UNIVERSITY OF STRATHCLYDE

DEPARTMENT OF MANAGEMENT SCIENCE

EXPLORING A BAYESIAN APPROACH FOR STRUCTURAL MODELLING OF COMMON CAUSE FAILURES

by

ATHENA ZITROU

A thesis presented in fulfilment of the requirements for the degree of Doctor of Philosophy

2006

To my parents

Acknowledgments

I would like to express my gratitude to all those who have helped me in the study for and preparation of this thesis. First and foremost, I would like to express my sincere gratitude to my first supervisor, Professor Tim Bedford. Without his knowledge, experience, guidance, support, and certainly patience, I would have never been able to produce this work. Working with Professor Bedford has been a source of inspiration and a great pleasure. I would also like to thank my second supervisor, Professor Lesley Walls, for her invaluable support, input and feedback.

The research has been financially supported by the Health and Safety Executive. I would like to thank Dr. Phil Brighton and Ms Ana Gomez, for their valuable feedback, comments and cooperation. A special thanks goes to Mr Dave Hamblen. Without his participation, experience and cooperation, this thesis would never have come to fruition. I would also like to thank Ian Muir, Dave Fiddler, Bret Commandeur, Ian Morris and Tony Hindle for their very useful input. Finally, I would like to express my gratitude to Rijkswaterstaat, Holland, for their financial assistance.

Above all, I am immensely grateful to my family. My parents Dimitrios and Archontou and my brother Vasilis deserve my highest respect and deepest gratitude for their constant encouragement and support through the years. My special appreciation goes to my grandmother, Garyfalia, for her endless love and care. Although she is no longer with us, she will be always remembered.

Finally, I would like to thank my friends, both in Greece and in Scotland, for their support, love and never-ending patience.

Abstract

Common Cause Failures (CCFs) are a class of dependent failures that occur to complex technological systems, such as nuclear power plants, where redundant components serve as multiple layers of defence. For the purposes of quantitative assessment of CCFs, parametric models are used. A common feature of all parametric models is the difficulty in parameter estimation due to limited available observational data.

The Unified Partial Method (UPM) for CCF modelling is a systematic methodology that takes into consideration physical and operational system defences. This research explores the application of the Influence Diagram (ID) formalism in order to extend UPM, through an example of Emergency Diesel Generators from nuclear power plants.

The proposed model incorporates intermediate stages in the modelling process, namely root causes and coupling factors, to allow for a representation of the CCF mechanisms. Moreover, it captures interactions existing amongst the system's defences, in their contribution to risk. With an underlying Bayesian approach to risk, the model quantifies operational experience, accounts for the epistemic uncertainty, and allows for a coherent combination of expert opinion with observations. This thesis proposes a model structure, which integrates with the ICDE generic database for CCFs. Finally, the ID formalism allows for the propagation of uncertainty within the model structure, and provides a tool for decision-making.

The construction of the ID model has been entirely based on expert judgment: the model network has been constructed with the help of experts, whilst a suggested model quantification methodology has been explored. This thesis documents the building process, and explores the behaviour of the resulting model. Findings within this research suggest the feasibility of the proposed methodology for development of a CCF model with a structural and exploratory character.

Contents

List of Figures

List of Tables

Abbreviations

AF	Alpha Factor
ALT	Accelerated Life Testing
BBN	Bayesian Belief Network
BF	Beta Factor
BFR	Binomial Failure Rate
BP	Basic Parameter
CCCG	Common Cause Component Group
CCF	Common Cause Failure
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
GS	Geometric Scaling
HSE	Health and Safety Executive
ICDE	International Common Cause Data Exchange Project
ID	Influence Diagram
LOCA	Loss of Coolant Accident
MAVT	Multiattribute Value Theory
MBF	Multiple Beta Factor
MCBFR	Multi-class Binomial Failure Rate
MCC	Motor Control Centre
MGL	Multiple Greek Letter

PBF	Partial Beta Factor
POS	Process-Oriented Simulation
PRA	Probabilistic Risk Assessment
UPM	Unified Partial Method

Notation

rc root cause

cf coupling factor

λ_{CCF} rate of system CCF events

p_{ij} probability of a CCF event via coupling factor j, given a failure due to root cause i, $i = 1, ..., \rho$, $j = 1, .., \kappa$

r_i rate of system failures due to root cause i, $i = 1, ..., \rho$

λ_i rate of CCF system failures due to root cause i, $i = 1, ..., \rho$

D_k system defence k, $k = 1, ..., m$

x_k level of defence D_k, $x_k \in \{1, ..., m_k\}$

$\underline{x}$ configuration vector of n defences, $\underline{x} = (x_1, ..., x_n)$

Ω_k state space of level x_k, $\Omega = \{1, ..., m_k\}$

$X_{k,\theta}$ partition of Ω_k, $\theta = 1, ..., s_k$

$I_i(x_1, ..., x_n)$ proportion by which V decreases, when the level of D_i changes from x_i to $x_i + 1$, while the levels of the other defences x_j, $j \neq i$ are kept fixed

$V_{\underline{x}}$ r.v. V at configuration vector $\underline{x}$

$r_{i,\underline{x}}$ rate r_i of failures due to root cause i occurring to a system with configuration vector $\underline{x}$

$p_{ij,\underline{x}}$ coupling factor intensity p_{ij} characterising a system with configuration vector $\underline{x}$

a_i, b_i	gamma parameters of the distribution of the base-level variable $r_{i,\underline{\mu}}$
$a_{i,\underline{x}}, b_{i,\underline{x}}$	gamma parameters of the distribution of variable $r_{i,\underline{x}}$ at configuration vector $\underline{x}$
γ_{ij}, δ_{ij}	beta parameters of the distribution of the base-level variable $p_{ij,\underline{\mu}}$
$\gamma_{ij,\underline{x}}, \delta_{ij,\underline{x}}$	beta parameters of the distribution of the base-level variable $p_{ij,\underline{x}}$ at configuration vector $\underline{x}$
K	set of indices of defences $D_1, ..., D_n$
H_π	set of all pairs of indices of functionally independent defences
H	set of indices of all defences that exhibit functional independence with some defence
M_π	set of all pairs of indices of functionally dependent defences
M	set of indices of all defences that exhibit functional dependence with some defence
Q	set of indices of threshold functionally dependent defences
L_k	set of indices of counterpart defences of threshold dependence of defence D_k, $k \in Q$
L	set of indices of all defences that are a counterpart of threshold functional dependence
ϕ_{ij}	cross-term corresponding to functionally dependent pair $\{i, j\} \in M_\pi$
$\underline{\phi_i}$	vector of proportion variables related to r_i
$\underline{\varphi_{ij}}$	vector of proportion variables related to p_{ij}
$d_{\underline{x}}$	data relevant to variable $V_{\underline{x}}$
$h(\underline{x})$	log-linear function of configuration vector $\underline{x}$

Chapter 1

Introduction

1.1 Introduction

A significant proportion of current electricity production is generated in commercial nuclear power stations. Nuclear fission is a powerful process used in the production of energy. However, it involves a number of potential risks. For instance, the accidental release of radioactive material would have considerable health and environmental effects. Within this context, assessing and controlling the risk related to the operation of nuclear power stations constitutes a central concern in the nuclear power sector. The same way as in any hazardous industrial operation, in this case it is also crucial to ensure that the risks involved do not outweigh the benefits, and high reliability along with cost effectiveness are achieved in practice. The technical area concerned with the analytical techniques and methods developed for the assessment of risk is Probabilistic Risk Analysis (PRA). In principle, results of PRA studies are used in order to support meaningful decisions regarding the design and operation of systems, both from an operator and a regulator perspective.

To this end, safe design is crucial in such complex, technological systems. In order to attain acceptable safety levels, these systems can be designed in accordance with the 'Defence-In-Depth' philosophy [Fleming et al., 1983], where redundant and diverse components are employed to serve as multiple layers of defence: in the event of a component failure, other components are in place to compensate the intended function of the failed component. Assuming that components fail independently, the 'Defence-In-Depth' philosophy would offer a high level of protection, as loss of system function could only result from coincidental independent component failures. However, components may also fail dependently, defeating the redundancy or diversity that is employed by the system design [Mosleh et al., 1987]; therefore, performing a risk analysis under the independence assumption would result in a considerable underestimation of the risk posed to the system. Indeed, operating experience and PRA results have shown that dependent component failures are a significant contributor to system unavailability [Fleming et al., 1983; Parry, 1991].

Mathematically, a dependent failure occurs to a system of n components when the failure of two or more components is not probabilistically independent. Let A_i be the event of component i failing, for $i = 1, ..., n$. The components fail dependently when

$$P(A_1, A_2, \ldots, A_n) \neq P(A_1)P(A_2)\ldots P(A_n)$$

Recognition of the contribution of dependent failures to the overall reliability of a system led to the development of dependent failure analysis as part of an overall PRA. For incorporation into the analysis, dependent failures are classified into categories. Procedural guides [Johanson et al., 2003; Mosleh et al., 1987, 1998c] suggest taxonomies for dependent failures that classify them in terms of the nature of the dependency existing amongst the components. In particular, the scheme distinguishes between

1. Intrinsic (or intersystem) dependencies that stem from design system characteristics; these describe situations where the status of one component influences the status of another component in the system. A subcategory of intrinsic failures is cascading failures, where the failure of one component increases the failure tendency of another component belonging to the same system [Høland and Rausand, 1994].

2. Extrinsic (or intrasystem) dependencies that stem from factors physically external to the system. Such factors are environmental or human.

In quantitative analysis, particular classes of dependent failures are addressed explicitly. Such failures include known intrinsic failures, and a large class of extrinsic failures, like certain operator errors and external events [Paula, 1995]. Explicit treatment of dependent failures involves the identification and direct incorporation of the initiating event into event tree and fault tree logic models [Fleming et al., 1983]. Therefore, explicit models are only appropriate for specific failure classes.

