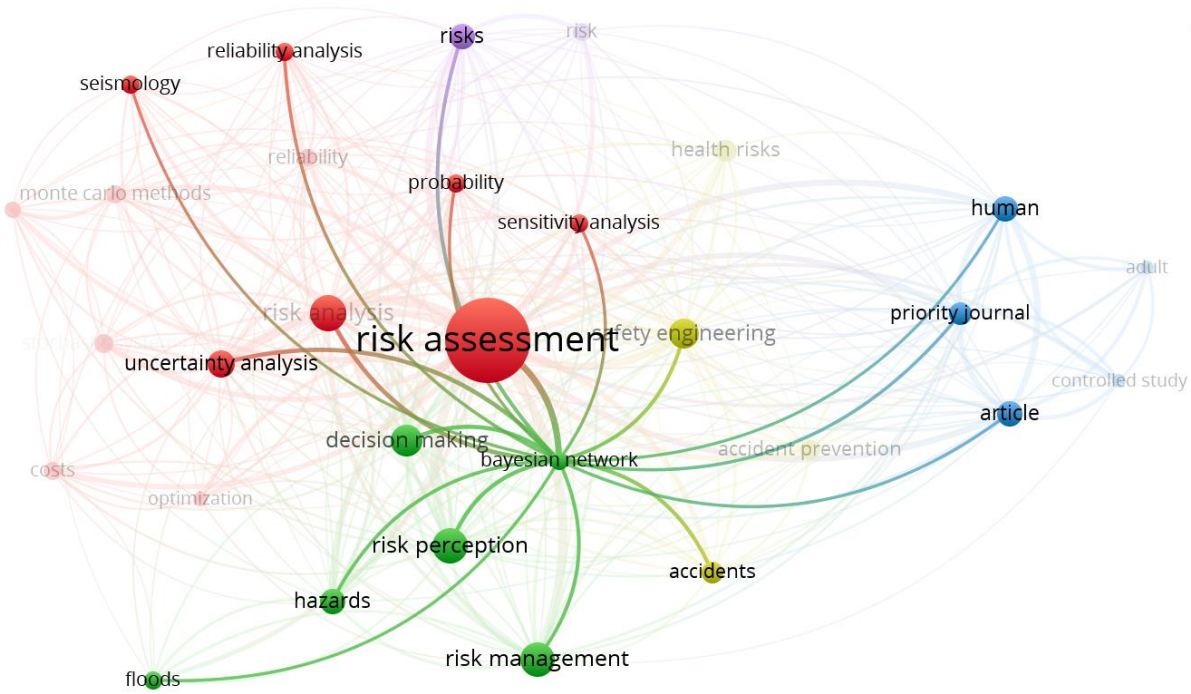

Figure 33: Most occurrences of keywords associated with "risk assessments" in engineering publications (top 30 occurrences among 2000 most relevant publications, based on data from the website www.scopus.com)

BNs have been extensively used for risk analysis applications in various engineering and other fields. In this section we will review some of the applications in engineering that contain transposable aspects to NPP risk assessments.

In Section 3, we saw several applications of BNs with regards to their use in integrating various multi-risk aspects. Table 4 provides a summary of relevant studies that have integrated multi-risk aspects such as multi-hazard, multi-vulnerability, complex systems, low probability events, HOF, expert judgements, and uncertainty modelling. The BN features along with BN-specific conclusions from these studies are highlighted. In addition to this summary, it will be useful to understand the implementation of deterministic and probabilistic aspects within these BN applications. In other words, it is of interest in the NARSIS context, to examine the modelling of various random variables within the BN framework while performing risk assessments for these different applications. For instance, to evaluate the risk from external hazards leading to a station blackout or release of radioactive material from the power plant, the BN would model the interaction between the following random variables characterizing the following (non-exhaustive list):

- external hazards and their intensities;
- interaction of the hazards with protective structures (e.g. flood defence) as well as service structures and components within the power plant, in terms of failure/damage types;
- damage states/extents of relevant structures and components;
- emergency alarm network;
- human response and decision making;
- probability of eventual adverse consequence of interest.

All of these variables and their dependencies would act as input to the BN, while the output can be the probability of a particular state of any given variable conditional on the state of the remaining variables. Existing risk models for undesired events in the NPP, like FTs, can be converted to BNs (e.g. Boudali and Dougan, 2005).

Some of the major advantages of using BNs in risk assessments are the following:

(i) BNs allow for the complete representation of processes whose risk is being modelled, and the graphical representation works to help the decision maker in (a) understanding the risk model, and (b) following the process that led to the probabilistic answer.
(ii) BNs enable updating the risk analysis network with new evidence and studying the impact or the value of the information added.
(iii) Variables modelled in the network can be multi-state in nature - either discrete or continuous.
(iv) Probabilistic inference can be performed with relatively efficient computational algorithms, particularly for discrete or discretised variables.
(v) Probabilistic inference can be causal as well as diagnostic.
(vi) BNs can be extended to decision graphs (or influence diagrams) where optimal decisions yielding maximum utility can be identified.
(vii) Inherently, they allow for the modelling of interdependencies and cascading effects.
(viii) BNs ensure consistent treatment of uncertainty and risk.
(ix) They allow integration with other methods such as fault trees, event trees etc. that can be converted to BNs. Root cause analysis methods described in Section 6, and other deterministic risk methods can be applied to provide information to the BN either to form its structure of nodes and dependencies or to feed probabilistic data to the nodes. Thus, it serves as a good framework for integrating probabilistic and deterministic approaches.

Some disadvantages of BNs include:

(i) When the network is made up of continuous variables, either normal distribution of variables is assumed or the distribution is discretised to improve computational efficiency; both approaches could lead add to modelling error. As discussed in Section 6.4.1, using NPBNs is an efficient workaround for this problem in the case where continuous variables outnumber discrete ones. This approach, as well, assumes a normal copula dependence between variables
(ii) When the number of discretisations is increased to improve accuracy, increased conditional probabilities could lead to casual or erroneous quantification due to lack of data across all discrete states.

Overall, BNs are well-suited for risk analysis applications and demand further exploration for applications in NPPs.

Table 4: Bayesian network applications in engineering risk analysis

Study	Industry or Area of Application	Application/Research Description	Multi-risk aspects covered	BN Features				Main Conclusions	Notes
				Type of BN	Inference Method	Sampling Techniques	Number of RVs		
Boudali and Dugan (2005)	Reliability Modelling	Timed BN as a reliability analysis framework for complex dynamic systems	- Complex systems	Discrete- time BNs (explicit modelling of time as a RV)	Junction Tree (Exact)	-	17	- BNs effective option for reliability modelling and addresses issues of state space explosion and provides increased modelling power for complex systems	- Dynamic FT converted to BN - Uses Hugin Expert
Lee and Lee (2006)	Nuclear	BN-based framework for PRA of nuclear waste disposal	- Low probability events - Uncertainty propagation model	-	Bounded-variance likelihood weighting algorithm presented in this study	-	-	- Bayesian inference method presented within framework - Uncertainty propagation model with relevant parameters is presented - "Altering Evolution Scenarios" or situations that lead to deviation from normal circumstances are suggested for nuclear waste disposal problem	- Methodological framework specific to nuclear waste disposal
Ale et al. (2008)	Aviation	Integrating deterministic techniques with the BN, including human performance models (HPM) to calculate overall accident probability of planes.	- Complex socio-technical systems	Discrete	Junction tree (exact)		1400 nodes and 5000 arcs	- The Causal model for Air Transport Safety (CATS) integrates models for technical failures such as event sequence diagrams, Fault Trees, event trees and models for human behaviour in a single BBN.	- UNINET is the software to drive the BBN and is open source, written by TU Delft.
Ren et al. (2008)	Offshore Safety	Multi-risk model for offshore safety combining BNs and the "Swiss cheese" model for human and organisational factors (HOF). Five-level framework addressing latent failures	- HOF	Discrete	Marginalisation (Exact)	-	10	- "Swiss Cheese" model can be integrated with BN for modelling HOFs. - Performs better and can replace Fault Tree Analysis, Event Tree Analysis, Failure Mode and Effect Analysis, and Hazard and Operability Studies	- Fuzzy probabilities used in BNs
Mohaghegh et al. (2009)	PRA/aviation	PRA framework developed to incorporate organisational factors for complex systems. A hybrid integration approach is presented with an example using system dynamics, BNs, Event Sequence Diagrams and FTs. An example for aviation industry is provided	- HOF	Discrete	-	-	-	- Framework integrates deterministic and probabilistic methods in modelling organisational factors - Methods described to integrate different methods into a BN framework - Examples show interaction of organisational factors with technical system risk	- IRIS integrated risk analysis software used
Weber et al. (2012)	-	Literature review study for applications of BNs in dependability, risk analysis and maintenance	-	-	-	-	-	- BNs chosen due to ease of use with domain experts - Suited to represent knowledge in uncertain areas - Can be used predictively or diagnostically, for optimisation etc. - Graphical structure helps understand model and complexity - No specific semantics for BN construction	200 studies examined in chosen areas
Hossain and Muromachi (2012)	Road Transportation systems	Real-time crash prediction model for two expressways in Japan	- Complex systems	Discrete	Junction Tree (Exact)	-	4	- Model complexity can be reduced by "parent-divorcing" technique	-
Garcia-Herrero et al. (2013)	Nuclear	BN analysis of relation between organisational factors and safety culture in NPPs	- HOF	Discrete	Junction Tree (Exact)	-	13	- BN was able to identify critical organisational factors that impact safety culture in a NPP using data from a model plant in Spain - Structural learning algorithms were implemented	- 292 surveys collected from 323 workers - 120 questions on organisational culture and 35 on safety culture - 12 organisational variables linked to safety culture - Uses Hugin
Khakzad et al. (2013)	Chemical	Methodology for modelling the propagation patterns for domino effects. A BN example is demonstrated modelling both domino effects as well	- Cascading effects - Uncertainty modelling	Discrete	Junction Tree (Exact)	-	Up to 14	- New method for domino effects in chemical plants - Novelty in modelling domino effect and allowing for calculation of probability of domino effect at each level	- Uses Hugin

Study	Industry or Area of Application	Application/Research Description	Multi-risk aspects covered	BN Features				Main Conclusions	Notes
				Type of BN	Inference Method	Sampling Techniques	Number of RVs		
		as measurement of effects at different levels. Example is for the processes in a tank farm.						- Conditional probability tables populated accounting for synergistic effects	
Morales-Napoles et al. (2014)	Infrastructure	NPBN approach for modelling risk of seven earth dams in Mexico	- Multi-hazard - Low probability events	NPBN	Analytical - Gaussian copula-based inference	-	11	- Earth dam failure and failure modes modelled using continuous variables in the NPBN approach - Technique for elicitation of structured expert judgement (SEJ) presented for determining dependence structure in NPBN	- Uninet used - Some nodes data-based others fully based on SEJ
Wu et al. (2015)	Construction	BN-based decision support system for tunnel construction safety	- Complex dynamic systems - Uncertainty/sensitivity analysis	Discrete	Unknown	-	11	- DBN can model geological, design and mechanical variables during construction - DBN useful for prediction, performing sensitivity analysis as well as diagnostic analysis. Helps decision-making - DBN provides higher accuracy of results than static-BN for a time-variant problem	- Inference algorithms and software tools used are not mentioned
Liu et al. (2015)	Regional	Multi-risk framework that uses BNs for evaluating hazard and vulnerability interactions. Test case of debris flows triggered by earthquakes and precipitation is presented	- Multi-hazard - Multi-vulnerability - Low probability events	Discrete (may be discretised from continuous variables)	Junction Tree (Exact)	-	17 (19 arcs)	- Effects of interactions between hazards and vulnerabilities are quantified with necessary accuracy - Cascading effects and time-variant vulnerability are captured	- Uses Bayes Net Toolbox in MATLAB.
Gehl and d'Ayala (2016)	Infrastructure	Derivation of multi-hazard fragility functions using reliability methods and BN for a bridge system. Applied to test bridge system for earthquake, flood and ground failure scenarios.	- Multi-hazard - Multi-vulnerability - Low probability events	Continuous (discretised)	Junction Tree (Exact)	-	Up to 64 nodes (140 edges)	- BN method able to solve complex systems with multiple failure modes and damage states - BN provides unified framework for hazard and vulnerability analysis for seismic risk	- Uses Bayes Net Toolbox
Van Erp et al. (2017)	Land-based infrastructures	Risk analysis framework for collateral impacts of cascading effects in land-based infrastructures due to extreme weather events	- Cascading effects	Continuous (discretised)	Exact by product- and sum rules		20	- Bayesian methodology by which system state probabilities may be estimated for systems that are subjected to cascading/domino effect hazards. The methodology makes use of a newly developed Probability Sort algorithm in order to estimate Markov Chains for what otherwise would have been intractable (in)homogeneous transition matrices.	- Probabilistic sort algorithm developed in Matlab (Open Source)

6.5 Conclusions

For the use of different event investigation and risk integration techniques it can be generally concluded that:

- The Root Cause Analyses remain the predominant technique for incident evaluation as it reveals the true root causes that have caused the event to happen.
- Precursor analyses are the state-of-the-art method for the determination of safety significance of events.
- The Deterministic Transient Analyses are the only way to fully understand the physical behaviour of the plant during fast developing transients or design basis accidents. The analysis can of course be also applied to the Design Extension Conditions (DEC).
- Bayesian networks are able to capture highly complex integrated situations and can be used to identify weaknesses.

All methods complement each other and therefore each has its place in practice.

7 Methods applied in high-risk industries

7.1 Nuclear industry

7.1.1 Introduction

The current approach to nuclear safety adopts the complementary use of PSA and more “classical” deterministic principles in a risk-informed approach. A risk-informed regulatory approach implies that risk insights be used as supplement of deterministic information for safety decision-making purposes. In this view, the use of risk assessment techniques is expected to lead to improved safety and a more rational allocation of the available resources.

PSA and PRA have evolved over many years and in various jurisdictions as a useful tool to evaluate NPP risk and support risk-informed decision making, e.g., providing insights on design vulnerabilities. By means of PSA, established safety goals have been quantitatively analysed as one method of demonstrating reactor safety: it includes a comprehensive treatment of all operating states as well as of internal and external events.

The starting point of the risk-informed framework is that safety justification must be based on the coupling of deterministic (consequences) and probabilistic (frequency) considerations to address the mutual interactions between:

- stochastic disturbances (e.g. failures of the equipment) and
- deterministic response of the plant (i.e. transients).

In order to illustrate these new possibilities provided by the frontiers in safety assessment process a foreword to recall main features of either methodology is given, with greater emphasis on PSA, to achieve risk-informed decision-making approach, which will be extensively described in Section 7.1.3.4.

7.1.2 Deterministic approach

This analytical procedure has been widely used throughout the world in the design of nuclear reactors for the purpose of generating electricity. It attempts to ensure that the various situations, and in particular accidents, that are considered to be plausible, have been taken into account, and that the monitoring systems and engineered safety and safeguard systems will be capable of ensuring the containment of radioactive materials. The deterministic approach is based on the two principles referred to as leak tight barriers between the radioactive source and the public and the concept of defence-in-depth (DiD). The leak tight "barriers", of which there are generally three, consist of: the fuel cladding, the primary reactor coolant system, and the containment building. DiD consists of taking into account potential equipment failures and human errors, so that suitable preventive measures may be applied, and of making provisions for the installation of successive devices to counter such failures and limit their consequences. It consists of several successive stages (or levels), hence the term "defence-in-depth" (IAEA, 1996a):

- Prevention and surveillance: all necessary measures are taken to ensure that the plant is safe; items of equipment are designed with adequate safety margins and constructed in such a way that under normal operating conditions the risk of an accident occurring in the plant is kept to a minimum.
- Protection: it is assumed that operating incidents may occur; provisions are made to detect such incidents and to prevent them from escalating. This is achieved by designing safety systems that will restore the plant to a normal state and maintain it under safe conditions.
- Safeguard: it is assumed that severe accidents might occur that could have serious consequences for the public and the environment. Special safety systems are therefore designed to limit the consequences to an acceptable level.

- Control of Severity: complementary measures and accident management procedures will help in controlling extreme plant conditions from severe accidents and in managing multiple failures.
- Mitigation: off-site emergency response measures are put in place to mitigate consequences of significant release of radioactive material.

Since, the above early definition of DiD, the IAEA (IAEA, 2005a) and the Western European Nuclear Regulators Association (WENRA, 2013) have since developed the concept further, to adapt to latest designs but as well to increase overall safety. The key improvements in the WENRA approach to DiD is in the following aspects of focus (WENRA, 2013):

- A new approach for latest nuclear power plants;
- Further consideration of multiple failure events previously thought to be “beyond design” and prevention of escalation to core melt conditions. Here a distinction is made distinguishing between accidents with and without core melt considerations
- Methods for identifying multiple failure events to be considered in design;
- Independence amidst the various levels of DiD such that failure of one level does not impede the prevention of accident or mitigation objectives of another level.

Further, the OECD NEA issued a booklet with DiD lessons learnt from the Fukushima Daiichi accident in 2011 (OECD, 2016). The following key lessons were identified (OECD, 2016):

- There is a need to reinforce the importance of independent function of safety provisions within various DiD levels.
- Common cause and common mode failure, particularly for concomitant external events, should not breach safety provisions at different DiD levels.
- Particular focus is required at the DiD level (typically level 4) where severity of consequences is controlled or mitigated.
- Human and organisational factors are key considerations.
- In the mitigation level of DiD (typically level 5), players involved are different and these leads to issues, particularly for long-term or multi-unit accidents.
- ‘practical elimination’ of radioactive release should be considered with respect to both prevention and mitigation measures.

7.1.3 Probabilistic Safety Assessment (PSA)

7.1.3.1 Concept of risk

Nuclear facilities are designed so that the risks associated with their operation are within acceptable limits for both the public and the environment. The acceptance of risk is generally governed by the degree to which it is considered to be relatively improbable and of limited consequence. In a nuclear facility, as in any industrial plant, risk assessment distinguishes between the potential hazards that might be encountered in the absence of any protective measures, and the residual risks that will still remain despite the measures taken. The problem lies in assessing the latter, since there is no way of ensuring that they have been completely eliminated.

The concept of event probability and its associated consequences was rapidly incorporated into safety analysis procedures, by taking account of the fact that the probability of an accident must be inversely proportional to the severity of the potential consequences for the public and the environment. This approach may be represented schematically in a probability/consequence diagram, known as a "Farmer curve", (Farmer, 1967), which sets out acceptable and prohibited domains (Figure 34).