1.2 Common Cause Failures

Nevertheless, the sources of dependencies are numerous, and often cannot be addressed explicitly in a practical manner. Common Cause Failures (CCFs) are a subset of the more general category of dependent failures. The main distinction between CCFs and other dependent failures is the fact that the former are not explicitly modelled; they constitute the residual part of the wider class of dependent failures. The impact of CCF events to the system is implicitly quantified through parameters, without distinguishing between particular causes or dependencies. Particularly in the nuclear area, it has been shown that CCF events may contribute between 20% and 80% to the unavailability of safety systems of nuclear power reactors [Hauptmanns, 1996]. Subsequently, the issue of modelling CCFs in particular has received much attention in the field of system safety.

Given the different types of dependencies related to CCF events, and the different methodologies and techniques developed in order to address them, a clear definition of CCFs is of key importance. In the literature, a broad spectrum of CCF definitions can be found [Paula, 1995]. For the purpose of PRA applications *sensu lato*, "CCF events are dependent failures resulting from causes that are not explicitly modelled" [Paula, 1995]. Moreover, CCF events describe multiple component failures that are the result of a shared cause [Mosleh et al., 1987]. Examples of CCFs include miscalibration of sensors, incorrect maintenance, environmental impact on the system [Berg et al., 2006].

It is worth noting that in the literature the term Common Mode Failures (CMF) is commonly used. In [Edwards and Watson, 1979], a CMF is defined as an event which causes, due to existing dependencies, a coincidence of failure states of redundant components. In the earlier literature these two terms have been used interchangeably [Fleming et al., 1983], despite the fact that it is possible for a CCF not to fail components in the same mode, or for a CMF not to be the result of a shared cause. In practical applications, the difference between CCFs and CMFs is considered insignificant, and the two sets of failures are not separated in the modelling [Smith, 2000].

Within the scope of this thesis, CCF events are defined as within the International Common Cause Failure Data Exchange (ICDE) coding guidelines [Werner et al., 2004]. According to the guidelines,

> A CCF event is an impairment of two or more components of a redundant system over a relevant time interval, as the direct result of a shared cause.

The impairment of components is defined with respect to their performing action. The timing of component failures constitutes an important characteristic of CCF events. For systems operating on demand, an impairment of components due to a CCF event may be not simultaneous, but if it occurs during the period the system is idle, it may result to a system failure. On this basis, the relevant time interval may be two pertinent inspection periods. For systems that are operating on demand, the detection strategy influences the contribution of CCF events to the overall unavailability of the system, as it determines the time that the failures remain undetected.

1.3 Treatment of Common Cause Failures

Procedural guides for CCF treatment [Mosleh et al., 1987; Fleming et al., 1988; Mosleh et al., 1998c] have been developed in an effort to provide a structured framework for the understanding and assessment of the impact of CCF events on the functioning of systems. The CCF modelling stages that comprise the framework are summarised in Figure 1.1. A comprehensive CCF treatment requires the stages to be completed sequentially, as the results obtained from one stage are used in the next one. Next, a brief overview of the main stages is given.

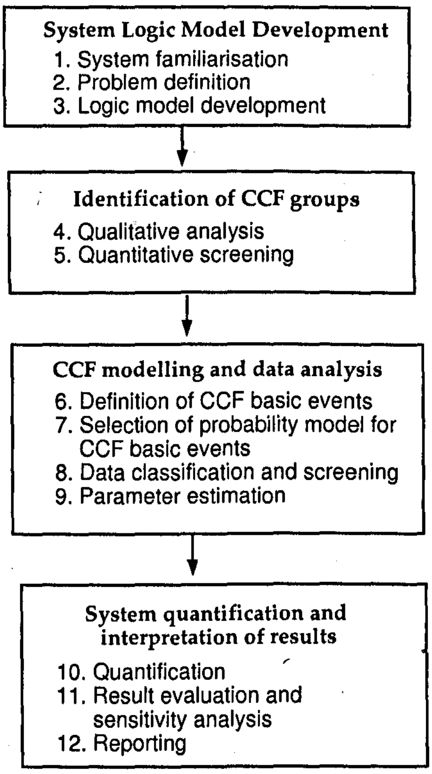

System Logic Model Development
1. System familiarisation
2. Problem definition
3. Logic model development
Identification of CCF groups
4. Qualitative analysis
5. Quantitative screening
CCF modelling and data analysis
6. Definition of CCF basic events
7. Selection of probability model for CCF basic events
8. Data classification and screening
9. Parameter estimation
System quantification and interpretation of results
10. Quantification
11. Result evaluation and sensitivity analysis
12. Reporting

Figure 1.1: CCF modelling procedural framework taken from [Mosleh et al., 1987]

1. *System Logic Model Development.* This stage includes the process of familiarisation with the system of interest, its design and intended function. The design characteristics of the system are studied, along with its physical and operational environment. Next, the problem is defined: the physical and functional boundaries of the system and components are agreed, and the types of dependent failures to be explicitly modelled are decided. The focus of the next stage of the analysis is the residual part of dependent failures (CCFs), which is modelled parametrically. From a CCF perspective, it is important to qualitatively analyse the potential vulnerabilities of the system of interest (target system) towards CCF

events. Understanding the failure mechanisms is imperative, not only because a thorough insight in the system is gained, but also because, during the later stage of data analysis, it will allow to appropriately identify the generic data to be used for the specific system [Mosleh et al., 1994].

Finally, the logic model of the system is developed. Techniques for logic model development include event and fault trees, reliability block diagrams, Go diagrams. The most widely used type of analysis is fault trees [Roberts et al., 1981]. The output of the analysis is a Boolean representation that relates a top event, e.g. system unavailability, to a combination of basic events (component states), which lead to the top event. During the logic model development, the combination of component states that lead to system unavailability are identified.

2. *Identification of Common Cause Component Groups.*

   The objective of this step is to identify the groups of components that will be eventually included in the analysis, by using qualitative and quantitative screening.

   Initially, understanding is developed regarding the particular vulnerabilities of the system towards CCFs. Based on engineering and operating experience particular common attributes amongst components and coupling mechanisms that may be in place are identified and their effectiveness is evaluated. The resulting groups of components are further studied in terms of the root causes that are susceptible to, and the related system defences that are in place. The outcome of qualitative screening is a candidate list comprising of Common Cause Component Groups (CCCGs) that have been recognised as susceptible to CCFs.

   For large systems, it is important to restrict the size of the problem to a manageable size. Therefore, the candidate list is further reduced by quantitative screening. At this stage, the logic model developed previously is modified to include a single common cause failure event for each component in a CCCG, that fails all members of the group. By using a simple global parametric model, numerical values for the CCF basic events are approximately estimated. Based on this conservative assessment, the CCCGs that have an insignificant contribution to the top event are identified and omitted from the analysis.

3. *Common Cause Modelling and Data Analysis.* Next a detailed quantitative analysis for the CCCGs that survived the screening process takes place. At this stage, the system logic model is expanded in more detail, to include CCF basic events of specific sets of components. The difference between this and the previous step is that now, basic events are included that describe CCFs of different multiplicities. The Boolean representation of the top event is transformed to a parametric representation, and an appropriate probabilistic model is selected. Available data is analysed, in order to produce numerical values for the parameters involved.

4. *System quantification and interpretation of the results.* The estimators of the parameters are entered in the probability model in order to quantify the overall system unavailability. Uncertainty and 'what-if' analyses are also an important part of this stage. The final step of the framework is the reporting and documentation of the analysis.

1.4 Objectives of the research

In the nuclear industry worldwide, the models used for the quantitative modelling of CCFs are typically parametric. Main CCF parametric models include the Multiple Greek Letter model [Apostolakis and Moieni, 1987], the Alpha Factor model [Siu and Mosleh, 1989], and the Beta Factor model [Fleming, 1975]. The UK nuclear industry, instead, has adopted its own approach, the Unified Partial Method (UPM)[Brand and Gabbot, 1993].

In parametric models, the impact of CCFs on the system under assessment is being expressed by parameters, which need to be quantified through statistical analysis. However, the statistical analysis of CCF data is a process that bears a number of particularities. Firstly, CCF events are relatively complex events. As a result, event reports often contain vague descriptions, requiring a number of assumptions from the behalf of the analyst concerning the component statuses or other physical and operational characteristics of the system. This fact leads to the incorporation of considerable uncertainty in the analysis [Siu and Mosleh, 1989]. Secondly, CCF events are rare events, resulting in a limited amount of system-specific data that is frequently insufficient for robust statistical analysis [Vaurio, 1994b; Parry, 1996; Siu and Kelly, 1998; Spitzer, 2006]. To this end, the quantification of the parameters of the parametric models reveal certain problematic points.

In this view, UPM has a practical advantage over other CCF models. Having been initially quantified by experts, it can be applied by less knowledgeable analysts for the purposes of standard PRAs, by simply scoring the system across a set of factors. Moreover, in contrast to other parametric models, UPM incorporates 'softer' aspects of the system when assessing its defence level, such as information concerning operator interaction and other system-specific characteristics. Overall, UPM constitutes a systematic procedural framework for CCF modelling of standard systems. This results in a modelling process that is reproducible and auditable.

Despite the attractive particular features of UPM, certain deficiencies in its behaviour have been identified. UPM has been characterised as simplistic and, to some extent, crude [Zitrou, 2002]. Thereby, a need for further development has been created. This thesis aims to contribute towards this direction. To be more precise, it aims to *explore the application of advanced mathematical techniques in order to further extend the Unified Partial Method (UPM) for CCF modelling*. The mathematical technique used in order to attain the objectives of this thesis is the Influence Diagram formalism.

The objectives of the research may be described across two facets. On the one hand, the proposed model intends to use certain strong features of the UPM framework. These are the incorporation of design, operational and environmental aspects in assessing the risk contribution to the system, and, the use of expert judgment in a quantitative way. On the other hand, the new model intends to extend certain features of the UPM methodology. These are discussed within the following sections.

1.4.1 A structural approach

In principle, parametric models address CCFs in an implicit manner. Underlying assumptions mainly concern the CCF manifestation on the system, and causal mechanisms are not taken into account explicitly. To this end, parametric models are mostly characterised by their input, output, and model properties (Figure 1.2). The model input relates to the statistical information required for the estimation of the model's parameters. The model output relates to the different kinds (multiplicity) of CCF events whose impact on the system is quantified. Finally, the model properties relate to features such as subgroup invariance[1], or whether the model, once quantified, can be used to make predictions regarding non-observed events.

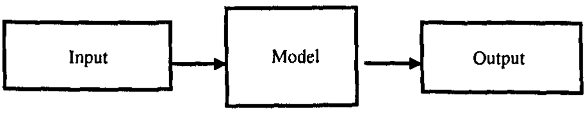


Figure 1.2: Parametric Models

In order to model CCF events in a meaningful and comprehensive manner, it is important to understand the mechanisms behind the occurrence of CCF events (qualitative analysis). Within the literature, three concepts are identified as the key issues to be discussed when addressing CCFs, namely root causes, coupling factors and system defences [Fleming et al., 1988; Mosleh et al., 1998c; Parry, 1991; Edwards and Watson, 1979; Mosleh et al., 1987]. Root causes are defined as the most readily identifiable direct cause of the CCF event. A particular cause of failure results in a dependent failure through the existence of coupling mechanisms, that create dependency conditions and propagate the failure to multiple components. Finally, the defences describe the existence or lack of design, operational or managerial characteristics of the system that are acknowledged as offering levels of protection against CCF events.

In principle, the consideration of system defences, root causes and coupling factors and the use of parametric models consist independent parts of the overall CCF

[1] When a model is "subgroup invariant", it may be applied to subgroups within the system under investigation without requiring re-estimation of the model parameters.

assessment process (See Figure 1.1). In particular, parametric models are used after the qualitative stage of the analysis, for quantitatively assessing the impact of CCF events on the system of interest. UPM constitutes an attempt to merge those two stages by incorporating defence aspects of the system in the actual quantitative assessment. These defence aspects are described by eight subfactors (Figure 1.3).

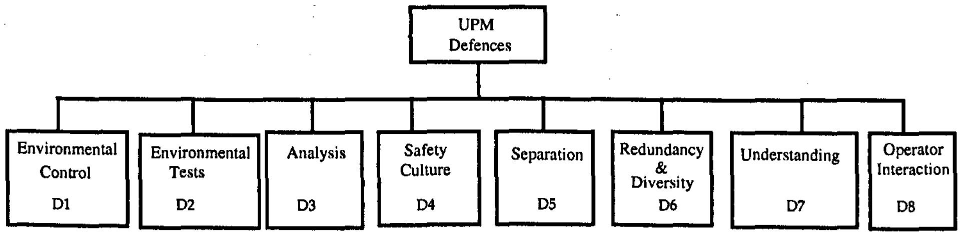


Figure 1.3: UPM subfactors

The modelling approach proposed within this thesis attempts to further extend this feature of UPM, by incorporating root cause and coupling factor issues, along with the system defences in the actual theoretical structure of the model. The proposed model builds in its theoretical framework a cause - effect - prevention structure: a CCF event is described in terms of a trigger mechanism (root cause event) and a filter (coupling factors), both affected by the defence characteristics of the system (Figure 1.4). In essence, this thesis seeks to move from a black-box, to a more structural approach [Mitchell, 1993] to CCF modelling through explicitly taking into account cause and effect.

The proposed model attempts to describe the actual causal mechanisms of CCF events, and, the way these can be modified by changing the system's defence aspects. Speculative interventions may be performed in the model, allowing to explore the effect of different realities, and support meaningful decisions in terms of the defence characteristics of the system. On this basis, the proposed model has a strong exploratory character. Compared to UPM, the distinctive feature of the new model is that *it allows* *for a more detailed modelling of the CCF events, as it incorporates intermediate stages in the modelling process, namely root causes and coupling factors, and it captures the types of CCFs that each defence is able to modulate.* These aspects provide a more detailed understanding of the CCF mechanisms.

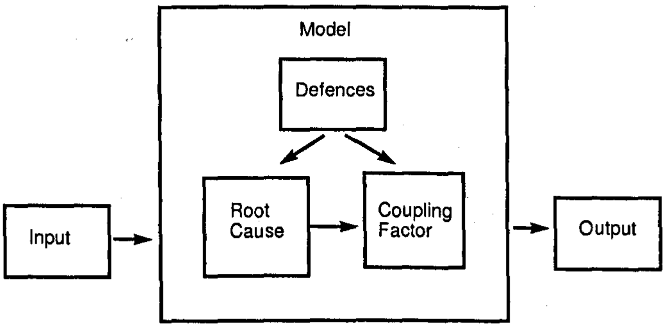


Figure 1.4: Proposed modelling approach

1.4.2 A further generalisation

One of the most basic parametric models is the Beta Factor model. The Beta Factor model is the simplest and most popular approach to CCF modelling [Hirschberg and Pulkkinen, 1985; Hanks, 1998; Hokstad and Corneliussen, 2004]. Its simplicity stems from a fundamental assumption, according to which a given component in a system may fail either independently, or due to a CCF event that leads to the failure of all components in the system. As a result, CCF events of different multiplicities are not allowed, and the model fails to distinguish between different system success logics.

Due to its simplicity, the Beta Factor model provides the basis for more sophisticated model structures. One the one hand, models like the Multiple Greek Letter (MGL) model [Apostolakis and Moieni, 1987] and the Multiple Beta Factor (MBF) model [Hokstad and Corneliussen, 2004] generalise the Beta Factor model in order to allow for different failure multiplicities, and discern the performance of different system architectures. One the other hand, models like the Partial Beta Factor model and UPM generalise it towards a different direction: they attempt to model the impact of

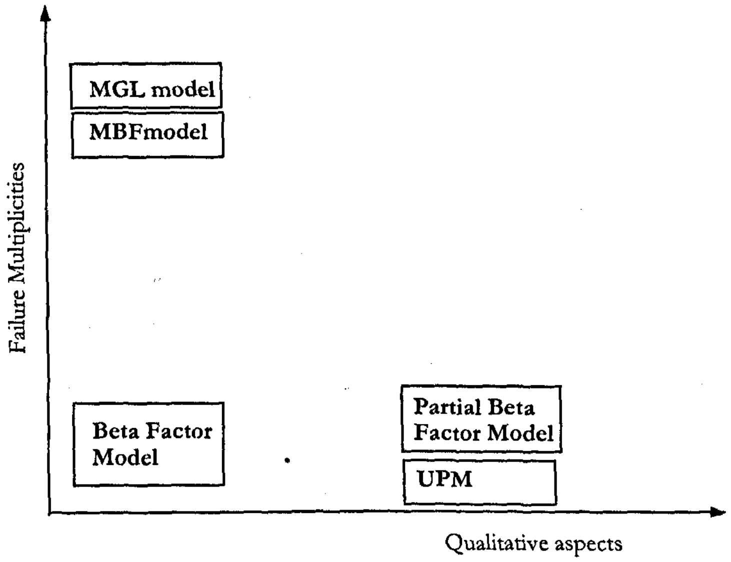


Figure 1.5: Model-development dimensions

managerial, design and environmental aspects of the system on the system vulnerability towards CCF events. Figure 1.5 illustrates the directions towards which different models generalise the Beta Factor model. Figure 1.6 illustrates the position of the model proposed in this thesis within this context. To be more precise, *the proposed model provides a generalisation of UPM (and, thus, the Beta Factor model) through addressing issues that UPM fails to do, such as the interactions existing amongst the system defences*. However, it does not address the issue of different failure multiplicities of CCF events, which is why it is positioned at the same height as UPM and the Beta Factor model. By contrast, models like the MBF model can be in principle generalised by using a similar methodological approach, in order to result in models that achieve both (Figure 1.7). Effectively, this research may provide a protocol for such a development.