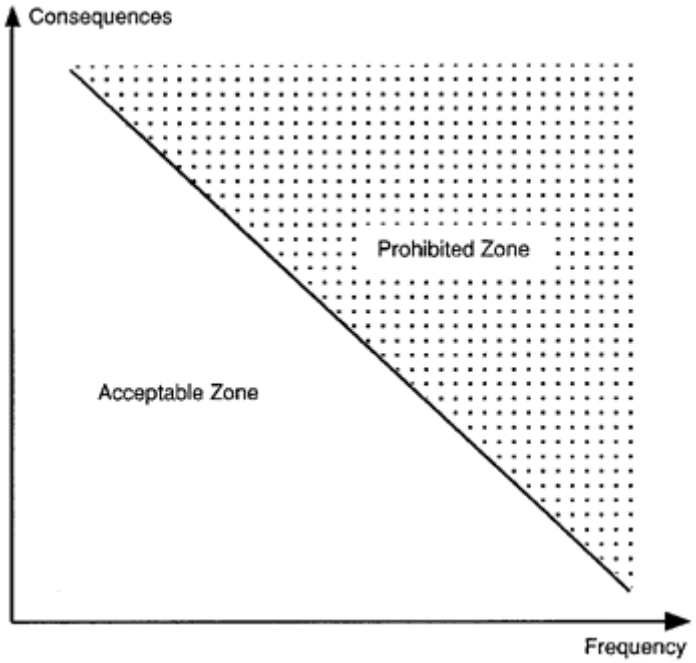

Figure 34: Probability consequence diagram (Farmer, 1967)

The question that the analyst asks himself when performing a risk assessment is which accident conditions he should take into consideration and to what level of probability should he pursue his analysis. As the use of probabilistic risk analysis became more widespread, the safety authorities asked design engineers to introduce appropriate measures whenever such analyses indicated that the probability of an event occurring that might potentially have unacceptable consequences for the public and the environment was sufficiently high.

7.1.3.2 Risk criteria

The risk criterion is a term, which distinguishes between what is considered as an acceptable level of safety and what it is not.

The national approaches about risk criteria differ notably from country to country, so no commonly accepted international agreement exists.

Quantitative risk objectives in United States of America consider individual and societal risk:

- The mean risk of an individual near a nuclear power plant (living within 1 mile radius) to receive an acutely lethal dose through a reactor accident is not to exceed 5E-7/year (this corresponds roughly to 0.1% of the risk from all fatal accidents).
- The risk for the general population within ten-mile-radius around a nuclear power plant to die of cancer as a result of the reactor operation should not exceed 2E-6/year (this corresponds to about 0.1% of the total cancer risk conditional on industrial activities).

Within Europe, WENRA strives to develop a harmonized approach to nuclear safety. As part of this effort a report was issued in 2006 combining up to 300 ‘Reference Levels’ and updated in 2008 (WENRA 2006; WENRA 2008).The latest WENRA safety objectives to nuclear safety have been directed to improve the safety of new reactors in comparison to existing reactors. These objectives are (WENRA, 2010):

- Reducing likelihood of extreme events by improving the ability of the plant to remain in normal operating conditions and to control extreme conditions;
- Ensuring that accidents that do not involve core melt do no result in off-site radiological impact;

- 'Practically eliminate' core melt accidents that would cause early or large release of radioactive material. If not eliminated, design provisions to control, limit and mitigate effects;
- Ensuring independence between the levels of DiD such that failure at one level does not impair functioning of other levels;
- Integrating design and implementation of safety and security measures;
- Including design provisions to reduce individual and collective doses for workers, discharges to environment and the quantity and activity of radioactive waste;
- Increasing and ensuring leadership, management and awareness for the entire power plant towards ensuring safety.

WENRA considered providing quantitative risk criteria but decided that quantitative safety objectives would not add more information over qualitative objectives. Particularly, it was recognized that formulation of quantitative safety objectives would require the prior development of standardized methodologies. Moreover, meeting standards based purely on numerical values would not be sufficient in any case (WENRA, 2010).

In spite of the fact that no common criteria exist internationally, one can conclude that the production of electrical energy from nuclear power should not contribute notably to the overall risk is common to the national approaches. The ALARA (As Low As Reasonably Achievable) principle is mostly acceptable, which states that the risk should be as low as it is reasonably achievable. In addition, a common position exists that the future power plants should be better and safer than the current ones, which is the position of IAEA. Namely, existing and future plants are distinguished in sense that the criteria are stricter in case of future plants by an order of magnitude. The objective for core damage frequency for existing plants is $1x10^{-4}$/reactor-year and for future plants it is 1 $x10^{-5}$/ reactor-year. The objective for large early release frequency for existing plants is $1x10^{-5}$/ reactor-year and for future plants it is $1x10^{-6}$/ reactor-year (IAEA, 1999).

Design based on risk criteria or risk-targetted design is an important concept to establish performance requirements for design. Particularly, in the NARSIS context, the risks from natural events are of importance and hence, the concept of 'residual risk' and type of risk measures employed become relevant to the risk criteria. The United Nations International Strategy for Disaster Reduction (UNISDR 2009) defines residual risk as "the risk that remains in unmanaged form, even when effective disaster risk reduction measures are in place, and for which emergency response and recovery capacities must be maintained." It is important for design criteria of NPP systems, structures and components to consider residual risk. For example, Tsang et al. (2018) presents a methodology to limit residual seismic risk to structures within the ALARA region, from an individual and societal risk viewpoint. Such methods could be applied to risk criteria for NPP structures exposed to natural hazards. Also, a variety of risk criteria can be established for any hazards, particularly natural events. Jonkman et al. (2002) present a host of risk measures for evaluating flood risk including criteria based on individual and societal fatalities, economic damage, environmental damage, potential consequences, and integrated risk criteria that consider more than one of the above measures.

7.1.3.3 Methods of probabilistic safety assessment

PSA methodology widely used in the nuclear power industry is deemed helpful to the safety assessment of the facility and along the correspondent licensing process: probabilistic safety assessment can provide insights into safety and identify measures for informing designers of the safety of the plant (ASME, 2002; ASME, 2008).

The first comprehensive application of the PSA dates back to 1975, to the United States Nuclear Regulatory Commission's (US NRC) Reactor Safety Study (US NRC, 1975). Since that pioneering study, there has been substantial methodological development, and PSA techniques have become a standard tool in the safety evaluation of the nuclear power plants

(NPPs) and industrial installations in general (US NRC, 1982; US NRC, 1983; US NRC, 1984; US NRC, 1989).

As the most important area of PSA projects remains nuclear power plants, mainly due to the specific features of the nuclear installations, three levels of PSA have evolved (IAEA, 1992; IAEA, 1995; IAEA, 1996):

Level 1: The assessment of plant failures leading to core damage and the estimation of core damage frequency. A Level 1 PSA provides insights into design weaknesses and ways of preventing core damage. In the case of other industrial assessments, Level 1 PSA provides estimates of the accidents frequency and the main contributors.

Level 2: As possible releases are additionally protected by containment in most NPPs, PSA at this response and severe accident management possibilities. The results obtained in Level 1 are the basis for Level 2 quantification. In the case of other industrial assessments, Level 2 PSA might be fully covered by Level 1, as containment function is rather unique feature and is not common in other industries.

Level 3: The assessment of off-site consequences leading to estimates of risks to the public. Level 3 incorporates results on both previous levels.

Level 1 PSA is the most important level and creates the background for further risk assessment; therefore it will be presented in detail. The structure of the other levels is much more application specific, and will be discussed only in general.

The methodology is based on systematically: 1) postulating potential accident scenarios triggered by an initiating event (IE), 2) identifying the systems acting as “defences” against these scenarios, 3) decomposing the systems into components, associating the failure modes and relative probabilities, 4) assessing the frequency of the accident scenarios. Two elements of the PSA methodology typically stand out:

- The event tree (ET) which is used to model the accident scenarios: it represents the main sequences of functional success and failure of safety systems appointed to cope with the initiating events and the consequences of each sequence. These consequences, denoted also as end states, are identified either as a safe end state or an accident end state.
- The fault tree (FT) which documents the systematic, deductive analysis of all the possible causes for the failure of the required function within an accident scenario modelled by the ET. A FT analysis is performed for each of the safety systems, required in response to the IE.

Assigning the safe end state to a sequence means that the scenario has been successfully terminated and undesired consequences have not occurred. In contrast the accident end state means that the sequence has resulted in undesired consequences.

Synthetically, the methodology embraced for the analysis consists of the following major tasks:

- identification of initiating events or initiating event groups of accident sequences: each initiator is defined by a frequency of occurrence;
- systems analysis: identification of functions to be performed in response to each initiating events to successfully prevent plant damage or to mitigate the consequences and identification of the correspondent plant systems that perform these functions (termed front-line systems): for each system the probability of failure is assessed, by fault tree model;
- accident sequences development by constructing event trees for each initiating event or initiating event groups;
- accident sequences analysis to assess the frequencies of all relevant accident sequences;

- identification of dominant sequences on a frequency-consequence base, i.e. the ones presenting the most severe consequences to the personnel, the plant, the public and the environment and definition of the reference accident scenarios to be further analysed through deterministic transient analysis (for instance by TH code simulation), in order to verify the fulfilment of the safety criteria. Consequences in the case of Level 1 PSA of NPPs are usually defined as degrees of reactor core damage, including 'safe' state and 'severe' accident state.

One of the main issues encountered in probabilistic analysis concerns the availability of pertinent data for the quantification of the risk, which eventually raises a large uncertainty in the results achieved. Usually these data are accessible from consolidated data bases (e.g. IAEA), resulting from the operational experience of the plants. They pertain, for instance, to component failure rates, component probability on demand, initiating event frequency: for this reason within a PSA study usually an uncertainty analysis, in addition to a sensitivity analysis, is required in order to add credit to the model and to assess if sequences have been correctly evaluated on the probabilistic standpoint. Event trees are used for the graphical and logical presentation of the accident sequences. An example of an event tree is shown in Figure 35. The logical combinations of success/failure conditions of functions or systems (usually safety systems, also called front-line systems) in the event tree are modelled by the fault tree.

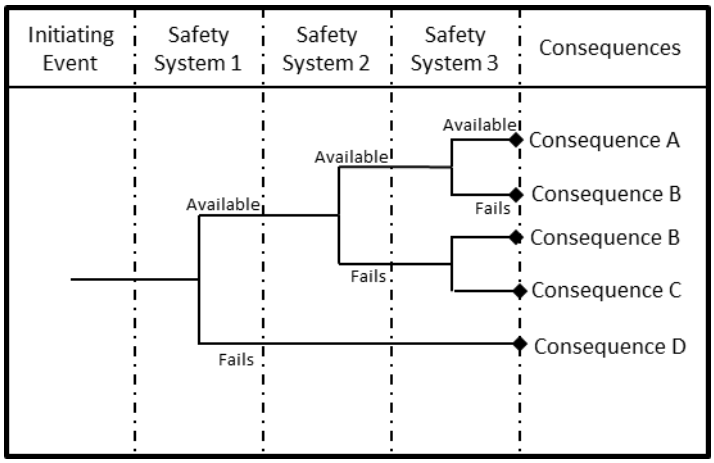

Figure 35: Example of an event tree (Burgazzi, 2012)

A fault tree logically combines the top event (e.g. complete failure of a support system) and the causes for that event (e.g. equipment failure, operator error etc.). An example of the fault tree is shown in Figure 36. The fault tree mainly consists of the basic events (all possible causes of the top event that are consistent with the level of detail of the study) and logical gates (OR, AND, M out of N and other logical operations). Other modelling tools, like common cause failures, house or area events are also used in the fault trees. All front-line and support systems are modelled by the fault trees and then combined in the event trees depending on the initiating event.

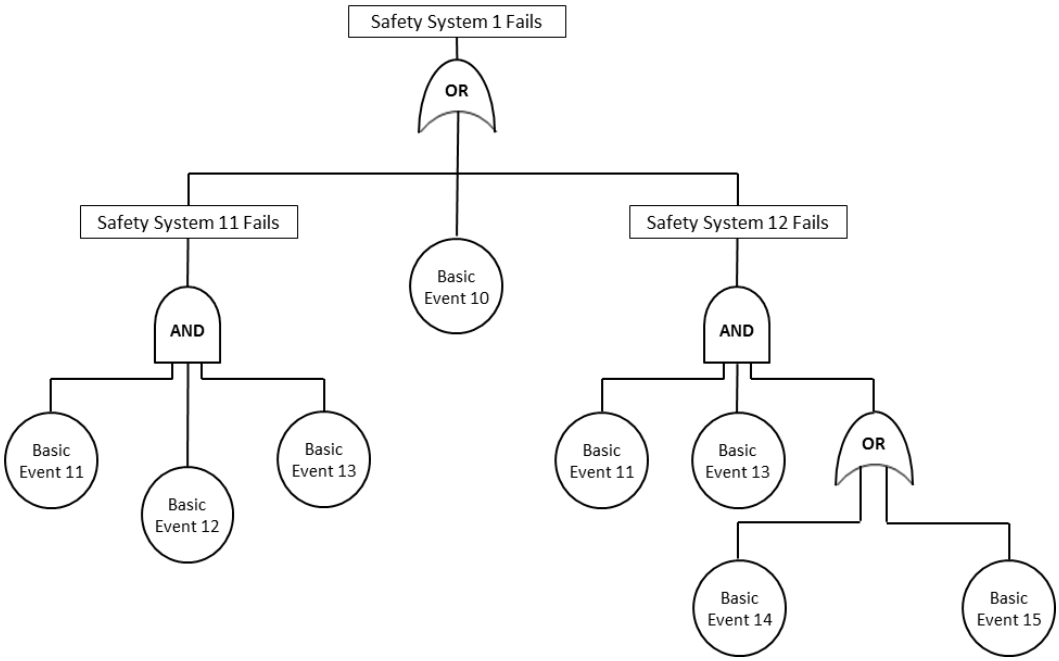

Figure 36: Example of a fault tree (Burgazzi, 2012)

A fault tree is capable to include rather special cases, usually identified in complex systems. These include system and components dependencies, called common cause failures (simultaneous failures of several components due to the same reason), area events (usually fire, flood etc., which damages groups of components in certain rooms), and human actions (operator errors or mitigation actions).

The PSA is a powerful tool that can be used in many different ways to assess, understand and manage risk. It's primarily objectives are the following:

- estimate risk level of the facility;
- identify dominant event sequences affecting safety of the facility;
- identify systems, components and human actions important for safety;
- assess important dependencies (among systems or man-machine interactions);
- provide decision support in various application areas.

The growing area of PSA use is extensive support of probabilistic results in risk management and decision-making processes. The main areas of the PSA applications are assessment of design modifications and back-fitting, risk informed optimisation of the Technical Specifications, accident management, emergency planning and others. Several modern tools of risk management are also based on the PSA model, such as risk monitoring, precursor analysis and others.

Despite its popularity among the risk assessment tools, the PSA has a number of limitations and drawbacks. The main limitations of the PSA model are the following:

- *Binary representation of the component state*. Only two states are analysed: failed state or fully functioning state. However, this is not always realistic, as intermediate states are also possible. The same limitation exists for the redundant systems with certain success criteria – system is in failed state (success criteria is not satisfied) or in full power. The intermediate states for redundant systems are even more important.
- *Independence*. In most cases, the components are assumed to be independent (except modelled by CCA), however there are many sources of dependencies, not treated by the model.
- *Aging effect*. The aging effect is often ignored because of the constant failure rate assumption, in which case the only conservative possibility to treat the aging impact

is to perform sensitivity study. However, this limitation has been overcome through methods such as those presented by Volkanovski (2012).
- *Time treatment*. The FT/ET model was originally not used to treat time explicitly during the accident progression. This was one of the major drawbacks of the methodology. In realistic systems, many parameters and functions depend on time and this is not encountered in the model and only approximate chronological order is assumed. However, this limitation has been overcome as shown, for example, in Volkanovski and Prošek (2013).
- *Uncertainty of the calculations*. Uncertainties are inevitable in the PSA results and calculations and therefore direct treatment of the quantitative PSA estimates might be misleading. Due to uncertainties, the qualitative PSA results, at times, assume greater importance than quantitative results.

7.1.3.4 Risk-informed decision making

Risk-informed decision-making is a term describing the process of assessing risks connected with technical decisions and considering of the risk results together with other means or with safety analyses to reach the most appropriate decisions (US NRC, 2011).

In addition to the risk criteria for the nuclear power plant operation, the risk criteria, in some countries, are developed in two aspects considering the acceptability of changes.

- The first aspect includes permanent changes; e.g. assessment of acceptability of plant modifications;
- The second aspect includes temporary changes; e.g. consideration about the on-line maintenance.

Plant modification is a permanent change in the plant, which may be a physical change (e.g. an upgrade of a system, an addition of redundant equipment, a replacement of some components) or a non-physical change (e.g. improved plant operating procedure or improved testing and maintenance procedure, a change connected with certain requirement). An assessment of acceptability of plant modifications requires the risk criteria for permanent changes in the plant, because modification is a permanent change and it represents a potential for permanent change in risk.

The main and the most general rule is that the activities, which results in decrease of risk, are appreciated and mostly approved. Further, the activities, for which a small increase of risk is evaluated, can be considered acceptable, if the risk increase is small and if there are benefits of the change, which overrule the increase of risk, or if there are no methods and tools to evaluate completely the proposed change in terms of positive and negative aspects in terms of risk. Namely, sometimes it is difficult to evaluate quantitatively all the positive and negative aspects of proposed change in such extent that risk models qualitatively and quantitatively include all the positive and negative aspects of the proposed change.

Finally, if a large increase of risk is connected with proposed change, such change is not acceptable. A typical example consists in the assessment of risk change, in terms of core damage frequency, related to inoperability of standby safety equipment due to test or maintenance.

7.1.4 Risk-informed regulatory approach

Previous treatment in Sections 7.1.3.3 through 7.1.3.4 laid the foundations for the development of a broader risk-informed framework, focused on regulating the risk from a nuclear power plant (US NRC, 2012). The “Risk-Informed Regulation Implementation Plan” (RIRIP) was first issued by the US NRC in 2000 to characterise the nature and purpose of PSAs. This has since been updated several times, the last of updates coming in 2007 including the ‘**R**isk-Informed and **P**erformance-Based **P**lan’ (RPP). The RPP issues several objectives The following important definitions are provided to aid in execution of the PSA in accordance with the RPP approach (US NRC, 2007):

- Risk-informed regulation – “A risk-informed approach to regulatory decision making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety.”
- Performance-based regulation – “A performance-based regulatory approach is one that establishes performance and results as the primary bases for regulatory decision-making, and incorporates the following attributes: (1) measurable (or calculable) parameters (i.e., direct measurement of the physical parameter of interest or of related parameters that can be used to calculate the parameter of interest) exist to monitor system, including facility and licensee, performance, (2) objective criteria to assess performance are established based on risk insights, deterministic analyses and/or performance history, (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes, and (4) a framework exists in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern.”
- Risk-informed and performance-based regulation – “A risk-informed and performance-based approach to regulatory decision-making combines the risk-informed and performance-based elements discussed . . . above, and applies these concepts to NRC rulemaking, licensing, inspection, assessment, enforcement, and other decision-making.

Classically, the control of the risk associated to the operation of a nuclear power plant has been founded on the definition of a group of events representing credible worst-case accident scenarios (the so-called DBAs) and on the prediction and analysis of their consequences by deterministic calculations. Then, the safety and protection of the system is designed against such events, to prevent them and to protect from, and mitigate their associated consequences. This traditional approach to regulating nuclear safety by the verification that a nuclear plant can withstand a set of prescribed accident scenarios judged as most adverse, conjectures that if a plant can cope with the DBAs, it will also be capable of handling any other accident.

In this view to safety, the underlying concept for protecting a nuclear power plant is the so called defence-in-depth which has become the design philosophy for attaining acceptable levels of safety. This structuralist DiD viewpoint and the safety margins derived from it, have been embedded into conservative regulations aimed at enveloping all credible accidents, for what concerns the challenges and stresses posed on the system and its protections. In fact, such view to nuclear safety has been embraced into a number of design and operating regulatory requirements, including: i) the use of redundant active and/or passive engineered safety systems, to avoid the risks from single failures; ii) the use of large design safety margins to cope with the uncertainty in the actual response of the safety systems under accident conditions; iii) the demand of quality assurance practices on materials, manufacturing and construction; iv) the restriction of system operation within predetermined bounds; v) the definition of requirements for the testing, inspection and maintenance of the structures, systems and components to guarantee the desired safety levels.

The approach to safety above illustrated has been regarded effective in providing a conservative means for managing the uncertainties in the system behaviour and its modelling within the safety analyses. However, it is widely recognised that the reliance on purely deterministic analyses for the verification of nuclear safety may not be rational or sufficient for bounding the required high levels of safety across all potential accident events and protective safety systems. On one side, the practice of referring to DBAs may lead to the consideration of excessively conservative scenarios, but also highly unlikely, with a penalisation of the industry due to the imposition of unnecessarily stringent regulatory burdens on the protective barriers for DiD. On the other hand, the conjecture that protecting

from DBAs would give reasonable assurance of protecting from any accident has been proven wrong, e.g. by the occurrence of the Three Mile Island accident in 1979.

The above considerations have led to the arising of the PSA approach for nuclear safety, based on the inclusion into the analysis of the likelihood of all potential accident scenarios by considering the reliability of the protection systems through the introduction of probabilistic measures for the treatment of the uncertainty in their behaviour, as detailed in Section 7.1.3. This allows addressing some of the shortcomings of the DBAs thanks to a systematic modelling of more realistic scenarios, including multiple failure events (the so-called Beyond Design Basis Accidents, BDBAs) and to the definition of the level of risk from the plant in quantitative terms. Furthermore, the PSA can be used to prioritise improvements in the design and operation of the plant for greatest risk reduction. On the other hand, it is impossible to guarantee that PSA captures all the accident events and scenarios contributing to risk and its quantitative results may be affected by very large uncertainties which make difficult their direct use for decision making.

Today's trend in the control of nuclear safety is drifting towards an integrated decision making process that combines the insights from the deterministic and probabilistic analyses with the regulatory requirements and cost-benefit considerations. This approach is increasingly adopted for a more efficient use of resources for increased safety and reduced regulatory burden in the application of a rationalist defence-in-depth philosophy. Since according to this approach risk information is to be used as adjunct to the deterministic and prescriptive body of regulations, it is often termed risk-informed, to unambiguously differentiate it from the risk-based approach based solely on insights from a PSA.

The risk-informed approach aims at systematically integrating deterministic and probabilistic results to obtain a rational decision on the utilisation of resources for safety. In such rationalisation, explicit consideration is given to the likelihood of events and to their potential consequences. The undertaking of these approaches has led to a number of efforts of risk-informing of existing regulations, i.e. rationalising regulatory requirements by risk information. This has meant in particular the possibility of allowing changes in safety requirements upon demonstration that the corresponding change in the risk from the plant is acceptably small and still within the design bounds. Several instances of these efforts have demonstrated the effectiveness of the approach, perhaps the best still being the application in practice of the maintenance rule which has provided a foundation for making risk insights and prioritisation of use in day to day operations.

In order for the integrated, risk-informed decision making process to virtuously benefiting from the combination of the systematic deterministic and probabilistic analyses of the safety of a nuclear power plant, it is necessary to address some relevant issues: for instance an adequate representation and treatment of the related uncertainties has to be provided. This motivates the research on the implementation of new tools in safety assessment practice.

7.2 Chemical industry

7.2.1 Introduction

PSA is a standardised tool also used for assessment and improvement of the reliability of various systems in other industries, e.g. aviation and space industry and chemical industry.

The objective of this section is to briefly outline some of the available methods and procedures for the assessment of the risks from complex industrial installations, using the chemical industry as an example.

Accidents like those involving chemical plants, e.g. Seveso in Italy, have intensified the public awareness of the possibility of undesirable consequences, resulting in the development of a general methodology for the assessment of the risk from complex systems, which is based on probabilistic and/or statistical techniques, (Green, 1982; Rowe, 1982).

7.2.2 Concept of risk

The concept of risk entails the concepts of an undesirable consequence and uncertainty: an activity is considered risky if it is possible as a result of this activity to experience an undesirable consequence but at the same time the consequence is not going to happen with certainty but it is stochastic in nature.

The first step in the assessment process is the qualitative and quantitative determination of the possible undesirable consequences. Qualitative determination means identification of general “areas of concern”, on which the undertaking of specific complex industrial installations activities might have a detrimental effect, such as environment or public and occupational health or economics. Quantitative determination involves the definition of attributes or performance indices that measure the degree to which a particular area of concern has been affected.

Consequences on occupational and public health, for example, can be assessed by the number of fatalities (to be eventually distinguished in acute and latent) caused by an accident, as an attribute measuring the impact of the accident.

The next step consists then in determining the relative likelihood with which each of the possible values of the consequences can occur. Several syntheses of these fundamentals elements into a composite risk index have been proposed with varying degree of theoretical basis: however the combination of undesirable consequences and associated uncertainties in a risk index is not a trivial exercise.

For the purpose of this treatment, risk assessment is meant as the assessment of: a) the nature (types) of undesirable consequences; b) attributes that provide quantitative measures for these consequences; c) the range of possible values for the attributes; and d) the probability with which each possible value can occur.

7.2.3 Risk assessment: major methodological steps

The principles of the methodology are referred to chemical industry, i.e. those industrial installations that handle one or more hazardous substances like toxic or flammable substances.

The risk that the operation of such facilities pose stems from the possibility of release of substantial quantities of these substances, as a result of a major accident, which in turn have the potential of detrimental health, environmental, social and economic effects.

Obviously most major facilities that handle hazardous include in their design safeguards and other safety measures aiming at avoiding such accidents.

Possibility of accident with undesirable consequences to occur entails:

- An event takes place that disturbs the normal operation of the plant (initiating event).
- A series of failures incapacitate one or more safety systems and make them incapable of stopping the incident or contain the release of the hazardous substances.
- The hazardous substances are released in the immediate environment of the installation and it is dispersed - depending on the prevailing atmospheric conditions – in the air, the soil and the water. The dispersed substance is then causing the undesirable health, social and environmental conditions.

The methodology for the risk assessment consists in the determination of the possible ways in which accidents can happen, the associated consequences and their relative likelihood of consequences.

Four major methodological steps can be distinguished; three corresponding to the analysis of the three major phases of the accidents described above, and a fourth that integrates the partial results in an estimation of the risk.

The four major methodological steps are further discussed in the following sections.

7.2.4 Accident initiators

The first methodological step of the risk assessment process consists in the understanding of the design and operation of the installation, the identification of the possible initiating events that can upset the normal operation of the installation, the response of the installation and the possible ways in which this response might fail to control the disturbance and result in a release of a hazardous substance.

In particular we can distinguish:

1. Familiarisation with the design and operation of the plant. This is of fundamental importance for a successful and meaningful risk assessment, which in turn means that it is not possible to perform such an analysis without the involvement of persons very familiar with the plant.
2. Identification of initiating events. These are events that disturb the normal operation of the plant and they can be distinguished in internal (those that are due to a malfunction or an event internal to the plant) and external (those that are due to events external to the plant as extreme natural phenomena, etc.).
3. Analysis of the response of the plant to each and every of the initiating event. This includes determination of the control and safety engineered systems that are incorporated in the design of the plant and their required response in order to control the disturbances and avoid release of hazardous substances.
4. Grouping of initiating events in such a way that each initiator of a group requires the same response from the various safety systems. These groups form “generalised” initiators that are going to be used in the rest of the study. The frequency of each group is then assessed.

The final result of this first case consists of a list of generalised initiators (a_i) and the corresponding frequencies of occurrence (q_i).

7.2.5 Accident sequences

The second major methodological step in risk assessment determines the specific combination of hardware and human failures that constitute an accident resulting in a release, along with their probability of occurrence, and in particular:

5. For each generalised initiator, the possible responses of the various control and safety systems are examined and combinations of failures of these systems that lead to a release are determined. These failures combinations are called accident sequences: as for the nuclear case, one of the most frequently used techniques for accident sequence delineation is the Event Trees.
6. This stage calculates the probability of occurrence of each accident sequence. This implies the calculation of the probabilities of failure of the various systems that form an accident sequence conditional on the initiating event and the other system failures. The probability that a system will fail to perform its intended function is based on well-known approaches to reliability such as fault tree technique, like in the nuclear case.
7. The accident sequences that lead to the same type of releases (qualitatively and quantitatively) are grouped to form categories of accident sequences that result in particular “release category”.

The final outcome of this phase includes the release categories r_j and the corresponding probabilities of occurrence conditional on a particular initiating event a_i. Denoting this probability by f_{ji}, the matrix of release probabilities F can be written in the form: $f_{ji} = P(r = r_j/a = a_i)$.

7.2.6 Dispersion of hazardous substances

Once the hazardous substance is released in the immediate environment of the installations, it starts its transport through the air, soil and liquid pathways. The third major methodological

step begins with the analysis of this transport. Of major importance for chemical as well as nuclear installations is the transport of the hazardous material through the air.

8. For each release category r_j, the dispersion of the released substance in the atmosphere, is evaluated by means of a suitable atmospheric dispersion model and on the basis of the possible atmospheric conditions. The results of this step provide for each release category r_j the concentration $(x,y,z,t)_j$ of the toxic substance at each point (x,y,z) and instant t.

   One can distinguish in a very succinct way, three different modes of atmospheric dispersion:

- Passive dispersion. In this dispersion mode the behaviour of the gases does not modify the ambient turbulence and it is the properties of the boundary layer that determine how the toxic gas is dispersed and diluted. Gaussian diffusion models are the most frequently used.
- Buoyant releases. This dispersion mode characterises gases that are released in elevated temperatures causing an initial plume rise. Models that calculate the rise of the plume are based on the principles of: a) conservation of mass, b) conservation of momentum, c) conservation of enthalpy and d) an entrainment hypothesis.
- Heavy releases. Vapour clouds that are denser than the surrounding atmosphere require special dispersion models. They should include: a) specification of the source term for atmospheric dispersion, b) gravitational slumping, c) entrainment of air, d) heating of the cloud.

A detailed review of the techniques for assessing the atmospheric dispersions can be found in the related literature.

7.2.7 Dose, dose-response, consequences

The third methodological step continues with the calculation of the consequences in which the calculated dispersion of the hazardous substance might result and the corresponding probabilities. This is done by a dose or exposure assessment and a dose-response assessment.

One can distinguish the following two specific steps:

9. Dose or exposure assessment is the process of measuring or estimating the intensity, frequency and duration of human or other exposures to a risk agent. In the previous step the movement of the hazardous substance from its source through the environment and its degradation or reaction with other substances has been determined.

   The concentration of the toxic materials in space and time is now interfaced with the target populations and the existing emergency measures (e.g. evacuation, sheltering), to evaluate the exposure to the risk agent.

10. Dose-response assessment methods are concerned with characterizing the relationship between the dose of the risk agent received and the health and other consequences to exposed populations.

    These consequences can include fatalities and injuries, latent cancer fatalities, genetic effects, environmental degradation and economic losses. Most of the efforts devoted to the development of methods for dose-response assessment have been directed at understanding human health rather than on the more general ecological consequences of exposures to hazardous chemical substances.

    The final product of this step is the assessment of a number of consequence levels c_k and the probabilities g_{kj} of observing a consequence c_k, conditional on having experienced a release r_j.

In matrix form one has:

Consequence matrix G $G = \{g_{kj}\}$ *Equation 11*

7.2.8 Integration of results and risk quantification

The fourth major methodological step in risk assessment integrates the partial results of the previous steps in a final quantification of risk. As already mentioned, risk quantification is meant as the assessment of the possible ranges of consequences and the probabilities with which each level can occur:

11. Step 10 has already determined the various consequences and their possible levels. The frequency h_k with which each of these possible levels can be observed is evaluated as the product of the frequency of the initiator q_i, the release probability f_{ji} and the probability of the consequence g_{kj}. That is:

$h_k = g_{kj} f_{ji} q_i$ or in matrix form $h = G*F*q$ *Equation 12*

Finally the risk can be calculated as:

Risk = $\{c, h\}$ *Equation 13*

The overall risk assessment considerations discussed above are often supplemented by specific tools and methods. Among the most widely used risk analysis methods in the chemical industry are the complementary techniques of Hazard and Operability studies (HAZOP) and Hazard Analysis (HAZAN). A HAZOP analysis targets the identification of potential issues during the design stage, estimates the extent of their consequences, and evaluates the need for change. The need for change is given by (Simmons and Tyler, 1984):

Need for change $\propto$ *(frequency of event) x (magnitude of consequences)* *Equation 14*

A multi-disciplinary team of typically 4 to 8 members is assembled to perform the HAZOP analysis from start to end to ensure continuity. The team critically examines the design using a line diagram (e.g. piping and instrumentation in process industry) and flowchart. A basic assumption of the HAZOP study is that under normal operating conditions the existing design is adequate. So the method includes ‘guide words’ – e.g. MORE OF, LESS OF, PART OF, AS WELL AS, MORE THAN etc. - that prompt the team to think of deviations from design conditions. For each guide word considered the team members cognize deviations, identify possible causes and consequences, and determine required actions or modifications to the design. HAZOP studies are hence, suitable for new designs but also relevant at times of modification to existing design to avoid overlooking any resultant downstream changes.

Similar to the HAZOP study, HAZAN studies assume that existing design performs adequately under normal operating conditions. The purpose of a HAZAN study is similar in that the need for change is evaluated when a hazard is identified, but a more detailed analysis of the hazard is carried out. As a first step, for the considered hazard, a fault tree is constructed starting with the undesired consequence and tracing back with increasing detail to deviations and actions that constitute every scenario leading to the event. Basic events whose probability of occurrence is relatively known are used to construct the fault tree leading to the top, undesired event. Following such logical quantification of the undesired event probability, consequences in terms of finances or injuries/fatalities are estimated. The need or decision for design change is then based on the required consequence levels for the industry. These expectations vary based on industry history as well as the nature of the consequences (e.g. financial or fatalities).

7.3 Aviation industry

The aviation and aerospace industries have also been flagbearers for safe systems and employ some of the most detailed safety analyses with extremely stringent safety requirements. In this section, we will review some methods used by industry leaders such as the NASA and the Federal Aviation Administration (FAA) from the U.S., and the European Aviation Safety Agency (EASA).

7.3.1 Probabilistic Risk Assessment (PRA) – the NASA framework

Probabilistic Risk Assessment (PRA) is the preferred tool for safety assessment in the aerospace industry. NASA ubiquitously adopts PRAs in their missions and has issued a guide on PRA, associated concepts and procedures (Stamatelatos and Dezfuli, 2011). Within this document, the various elements of a PRA are outlined as described below (Stamatelatos and Dezfuli, 2011):

- *Identifying initiating events*

  The suggestion for identifying initiating events is the use of master logic diagrams (MLD) – a hierarchical representation of initiating events, displaying undesired events on top followed by detailed event description leading to the initiating events at the bottom of the diagram. Initiating events are identified typically by specifying normal operating conditions with respect to nominal values of physical variables of interest and the range of values for these variables that would be deemed as an initiating event. It is beneficial to identify consequences of interest while identifying initiating events to allow for the understanding of consequences that are necessarily not directly tied to the initiating event under consideration.

- *Applying event sequence diagrams and event trees*

  The next step is to track the sequence of events stemming from the initiating event. This is done using an ET or an event sequence diagram (ESD). The ESD is a flowchart that depicts routes to particular scenarios, and encourages interaction between risk engineers, design engineers and operating crew since it has the ability to fully reflect the design thought and operating procedures. Figure 37 shows the typical outline of an ESD.

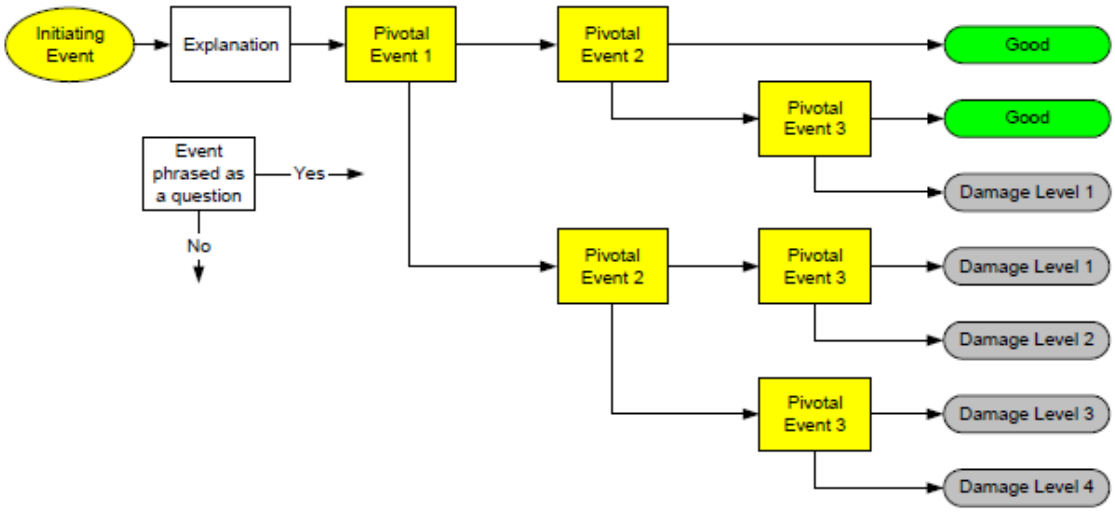

Figure 37: Event Sequence Diagram (ESD) structure (Stamatelatos and Dezfuli, 2011)

The pivotal event scenarios defined in the ESD are further broken down and represented in a tree structure such that the scenarios are classified based on their

consequence. The ET can be derived from the ESD as shown in Figure 38. The ET has been discussed previously in Section 7.1.3.3.

- *Modelling of pivotal events*

  Pivotal events need to be further analysed in detail to adequately quantify scenarios, while accounting for dependencies between various events. This detailed modelling of pivotal events is done using a FT. The FT represents logical relationships between top-level pivotal 'failure' events and associated combination of basic 'failure' events that lead to the pivotal failure events. This enables the representation of more complex consequential scenarios to be modelled using more basic failures in the system, facilitating quantification of the scenarios and the consideration of interdependencies via more granular, basic events. FTs have been discussed previously in Section 7.1.3.3.

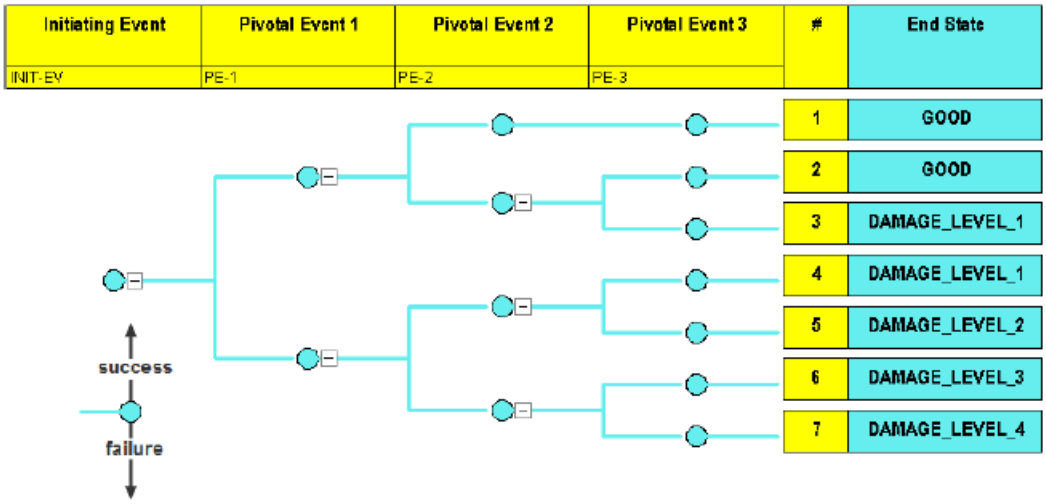

Figure 38: Event Tree (ET) derived from Event Sequence Diagram (ESD) shown in Figure 37 (Stamatelatos and Dezfuli, 2011)

- *Quantification of basic events*

  Complex consequential scenarios are broken down by modelling tools such as the FT, allowing for easier quantification since basic events are by definition, readily quantified from data. The conditional dependencies amidst basic events are also typically better understood or quantified. Further, when the granularity in the definition of events increases, it is more likely that events may be independent and hence, their joint probability becomes simply the product of their individual probabilities of occurrence. Probabilities of basic events are defined using probability density distributions, thus inherently accounting for uncertainty arising from our incomplete knowledge.