1.4.3 A model for uncertainty

In essence, the main objective of PRAs is to quantify the risk posed on systems. Risk is integrally related to uncertainty, and quantification of risk requires measuring uncertainty on particular events. Even though probability is unequivocally the numerical

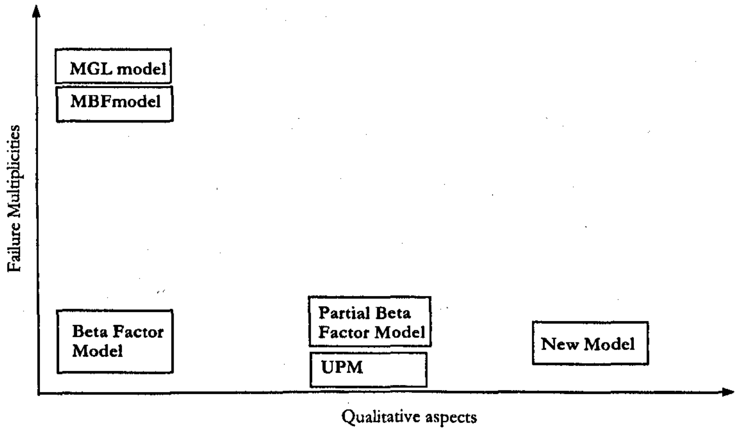


Figure 1.6: Position of particular research in model-development dimensions

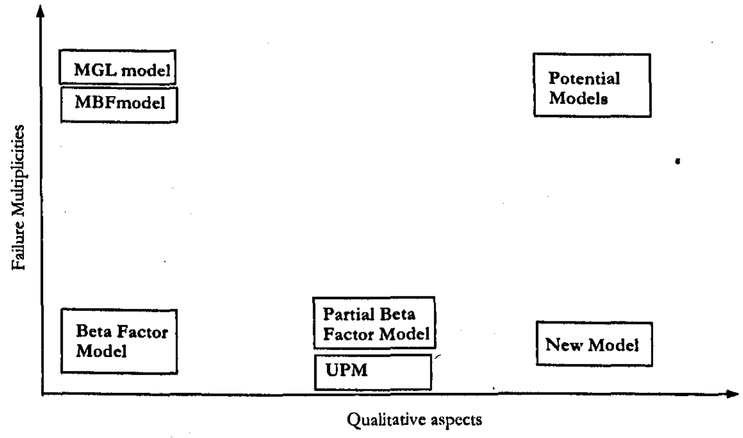


Figure 1.7: Position of potential research in model-development dimensions

measure of uncertainty, the interpretation of probability within the context of risk results in different methodological approaches. The frequentist approach constitutes the traditional choice within reliability analyses; however, over the last thirty years, the subjectivist approach has emerged [Apostolakis, 1988]. Within the subjectivist approach, the Bayesian methodology has gained popularity within the context of PRAs [Parry, 1996; Siu and Kelly, 1998; Aven and Kvaløy, 2002].

From a CCF viewpoint in particular, Bayesian techniques are often considered particularly suitable. Due to the rare and complex nature of CCF events, a significant amount of uncertainty is entered into the analysis. The Bayesian canon constitutes a consistent framework for representing inherent uncertainty on model parameters.

Moreover, it is a methodology that allows for the coherent combination of statistical data with expert judgment.

Even though UPM is a methodology that extensively uses expert judgment in a quantitative manner, it yields a point value for the model output, without accounting for any uncertainty in its determination. By adopting a Bayesian view to risk, the model proposed within this thesis attempts to *represent uncertainty in both the model inputs and output, and allow for the coherent propagation of this uncertainty within the model structure.*

The type of uncertainty captured by a Bayesian methodology arises from lack of knowledge of the system, and is referred to as epistemic uncertainty. Epistemic uncertainty is integrally related to observations, as the level of knowledge alters when additional information is obtained. Bayesian methodology, and as an extension the proposed model, offers a consistent mechanism for updating epistemic uncertainty in the light of statistical data. The International Common Cause Failure Data Exchange (ICDE) database constitutes an important development in the availability of CCF data. It is an extensive database that accumulates CCF events from different systems internationally, and represents many operating years.. On this basis, it is of interest to *create a bridge between the proposed model and ICDE, by merging the structure of the database with the model structure.*

1.4.4 A specific setting

The research goal and objectives of the research presented in this thesis are summarised in Table 1.1. This research has been funded by the Health and Safety Executive (HSE). HSE is the regulating body responsible for health and safety issues at nuclear sites. As a regulatory body, the mission of HSE is to ensure that risk is properly controlled and that the operation of nuclear power stations is performed under a satisfactory level of safety. It is the body that sets the safety standards, and ensures that these are met by nuclear operators within the UK. Within this context, PRA has a key role, and the conduct of related research constitutes a primary objective of HSE.

The aim of this thesis is to explore the feasibility of the proposed modelling approach within the particular context. Providing a definitive tool to be used in standard PRAs in industry has not been an objective. Thereby, a particular example has been chosen to attain the purposes of this research.

The example

The application example of the particular research lies in the nuclear field. More precisely, the research focuses on the CCF modelling of Emergency Diesel Generators (EDGs) in commercial nuclear power plants. The EDG system constitutes a particularly suitable subject for CCF modelling. Firstly, the EDG system plays a critical role to the safety of a nuclear power plant. Secondly, nuclear power plants usually employ at least two EDGs [Martz et al., 1996]. Finally, EDGs are frequently tested, and the availability of relevant data is comparatively increased [Hirschberg and Pulkkinen, 1985].

EDGs are systems that operate on demand; this type of systems are idle for a period of time and are only put into operation periodically. To this end, the failure of the system to operate on demand is classified into two categories: failure revealed by the demand and failure caused by the demand. This research focuses on the modelling of CCF events of the first category, that is of CCFs that occurred during the period the system was idle and only detected when the system was challenged into operation.

The modelling of this type of failure is based on the assumption that CCF events occur at random times during the idle period of the system, and at constant rates [Vaurio, 1994b]. The constant failure rate assumption is considered appropriate because CCF events are rare events, and the CCF rate is not driven by factors such as the aging of the component. To this end, the parameter of interest is the rate of CCF events occurring to the system, denoted by λ_{CCF}. This thesis presents an ID model that represents uncertainty on the model output λ_{CCF}.

Table 1.1: Research Goal and Objectives

OVERALL GOAL

Explore the feasability of the application of advanced modelling techniques within the Unified Partial Method (UPM) for CCF modelling framework, so as to result in a model with a structural and exploratory character, that allows the representation of epistemic uncertainty, and supports the decision - making process.

OBJECTIVES

1. Develop a model that takes into account physical, operational and managerial aspects in order to assess the risk contribution to the system, and supports the decision-making process.

2. Develop a model that uses expert judgment in a quantitative manner, and results in a tool that is approachable by analysts without the same level of insight in CCF mechanisms.

3. Develop a model that extends UPM by capturing the types of CCFs that each defence of the system is able to modulate, through incorporating root causes and coupling factors in the modelling process.

4. Develop a model that extends UPM by representing functional interactions amongst system defences, in the way that they impact on the overall vulnerability of the system to CCF events.

5. Develop a model that represents uncertainty on both the model inputs and outputs, and allows for coherent propagation of uncertainty within the model structure.

6. Develop a model that merges the structure of the ICDE database within the model structure.

The ID model

In an attempt to address the goals and objectives of this research, the use of the Influence Diagram formalism is proposed; Influence Diagrams (IDs) [Howard, 1990; Matheson, 1990; Lauritzen, 1996; Jensen, 1999] are extensions of Bayesian Belief Networks (BBNs) [Pearl, 1988]. A BBN is a network of nodes; the nodes represent the features of the problem, and the network portrays the logical relationships between these features. Associated with each node is a set of probabilistic expressions describing the impact of the influencing nodes to the values of this node [van der Gaag, 1996]. An ID extends this approach by incorporating features of the problem that represent decisions, uncertain quantities and goals/objectives of the decision maker.

As described in Section 1.4.1, the ID model builds a cause-effect-prevention structure: a CCF event is the result of a root cause failure, which is propagated amongst components via existing coupling mechanisms. The frequency of root cause failures and the intensity of the coupling mechanisms both depend on the defence characteristics that are employed by the system.

Assume that a categorisation of ρ root causes and κ coupling factors is used. Like the main parametric models, within the ID framework it is assumed that failures occur independently and at constant rates. Specifically, it is assumed that failures attributed to a particular root cause occur according to a Poisson process with constant rate r_i, $i = 1, ..., \rho$. At the occurrence of a root cause event, the failure is propagated amongst components via coupling mechanism j, $j = 1, ..., \kappa$, resulting into a CCF event, with probability

$$p_{ij} = P\{\text{CCF through coupling factor } j \mid \text{failure due to root cause } i\}$$

Therefore, CCF events due to root cause i occur according to an independent Poisson process with rate λ_i, where

$$\lambda_i = \sum_{j=1}^{\kappa} p_{ij} r_i$$

Under the assumption that a CCF event may occur as the propagation of only one root cause event, through only one coupling mechanism, the overall process of CCF events is a superposition of the independent Poisson processes. The rate of the superimposed process is λ_{CCF}, where

$$\lambda_{CCF} = \sum_{i=1}^{\rho} \lambda_i$$

Within this set-up, the rate of CCF events is expressed in terms of rates of root cause events, filtered through the intensity of coupling mechanisms. *The intention is to use an ID to represent the influences of the system defences, represented by the eight UPM subfactors, on the uncertainty on the root causes r_i and coupling factors p_{ij}, and hence to obtain an uncertainty distribution on the overall CCF rate λ_{CCF}.*

The features of the problem are represented in the ID model by nodes. The system defences, being in the complete control of the assessor, are deterministic variables and are represented by decision variables D_k $(k = 1, ..., n)$ (squares). Following a Bayesian approach, the interest lies in expressing uncertainty in both the model inputs and output; hence, parameters r_i and p_{ij} $(i = 1, ..., \rho$ and $j = 1, ..., \kappa)$ are considered random variables, represented by chance nodes (ovals). The relationships existing amongst these features are portrayed in the ID network given in Figure 1.8.

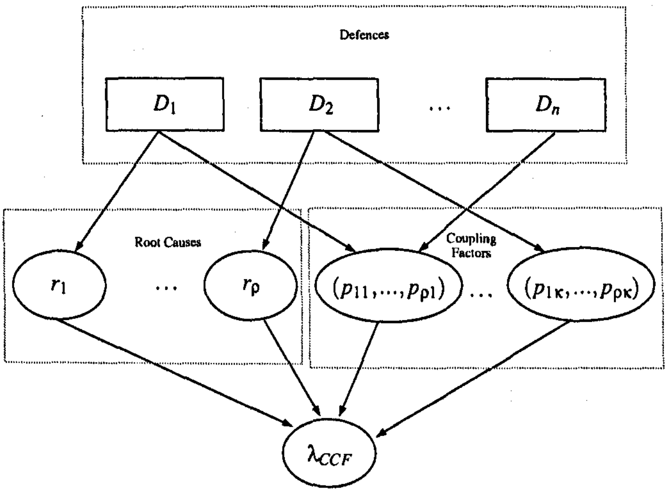


Figure 1.8: Relationships expressed in the ID model

This section proceeds with the system description and definition of component boundaries.

Description of the system

One of the most important objectives of the safe design of nuclear power plants is, in case of postulated accidents, to ensure that the radioactive fission products stay contained within the fuel, and radioactivity is not released in the environment. The distinctive feature of nuclear reactors is the fact that, even when the nuclear reaction is tripped, heat is produced by the decay of radioactive fission products (decay heat). Consequently, in emergency cases nuclear safety should provide not only for automatic shutdown of the reactor, but also for cooling of the fuel after the reactor shutdown. Decay heat removal is achieved by Emergency Core Cooling Systems (ECCSs). ECCSs are required to operate for a long time after the reactor shutdown, and, demand the availability of a stable source of electrical power.

At the occurrence of a loss of offsite power event, nuclear power plants are equipped to maintain electrical stability. In case of plant blackouts, where alternating current power supply fails, Emergency Diesel Generators (EDGs) provide the electrical supply to the ECCS and other equipment necessary for the safe shutdown of the reactor plant. These generators provide power only when needed, to special safety electrical distribution panels; their configuration ensures that they supply adequate electrical power in case of loss of offsite power events, with or without a concurrent large break loss-of-coolant accident (LOCA). According to the 'Defence-In-Depth' philosophy, nuclear power plants are equipped with at least two EDGs. The EDG system is automatically actuated by signals that sense either loss of coolant accident, or a loss of, or degraded, electrical power to its safety bus. Manual initiation of the EDG system is also possible from the operator control room.

In general, EDGs are on standby, whether the plant is operating or in a shutdown state.

Component boundaries

Following, is a description of the EDG component, as defined in [Wierman et al., 2000].

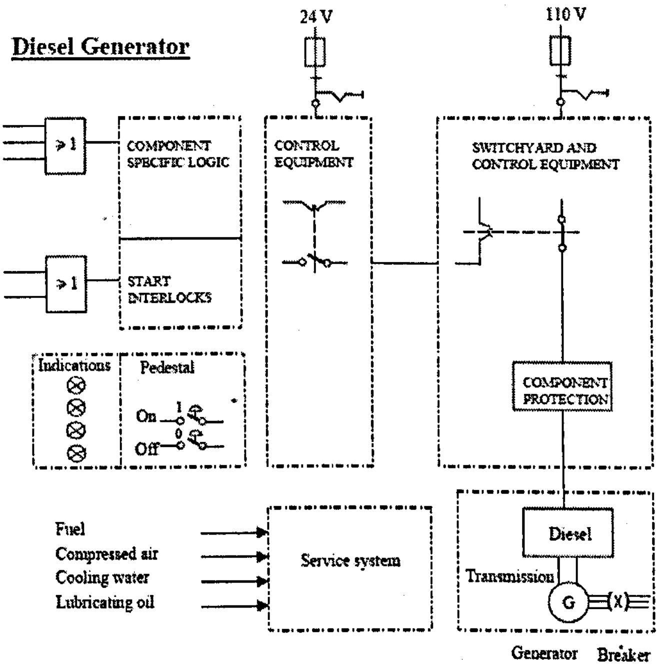


Figure 1.9: Emergency Diesel Generator and subsystems

The EDG is defined as the combination of the diesel engine with all components in the exhaust path, electrical generator, generator exciter, output breaker, combustion air, lube oil systems, cooling system, fuel oil system, and the starting compressed air system. All pumps, valves, and valve operators with their power supply breakers and associated piping for the above systems are included. The only portions of the EDG cooling systems included are the specific devices that control cooling medium flow to the individual EDG auxiliary heat exchangers, including the control instruments. The service water system (cooling medium) outside the control valves is excluded. The EDG room ventilation is included if the licensee reports ventilation failures that affected EDG functional operability.

Included within the EDG system are the circuit breakers that are located at the motor control centres (MCCs) and the associated power boards that supply power specifically to any of the EDG equipment. The MCCs and the power boards are not included except for the load shedding and load sequencing circuitry/devices that are, in some cases, physically located within the MCCs. Load shedding of the safety bus and subsequent load sequencing onto the bus of vital electrical loads is considered integral to the EDG function and is therefore considered within the component boundaries. All instrumentation, control logic, and the attendant process detectors for system initiations, trips, and operational control are included.

1.5 Structure of the thesis

The structure of the thesis is presented in Figure 1.10.

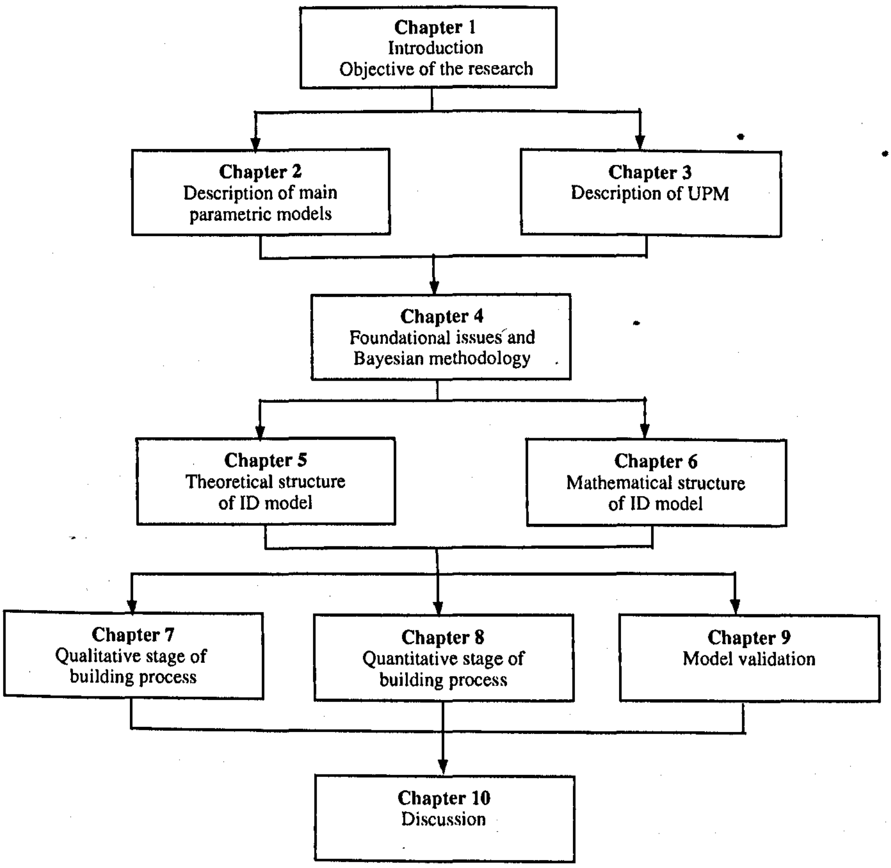

Chapter 1
Introduction
Objective of the research
Chapter 2
Description of main parametric models
Chapter 3
Description of UPM
Chapter 4
Foundational issues and Bayesian methodology
Chapter 5
Theoretical structure of ID model
Chapter 6
Mathematical structure of ID model
Chapter 7
Qualitative stage of building process
Chapter 8
Quantitative stage of building process
Chapter 9
Model validation
Chapter 10
Discussion

Figure 1.10: Structure of the thesis

Chapter 2

Main models for CCF modelling

2.1 Introduction

The previous chapter provided an introduction to CCF events, and an overview of their treatment in risk analyses. Within this context, the aims and objectives of the research have been described. This chapter aims to give a more detailed insight into the quantitative modelling of CCF events which occurs during the *Common Cause Modelling and Data Analysis* stage of the overall CCF procedural framework (given in Figure 1.1). In particular, the main parametric models are presented and compared. For the presentation of the models a practical example is used, namely a redundant system of identical components with success logic 2*oo*3.

This chapter is structured as follows: Section 2.2 illustrates the description of the system under study in terms of basic failure events, by considering the contribution of CCF events. Section 2.3 describes the main parametric models used for the quantification of the basic events, and gives a brief overview of other models suggested in the literature for this purpose. Section 2.4 addresses the model quantification issue, and describes the existing difficulties associated with the quantification of parametric models. Section 2.5 comments on the presented CCF models, and finally, Section 2.6 concludes the chapter.

2.2 CCF modelling

Essentially, the treatment of CCF events may be separated into a qualitative and a quantitative phase. The qualitative phase covers stages 1 and 2 of the overall procedural framework (Figure 1.1 in Chapter 1), whereas the quantitative phase relates to the next two stages.

2.2.1 Logic model development

During the qualitative phase of the CCF treatment, the system under study is described in terms of basic events that result in loss of its function. This is accomplished during the *System Logic Model Development* stage, with techniques such as Fault Tree Analysis (FTA). FTA is a popular modelling tool for logically representing systems [Roberts et al., 1981]. By using a top-down approach and logical AND and OR connectors, the top event (system failure) is described in terms of the intermediate events that lead to it. The construction proceeds gradually to finer levels of detail, until the top event is described in terms of failures of specific components.

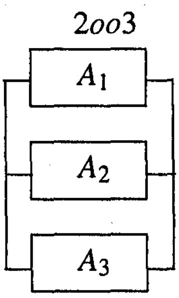


Figure 2.1: Reliability block diagram

For illustrative purposes, a practical example is used. Consider a system of three components that operates with a $2oo3$ success logic. The reliability block diagram representation of the system is given in Figure 2.1. By using a fault tree technique, the failure of the system is graphically represented in terms of events (Figure 2.2). With the help of this representation, the sets of basic events that, if they occur, lead to the top event (minimal cut sets) can be delivered. In the particular 2*oo*3 example, these are

$$\{A_i, A_j\} \quad i \neq j \text{ and } i, j = 1, 2, 3$$

where A_i denotes the failure of component i, for $i = 1, 2, 3$.