- *Quantification of Uncertainty*

  The formulation of event scenarios discussed above involves uncertainties both in modelling methodology and involved parameters, and the nature of uncertainty tends to originate both from our limited knowledge of event mechanisms, incomplete information about the events (aleatory) and as well from inherent stochasticity in the nature of these events (epistemic). Uncertainty associated with our chosen risk metric is often evaluated and represented using two major concepts or tools – MC sampling and Bayes' theorem-based methodologies.

- *Formulation and quantification of integrated risk model*

  The risks associated from various event scenarios considered are bound to be heterogeneous, and hence, there is a need for an integrated representation of the

final risk from our modelling. This is typically achieved through the selection of a suitable risk metric and the presentation of the variation of this risk metric with respect to the basic event probabilities defined in our scenarios. The probability density distribution of the risk metric is obtained (as discussed above) using sampling methods such as MC simulation or Bayesian inference, which in turn inherently represents the uncertainty associated with the chosen risk metric.

The various steps of the process as described in NASA's guide for PRAs, are shown in Figure 39.

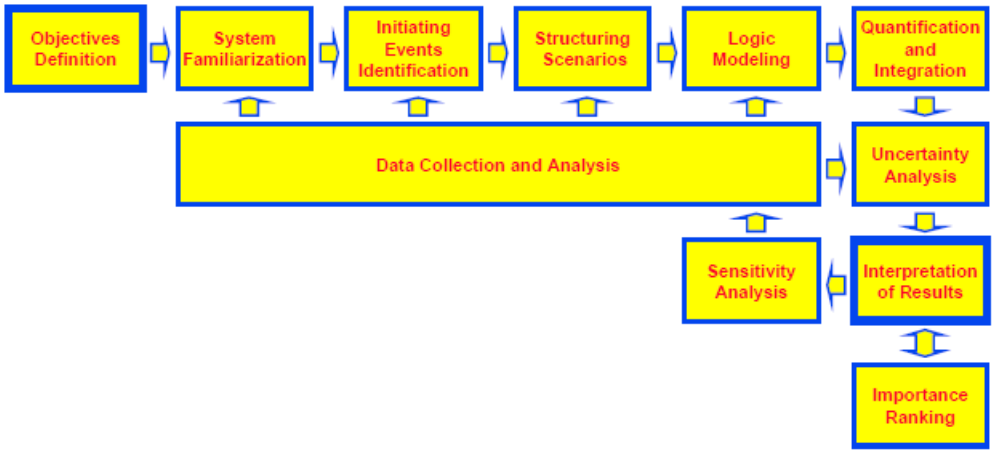

Figure 39: Task flow within PRAs (Stamatelatos and Dezfuli, 2011)

While PRAs are widely used in the aviation and aerospace industries and procedures largely fall under the above discussed framework, we now examine the unique risk analysis methods and recommendations from leading aviation authorities in the world such as the FAA and the EASA.

7.3.2 International aviation safety analysis methods – APR4761

"Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment" – ARP4761 (SAE International, 1996) is one of the documents used in demonstrating compliance with FAA and EASA standards for 'airworthiness' of transport aircrafts. Relevant methods prescribed as part of ARP4761, also summarised in detail by Balakrishnan (2015), are discussed below.

7.3.2.1 Functional Hazard Assessment (FHA)

FHAs are carried out at the inception of building a system – either a fully completed aircraft or individual sub-systems - and its primary objective is to identify the various scenarios under which system failure occurs and classify them according to the extent of damage. The first step of the FHA is to identify all functions contained at the top, aircraft level – for e.g., passenger load, thrust, customer requirements etc. – and at the lower individual subs-systems level – braking, control, transmission etc. From there, the FHA is composed of the following steps (ARP4761 - SAE International, 1996):

- List all functions with their corresponding levels of classification including within underlying sub-systems;
- For each function, list the various failure scenarios under various environmental conditions including combinations of failures;
- Determine the consequences of failure;
- Classify failures into varying levels of impact;
- Justify the classification of failure levels either using data, simulations or experience;
- List methods of testing compliance against requirements for each failure condition.

Thus, the FHA is a top-down, largely qualitative effort performed at the level of the global system but as well, at the level of constituent sub-systems. Therefore, it involves collaboration across various disciplines that are involved in system development. The FHA is followed up by the preliminary system safety assessment (PSSA).

7.3.2.2 Preliminary System Safety Assessment

PSSA involves a thorough review of the system architecture to identify the pathway from a failure event to the functional hazards identified in the FHA. FT analysis, dependence diagrams (DD), Markov analysis (MA), etc. are tools that are typically employed to identify potential faults in the system. Each failure scenario identified in the FHA is considered in the PSSA, and the process is performed iteratively at the top-level system (aircraft) and at the sub-system level. The PSSA can be summarised briefly in the following steps:

- Establish the safety requirements at the system level (aircraft) from outputs of FHA or CCA – described later);
- Assess if design will meet the established safety requirements (typically performed using a FT Analysis);
- The previously determined safety requirements are applied to lower level systems.

7.3.2.3 Fault Tree (FT) Analysis

For identifying failure modes, the analysis methods can be either inductive or deductive. In inductive methods, a particular fault is chosen and its impact on overall system operation is considered. An example of inductive analyses is the failure mode and effect analysis (FMEA) discussed below. In deductive analysis, a specific case of system failure is the starting point and the pathway to failure and the reasons for it are deduced. By design, deductive methods are well-suited for investigation of accident scenarios. The fault tree analysis is an example of deductive analyses and has been discussed previously in Sections 7.1.3.3 and 7.3.1.

7.3.2.4 Common Cause Analysis (CCA)

CCA is composed of three methods which aim to identify potential common causes that would invalidate independence assumptions amidst failure scenario pathways.

Common Mode Analysis (CMA)

Usually, CMA is used to verify if logical AND events within a FT are actually independent. It is a qualitative tool which assesses the common vulnerabilities. The analysis is performed by inspecting each AND gate within the FT and checking for independence, for every hazard considered. A separate analysis follows for events not modelled in the FT. If common failure modes are identified, the design needs to be revised and the FTA and CMA are iteratively performed.

Zonal Safety Analysis (ZSA)

ZSA examines the effect of physical proximity amidst systems, where the failure of one system can cause failure of another purely due to the proximity of the systems. For example, if one control system were to catch fire, adjacent control/computer systems may fail as well. This would clearly impede independence assumptions between failure scenarios of these systems. ZSA is performed early in the design phase to avoid cumbersome modifications at a later stage.

Particular Risk Analysis

Particular risk analyses are used to identify the hazards that lead to violation of independence assumptions, such as fire, radiation, earthquakes, explosions etc. The cascading effects of each of these hazards are carefully analysed.

Thus, we examined the various methods that are widely adopted in the aviation and aerospace industries. Previously, standard methods within the nuclear and chemical industry were also reviewed. While there is considerable overlap in the methodologies used across

these high-risk industries every industry tends to offer a unique perspective and approach to the risk integration problem, and as well employs some different methods.

7.3.2.5 Dependence Diagrams (DD)

DDs, also known as reliability diagrams, are similar to FTs in that they utilise the same logical operators of OR and AND. However, instead of gates they are represented by events in either series or parallel connections.

7.3.2.6 Markov Analysis (MA)

Markov analyses are similar to FTs and DDs where the Markov chain links various states of the system using failure/degradation rates and repair rates. At a given time, the probability of the system existing in a given state can be calculated by solving a system of differential equations. Predictions of future states are solely dependent on the current state. Thus, the system is conditional on its existing state and independent of future and past states.

7.3.2.7 Failure Modes and Effect Analysis

As mentioned earlier, FMEA is an inductive analysis method for identifying failure modes within a system and assessing impact on the next level of design. FMEA can be purely qualitative or quantitative and can be performed at any given level of a system. An example of a FMEA is shown in Table 5 for the system depicted in Figure 40 (ARP4761 - SAE International, 1996; US NRC, 1981).

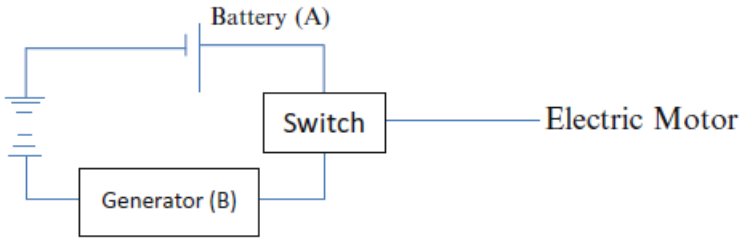

Figure 40: Electric power to the motor is supplied either by the diesel generator or battery (ARP4761 - SAE International, 1996; US NRC, 1981)

Table 5: FMEA for system shown in Figure 40 (battery (ARP4761 - SAE International, 1996; Roberts et al., 1981)

Component	Failure Mode	Probability	Effects on Motor
Battery	Low voltage	1×10^{-3}	Major
	Short circuit	1×10^{-6}	Critical
	Fluctuating voltage	1×10^{-2}	Minor
Diesel generator	Engine failure	1×10^{-4}	Severe
	Alternator failure	1×10^{-8}	Severe
	Fluctuating voltage	1×10^{-2}	Minor
Switch	Stuck in generator	1×10^{-6}	Major
	Contacts broken	5×10^{-3}	Critical

From the above FMEA, it can be observed that the probability of critical failure is approximately 5×10^{-3}, contributed largely by the chance that contacts are broken within the switch. This indicates to the designer which area to increase their focus on to bring down the probability of failure to acceptable levels defined in the PSSA.

The various steps in the FMEA can be broken down as follows:

- Prepare for the analysis by understanding the system being analysed and obtaining all relevant documentation regarding safety requirements, failure rates, failure modes etc. Use failure detection methods to identify the various failure modes;
- Divide the system into functional blocks assessing the internal functions within the block as well as interactions with systems connected to the block;
- Assign failure modes for each functional block;
- Analyse consequences for each failure mode, and classify effects by potential damage extent;
- Maintain documentation for rationale and justifications for various choices of failure rate, consequences and damage extents, both for effect on the functional block as well as the next level of design function. Due to the qualitative nature of the FMEA, the analyst needs to have high expertise while translating his thinking into documentation;
- Further resolution is added to the FMEA by looking at each individual component within the functional block.

7.3.3 Causal Model for Air Transport Safety (CATS)

An approach to safety and risk assessment that is unique to the aviation industry is the Causal Model for Air Transport Safety (CATS), although it is currently not a prescribed industry-wide standard. The CATS model was developed as part of an effort by the Netherlands Ministry of Transport, Public Works and Water Management to build a scientific framework and database to improve air transport safety. The following description of the CATS model is based on Ale et al. (2009).

Since aviation accidents occur as a result of a combination of several factors, FTs and ESDs (described earlier) are used to develop separate causal models for each accident category belonging to each flight phase. The unique approach of the CATS model compared to other high-risk industry methods lies primarily in the sequential use of ESDs and FTs and their conversion into a BN to eventually calculate accident probability. The properties and advantages of BNs have already been discussed in Section 6.4. The accident sequences used in CATs are developed based on the Integrated Risk Picture (IRP) model used in EUROCONTROL (Eurocontrol, 2006).

A list of potential accidents is created and for each accident ESDs are developed to depict the hazards that each flight has to overcome for safe completion of journey. The possibility of encountering a hazard is determined by whether the required initiator occurs. The possibility of the flight overcoming the hazard depends on whether the systems and/or crew are able to counter the hazard. Accordingly, each event is represented by an ESD that has binary outcomes and the probability of either outcome materializing is determined by FTs. Therefore, for every pivotal event in the ESD a FT is developed. The FT is also constructed with Boolean states of failure or no failure based on analysis of accident description data. The FTs are built from the top event – the pivotal event featuring in the ESD – which is split into subsequent unsuccessful performance of barrier events. The failed barrier events are further broken down into the causes for failure. The FT is quantified using data from event experience. When ESDs have sufficient historical data, the FT is quantified from a representative sample. When data is scarce for the ESD, expert opinion from precursor incidents are used to quantify the FT. The FT is eventually converted to a BN where multiple states of variables were allowed and the Boolean logic of the FT is substituted by probabilistic relationships within the BN.

In several accident cases reviewed in building the CATS model, human intervention was needed for prevention. HPMs influence human error probability (HEP) that predicts the chance that human intervention will not yield the desired effect in preventing the accident. The three models in consideration for CATS are Crew (Roelen et al., 2007), ATC Controller (Roelen et al., 2007a), and Maintenance Technician (Roelen et al., 2008). Since HPMs are

models of influence on the HEP, they are directly modelled as a BN, built based on recommendations for HPM by US NRC (US NRC, 2005). Performance shaping factors were analysed for applicability to the air transport industry and were appropriately modified for quantification within the CATS context. Figure 41 shows the methodological constituents of the CATS model and Figure 42 shows the overall BN structure used. The CATS model is particularly relevant in the NARSIS context in that it combines the advantages of more than one risk analysis tools available to better quantify accident probability and its methodology that is easily transferrable to the nuclear industry.

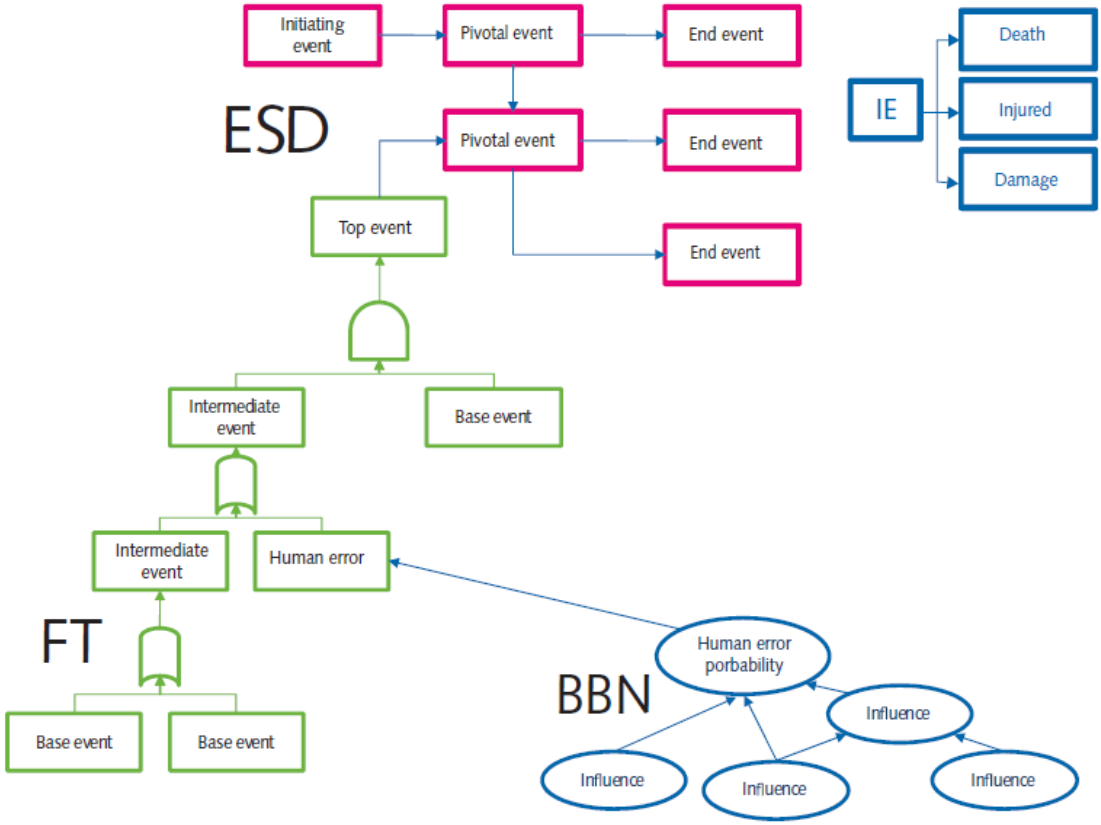

Figure 41: Constituents of CATS methodology (Ale et al., 2009)

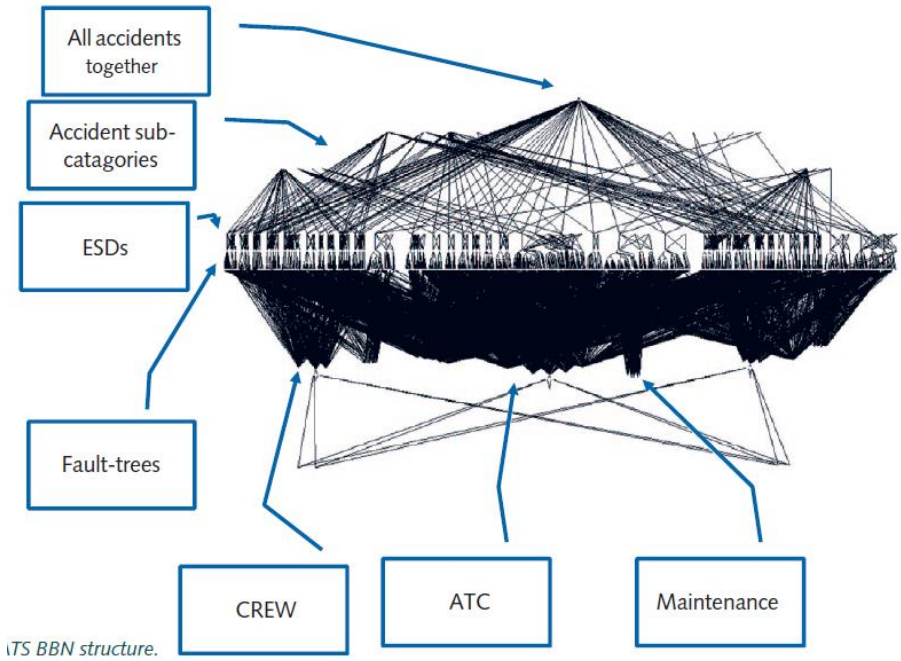

Figure 42: CATS Model - integrated Bayesian Network structure (Ale et al., 2009)

7.4 Summary

Risk analysis outlooks and methodologies from high-risk industries such as the nuclear, chemical and aviation industries were reviewed. PSAs are standard of practice in all these industries, and fault trees and event trees are the most widely used risk analysis tools. The chemical industry extensively uses HAZOP and HAZAN studies to supplement their PSAs, while the aviation industry standard prefers methods such as FMEA and FHA. While these methods are not regulatory standard of practice in the nuclear industry, they are not completely new and have been recognized by nuclear industry regulators (IAEA, 2002). However, the CATS model built for the aviation industry is of particular interest as it uses methods such as ESDs and FTs, but converts them into BNs which allow for better integration and computation of accident probability. Khakzad et al. (2011) compare FTs to BNs and list the following advantages for using BNs over a typical FT approach:

- BNs can be updated with new observations to calculate posterior probabilities from prior probabilities. This is advantageous as prior probabilities tend to be estimated from often limited data and expert opinion, while posterior probabilities are typically more robust, specific evidence that is associated with the undesired event being modelled.
- While usually estimated probabilistically using data and expert opinion, conditional probabilities calculated by deterministic means (in data-scarce problems) within a BN still yield superior performance to FTs.
- BNs provide a most probable configuration of events that lead to an accident which can be used to estimate the probability of both occurrence and non-occurrence of an undesired event. FTs yield a minimum cut-set – a set of primary events leading to a top event (say, system failure), where the removal of even one primary event would render the chain of events leading to system failure invalid. Minimal cut-sets cannot be used for estimating the probability of non-occurrence of primary events.
- FTs can be converted to a BN while the converse is not always true since, BNs can involve variables existing in multiple states (discrete or continuous) with complex interdependencies with other variables. The FT typically uses only Boolean causal relationships between variables with a limited number of discrete states.
- BNs can inherently handle uncertainty without the need for other coupling methods.

Hence, methods such as the CATS approach used in air transport safety, where deterministic and probabilistic tools are combined, are of relevance to the NARSIS context. The use of BNs as a risk integration methodology for NPPs requires further exploration. Likewise, combination of BNs with methods such as FTs, HAZOP and FMEA studies will allow for better definition of event scenarios and dependencies amongst events, and more such combinations should be assessed.

8 On-site incident investigations and corrective actions

Following the review of case histories of accidents (in Section 4) and analysis methods for RCA (Section 6), it is of interest to examine the protocol for incident investigations and corrective actions at NPPs. Following this, the next section (Section 9) discusses the international initiatives undertaken after major nuclear accidents. Sections 8 and 9 supplement Section 4 by providing typical organisational and international reactions to undesired events.

8.1 Role and qualifications of incident investigators/ interview techniques

The most valuable insights and lessons are gained when a team of independent investigators is sent to the site to investigate an event. Before the team is sent out, regardless of the reason and the role of the initiator for such request, at least a brief Charter has to be written down underlying the basic rules for the investigation (IAEA, 2004).

The Charter establishes the investigation team, clearly stating the **purpose, type and scope of investigation**. It specifies the team composition, defines the roles of team members, and roles of consultants/advisors, as well as the liaison personnel and counterparts. The Charter further specifies the team responsibilities and accountability and milestones to be met. The Charter is then distributed to all people involved before the investigation starts.

For a successful and fruitful investigation a team selection is crucial. Appointing top level people on the team reflects organisation's concern and commitment to investigation. Such top level people are more likely to get faster actions during the investigation; they will also assure faster implementation of corrective actions and they will generally handle the politics of investigation better.

The choice of team leader is also crucial for the success of investigation. The team leader is responsible for:

- Assembling and managing the team,
- Briefing the team and the counterpart on the scope and methods of investigation at the entrance meeting,
- Guiding the analysis,
- Documenting findings,
- Leading daily meetings with the team,
- Leading daily meetings with the counterpart,
- Reporting to the appropriate persons after the investigation has been completed during the exit meeting.

For this reason, the team manager is normally selected among the senior managers with knowledge in root cause methods and with experience in conducting root cause analysis investigations.

For the team members the following characteristics and qualifications should be considered:

- Ability to work in a team,
- Knowledgeable in root cause analysis techniques,
- Without the conflict of interest,
- One member for each topical area (for example human factors, Instrumentation and control, operations….),
- Ability to gather information through:
    - Document review,
    - Interviewing,
    - Site visits,
- Good writing skills.

By selecting team members, one should be careful as exclusive selection of outside investigators may imply that the local staff is incompetent or not to be trusted. It is therefore recommended to always have a proper balance between on-site and outside investigators. A certain number of on-site team members can also be useful in understanding the local situation.

Specialists in certain areas can be assigned as consultants and not as team members if their specialisation is needed for understanding certain phenomena that has impacted the event but their presence on the team is limited only to that particular aspect of investigation.

Before starting the investigation certain elements have to be specified that will later on influence the conduct of investigation. The team should have a written document that specifies:

- Scope of investigation covering information on:
  - Which event will be analysed;
  - Which planning processes have produced the event;
  - Management systems that should have controlled it.
- Authority, resources, deliverables and schedule.
- At the beginning of the investigation three lists should be created:
  - People to interview (as a minimum people that were involved in the event. Note that readiness to respond can fail through forgetfulness, external influences, internal conflicts, misinterpretation, embarrassment, stress etc.);
  - Documents to review (as a minimum documents used during the incident, procedures, work orders, operation logs, surveillance reports etc.);
  - Places to visit (as a minimum the place of the event, similar places, control room etc.).

As the investigation progresses the initial list is being updated as new evidence appears.

Probably the most important phase in an investigation is gathering information through interviews. It is therefore of utmost importance to conduct those in an open and professional manner, being well prepared for them. There are generally 4 phases on an interview:

- Planning and preparing,
- Opening phase,
- Question and answer phase,
- Closing phase.

In **planning** for the interview it is important to select a suitable location, get familiar with people that will be interviewed, prepare in advance the list of questions to be asked during the interview, select questions that will cover also positive and not only negative aspects of the event and leave enough time between interviews for yourself in order to expand the notes taken during the interview.

In **opening** the interview, make sure that interviewee is comfortable by answering the possible questions that he/she might have before the interview starts. Such questions can be; why do you want to talk to me, what will you do with such information, will my name appear in the report, etc. Answer all questions sincerely and openly.

In the **question and answer** phase, questions are generally characterised in three groups:

- *Open and closed questions*

  Open questions leave plenty of room for the interviewee to answer and elaborate on the topic in question. An example of an open question would be “tell me about the organisation that you work for”.

  Closed question would be one that demands a precise answer. An example of the closed question would be “what did you have for lunch today?”

- *Primary and secondary questions*

  The primary questions open a new topic in the discussion. An example would be “when did you hear about the event?”

  The secondary questions follow the primary question on the same topic if additional information is needed. There can be numerous secondary questions to follow the primary question.

- *Natural and leading questions*

  Natural questions leave an open space for the answer and do not suggest the possible answers. An example of the natural question would be “what type of food do you like?”

  Leading questions suggest an answer and should be avoided during interviews whenever possible.

All questions asked during an interview must be phrased in an understandable manner, be relevant to the person being interviewed and always asked one at a time.

In **closing** the interviewer provides the summary and tells the person being interviewed what will happen next. Ask for any final thoughts that he/she might have and invite them to contact you in case they would have any later thoughts after the interview.

8.2 Corrective actions

Every incident investigation should be concluded with the identification of corrective actions that need to be implemented. Corrective actions are focussed on near term and long term impacts and are put in place in order to:

- Mitigate the immediate effects of the event;
- Ensure that the same or similar events will not happen again.

For corrective actions applied after the event it is usually stated that they must be reasonable, affordable and acceptable. In many cases the proposed corrective actions do not fulfil the expectations and often it is blamed on identifying the wrong root cause by not going sufficiently in-depth of the problem, the investigation staying on the surface addressing only the direct causes.

In order to identify the best corrective actions, several conditions must be fulfilled:

- First, it must be verified that the true root causes have been identified. If this condition is not fulfilled, there is no way to come up with the correct corrective actions. Once that the real root causes have been identified it is necessary to directly link the proposed corrective actions to each root cause. This link must be clear and traceable.
- It should be possible to demonstrate by safety analyses that the corrective actions have reduced the probability of recurrence of similar events and their consequences. Corrective actions need to take into account the experience from previous similar events that have happened on the same site or were reported through the feedback of operating experience database system by others.
- Corrective actions should be reasonable with respect to the use of resources versus the risk of recurrence and this has to be clearly demonstrated. Corrective actions should have a measurable impact and this impact should be adequately recorded.
- Only the corrective actions that have a full support of the plant management will at the end be successful.

9 International initiatives taken after three major nuclear accidents (TMI, Chernobyl, Fukushima Daiichi)

This section will discuss the international initiatives that were undertaken as a response to three major nuclear accidents that have happened in nuclear industry.

On March 28, 1979 the first core melt happened at the TMI nuclear power plant. No radiological consequences were present during or after the event but nevertheless the nuclear industry responded immediately as until then such serious accident were not considered to be feasible in commercial nuclear facilities. The industry responded by creating a so-called Post-TMI Action Plan that implemented numerous improvements to the existing fleet of nuclear power plants in operation and requirements for new builds. Maybe the best known improvement was the introduction of the Safety Parameter Display Systems (SPDS) in the Main Control Rooms to improve the operator's diagnostic capabilities.

In the international arena, it was recognised that the industry must learn from the mistakes or near misses of others and in 1981 the OECD/NEA and the IAEA decided to create a system for the exchange of operating experience, known as the **IRS – Incident Reporting System** (IAEA, 2010) (today it is called International Reporting System, with the same acronym of IRS). The objective of the system was to promote the international cooperation in the exchange of operating experience and to complement national reporting schemes. The information reported under the IRS was assessed, analysed and fed back to operators to prevent similar occurrences in the future.

Apart from simply exchanging the information, the system also enabled the performance of topical studies on selected issues as with time sufficient data was collected to enable meaningful conclusions form a number of reported incidents. It also enabled the performance of studies to identify potential accident precursors. The system also encouraged the reporting of low-level events and near misses as well as recurrent events.

The OECD/NEA-IAEA IRS is still today in operation and is designed to serve the nuclear safety specialists and not the public (INES is used to inform the public). The system intends to increase the worldwide awareness of potential and actual problems in NPP operation. The feedback process which is an essential part of the system results in improvements in equipment, procedures and training. Results from the IRS studies are also used for the improvements in future NPP designs.

Thirty one countries with operating NPPs participate in the system by nominating national coordinators. They report safety significant events or events with lower safety significant but which carry important lessons to be learned. Each event can be reported in three stages:

- Preliminary report within a month,
- The Main Report with full analysis,
- Follow-up report, if new findings appear.

In order to participate in the IRS a country is expected to fulfil certain conditions such as, it:

- Has effectively embarked on a NPP Program;
- Has established an independent regulatory body with appropriate authority;
- Has established a national system for the feedback of operating experience;
- Has given to an appropriate organisation the IRS responsibility and has nominated the national coordinator;
- Is a contracting party to the Nuclear Safety Convention.

Until 1995 only abstracts were stored in the IRS database. In 1995, the advanced IRS (AIRS) was created with the capability of storing the full text reports. In 2006, web-based IRS (WB-IRS) was created, when password protected users were informed by email of changes in the IRS database. Currently around 3500 reports are stored in the data base with approximately 80 new reports being added annually.

On April 26, 1986 the **Chernobyl** accident happened with substantial off-site consequences. Within few months the international community reacted by establishing two international conventions. Never before did nuclear community agreed so quickly on the establishment and ratification of international obligatory conventions. The two conventions were:

- **"The Convention on Early Notification of a Nuclear Accident"** (IAEA, 1986a)**,**
- **"The Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency"** (IAEA, 1986b).

The first convention on early notification of a nuclear accident provides relevant information about the accident as early as possible so that transboundary consequences can be minimised. Accident state notifies countries that may be affected plus the IAEA whose role is to disseminate information to all convention signatories. Currently, 119 countries and international organisations are parties to this convention.

The second convention on assistance in the case of a nuclear accident or radiological emergency sets an international framework for cooperation. Also in this case the IAEA serves as a focal point for such cooperation. Currently, 112 countries and international organisations are parties to this convention.

On March 11, 2011, a major earthquake followed by a large tsunami destroyed **Fukushima Daiichi** nuclear power plant in Japan. The international community reacted promptly. On a regional level, the European countries, on the request of ENSREG, the European Association of Nuclear safety Regulators, decided to perform the so called **stress tests** (European Commission, 2012) on all nuclear power plants in Europe. They were joined by several non-EU countries that used the same methodology for their domestic review. The Stress tests were performed by the following EU Nuclear Member States: Belgium, Bulgaria, Czech Republic, Finland, France, Germany, Hungary, Lithuania, Netherlands, Romania, Slovakia, Slovenia, Sweden, Spain, United Kingdom, and European Commission. The following Non-Nuclear EU Member States joined the effort: Austria, Italy, Ireland and Luxembourg. Two Nuclear Non=Member States also joined, namely Ukraine and Switzerland (and much later Belarus). As observers, Armenia, Canada, Croatia, Japan, UAE and the IAEA participated in the effort. The stress tests focused on issues highlighted by the Fukushima Daiichi accident, namely:

- *Topic 1 – External hazards*

Covering earthquakes, flooding and other extreme natural (weather) conditions

- *Topic 2 – Consequential loss of safety functions (systems)*

Covering prolonged total loss of electric power (station blackout), prolonged total loss of the main ultimate heat sink and the combination of both situations.

- *Topic 3 – severe accident management issues, including core melt accident management.*

At the same time, the IAEA responded by establishing the **IAEA Post Fukushima Action Plan** (IAEA, 2011). The plan was prepared by the IAEA Secretariat, adopted by the IAEA Board of Governors and unanimously endorsed by the IAEA General Conference in September 2011. The purpose of the plan was to define a programme of work to strengthen the global nuclear safety framework. The Action plan covered 12 overreaching areas:

- Safety assessment of nuclear power plants,
- IAEA peer reviews,
- Emergency preparedness and response,
- Effectiveness of national regulatory bodies,
- Effectiveness of operating organisations with respect to nuclear safety,
- IAEA safety standards,
- Effectiveness of the international legal framework,

- Development of the infrastructure necessary for member states embarking on nuclear programme,
- Strengthening and maintaining capacity building,
- Protection of people and the environment from ionizing radiation,
- Transparency and effectiveness of communication,
- Utilisation of research and development.

The main activities under the Action Plan have been completed by the end of 2015 but most of the issues are demanding a continuous attention also in the future.

The contracting parties under the Nuclear Safety Convention have also agreed to respond to the Fukushima Daiichi accident and convened the Diplomatic Conference which on February 9, 2015 adopted the **Vienna Declaration on Nuclear Safety** (IAEA, 2015). It is a declaration on principles for the implementation of the objectives of the Nuclear Safety Convention to prevent accidents and mitigate radiological consequences should they occur. The Vienna Declaration on Nuclear safety has three major points:

- More stringent requirements for new NPPs,
- Comprehensive and systematic safety assessment of operating plants to be performed periodically,
- National requirements and regulations are to take into account the relevant IAEA Safety Standards.

The exact wording of all three points is the following:

> "1. New nuclear power plants are to be designed, sited, and constructed, consistent with the objective of preventing accidents in the commissioning and operation and, should an accident occur, mitigating possible releases of radionuclides causing long-term off site contamination and avoiding early radioactive releases or radioactive releases large enough to require long-term protective measures and actions.
>
> 2. Comprehensive and systematic safety assessments are to be carried out periodically and regularly for existing installations throughout their lifetime in order to identify safety improvements that are oriented to meet the above objective. Reasonably practicable or achievable safety improvements are to be implemented in a timely manner.
>
> 3. National requirements and regulations for addressing this objective throughout the lifetime of nuclear power plants are to take into account the relevant IAEA Safety Standards and, as appropriate, other good practices as identified inter alia in the Review Meetings of the CNS [Convention on Nuclear Safety]."

The contracting parties to the Nuclear Safety Convention should report on the regular meeting taking place every 3 years on the implementation of the Vienna declaration. The first such reporting took place during the 7th regular review meeting which took place from 27 March – 7 April 2017.

In conclusion, it can be stated that the international cooperation is essential for minimising the likelihood of another accident and the above three cases of international initiatives after three major nuclear accident demonstrate that the nuclear community has reacted promptly and adequately.

10 Summary and discussion

NPPs are exposed to a multitude of hazards from each of these factors and require a multi-risk framework for integration. The various state-of-the-art multi-risk methodologies available in the literature were summarised. It was found that the risk analysis framework adopted must be capable of addressing multi-hazard and multi-vulnerability demands. In particular, cascading effects and risks from low probability-high consequence events are of significance and must be considered for NPPs, for which there are few historical data points. This in turn places a considerable onus on domain experts to provide structured knowledge to risk assessments. NPPs are also complex facilities composed of technical (systems, structures, and components), social/organisational and human factors. Given the complexity of the facility, the lack of prior data, and potential subjectivity of expert opinion, considerable uncertainty accompanies a risk assessment effort, rendering uncertainty tracking and quantification extremely important. Therefore, a NPP risk framework must be capable of addressing these demands sufficiently and provide the necessary inputs for risk-informed decision making. Analytical tools such as BNs and fault trees have been applied extensively for each of the above challenges of the multi-risk problem. Multi-Risk frameworks that can integrate the use of such tools are required within the NARSIS project, to capture complex event dependencies, include expert opinion, and track uncertainty within the risk model.

A prerequisite to NPP risk analysis is establishing accident scenarios that need to be considered. In this regard, case histories of accidents and RCA methods are highly relevant to understand pre-existing latent weaknesses and reasons for accidents. Seven case studies were reviewed, from non-nuclear and nuclear fields, where a number of pre-existing and long lasting latent weaknesses existed. Deficiencies vary from case to case but most of them relate to deficiencies in management, design verification, procedures and work practices. In all cases it was found that procedures and practices were centred on productivity, and in all cases the surveillance programmes were not in place or capable of detecting and eliminating those latent weaknesses. For all the cases, deficiencies in safety culture could be identified. The organisational and regulatory outlook on safety culture is of paramount importance in preventing adverse events. When undesired events occur, incident investigation and corrective action protocols are important and were reviewed. Past initiatives following major nuclear accidents were also reviewed in this document.

RCA methods form a key part of identifying latent weaknesses in industrial facilities. As mentioned earlier, they are also useful in establishing accident scenarios for quantitative risk assessment either by analysis of past accidents or analysis of undesirable events at the time of design. Precursor analyses are used to determine the safety significance of events. Deterministic Transient Analyses are valuable in understanding the physical behaviour of a plant, typically during quickly occurring events or design basis accidents. Tools and methods associated with RCA, precursor analyses and transient analyses form an important part of risk integration. Several RCA methods were reviewed and their pros and cons were highlighted, indicating that all methods have their place in practice. Depending on the risk integration framework being used, the accident scenarios being modelled and available information any of these methods or their combination can be used.

The BN methodology has been used for multi-risk aspects including modelling cascading events of low probability with complex interdependencies, integrating expert judgement, and modelling of human and organisational factors. The BN is also an effective tool for handling uncertainty in risk analysis. Among methods for probabilistic risk integration, BNs have been implemented effectively for risk analysis applications in the literature, for nuclear, chemical, offshore and aviation industries. BNs provide several advantages over widely used risk analysis tools such as the FT. Nevertheless, it is not standard of practice in any of these industries

PSAs are standard of practice across high-risk industries such as the nuclear, chemical and aviation industries, involving integration tools such as the FT and ET. The chemical industry

employs unique methods such as the HAZOP and HAZAN approaches, while the FHA and FMEA, along with CCA are tools that are often applied in the aviation industry to complement PSAs. These methods are not alien to the nuclear industry and can be integrated easily into standard practice. The Causal Model for Air Transport Safety (CATS) is a unique approach from the aviation industry that is of interest in the NARSIS context and provides a means to combine advantages of Event Sequence Diagrams (ESD), FTs, and BNs.