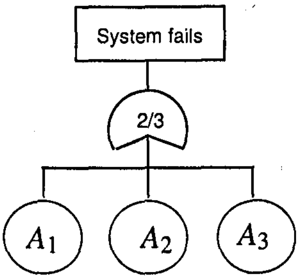


Figure 2.2: Fault tree model

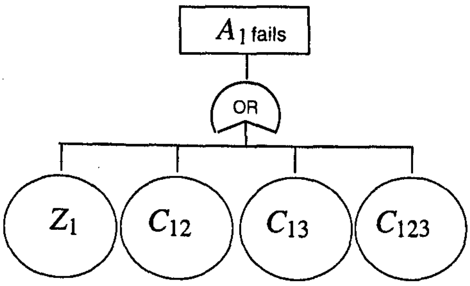


Figure 2.3: Sub-fault tree for failure of single component

For the incorporation of CCF events in the analysis, the fault tree is further expanded to include CCF basic events, which describe the dependent failure of particular subsets of components. This is achieved by further expanding the individual component failure basic events included in the initial fault tree, to include the effect of CCFs (Figure 2.3). The expanded fault tree yields the following cut sets

$$\{Z_i, Z_j\} \quad i \neq j \text{ and } i, j = 1, 2, 3$$
$$\{C_{ij}\} \quad i \neq j \text{ and } i, j = 1, 2, 3$$
$$\{C_{123}\}$$

where Z_i represents the *independent* failure of component A_i, C_{ij} represents the *dependent* failure of components A_i and A_j due to a common cause event, and C_{123} represents the *dependent* failure of all three components due to a common cause event.

2.2.2 CCF quantification

Based on the FTA of the system, the impact of CCFs is being modelled by producing a performance indicator of the system subject to CCF events. The operating mode of the system of interest strongly influences the choice of this performance indicator, and thus, the parameterisation used for the determination of this indicator.

The system' s operating mode is typically distinguished between two types: operating on demand and operating continuously. This section considers separately these two different operating modes. Next, it will be shown that in both cases assessing the performance of the system requires the determination of the CCF basic parameters - these are either basic probabilities on demand or basic failure rates, depending on the operation mode of the system.

System operating on demand

Systems that are operating on demand are idle for a period of time (on stand-by), and are only challenged to deliver their intended function periodically. A performance indicator that is widely used for this operating mode is the *unavailability of the system.* A definition of unavailability is the following [Ebeling, 1997]:

> A piece of equipment (system) is considered unavailable at time t, $t \in [0,+\infty)$, if it is not performing its required function at this time; and the probability that the component (system) is unavailable at time t is denoted with $U(t)$.

In order to determine the system unavailability at time t, $t \in [0,+\infty)$, the event that needs to be quantified is 'system failing at time t', which is denoted by S. Based on the FTA of the system, a deterministic expression of the event of interest (top event) is produced in terms of the basic events, which is used for quantification purposes.

Essentially, a fault tree is a Boolean representation. In the particular example, based on the trees in Figures 2.2 and 2.3, the derived Boolean representation of the system failure on demand S is

$$S = Z_1Z_2 + Z_1Z_3 + Z_2Z_3 + C_{12} + C_{13} + C_{23} + C_{123} \qquad (2.1)$$

Note that S, Z_i and C_{ij} are now boolean variables, taking value 1 for *true* and 0 for *false.*

The failure of the system to operate on demand is classified by two different categories: failure revealed by the demand, and failure caused by the demand. Each categorisation postulates different failure mechanisms, and, thus, needs to be considered separately.

Failures revealed by the demand Failures revealed by the demand involve failure events that bring the system into a failed state during the period the system is idle; these failures are unobserved and only detected when the system is challenged. Such failure mechanisms include corrosion, degradation, or shocks that occur to the system during the idle period. The modelling of this type of failures is based on the assumption that failures occur in continuous time over the period the system is idle [Vaurio, 1994b], infringing on the system a lifetime distribution F.

The general approach to CCF modelling [Marshall and Olkin, 1967; Vesely, 1977] assumes that CCF events of different multiplicities occur at random times and independently of each other, failing specific groups of redundant components at constant rates (Poisson processes). Single component failures are referred to as independent failures, whereas failures of groups of components due to a CCF event are referred to as dependent failures. It is typical to make the internal symmetry assumption, according to which all components in the group have the same failure rate, and the rate of CCF events failing a component subgroup is the same for all subgroups of the same size. In the particular $2oo3$ system example, it is

$T_{1/3}$ = time to failure (independently) of component i $\quad (i = 1,2,3)$

$T_{2/3}$ = time to failure (dependently) of components i and j $\quad (i \neq j$ and $i, j = 1,2,3)$

$T_{3/3}$ = time to failure (dependently) of components $1,2,3$

Let $F_{k/3}$ be the cumulative probability distribution of r.v. $T_{k/3}$, $k = 1,2,3$. It is assumed that once a component is found failed, it is getting repaired immediately, and the repair time is insignificantly short compared to the test interval. If $T_{k/3}$ is the time to failure of a specific subgroup of k components in the group of three components, then it is an exponentially distributed r.v. with parameter $\lambda_{k/3}$, viz.

$$T_{k/3} \sim \mathcal{E}(\lambda_{k/3})$$

The inspection strategy employed on a stand-by system influences the detection time of failures and affects the prevention of potential failures. Thus, the unavailability of a stand-by system is a function of the testing scheme and its characteristics. Vaurio [Vaurio, 1994b, 1995] considers different repair strategies and maintenance policies in order to determine the effect of CCF events on system unavailability. Next, two simple examples of testing scheme are considered for illustrative purposes.

At a sequential testing scheme all components are tested almost 'simultaneously', meaning that they are tested successively and the overall test duration is insignificantly small compared to the test interval. The unavailability of a system which is subject to CCFs is determined with the help of the Boolean expression (2.1), obtained during the logic model development of the system, where the top event S is 'system failing at time t', $t \in [0, +\infty)$. In reliability analyses it is typical to make the rare events approximation [Mosleh et al., 1998c][1], which leads to

$$\begin{aligned} P(S) = {} & P(Z_1)P(Z_2) + P(Z_1)P(Z_3) + P(Z_2)P(Z_3) \\ & + P(C_{12}) + P(C_{13}) + P(C_{23}) + P(C_{123}) \end{aligned}$$

For the $2oo3$ system under study to fail to start on demand, failure events must have occurred during the idle period of the system, which is equal to the test interval (denoted by Δ). For $t \in [0, \Delta]$, it holds that

$$P(Z_i) = P(T_{1/3} \le t), P(C_{ij}) = P(T_{2/3} \le t), P(C_{123}) = P(T_{3/3} \le t)$$

[1] The rare events approximation suggests that for small values of $P(A)$ and $P(B)$ ($\ll 0.1$), omitting $P(A \cap B)$ from the expression

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

incorporates a negligible amount of error and the time-dependent unavailability at time $t \in [0, \Delta]$ is

$$\begin{aligned} U(t) &= 3P(T_{1/3} \leq t)^2 + 3P(T_{2/3} \leq t) + P(T_{3/3} \leq t) \\ &= 3F_{1/3}(t)^2 + 3F_{2/3}(t) + F_{3/3}(t) \end{aligned} \tag{2.2}$$

which is expressed in terms of failure rates $\lambda_{k/m}$ ($k = 1, 2, 3$). Under the assumption that a demand can occur at any time during the test interval Δ, the time-average unavailability over the period between tests $[0, \Delta]$ is

$$U_\Delta = \frac{1}{\Delta} \int_0^\Delta U(t) \mathrm{d}t$$

A staggering testing scheme describes the situation where m components are tested at staggered intervals, with distance between the tests of time $\frac{\Delta}{m}$ (Figure 2.4). The probability of the system being unable to operate at time $t \in (0, \frac{\Delta}{m}]$ between the sequential tests is determined by considering the earliest possible occurrence time of each failure combination, taking into account the tests before time 0 [Vaurio, 1994b]. For the 2*oo*3 system it is

$$\begin{aligned} U(t) = {} & P(T_{3/3} \leq t + \frac{\Delta}{3}) + P(T_{2/3} \leq t + \frac{\Delta}{3}) + 2P(T_{2/3} \leq t) \\ & + P(T_{1/3} \leq t)P(T_{1/3} \leq t + \frac{2\Delta}{3}) + P(T_{1/3} \leq t)P(T_{1/3} \leq t + \frac{\Delta}{3}) \\ & + P(T_{1/3} \leq t + \frac{\Delta}{3})P(T_{1/3} \leq t + \frac{2\Delta}{3}) \\ = {} & F_{3/3}(t + \frac{\Delta}{3}) + F_{2/3}(t + \frac{\Delta}{3}) + 2F_{2/3}(t) + F_{1/3}(t)F_{1/3}(t + \frac{2\Delta}{3}) \\ & + F_{1/3}(t)F_{1/3}(t + \frac{\Delta}{3}) + F_{1/3}(t + \frac{\Delta}{3})F_{1/3}(t + \frac{2\Delta}{3}) \end{aligned} \tag{2.3}$$

which is expressed in terms of failure rates $\lambda_{k/3}$ ($k = 1, 2, 3$). The average unavailability over the period between staggered tests is determined as

$$U_\Delta = \frac{m}{\Delta} \int_0^{\frac{\Delta}{m}} U(t) \mathrm{d}t$$

Therefore, the quantification of unavailability of a system of m redundant compo-

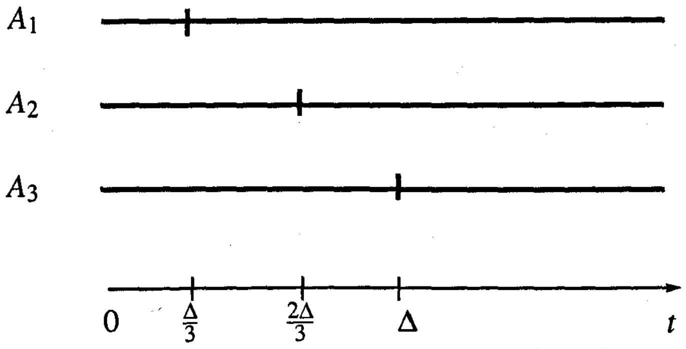


Figure 2.4: Staggering testing scheme

nents, which is operating on demand, due to failures revealed by the demand requires the estimation of the following basic rates per unit time:

$$\lambda_{k/m} := \text{rate at which } \textit{specific } k \text{ components fail in a group of } m \text{ components}$$

for $k = 1, ..., m$.