None of the risk frameworks and analysis methods reviewed in this report is immune to pitfalls. Nevertheless, some of their advantages make them attractive for implementation in NPPs, and override the shortcomings. Moreover, the shortcomings may be simply managed or overcome by merging more than one of the deterministic and probabilistic methods discussed here or otherwise. Historically, deterministic methods have been used and have performed reasonably well. Part of their success, however, stems from the fact that their limitations were/are often compensated with relatively larger factors of safety in design. This results in excessively expensive, unsustainable or redundant design that despite its overdesign does not ensure safety (Modarres, 2006). Such purely deterministic designs are fast becoming a thing of the past and to varying extents, the use of probabilistic methods is now standard across many industries. The increased availability of data, improved understanding of equipment and materials, advanced numerical and simulation techniques and cumulative experiences have made probabilistic methods both possible and effective. Thereby, the IAEA standards mandate the use of both deterministic and probabilistic methods in safety demonstrations (IAEA, 2009) and such an approach integrates well into the decision making process and requirements (IAEA, 2011). Despite the increased popularity of feasibility of probabilistic methods, deterministic methods add value in specific areas and are often useful in providing the necessary inputs to a larger probabilistic risk framework. The strengths and weaknesses of some of the popular deterministic and probabilistic approaches have been reviewed in Section 6. When used in combination, deterministic and probabilistic methods can provide holistic solutions to risk analysis problems (Varde and Pecht, 2018), each serving to offset the weakness from the other approach. Such combined approaches also allow for integration of qualitative and quantitative information which is vital in data scarce environments. In general, a combination of deterministic and probabilistic approaches is concluded to yield best results in high-risk industries, where, for example, deterministic methods can be used to identify high-risk scenarios and probabilistic methods can be used to integrate the risks from different hazards and cascading events.

The IAEA Specific Safety Guide SSG-2 on Deterministic Safety Analyses recognises 4 options (IAEA, 2009). The first option is the strictly conservative option which used conservative computer codes/models with conservative input data on initial and boundary conditions. It is known as the Conservative option. The second option uses BE codes i.e. more realistic codes but still utilises conservative initial and boundary conditions. It is termed as the BE option. The third option uses BE codes and realistic input data for initial and boundary conditions but requires the evaluation of uncertainties. This is the BEPU option. All three above options have in common that the assumptions on the availability of safety systems are conservative. The fourth option is the extension of the BEPU where the assumptions on the availability of safety systems is based on the PSA or rather system reliability results. It is known as Extended BEPU analyses option or in short E-BEPU. The E-BEPU analysis offers considerable promise in terms of a methodology that allows for integration of probabilistic and deterministic methods.

Hence, in this study, it is concluded that the E-BEPU analyses and the BN framework are options for NPP risk assessments that demand further exploration.

11 References

Abrahamson, N. A. (2000). State of the practice of seismic hazard evaluation. Paper presented at the ISRM International Symposium.

Akiyama, M., & Frangopol, D. (2013). Life-cycle design of bridges under multiple hazards: Earthquake, tsunami, and continuous deterioration. Paper presented at the Proc., Eleventh Int. Conf. on Structural Safety and Reliability, ICOSSAR2013, Safety, and Reliability, ICOSSAR2013, Safety, reliability, risk, and life-cycle performance of structures and infrastructures.

Ale, B., Bellamy, L., Cooke, R., Duyvis, M., Kurowicka, D., Lin, C., Morales, O., Roelen, A. and Spouge, J., (2008). Causal model for air transport safety. Final Report, July, 31.

Amaral, L. A., & Ottino, J. M. (2004). Complex networks. The European Physical Journal B, 38(2), 147-162.

Anderson, K. (2018). The 1984 Bhopal Disaster in India—A Message for Industrialists Accessed July 2018 {URL: https://medium.com/kayla-anderson/the-1984-bhopal-disaster-in-india-a-message-for-industrialists-10abb3d1e8b6}

ASME, (2002). Standard for probabilistic risk assessment for nuclear power plant applications. The American Society of Mechanical Engineers.

ASME, (2008). Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications. American Society of Mechanical Engineers.

ASME, (2009). Addenda to ASME/ANS RA-S–2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009. In: American Society of Mechanical Engineers New York.

Aspinall, W. P., & Cooke, R. M. (2013). Quantifying scientific uncertainty from expert judgement elicitation. In J. Rougier, L. J. Hill, & S. Sparks (Eds.), Risk and Uncertainty Assessment for Natural Hazards (pp. 64-99). Cambridge: Cambridge University Press.

Asprone, D., Jalayer, F., Prota, A., & Manfredi, G. (2010). Proposal of a probabilistic model for multi-hazard risk assessment of structures in seismic zones subjected to blast for the limit state of collapse. Structural Safety, 32(1), 25-34. doi:https://doi.org/10.1016/j.strusafe.2009.04.002

Au, S.-K., & Wang, Y. (2014). Engineering risk assessment with subset simulation: John Wiley & Sons.

Aven, T. (2015). Implications of black swans to the foundations and practice of risk assessment and management. Reliability Engineering & System Safety, 134, 83-91. doi:https://doi.org/10.1016/j.ress.2014.10.004

Balakrishnan, N. (2015). An overview of system safety assessment. In Dependability in Medicine and Neurology (pp. 33-81): Springer.

Bellamy, L., Papazoglou, I., Hale, A., Aneziris, O., Ale, B., Morris, M., & Oh, J. (1999). I-Risk: Development of an integrated technical and management risk control and monitoring methodology for managing and quantifying on-site and off-site risks. Contract ENVA-CT96-0243. Report to European Union. Ministry of Social Affairs and Employment. Den Haag.

Bernal, G. (2010). CAPRA: Multi-hazard approach. Paper presented at the Conference Presentation in the Understanding Risk Forum.
{URL: http://www.understandrisk.org/ur/node/4573} (last access 19.03. 14.).

Bernal, G. A., Salgado-Gálvez, M. A., Zuloaga, D., Tristancho, J., González, D., & Cardona, O.-D. (2017). Integration of Probabilistic and Multi-Hazard Risk Assessment Within Urban Development Planning and Emergency Preparedness and Response: Application to Manizales, Colombia. International Journal of Disaster Risk Science, 8(3), 270-283. doi:10.1007/s13753-017-0135-8

Bier, V. M., Haimes, Y. Y., Lambert, J. H., Matalas, N. C., & Zimmerman, R. (1999). A Survey of Approaches for Assessing and Managing the Risk of Extremes. Risk Analysis, 19(1), 83-94. doi:doi:10.1111/j.1539-6924.1999.tb00391.x

Biondi, E. L. (1998). Organizational factors in the reliability assessment of offshore systems.

Bonacho, J., & Oliveira, C. S. (2018). Multi-hazard analysis of earthquake shaking and tsunami impact. International Journal of Disaster Risk Reduction, 31, 275-280. doi:https://doi.org/10.1016/j.ijdrr.2018.05.023

Borgonovo, E., & Smith, C. L. (2011). A study of interactions in the risk assessment of complex engineering systems: An application to space PSA. Operations Research, 59(6), 1461-1476.

Boudali, H., & Dugan, J. B. (2005). A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering & System Safety, 87(3), 337-349.

Burgazzi, L. (2012). Reliability of Passive Systems in Nuclear Power Plants, Nuclear Power Wael Ahmed, IntechOpen, October, 2012. DOI: 10.5772/47862.
{URL: https://www.intechopen.com/books/nuclear-power-practical-aspects/reliability-of-passive-systems-in-nuclear-power-plants}

Burgman, M. A. (2015). Trusting judgements: how to get the best out of experts: Cambridge University Press.

Burgman, M. A., McBride, M., Ashton, R., Speirs-Bridge, A., Flander, L., Wintle, B., . . . Twardy, C. (2011). Expert status and performance. PLOS ONE, 6(7), e22998.

Carpignano, A., Golia, E., Di Mauro, C., Bouchon, S., & Nordvik, J. P. (2009). A methodological approach for the definition of multi-risk maps at regional level: first application. Journal of Risk Research, 12(3-4), 513-534. doi:10.1080/13669870903050269

Caselton, W. F., & Luo, W. (1992). Decision making with imprecise probabilities: Dempster-Shafer theory and application. Water Resources Research, 28(12), 3071-3083.

Castillo, E. (2012). Extreme value theory in engineering: Elsevier.

Chang, Y., & Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: Part 1: Overview of the IDAC Model. Reliability Engineering & System Safety, 92(8), 997-1013.

Chang, Y., & Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: Part 2: IDAC performance influencing factors model. Reliability Engineering & System Safety, 92(8), 1014-1040.

Chang, Y., & Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: Part 3: IDAC operator response model. Reliability Engineering & System Safety, 92(8), 1041-1060.

Chen, H. X., Zhang, S., Peng, M., & Zhang, L. M. (2016). A physically-based multi-hazard risk assessment platform for regional rainfall-induced slope failures and debris flows. Engineering Geology, 203, 15-29. doi:https://doi.org/10.1016/j.enggeo.2015.12.009

Ciurean, R. L., Schröter, D., & Glade, T. (2013). Conceptual frameworks of vulnerability assessments for natural disasters reduction. In Approaches to disaster management-Examining the implications of hazards, emergencies and disasters: InTech.

Cizelj, L., Mavko, B., & Riesch-Oppermann, H. (1994). Application of first and second order reliability methods in the safety assessment of cracked steam generator tubing. Nuclear Engineering and Design, 147(3), 359-368.

Clemen, R. T. (2008). Comment on Cooke's classical method. Reliability Engineering & System Safety, 93(5), 760-765.

Clemen, R. T., & Winkler, R. L. (1999). Combining probability distributions from experts in risk analysis. Risk Analysis, 19(2), 187-203.

Colson, A. R., & Cooke, R. M. (2017). Cross validation for the classical model of structured expert judgment. Reliability Engineering & System Safety, 163, 109-120. doi:https://doi.org/10.1016/j.ress.2017.02.003

Cooke, D. L. (2004). The dynamics and control of operational risk: Calgary.

Cooke, R., Mendel, M., & Thijs, W. (1988). Calibration and information in expert resolution; a classical approach. Automatica, 24(1), 87-94.

Cooke, R. M. (1991). Experts in uncertainty. In: Oxford University Press Oxford.

Cooke, R. M., ElSaadany, S., & Huang, X. (2008). On the performance of social network and likelihood-based expert weighting schemes. Reliability Engineering & System Safety, 93(5), 745-756.

Cooke, R. M., & Goossens, L. L. H. J. (2008). TU Delft expert judgment data base. Reliability Engineering and System Safety, 93(5), 657-674. doi:10.1016/j.ress.2007.03.005

Cooper, S.E., Ramey-Smith, A.M., Wreathall, J. and Parry, G.W., 1996. A technique for human error analysis (ATHEANA) (No. NUREG/CR-6350; BNL-NUREG-52467). Nuclear Regulatory Commission, Washington, DC (United States). Div. of Systems Technology; Brookhaven National Lab., Upton, NY (United States); Science Applications International Corp., Reston, VA (United States); NUS Corp., Gaithersburg, MD (United States).Cornell, C. A. & Krawinkler, H. 2000. Progress and challenges in seismic performance assessment, PEER Center News.

Cowell, R., Dawid, A., Lauritzen, S. & Spiegelhalter, D. (1999). Probabilistic networks and expert systems, 1999. ISBN: 0-387-98767-3.

Cullen, H. (1990). The public inquiry into the Piper Alpha disaster (Report to the Parliament by the Secretary of State for Energy by Command of Her Majesty Vols. 1 and 2). In: London: HMSO.

Dalton, A., Brothers, A., Walsh, S., White, A., & Whitney, P. (2012). 10 Expert elicitation method selection process and method comparison. Neuroscience and the Economics of Decision Making, 5, 182.

Damnjanovic, I., & Aven, T. (2017). Critical Slowing-down Framework for Monitoring Early Warning Signs of Surprise and Unforeseen Events. In Knowledge in Risk Assessment and Management.

Daniell, J., Schaefer, A., Wenzel F., Häcker, E. (2018). Del 1.1 Review of state-of-the art for hazard and multi-hazard characterisation. NARSIS report, H2020 project.

Daniell, J., Simpson, A., Murnane, R., Tijssen, A., Nunez, A., Deparday, V., Gunasekera, R., Baca, A., Ishizawa, O. and Schäfer, A., 2014. Review of open source and open access software packages available to quantify risk from natural hazards. Washington, DC: World Bank and Global Facility for Disaster Reduction and Recovery.

Davoudian, K., Wu, J.-S., & Apostolakis, G. (1994a). Incorporating organizational factors into risk assessment through the analysis of work processes. Reliability Engineering & System Safety, 45(1), 85-105.

Davoudian, K., Wu, J.-S., & Apostolakis, G. (1994b). The work process analysis model (WPAM). Reliability Engineering & System Safety, 45(1), 107-125.

de Waal, A., Koen, H., de Villiers, J. P., Roodt, H., Moorosi, N., & Pavlin, G. (2016). Construction and evaluation of Bayesian networks with expert-defined latent variables. Paper presented at the FUSION.

Delmonaco, G., Margottini, C., & Spizzichino, D. (2006). ARMONIA methodology for multi-risk assessment and the harmonisation of different natural risk maps. Deliverable 3.1. 1, ARMONIA.

Dempster, A. P. (1967). Upper and Lower Probabilities Induced by a Multivalued Mapping. Ann. Math. Statist., 38(2), 325-339. doi:10.1214/aoms/1177698950

DOE. (2012). DOE HANDBOOK Accident and Operational Safety Analysis. Volume I: Accident Analysis Techniques. Department of Energy, USA. {URL: https://www.standards.doe.gov/standards-documents/1200/1208-bhdbk-2012-v1/@@images/file

Dong, Y., Frangopol, D. M., & Saydam, D. (2013). Time-variant sustainability assessment of seismically vulnerable bridges subjected to multiple hazards. Earthquake Engineering & Structural Dynamics, 42(10), 1451-1467. doi:doi:10.1002/eqe.2281

Dubois, D., & Guyonnet, D. (2011). Risk-informed decision-making in the presence of epistemic uncertainty. International Journal of General Systems, 40(02), 145-167.

Dusic, M. (2018). Personal communication.

Eckerman, I. (2005). The Bhopal saga: causes and consequences of the world's largest industrial disaster: Universities press.

Electrabel. (2010). Technical Meeting on Experience with Risk-based Precursor Analysis. Electrabel, Brussels, Belgium, 24 – 26 November 2010.

Embrey, D., Humphreys, P., Rosa, E., Kirwan, B., & Rea, K. (1984). SLIM-MAUD: an approach to assessing human error probabilities using structured expert judgment. Volume II. Detailed analysis of the technical issues. (No. NUREG/CR--3518-VOL. 2). Brookhaven National Lab.

Embrey, D. E. (1992). Incorporating management and organisational factors into probabilistic safety assessment. Reliability Engineering & System Safety, 38(1-2), 199-208.

European Commission. (2012). Communication from the commission to the council and the european parliament on the comprehensive risk and safety assessments ("stress tests") of nuclear power plants in the European Union and related activities. European Comission. COM/2012/0571 final, EC, {URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012DC0571}

EUROCONTROL (2006) , “Main Report for the 2005/2012 Integrated Risk Picture for Air Traffic Management in Europe”, EEC Note 05/06, March 2006.

Farmer, F. R. (1967). Reactor safety and siting: a proposed risk criterion, Nuclear Safety, 8, 539-548.

FEMA. (2011). Getting Started with HAZUS-MH 2.1. Tech. Rep. U.S. Department of Homeland Security. Federal Emergency Management Agency.

Fernández, A., Pérez-Bernabé, I., Rumí, R., & Salmerón, A. (2013). Incorporating Prior Knowledge when Learning Mixtures of Truncated Basis Functions from Data. Paper presented at the SCAI.

Ferrell, W. R. (1994). Discrete subjective probabilities and decision analysis: Elicitation, calibration and combination.

Fiering, M. B., and J. Kindler. (1984). Surprise in Water-Resource Design. Int. J. Water Res. Devel. 2, 1–10.

Flandoli, F., Giorgi, E., Aspinall, W. P., & Neri, A. (2011). Comparison of a new expert elicitation model with the Classical Model, equal weights and single experts, using a cross-validation technique. Reliability Engineering & System Safety, 96(10), 1292-1310.

Gallina, V., Torresan, S., Critto, A., Sperotto, A., Glade, T., & Marcomini, A. (2016). A review of multi-risk methodologies for natural hazards: Consequences and challenges for a climate change impact assessment. Journal of Environmental Management, 168, 123-132. doi:https://doi.org/10.1016/j.jenvman.2015.11.011

Garcia, M. D., Varma, R., & Heger, A. S. (1996). Risk Assessment and Life Prediction of Complex Engineering Systems, London.

Garcia-Aristizabal, A., Gasparini, P., & Uhinga, G. (2015). Multi-risk Assessment as a Tool for Decision-Making. In S. Pauleit, A. Coly, S. Fohlmeister, P. Gasparini, G. Jørgensen, S. Kabisch, W. J. Kombe, S. Lindley, I. Simonis, & K. Yeshitela (Eds.), Urban Vulnerability and Climate Change in Africa: A Multidisciplinary Approach (pp. 229-258). Cham: Springer International Publishing.

Garcia-Aristizabal, A., Marzocchi, W., & Di Ruocco, A. (2013). Probabilistic framework for multi-hazard assessment. Technical Report D3.4, MATRIX Project (New Methodologies for Multi-Hazard and Multi-Risk Assessment Methods for Europe), Grant No. 265138.

Garcia-Aristizabal, A., & Marzocchi, W. (2012). Review of existing procedures for multi-hazard assessment. Technical Report D5.1, MATRIX Project (New Methodologies for Multi-Hazard and Multi-Risk Assessment Methods for Europe), Grant No. 265138.

García-Herrero, S., Mariscal, M., Gutiérrez, J. M., & Toca-Otero, A. (2013). Bayesian network analysis of safety culture and organizational culture in a nuclear power plant. Safety Science, 53, 82-95.

Gasparini, P., & Garcia-Aristizabal, A. (2014). Seismic Risk Assessment, Cascading Effects. In M. Beer, I. A. Kougioumtzoglou, E. Patelli, & I. S.-K. Au (Eds.), Encyclopedia of Earthquake Engineering (pp. 1-20). Berlin, Heidelberg: Springer Berlin Heidelberg.

Gehl, P., & D'Ayala, D. (2016). Development of Bayesian Networks for the multi-hazard fragility assessment of bridge systems. Structural Safety, 60, 37-46.

Gehman, H. W. (2003). Columbia Accident Investigation Board, Report Vol. 1, August 2003: Columbia Accident Investigation Board.

Gerstenberger, M., & Christophersen, A. (2016). A Bayesian network and structured expert elicitation for Otway Stage 2C: Detection of injected CO2 in a saline aquifer. International Journal of Greenhouse Gas Control, 51, 317-329.

Goda, K., & De Risi, R. (2018). Multi-hazard loss estimation for shaking and tsunami using stochastic rupture sources. International Journal of Disaster Risk Reduction, 28, 539-554. doi:https://doi.org/10.1016/j.ijdrr.2018.01.002

Green, A. E. (1982). High risk safety technology: John Wiley & Sons.

Groth, K., & Mosleh, A. (2009). A data-informed model of performance shaping factors and their interdependencies for use in human reliability analysis. Paper presented at the Proceedings of the European society for reliability annual meeting (ESREL 2009), Prague, Czech Republic.

Grozdanovic, M. (2005). Usage of Human Reliability Quantification Methods. International Journal of Occupational Safety and Ergonomics, 11(2), 153-159. doi:10.1080/10803548.2005.11076644

Grünthal, G., Thieken, A. H., Schwarz, J., Radtke, K. S., Smolka, A., & Merz, B. (2006). Comparative Risk Assessments for the City of Cologne – Storms, Floods, Earthquakes. Natural Hazards, 38(1), 21-44. doi:10.1007/s11069-005-8598-0

Guckenheimer J., Ottino J.M. (2008). Foundations for complex systems research in the physical sciences and engineering. Report from an NSF Workshop in September 2008. {URL: pi.math.cornell.edu/~gucken/PDF/nsf_complex_systems.pdf}

Guo, X., & Chen, Z. (2016). Lifecycle Multihazard Framework for Assessing Flood Scour and Earthquake Effects on Bridge Failure. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, 2(2), C4015004. doi:doi:10.1061/AJRUA6.0000844

Haimes, Y. Y. (1981). Hierarchical holographic modeling. IEEE Transactions on Systems, Man, and Cybernetics, 11(9), 606-617.

Haimes, Y. Y. (2018). Modeling and managing interdependent complex systems of systems: Wiley.

Hanea, A., Kurowicka, D., & Cooke, R. (2007). The population version of Spearman's rank correlation coefficient in the case of ordinal discrete random variables. Paper presented at the Proceedings of the Third Brazilian Conference on Statistical Modelling in Insurance and Finance.

Hanea, A., Napoles, O. M., & Ababei, D. (2015). Non-parametric Bayesian networks: Improving theory and reviewing applications. Reliability Engineering & System Safety, 144, 265-284.

Hanea, A. M., Kurowicka, D., & Cooke, R. M. (2006). Hybrid method for quantifying and analyzing Bayesian belief nets. Quality and Reliability Engineering International, 22(6), 709-729.

Hanea, A. M., Kurowicka, D., Cooke, R. M., & Ababei, D. A. (2010). Mining and visualising ordinal data with non-parametric continuous BBNs. Computational Statistics & Data Analysis, 54(3), 668-687. doi:https://doi.org/10.1016/j.csda.2008.09.032

Hanea, A. M., McBride, M. F., Burgman, M. A., & Wintle, B. C. (2018). Classical meets modern in the IDEA protocol for structured expert judgement. Journal of Risk Research, 21(4), 417-433. doi:10.1080/13669877.2016.1215346

Health & Safety Executive (HSE) (2002); Marine Risk Assessment. HSE Report OTO 2001/063. Det Norske Veritas. HSE Books, Norwich.

Helton, J. C., & Davis, F. J. (2003). Latin hypercube sampling and the propagation of uncertainty in analyses of complex systems. Reliability Engineering & System Safety, 81(1), 23-69.

Hemming, V., Burgman, M. A., Hanea, A. M., McBride, M. F., & Wintle, B. C. (2018). A practical guide to structured expert elicitation using the IDEA protocol. Methods in Ecology and Evolution, 9(1), 169-180. doi:doi:10.1111/2041-210X.12857

Heylighen, F. (2008). Complexity and self-organization. Encyclopedia of library and information sciences, 3, 1215-1224.

Hollnagel, E. (1998). Cognitive reliability and error analysis method (CREAM): Elsevier.

Hollnagel, E., & Fujita, Y. (2013). The Fukushima disaster–systemic failures as the lack of resilience. Nuclear Engineering and Technology, 45(1), 13-20.

Hora, S. C. (2007). Eliciting probabilities from experts. Advances in decision analysis: From foundations to applications, 129.

Hora, S. C., Fransen, B. R., Hawkins, N., & Susel, I. (2013). Median Aggregation of Distribution Functions. Decision Analysis, 10(4), 279-291. doi:10.1287/deca.2013.0282

Hossain, M., & Muromachi, Y. (2012). A Bayesian network based framework for real-time crash prediction on the basic freeway segments of urban expressways. Accident Analysis & Prevention, 45, 373-381.

Hourtolou, D., & Salvi, O. (2003). ARAMIS Project: development of an integrated Accidental Risk Assessment Methology for IndustrieS in the framework of SEVESO II directive. Paper presented at the International Conference on Safety and Reliability (ESREL 2003).

Huh, J., & Haldar, A. (2011). A novel risk assessment for complex structural systems. IEEE Transactions on Reliability, 60(1), 210-218.

IAEA. (1986a). Convention on Early Notification of a Nuclear Accident. INFCIRC/335. IAEA, Vienna. {URL: https://www.iaea.org/sites/default/files/infcirc335.pdf}

IAEA. (1986b). Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency. INFCIRC/336. IAEA, Vienna.
{URL: https://www.iaea.org/sites/default/files/infcirc336.pdf }

IAEA. (1991). Safety Culture. IAEA Safety Series No. 75-INSAG-4, International Nuclear Safety Advisory Group, IAEA, Vienna. {URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub882_web.pdf}

IAEA. (1992). 50-P-4, S. S. - Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1). IAEA, Vienna.

IAEA. (1994) IAEA TECDOC-743 ASCOT Guidelines, IAEA, Vienna. {URL: https://www-pub.iaea.org/books/IAEABooks/1005/Ascot-Guidelines}

IAEA. (1995). 50-P-8, S. S. - Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level 2) – Accident Progression, Containment Analysis and Estimation of Accident Source Terms". IAEA, Vienna.

IAEA. (1996). 50-P-12, S. S. - Procedures for Conduction Probabilistic Safety Assessments of Nuclear Power Plants (Level 3). IAEA, Vienna.

IAEA. (1996a). INSAG-10 – Defence in Depth in Nuclear Safety. A report by the International Nuclear Safety Advisory Group. IAEA, Vienna.
{URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1013e_web.pdf}

IAEA. (1999). INSAG-12 – Basic Safety Principles for Nuclear Power Plants - 75 – INSAG-3 Rev. 1. IAEA, Vienna, October, 1999.
{URL: https://www-pub.iaea.org/MTCD/Publications/PDF/P082_scr.pdf}

IAEA. (2001). Safety Series No. 11 - Developing safety culture in nuclear activities: practical suggestions to assist progress. IAEA, Vienna.

IAEA. (2002). Key practical issues in strengthening safety culture. INSAG-15. International Nuclear Safety Advisory Group, IAEA, Vienna.

IAEA. (2004). TECDOC-1417 - Precursor Analysis - The Use of Deterministic and PSA Based Methods in the Event Investigation Process at Nuclear Power Plants. IAEA, Vienna. {URL: https://www-pub.iaea.org/books/iaeabooks/7148/Precursor-Analyses-The-Use-of-Deterministic-and-PSA-Based-Methods-in-the-Event-Investigation-Process-at-Nuclear-Power-Plants}

IAEA. (2005). Safety Report Series No. 46 - Assessment of Defence in Depth for Nuclear Power Plants. STI/PUB/1218; (ISBN:92-0-114004-5). IAEA, Vienna, 2005.
{URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1218_web.pdf}

IAEA. (2009). Deterministic safety analysis for nuclear power plants. Safety Series Guide SSG-2. IAEA, Vienna.

IAEA. (2010). Services Series No. 19; IRS Guidelines; Joint IAEA/NEA International Reporting System for Operating Experience, IAEA, Vienna, 2010. {URL: https://www-ns.iaea.org/downloads/ni/irs/irs_guidelines2010.pdf}

IAEA. (2011). IAEA Action Plan on Nuclear Safety. IAEA, Vienna, 2011. {URL: https://www.iaea.org/topics/nuclear-safety-action-plan}

IAEA. (2012). Technical meeting on Lessons Learned from Precursor Analyses, Brussels, Belgium, 7 – 9 November 2012.

IAEA. (2014). TECDOC-1756 - Root Cause Analysis Following an Event at a Nuclear Installation: Reference Manual. International Atomic Energy Agency, Vienna

IAEA. (2015). CNS/DC/2015/2/Rev.1 - Vienna Declaration on Nuclear Safety. IAEA, Vienna, February 9, 2015.
{URL: https://www.iaea.org/sites/default/files/cns_viennadeclaration090215.pdf}

IAEA. (2016). GSR Part 2 - Leadership and Management for Safety. General Safety Requirements. IAEA, Vienna, June, 2016.
{URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1750web.pdf}

IAEA. (limited distribution a). IAEA Asset Review Mission Report (limited distribution)

IAEA. (limited distribution b). IAEA Incident Investigation Report (limited distribution)

Iervolino, I., Giorgio, M., & Polidoro, B. (2015). Reliability of structures to earthquake clusters. Bulletin of Earthquake Engineering, 13(4), 983-1002. doi:10.1007/s10518-014-9679-9

ISO. (2015). ISO 9001:2015 - Quality management systems – Requirements. Edition 5. Technical Committee: ISO/TC 176/SC 2 Quality systems
{URL: https://www.iso.org/standard/62085.html}

Iervolino, I., Massimiliano, G., & Eugenio, C. (2014). Closed-form aftershock reliability of damage-cumulating elastic-perfectly-plastic systems. Earthquake Engineering & Structural Dynamics, 43(4), 613-625. doi:doi:10.1002/eqe.2363

Jalayer, F., & Ebrahimian, H. (2017). Seismic risk assessment considering cumulative damage due to aftershocks. Earthquake Engineering & Structural Dynamics, 46(3), 369-389. doi:doi:10.1002/eqe.2792

Jamshidi, A., Ait-kadi, D., Ruiz, A., & Rebaiaia, M. L. (2018). Dynamic risk assessment of complex systems using FCM. International Journal of Production Research, 56(3), 1070-1088. doi:10.1080/00207543.2017.1370148

Jaynes, E. T. (1996). Probability theory: the logic of science: Washington University St. Louis, MO.

Jean-Baptiste, N., Kabisch, S., & Kuhlicke, C. (2013). Urban Vulnerability Assessment in Flood-Prone Areas in West and East Africa, Dordrecht.

Jonkman, S.N., Van Gelder, P.H.A.J.M. and Vrijling, J.K., 2003. An overview of quantitative risk measures for loss of life and economic damage. Journal of hazardous materials, 99(1), pp.1-30.

JRC. (2018). Training Course on Root Cause Analysis and Event Investigation 15. – 19. 05. 2018, European Commission, Joint Research Centre, Petten, Netherlands

Kaplan, S. (1992). 'Expert information'versus 'expert opinions'. Another approach to the problem of eliciting/combining/using expert knowledge in PRA. Reliability Engineering & System Safety, 35(1), 61-72.

Kappes, M., Keiler, M., & Glade, T. (2010). From single-to multi-hazard risk analyses: a concept addressing emerging challenges.

Kappes, M., 2011. Multi-hazard Risk Analyses: a Concept and its Implementation. PhD Thesis, University of Vienna. http://othes.univie.ac.at/15973/1/2011-08-03_0848032.pdf (access 19.03.14.).Karagiorgos, K., Thaler, T., Hübl, J., Maris, F., & Fuchs, S. (2016). Multi-vulnerability analysis for flash flood risk management. Natural Hazards, 82(1), 63-87. doi:10.1007/s11069-016-2296-y

Karapetrou, S. T., Fotopoulou, S. D., & Pitilakis, K. D. (2017). Seismic Vulnerability of RC Buildings under the Effect of Aging. Procedia Environmental Sciences, 38, 461-468. doi:https://doi.org/10.1016/j.proenv.2017.03.137

Kazemi, R., Mosleh, A., & Dierks, M. (2017). A Hybrid Methodology for Modeling Risk of Adverse Events in Complex Health-Care Settings. Risk Analysis, 37(3), 421-440.

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(8), 925-932. doi:https://doi.org/10.1016/j.ress.2011.03.012

Khakzad, N., Khan, F., & Amyotte, P. (2015). Major Accidents (Gray Swans) Likelihood Modeling Using Accident Precursors and Approximate Reasoning. Risk Analysis, 35(7), 1336-1347. doi:doi:10.1111/risa.12337

Khakzad, N., Khan, F., Amyotte, P., & Cozzani, V. (2013). Domino effect analysis using Bayesian networks. Risk Analysis: An International Journal, 33(2), 292-306.

Kinnison, R.R., 1983. Applied extreme-value statistics (No. PNL-4690). Pacific Northwest Lab., Richland, WA (USA).

Kleist, L., Thieken, A. H., KÃ¶hler, P., MÃ¼ller, M., Seifert, I., Borst, D., & Werner, U. (2006). Estimation of the regional stock of residential buildings as a basis for a comparative risk assessment in Germany. Nat. Hazards Earth Syst. Sci., 6(4), 541-552. doi:10.5194/nhess-6-541-2006

Koller, D., & Friedman, N. (2009). Probabilistic graphical models: principles and techniques: MIT press.

Komendantova, N., van Erp, N., van Gelder, P., & Patt, A. (2013). Individual and cognitive barriers to effective multi-hazard and multi-risk decision-making governance. In: D6 of the FP7 project MATRIX.

Korb, K. B., & Nicholson, A. E. (2010). Bayesian artificial intelligence: CRC press.

Kumamoto, H., & Henley, E. J. (2000). Probablistic risk assessment and management for engineers and scientists: Wiley-IEEE.

Kurowicka, D., & Cooke, R. M. Distribution-Free continuous Bayesian Belief Nets. In: Modern Statistical and Mathematical Methods in Reliability by World Scientific. (pp. 309-322).

Lamb R., Keef C., Tawn J., Laeger S., Meadowcroft I., Surendran S., Dunning P. & Batstone C. (2010). A new method to assess the risk of local and widespread flooding on rivers and coasts. J Flood Risk Management 2010, 3, (4), 323–336.

Langseth, H., Nielsen, T. D., Rumı, R., & Salmerón, A. (2010). Parameter estimation and model selection for mixtures of truncated exponentials. International Journal of Approximate Reasoning, 51(5), 485-498.

Langseth, H., Nielsen, T. D., Rumí, R., & Salmerón, A. (2009). Inference in hybrid Bayesian networks. Reliability Engineering & System Safety, 94(10), 1499-1509.

Lee, C.-J., & Lee, K. J. (2006). Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal. Reliability Engineering & System Safety, 91(5), 515-532.

Lee, S. J., Kim, J., & Jang, S.-C. (2011). Human error mode identification for NPP main control room operations using soft controls. Journal of nuclear science and technology, 48(6), 902-910.

Lee, S. J., & Seong, P. H. (2005). A dynamic neural network based accident diagnosis advisory system for nuclear power plants. Progress in Nuclear Energy, 46(3-4), 268-281.

Leveson, N. (2004). A new accident model for engineering safer systems. Safety science, 42(4), 237-270.

Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety: MIT press.

Levine, R. D., & Tribus, M. (1979). Maximum entropy formalism. Paper presented at the Maximum Entropy Formalism Conference (1978: Massachusetts Institute of Technology).

Li, P.-c., Zhang, L., Dai, L.-c., Li, X.-f., & Jiang, Y. (2018). A new organization-oriented technique of human error analysis in digital NPPs: Model and classification framework. Annals of Nuclear Energy, 120, 48-61.

Limbourg, P., & De Rocquigny, E. (2010). Uncertainty analysis using evidence theory–confronting level-1 and level-2 approaches with data availability and computational constraints. Reliability Engineering & System Safety, 95(5), 550-564.

Lin, S.-W., & Bier, V. M. (2008). A study of expert overconfidence. Reliability Engineering & System Safety, 93(5), 711-721.

Lin, S.-W., & Huang, S.-W. (2012). Effects of overconfidence and dependence on aggregated probability judgments. Journal of Modelling in Management, 7(1), 6-22.

Liu, P., Lyu, X., Qiu, Y., He, J., Tong, J., Zhao, J., & Li, Z. (2017). Identifying key performance shaping factors in digital main control rooms of nuclear power plants: A risk-based approach. Reliability Engineering & System Safety, 167, 264-275.

Liu, Q., Pérès, F., & Tchangani, A. (2016). Object Oriented Bayesian Network for complex system risk assessment. IFAC-PapersOnLine, 49(28), 31-36. doi:https://doi.org/10.1016/j.ifacol.2016.11.006

Liu, Z., Nadim, F., Garcia-Aristizabal, A., Mignan, A., Fleming, K., & Luna, B. Q. (2015). A three-level framework for multi-risk assessment. Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards, 9(2), 59-74. doi:10.1080/17499518.2015.1041989

Luxhøj, J. T. (2004). Building a safety risk management system: a proof of concept prototype. Paper presented at the FAA/NASA Risk Analysis Workshop, Arlington, VA, USA.

Marasco, S., Noori, A. Z., & Cimellaro, G. P. (2017). Cascading Hazard Analysis of a Hospital Building. Journal of Structural Engineering, 143(9), 04017100. doi:doi:10.1061/(ASCE)ST.1943-541X.0001808

Marshall, A., Stanton, N., Young, M., Salmon, P., Harris, D., Demagalski, J., Waldmann, T. and Dekker, S., (2003) Development of the human error Template – a new methodology for assessing design induced errors on aircraft flight decks. Final Report of the ERRORPRED Project E!1970, Department of Trade and Industry, London.

Marzocchi, W., Garcia-Aristizabal, A., Gasparini, P., Mastellone, M. L., & Di Ruocco, A. (2012). Basic principles of multi-risk assessment: a case study in Italy. Natural Hazards, 62(2), 551-573. doi:10.1007/s11069-012-0092-x

Marzocchi, W., Mastellone, M., Di Ruocco, A., Novelli, P., Romeo, E., & Gasparini, P. (2009). Principles of multi-risk assessment: interactions amongst natural and man-induced risks. European Commission, Directorate-General for Research, Environment Directorate.

Marzocchi, W., Sandri, L., Gasparini, P., Newhall, C., & Boschi, E. (2004). Quantifying probabilities of volcanic events: the example of volcanic hazard at Mount Vesuvius. Journal of Geophysical Research: Solid Earth, 109(B11).

Merz, B., & Thieken, A. H. (2005). Separating natural and epistemic uncertainty in flood frequency analysis. Journal of Hydrology, 309(1-4), 114-132.

Merz, B., & Thieken, A. H. (2009). Flood risk curves and uncertainty bounds. Natural Hazards, 51(3), 437-458. doi:10.1007/s11069-009-9452-6

Meyer, M., & Booker, J. (1991). Eliciting and analyzing expert judgement: A practical tour. In: London: Academic Press.

Mignan, A., Wiemer, S., & Giardini, D. (2014). The quantification of low-probability–high-consequences events: part I. A generic multi-risk approach. Natural Hazards, 73(3), 1999-2022. doi:10.1007/s11069-014-1178-4

Mkrtchyan, L., Podofillini, L., & Dang, V. N. (2015). Bayesian belief networks for human reliability analysis: A review of applications and gaps. Reliability Engineering & System Safety, 139, 1-16.

Modarres, M. (2016). Risk analysis in engineering: techniques, tools, and trends: CRC press.

Mohaghegh, Z., Kazemi, R., & Mosleh, A. (2009). Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization. Reliability Engineering & System Safety, 94(5), 1000-1018.