Failures caused by the demand Failures caused by the demand describe failure events that are a consequence of the load infringed on the system by the activation itself. In this case, the failure of the system to operate is not revealed by the demand, but caused by it. For this type of failure, the interest lies in estimating the probability that the system fails to operate when it is activated (probability of failure on demand), and the system unavailability is defined as

$$U(i) = P(\text{system fails on demand } i), \quad i = 1, 2...$$

The Boolean representation (2.1) needs to be transformed to an algebraic representation, expressing the probability of the system failing on demand (top event). Based on the rare events approximation, we have

$$\begin{aligned} P(S) &= P(Z_1)P(Z_2) + P(Z_1)P(Z_3) + P(Z_2)P(Z_3) \\ &\quad + P(C_{12}) + P(C_{13}) + P(C_{23}) + P(C_{123}) \end{aligned} \tag{2.4}$$

A typical assumption made in the case of identical components in order to reduce the number of parameters that need to be quantified, is the internal symmetry assumption [Mosleh et al., 1998c]. According to the internal symmetry assumption, the probability of a basic event within a given group of components is assumed to depend only on the number of components involved in that basic event, and not on the specific components. Therefore, the failure probabilities are the same for sub-groups of components of the same size. Consequently, the following probabilities are defined:

$$
\begin{aligned}
q_{1/3} &= P(Z_i) \quad (i = 1,2,3) \\
q_{2/3} &= P(C_{ij}) \quad (i \neq j \text{ and } i,j = 1,2,3) \\
q_{3/3} &= P(C_{123})
\end{aligned}
$$

Now, Relationship (2.4) gives the following expression for the system unavailability on demand $U(\cdot)$

$$U(i) = 3q_{1/3}^2 + 3q_{2/3} + q_{3/3}, \quad \text{for } i = 1,2,... \tag{2.5}$$

Therefore, the quantification of unavailability for a system of m components operating on demand, attributed to failures caused by the demand, requires the estimation of the basic probabilities

$$q_{k/m} = P(\textit{specific } k \text{ out of } m \text{ components fail on demand, while the other } m-k \text{ components do not fail})$$

for $k = 1,...,m$.

The average unavailability over a total of N demands is

$$U_N = \frac{1}{N}\sum_{i=1}^{N} U(i)$$

which is the discrete case of the time-average unavailability described previously. In this case, the system unavailability is not a function of time, and is not modulated by the testing scheme adopted.

Systems in continuous operation

For a system that is in continuous operation, the time when it stops delivering its intended function is usually immediately identified. This means that failures are directly observed as soon as they occur, and appropriate action is taken. For continuously operating system, it is assumed that CCF events occur at any time $t \in [0,+\infty)$, failing simultaneously subgroups of redundant components. Therefore, a useful performance indicator of a normally operating system is the *system reliability*. The system reliability is defined as the probability that system is operating at time t, $t \in [0,+\infty)$, i.e.

$$P(T \geq t) = R_S(t) = 1 - F_S(t)$$

where r.v. T denotes the failure time of the system. Based on the general model for CCF modelling [Marshall and Olkin, 1967; Vesely, 1977], it is assumed that CCFs of different multiplicities occur at independent Poisson processes. In the particular 2*oo*3 example, it is

$T_{1/3}$ = time to failure (independently) of component i $\quad (i = 1,2,3)$

$T_{2/3}$ = time to failure (dependently) of components i and j $\quad (i \neq j$ and $i,j = 1,2,3)$

$T_{3/3}$ = time to failure (dependently) of components $1,2,3$

Let $F_{k/3}$ be the cumulative probability distribution of r.v. $T_{k/3}$, $k = 1,2,3$. We have

$$T_{k/3} \sim \mathcal{E}(\lambda_{k/3}) \quad \text{for } k = 1,2,3$$

Generally, the impact of CCF events on the reliability of a system of m components may be represented by a system where strictly independent failures occur, which is connected in series with $m-1$ systems with reliability $R_k(t) = 1 - F_{k/m}(t)$ $(k = 2,...,m)$. In the particular 2*oo*3 example, this situation is represented in see Figure 2.5.

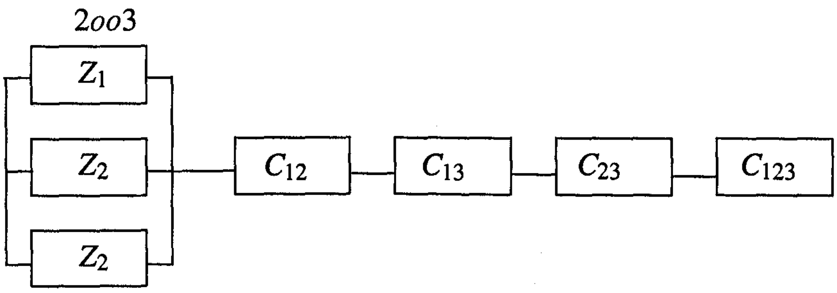


Figure 2.5: Expanded reliability block diagram including CCF events

Assuming identical components, the reliability of a *noom* system with only independent failures is given by the following formula [Ebeling, 1997]

$$R_{in}(t) = \sum_{x=n}^{m} \binom{m}{x} \left(1 - F_{1/m}(t)\right)^x F_{1/m}(t)^{m-x}$$

For the particular 2*oo*3 example the formula gives

$$R_{in}(t) = 3(1 - F_{1/3}(t))^2 F_{1/3}(t) + (1 - F_{1/3}(t))^3$$

In general, the reliability of an *m*-redundant series system subject to independent failures only, is given by the formula

$$R_{in}(t) = \prod_{x=1}^{m} (1 - F_x(t))$$

where F_x is the lifetime distribution of component x. The 2*oo*3 system reliability, including CCFs, is given by

$$\begin{aligned} R_s(t) &= \left(3(1 - F_{1/3}(t))^2 F_{1/3}(t) + (1 - F_{1/3}(t))^3\right) \left(1 - F_{2/3}(t)\right)^3 \left(1 - F_{3/3}(t)\right) \\ &= \left(3e^{-2\lambda_{1/3}t} - 2e^{-3\lambda_{1/3}t}\right) e^{-3\lambda_{2/3}t} e^{-\lambda_{3/3}t} \end{aligned} \tag{2.6}$$

Further analysis on the determination of the reliability characteristics of operating systems subject to CCF events may be found in [Vaurio, 1995]. Frequently, for repairable systems, the long-run equilibrium unavailability of the system is used. When it exists, it is determined as the limiting unavailability as Δ increases to infinity

$$U = \lim_{\Delta \to \infty} U_\Delta$$

where

$$U_\Delta = \frac{1}{\Delta} \int_0^\Delta P(T \leq t) \mathrm{d}t$$

and

$$P(T \leq t) = 1 - R(t), \quad t \in (0, +\infty]$$

Therefore, assessing the performance of a continuously operating system of m components requires the estimation of the following basic rates per unit time:

$$\lambda_{k/m} := \text{rate at which } \textit{specific } k \text{ out of } m \text{ components fail}$$

for $k = 1, ..., m$.

2.3 Parametric models

In essence, probabilities on demand and failure rates underlie different frameworks of assumptions, and are applicable within certain contexts. In general, quantifying the CCF basic events in terms of rates makes the assumption of the components failing almost 'simultaneously'. Quantification in terms of probabilities on demand makes far less assumptions regarding the failure mechanism, allowing to address cases where components failed dependently, but not as close in time. However, as shown in the previous section, for stand-by systems time-dependent unavailability cannot be defined when using probabilities on demand, implying that the average unavailability remains unaffected by the testing scheme. Time-dependent unavailability is determined in terms of failure rates, which are parameters of the model [Vaurio, 1994b]. In this case, the average unavailability captures the effect of different testing strategies and characteristics.

The quantification of Relationships (2.2), (2.3), (2.5) and (2.6) is typically performed by using parametric models. CCF models re-parameterise components $q_{k/m}$ and $\lambda_{k/m}$, for $k = 1,2,...,m$, in terms of other, more easily quantifiable quantities. Within the literature, a number of parametric models have been suggested based on either probabilities on demand, or failure rates. Essentially, depending on the overall framework of supporting assumptions, most parametric models can be used for both operating modes, provided that necessary changes are made in the definition of some of the model parameters, and, therefore, in the estimation procedures.

In the following sections the main parametric models are presented. The formulation of each model is described firstly in terms of probabilities on demand, and secondly in terms of failure rates, provided that the model assumptions allow for both parameterisations. Afterwards, estimation procedures for the model parameters are described.