Mohaghegh, Z., & Mosleh, A. (2009). Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations. Safety science, 47(8), 1139-1158. doi:https://doi.org/10.1016/j.ssci.2008.12.008

Morales-Nápoles, O., Delgado-Hernández, D. J., De-León-Escobedo, D., & Arteaga-Arcos, J. C. (2014). A continuous Bayesian network for earth dams' risk assessment: methodology and quantification. Structure and Infrastructure Engineering, 10(5), 589-603. doi:10.1080/15732479.2012.757789

Morgan, M. G. (2014). Use (and abuse) of expert elicitation in support of decision making for public policy. Proceedings of the National Academy of Sciences, 201319946.

Morgan, M. G., & Henrion, M. (1990). Uncertainty: a Guide to dealing with uncertainty in quantitative risk and policy analysis Cambridge University Press, New York.

Mosleh, A. Golfeiz., E. B. (1999). An approach for assessing the impact of organizational factors on risk. Technical Research Report CTRS-B3-08. University of Maryland.

MOVE. (2010). EU project “Methods for the Improvement of Vulnerability Assessment in Europe” (MOVE). Deliverable D6 Guidelines for development of different methods, 15 March 2010, www.move-fp7.eu

Murphy, K. P., & Russell, S. (2002). Dynamic bayesian networks: representation, inference and learning.

MunichRe (2011). NATHAN world map of natural hazards. Munich RE, Munich, Germany.

Musharraf, M., Hassan, J., Khan, F., Veitch, B., MacKinnon, S., & Imtiaz, S. (2013). Human reliability assessment during offshore emergency conditions. Safety science, 59, 19-27. doi:https://doi.org/10.1016/j.ssci.2013.04.001

Nadim, F., Liu, Z., Vidar Vangelsten, B., Aristizabal, A., Woo, G., Aspinall, W., Fleming, K.M., van Gelder, P. (2013). Framework for multi-risk assessment. Deliverable D5, 2 of the FP7 project MATRIX.
{URLs:
https://www.researchgate.net/publication/323416567_MATRIX_Framework_for_multi-risk_assessment
and https://www.researchgate.net/publication/324090021_MATRIX_D52}

Nelsen, R. B. (1999). An introduction to Copulas, Lectures Notes in Statistics, Vol. 139. In: Springer Verlag, New York.

Nielsen, T. D., & Jensen, F. V. (2009). Bayesian networks and decision graphs: Springer Science & Business Media.

Nilsen, T., & Aven, T. (2003). Models and model uncertainty in the context of risk analysis. Reliability Engineering & System Safety, 79(3), 309-317.

Nivolianitou, Z., Konstandinidou, M., & Michalis, C. (2006). Statistical analysis of major accidents in petrochemical industry notified to the major accident reporting system (MARS). Journal of Hazardous Materials, 137(1), 1-7. doi:https://doi.org/10.1016/j.jhazmat.2004.12.042

Niwa, Y., & Hollnagel, E. (2002). Integrated computerisation of operating procedures. Nuclear Engineering and Design, 213(2-3), 289-301.

OECD. (2007). Safety Margin Action Plan (SMAP) - Task Group on Safety Margins Action Plan (SMAP) Safety Margins Action Plan - Final Report. NEA/CSNI/R(2007)9, OECD. {URL: https://www.oecd-nea.org/nsd/docs/2007/csni-r2007-9.pdf}

OECD. (2011). Safety Margin Assessment and Application – Final Report. NEA/CSNI/R(2011)3, OECD. {URL: https://www.oecd-nea.org/nsd/docs/2011/csni-r2011-3.pdf}

OECD. (2016). Implementation of Defence in Depth at Nuclear Power Plants – lessons learnt from the Fukushima Daiichi Accident. OECD NEA No. 7248, 2016. {URL: https://www.oecd-nea.org/nsd/pubs/2016/7248-did-npp.pdf}

O'Hagan, A., Buck, C. E., Daneshkhah, A., Eiser, J. R., Garthwaite, P. H., Jenkinson, D. J., . . . Rakow, T. (2006). Uncertain judgements: eliciting experts' probabilities: John Wiley & Sons.

O'Hara, J., Stubler, W., & Higgins, J. (1996). Hybrid human-system interfaces: Human factors considerations. Brookhaven National Laboratory.

Øien, K. (2001). A framework for the establishment of organizational risk indicators. Reliability Engineering & System Safety, 74(2), 147-167.

Ottino, J. M. (2003). Complex systems. AIChE Journal, 49(2), 292-299. doi:doi:10.1002/aic.690490202

PA Images (2018) *Piper Alpha 30th anniversary* Accessed July 2018 {URL: https://www.paimages.co.uk/image-details/2.37327168}

Paté-Cornell, E. (2012). On “Black Swans” and “Perfect Storms”: Risk Analysis and Management When Statistics Are Not Enough. Risk Analysis, 32(11), 1823-1833. doi:doi:10.1111/j.1539-6924.2011.01787.x

Paté-Cornell, M. E. (1986). Warning systems in risk management. Risk Analysis, 6(2), 223-234.

Pate-Cornell, M. E., & Murphy, D. M. (1996). Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications. Reliability Engineering & System Safety, 53(2), 115-126.

Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann Publishers Inc.

Pitblado, R., Williams, J., & Slater, D. (1990). Quantitative assessment of process safety programs. Plant/Operations Progress, 9(3), 169-175.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. Safety science, 27(2-3), 183-213.

Ren, J., Jenkinson, I., Wang, J., Xu, D., & Yang, J. (2008). A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors. Journal of Safety Research, 39(1), 87-100.

Renooij, S. (2001). Probability elicitation for belief networks: issues to consider. The Knowledge Engineering Review, 16(3), 255-269.

Robert, C. P., & Casella, G. (2010). Introducing Monte Carlo methods with R (Vol. 18): Springer.

Roelen, A.L.C, G.B.van Baren, J.W. Smeltink, P.H. Lin and O.Morales (2007). A Generic Flight Crew Performance Model for Application in a Causal Model of Air Transport, , NLR-CR-2007-562, National Aerospace Laboratory, 2007.

Roelen, A.L.C., G.B. van Baren, P.H. Lin, O. Morales, D. Kurowicka and R.M. Cooke (2007), A generic air traffic controller performance model for application in a causal model of air transport, NLR-CR-2007-593.

Roelen, A.L.C., G.B. van Baren, O. Morales, K. Krugla (2008). A Generic Maintenance Technician Performance Model for Application in a Causal Model of Air Transport, NLR-CR-2008-445.

Rogers, W. P., Armstrong, N. A., Acheson, D. C., Covert, E. E., Feynman, R. P., & Hotz, R. B. (1986). Report of the presidential commission on the space shuttle challenger accident. In: US Government Accounting Office, Washington, DC.

Rohmer, J., (2013). Uncertainty quantification: Report on uncertainty quantification and comparison for single-type risk analyses. Technical Report D2.2, MATRIX Project (New Methodologies for Multi-Hazard and Multi-Risk Assessment Methods for Europe), Grant No. 265138.

Rowe, W. D. (1975). An" Anatomy" of risk: Environmental Protection Agency.

SAE International, (1996). APR-4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: SAE International.

Saleh, J. H., Marais, K. B., Bakolas, E., & Cowlagi, R. V. (2010). Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges. Reliability Engineering & System Safety, 95(11), 1105-1116.

Sarter, N. B., Mumaw, R. J., & Wickens, C. D. (2007). Pilots' Monitoring Strategies and Performance on Automated Flight Decks: An Empirical Study Combining Behavioral and Eye-Tracking Data. Human Factors, 49(3), 347-357. doi:10.1518/001872007x196685

Sarter, N. B., Woods, D. D., & Billings, C. E. (1997). Automation surprises. Handbook of human factors and ergonomics, 2, 1926-1943.

Schmidt, J., Matcham, I., Reese, S., King, A., Bell, R., Henderson, R., Heron, D. (2011). Quantitative multi-risk analysis for natural hazards: a framework for multi-risk modelling. Natural Hazards, 58(3), 1169-1192. doi:10.1007/s11069-011-9721-z

Selva, J. (2013). Long-term multi-risk assessment: statistical treatment of interaction among risks. Natural Hazards, 67(2), 701-722. doi:10.1007/s11069-013-0599-9

Shafer, G. (1976). A mathematical theory of evidence (Vol. 42): Princeton university press.

Shenoy, P. P., & West, J. C. (2011). Inference in hybrid Bayesian networks using mixtures of polynomials. International Journal of Approximate Reasoning, 52(5), 641-657.

Shorrock, S. T., & Kirwan, B. (2002). Development and application of a human error identification tool for air traffic control. Applied ergonomics, 33(4), 319-336.

Simmons, R., & Tyler, B. (1984). Hazard assessment techniques used in the chemical industry and their possible uses elsewhere. Fire and materials, 8(4), 199-205.

Siu, N. O., & Kelly, D. L. (1998). Bayesian parameter estimation in probabilistic risk assessment1. Reliability Engineering & System Safety, 62(1-2), 89-116.

Sklet, S., Aven, T., Hauge, S., & Vinnem, J. (2005). Incorporating human and organizational factors in risk analysis for offshore installations. Paper presented at the Proceedings ESREL.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979). Rating the Risks. Environment: Science and Policy for Sustainable Development, 21(3), 14-39. doi:10.1080/00139157.1979.9933091

Stamatelatos, M., Dezfuli, H., Apostolakis, G., Everline, C., Guarro, S., Mathias, D., Mosleh, A., Paulos, T., Riha, D., Smith, C., and Vesley, W. (2011). Probabilistic risk assessment procedures guide for NASA managers and practitioners. NASA. {URL: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120001369.pdf}

Straub, D., & Der Kiureghian, A. (2008). An investigation into the combination of Bayesian network with structural reliability methods. Paper presented at the Proc. IFIP WG 7.5 Working Conference on Reliability and Optimization of Structures.

Straub, D., & Der Kiureghian, A. (2009). Bayesian networks as a framework for structural reliability in infrastructure systems. Proc. ICOSSAR'09.

Straub, D., & Der Kiureghian, A. (2010). Bayesian network enhanced with structural reliability methods: methodology. Journal of engineering mechanics, 136(10), 1248-1258.

Straub, D., & Schubert, M. (2008). Modeling and managing uncertainties in rock-fall hazards. Georisk, 2(1), 1-15.

Swain, A., & Guttman, H. (1983). NUREG. CR-1278, Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications.

Todorovic, P., & Zelenhasic, E. (1970). A Stochastic Model for Flood Analysis. Water Resources Research, 6(6), 1641-1648. doi:doi:10.1029/WR006i006p01641.

Torres-Toledano, J. G., & Sucar, L. E. (1998). Bayesian networks for reliability analysis of complex systems. Paper presented at the Ibero-American Conference on Artificial Intelligence.

Tsang, H., Daniell, J.E., Wenzel, F. (2018). Earthquake Safety Requirements Based on Invidividual and Societal Fatality Risk. 16th European Conference on Earthquake Engineering, Thessaloniki, June, 2018.

Turati, P., Pedroni, N., & Zio, E. (2017). An Adaptive Simulation Framework for the Exploration of Extreme and Unexpected Events in Dynamic Engineered Systems. Risk Analysis, 37(1), 147-159. doi:doi:10.1111/risa.12593

UNISDR (2009). 2009 UNISDR Terminology on Disaster Risk Reduction. United Nations International Strategy for Disaster Reduction, Geneva, Switzerland, May 2009. 30 pp.

US Military (1993). System safety program requirements. MIL-STD-882c, US Department of Defense, USA. {URL: https://www.system-safety.org/Documents/MIL-STD-882C.pdf}

US NRC. (1975). WASH-1400 - Reactor safety study: An assessment of accident risks in US commercial nuclear power plants (Vol. 2). US Nuclear Regulatory Commission. {URL: https://www.nrc.gov/reading-rm/doc-collections/nuregs/knowledge/km0010/}

US NRC (1981). NUREG-0492, Handbook, Fault Tree. US Nuclear Regulatory Commission. {URL: https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/}

US NRC (1982). NUREG/CR-2300, A guide to the performance of probabilistic risk assessments for nuclear power plants. NUREG/CR, 2300. US Nuclear Regulatory Commission. {URL: https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr2300/}

US NRC (1983). NUREG/CR-2728, Interim Reliability Evaluation Program Procedures Guide. US NRC. US Nuclear Regulatory Commission. {URL: https://tmi2kml.inl.gov/

Documents/3c-REG-NUREG/NUREGCR-2728,%20Interim%20Reliability%20Evaluation%20Program%20Procedures%20Guide%20(1983-01).pdf}

US NRC (1984). NUREG/CR-2815, Probabilistic safety analysis procedures guide. US NRC. {URL: https://www.nrc.gov/docs/ML0635/ML063550253.pdf}

US NRC (1989). NUREG/CR-1150, Severe accident risks: An assessment for five US nuclear power plants: Appendices A, B, and C. US NRC. {URL: https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1150/v1/}

US NRC (1989a). Policy Statement on the Conduct of Nuclear Power Plant Operations. Federal Register, 54FR 3424, January 24, 1989. {URL: https://www.nrc.gov/reading-rm/doc-collections/commission/policy/54fr3424.pdf}

US NRC (1993) Development of the NRC's Human Performance Investigation Process (HPIP), NUREG/CR-5455, US NRC, Washington.

US NRC (2002) Davis-Besse reactor vessel head degradation lessons-learned task force report. US NRC {URL: https://www.nrc.gov/reactors/operating/ops-experience/vessel-head-degradation/lessons-learned/lessons-learned-files/lltf-rpt-ml022760172.pdf }

US NRC. (2005). Good Practices for Implementing Human Reliability Analysis. NUREG-1792, Washington, DC. {URL: https://www.nrc.gov/docs/ML0511/ML051160213.pdf}

US NRC. (2007). SECY-07-0074 – Policy Information Use: Update on the Improvements To the Risk-Informed Regulation Implementation Plan. US NRC, April, 2007. {URL:https://www.nrc.gov/reading-rm/doc-collections/commission/secys/2007/secy2007-0074/2007-0074scy.pdf}

US NRC. (2011). RG. 1.174, 2002, An approach for Using Probabilistic Risk Assessment in Risk Informed Decisions on Plant-Specific Changes to the Licensing Basis, US NRC. {URL: https://www.nrc.gov/docs/ML1009/ML100910006.pdf}

US NRC. (2012). A Proposed Risk Management Regulatory Framework. A report to NRC Chairman Gregory B. Jaczko from the Risk Management Task Force, April, 2012. {URL: https://www.nrc.gov/docs/ML1210/ML12109A277.pdf}

US NRC (2014) Safety Culture Common Language (NUREG-2165), US NRC, {URL: https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr2165/}

Varde, P. V., & Pecht, M. G. (2018). Risk-Based Engineering: An Integrated Approach to Complex Systems—Special Reference to Nuclear Plants: Springer.

van Erp. N., Linger. R., Khakzad, N., van Gelder. P. H. A. J. M. (2017). Report on risk analysis framework for collateral impacts of cascading effects. . Technical Report D5.2, RAIN Project (Risk Analysis of Infrastructure Networks in Response to Extreme Weather). Grant No. 608166.

van Erp. N., van Gelder. P. H. A. J. M. (2015). Risk Analysis framework for single and multiple hazards. . Technical Report D5.1, RAIN Project (Risk Analysis of Infrastructure Networks in Response to Extreme Weather). Grant No. 608166.

Vangelsten. B.V. (2013). Uncertainties in Multi-risk Assessment: Sources, Types and Quantification. . Technical Report D5.5, MATRIX Project (New Methodologies for Multi-Hazard and Multi-Risk Assessment Methods for Europe), Grant No. 265138.

Volkanovski, A. (2010). The method for assessment of ageing based on the results of PSA. Paper presented at the Proc. of the International Conference Nuclear Energy for New Europe.

Volkanovski, A., & Prošek, A. (2013). Extension of station blackout coping capability and implications on nuclear safety. Nuclear Engineering and Design, 255, 16-27. doi:https://doi.org/10.1016/j.nucengdes.2012.09.031

Volkanovski, A. (2015). Impact of component unavailability uncertainty on safety systems unavailability. Nuclear Engineering and Design, 283, 193-201. doi:https://doi.org/10.1016/j.nucengdes.2014.05.012

Walker, W. E., Harremoës, P., Rotmans, J., van der Sluijs, J. P., van Asselt, M. B., Janssen, P., & Krayer von Krauss, M. P. (2003). Defining uncertainty: a conceptual basis for uncertainty management in model-based decision support. Integrated assessment, 4(1), 5-17.

Wang, W. (2006). Comment: Expert Elicitation for Reliable System Design. Statistical Science, 21(4), 456-459.

Wang, Y. F., Xie, M., Ng, K. M., & Habibullah, M. S. (2011). Probability analysis of offshore fire by incorporating human and organizational factor. Ocean Engineering, 38(17-18), 2042-2055.

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(4), 671-682.

Weber, P., & Simon, C. (2016). Benefits of Bayesian Network Models: John Wiley & Sons.

WENRA. (2006). Harmonization of Reactor Safety in WENRA Countries – Report by WENRA Reactor Harmonization Working Group, January, 2006. {URL:http://www.wenra.org/media/filer_public/2012/11/05/rhwg_harmonization_report_final.pdf}

WENRA. (2008). Reactor Safety Reference Levels. WENRA Reactor Harmonization Working Group, January, 2008. {URL:http://www.wenra.org/media/filer_public/2012/11/05/list_of_reference_levels_january_2008.pdf}

WENRA. (2013). Report – Safety of new NPP designs - Study by Reactor Harmonization Working Group RHWG. March, 2013. {URL:http://www.wenra.org/media/filer_public/2013/08/23/rhwg_safety_of_new_npp_designs.pdf}

Wikipedia (2018a) *File:Challenger Launch.jpg* Accessed July 2018 {URL: http://en.wikipedia.org/wiki/Image:Challenger_Launch.jpg}

Wikipedia (2018b) *File: Trosky_Columbie.jpg* Accessed May 2018 {URL: http://en.wikipedia.org/wiki/Image:Trosky_Columbie.jpg}

Wikipedia (2018c) *File:Cathodic Protection diagram.svg* Accessed July 2018 {URL: https://commons.wikimedia.org/wiki/File:Cathodic_Protection_diagram.svg}

Williams, J. (1986). A proposed method for assessing and reducing human error. Paper presented at the Proc. 9th Advances in Reliability Technology Symp.

Wu, X., Liu, H., Zhang, L., Skibniewski, M. J., Deng, Q., & Teng, J. (2015). A dynamic Bayesian network based approach to safety decision support in tunnel construction. Reliability Engineering & System Safety, 134, 157-168.

Zadeh, L. A. (1965). Information and control. Fuzzy Sets, 8(3), 338-353.

Zhang, H., & Marsh, D. (2016). Bayesian network models for making maintenance decisions from data and expert judgment.

Zhang, L., Nadim, F., & Lacasse, S. (2013). Multi-risk assessment for landslide hazards. Paper presented at the Proceeding of Pacific Rim Workshop on Innovations in Civil Infrastructure Engineering.

Zhang, N. L. & Poole, D. (1994). A simple approach to Bayesian network computations. Proc. of the Tenth Canadian Conference on Artificial Intelligence, 1994.

Zhang, S. (2014). Assessment of human risks posed by cascading landslides in the Wenchuan earthquake area: Hong Kong University of Science and Technology (Hong Kong).

Zio, E., & Sansavini, G. (2011). Modeling cascading failures in" systems of systems" with uncertain behavior. Paper presented at the ICASP11.