2.3.1 Notation

$q_{k/m}$ probability that *specific* k components fail on demand in a group of m components, while the other $m-k$ components do not fail

$Q_{k/m}$ probability that *exactly* k components fail on demand in a group of m components

$\lambda_{k/m}$ rate at which *specific* k components fail in a group of m components

$\Lambda_{k/m}$ rate at which *exactly* k components fail in a group of m components

p_{in} probability that a given component fails on demand independently in a group of m components

p_d probability that a given component fails on demand dependently in a group of m components

p probability that a given component fails on demand (independently or dependently) in a group of m components

$\pi_{k/m}$	probability that a given component fails on demand with other *exactly* $k-1$ components in a group of m components
$l_{k/m}$	rate at which a given component fails with other *exactly* $k-1$ components in a group of m components
Q_T	probability that a failure event of any possible multiplicity occurs (dependent or independent)
Λ_T	rate of failures (dependent or independent)
$P_{k/m}$	probability that exactly k components fail dependently out of m, given that a failure occurs
n_k	number of failure events of multiplicity k
N_k	number of component failures of multiplicity k
n_T	total number of failures
N_T	total number of component failures
n_{in}	number of independent component failures
T	system observation time
N	number of system demands

2.3.2 The Basic Parameter Model

From a formulation point of view, the Basic Parameter (BP) model [Fleming et al., 1983] constitutes one of the simplest approaches towards the quantification of the CCF basic events. The simplicity of its framework stems from the fact that no intermediate parameters are defined for the estimation of the basic events.

Probabilities on demand

For a system of m components the BP parameters are

$$q_{k/m} = P(\textit{specific } k \text{ components fail on demand in a group of } m \text{ components,} \\ \text{while the other } m-k \text{ components do not fail})$$

for $k = 1,\ldots,m$.

Parameter Estimation The data required for the estimation of parameters q_k is of the form

$$\underline{n} = (n_0, n_1, ..., n_m)$$

where n_k is the number of events where k components are found unavailable on demand (failure events of multiplicity k), out of in total N system demands. Note that $n_0 = N - \sum_{k=1}^{m} n_k$.

Classical Estimation According to the internal symmetry property the failure probability is the same for all subgroups of the same size, and the probability that *exactly* k components are unavailable on demand in a group of m components $Q_{k/m}$ is expressed as

$$Q_{k/m} = \binom{m}{k} q_{k/m} \Leftrightarrow q_{k/m} = \frac{1}{\binom{m}{k}} Q_{k/m} \tag{2.7}$$

The likelihood function of the data set $\underline{n}$ is a multinomial distribution with parameters $\underline{Q} = (Q_{0/m}, Q_{1/m}, ..., Q_{m/m})$

$$f(\underline{n}|\underline{Q}) = \frac{N!}{n_0! n_1! ... n_m!} \prod_{k=0}^{m} Q_{k/m}^{n_k}$$

The Maximum Likelihood Estimators (MLEs) for $Q_{k/m}$ are obtained by maximising the logarithm of the likelihood function $f(\underline{n}|\underline{Q})$, under the constraint $\sum_{k=0}^{m} Q_{k/m} = 1$, and they are

$$\hat{Q}_{k/m} = \frac{n_k}{N}, \quad k = 0, ..., m$$

Relationship (2.7) is invertible, thus

$$\hat{q}_{k/m} = \frac{1}{\binom{m}{k}} \hat{Q}_{k/m} = \frac{n_k}{\binom{m}{k} N}$$

Bayesian Estimation By adopting a Bayesian approach, alternatively, parameter vector $\underline{Q} = (Q_{0/m}, Q_{1/m}, ..., Q_{m/m})$ is considered as a vector of random variables. The natural choice for the joint prior distribution $f(\underline{Q})$ is the Dirichlet distribution, as the later is conjugate with the multinomial likelihood. The joint posterior $f(\underline{Q}|\underline{n})$, in the light of data $\underline{n}$, is obtained by Bayes' law:

$$f(\underline{Q}|\underline{n}) \propto f(\underline{n}|\underline{Q})f(\underline{Q})$$

and it is again a multinomial distribution, with parameter vector $(d_0+n_0, d_1+n_1, ..., d_m+n_m)$, where $d_0, d_1, ..., d_m$ are the parameters of the prior $f(\underline{Q})$. The marginal posterior distribution on $Q_{k/m}$ is obtained as

$$f(Q_{k/m}|\underline{n}) = \int_0^1 \cdots \int_0^1 f(\underline{Q}|\underline{n})\mathrm{d}Q_{0/m}...\mathrm{d}Q_{k-1/m}\mathrm{d}Q_{k+1/m}...\mathrm{d}Q_{m/m}$$

and the posterior on $q_{k/m}$ is obtained through the random variable transformation

$$q_{k/m} = \frac{1}{\binom{m}{k}}Q_{k/m}$$

Failure rates

For a system of m components the BP parameters are

$\lambda_{k/m}$:= rate at which *specific* k components fail in a group of m components

for $k = 1, ..., m$.

Parameter Estimation The data required for the estimation of the Basic Parameters is of the form

$$\underline{n} = (n_1, ..., n_m)$$

where n_k is the number of events where k components are found unavailable on demand (failure events of multiplicity k) observed during system exposure time T.

Classical Estimation Failures of *specific* k components in a group of m components during a specified (fixed) interval T occur according to a Poisson process with rate $\lambda_{k/m}$. Thus, CCF events failing *exactly* k components occur according to a Poisson distribution with rate $\Lambda_{k/m}$, where

$$\Lambda_{k/m} = \binom{m}{k}\lambda_{k/m}$$

and the likelihood function of the data n_k is a Poisson distribution with rate $\Lambda_{k/m}$, where

$$f(n_k \mid \Lambda_{k/m}) = \frac{(\Lambda_{k/m} \cdot T)^{n_k}}{n_k!} e^{-\Lambda_{k/m} \cdot T}$$

Maximising the logarithm of the likelihood function yields the MLE for the rate Λ_k:

$$\hat{\Lambda}_{k/m} = \frac{n_k}{T} \quad \text{for } k = 1,..m$$

The function $f(x) = \frac{x}{\binom{m}{k}}$ is invertible, so the MLE for the group-specific rate λ_k is

$$\hat{\lambda}_{k/m} = \frac{1}{\binom{m}{k}}\hat{\Lambda}_{k/m} = \frac{n_k}{\binom{m}{k}T} \quad \text{for } k = 1,..m$$

Bayesian Estimation In a Bayesian context and for fixed observation period T, a gamma distribution is used for the prior on $\Lambda_{k/m}$. Let $f(\Lambda_{k/m}) := \mathcal{G}(C,D)$. Once data is attained, the prior distribution $f(\Lambda_{k/m})$ is updated in the light of the new information:

$$f(\Lambda_{k/m} \mid n_k) \propto f(n_k \mid \Lambda_{k/m}) f(\Lambda_k)$$

Due to the conjugate properties of the Gamma and Poisson distributions, the posterior $f(\Lambda_{k/m} \mid (n_k, T))$ is again a gamma distribution with parameters $C + n_k$ and $D + T$. The posterior distribution on the group-specific rate $\lambda_{k/m}$ is now obtained through variable transformation, which yields a gamma distribution with parameters $c + n_k$ and $\binom{m}{k}(d+T)$.

Discussion

The Basic Parameter model is the simplest approach for quantifying CCFs. The model parameters are defined in terms of the basic events and are directly estimated from the data. In other words, no intermediate parameterisation is used. The number of parameters defined within the model depends on the number of components that comprise the group.

2.3.3 The Beta Factor Model

The Beta Factor (BF) model [Fleming, 1975] constitutes the most widely used model for the quantification of CCF basic events. Its popularity stems mainly from its simple framework. The BF model assumes that a constant fraction of the total failure probability on demand or failure rate is associated with CCFs. The BF parameters describe the failure behaviour of a specific component, therefore it is a component-oriented approach. The theoretical structure behind the model acknowledges only two kind of failures: independent component failures, and CCF events that affect all components in the group.

The BF model introduces parameter β, which is defined as the conditional probability that a specific component fails due to a CCF, given that it fails, viz.

$$\beta = P(\text{component fails dependently} \mid \text{component fails})$$

Probabilities on demand

Consider a redundant system of m components. Let p_{in} denote the probability that a component fails on demand independently in a group of components, and p_d denote the probability that it fails on demand dependently, along with all m components. It holds that

$$p_{in} = (1-\beta)p \text{ and } p_d = \beta p$$

where p is the total probability that the component fails on demand. Therefore, β is the fraction of the total component failure probability attributed to dependent failures

$$\beta = \frac{p_d}{p_{in} + p_d} = \frac{p_d}{p}$$

and $1 - \beta$ is the fraction of the total component failure probability on demand which is due to independent failures.

Parameter Estimation The BF model is a component oriented approach; therefore, the data required for the quantification of each parameter needs to be in the form of component failures. The form of the component-specific data is:

$$(n_{in}, n_d)$$

where n_{in} is the number of times the component failed independently and n_d is the number of times the component failed dependently, out of N component demands.

Classical Estimation The likelihood function of the data set (n_{in}, n_d) may be represented by a binomial distribution with probability of success β, viz.

$$f(n_{in}, n_d \mid \beta) = \binom{n}{n_d} \beta^{n_d} (1 - \beta)^{n - n_d}$$

where $n = n_{in} + n_d$. In a similar fashion, a Binomial distribution is used to model the likelihood of observing n in total failures out of the N component demands

$$f(n, N \mid p) = \binom{N}{n} p^n (1 - p)^{N - n}$$

The MLE for β is determined by maximising the logarithm of the likelihood function $f(n_{in}, n_d | \beta)$

$$\hat{\beta} = \frac{n_d}{n} = \frac{n_d}{n_{in} + n_d}$$

The MLE for p is determined by maximising the logarithm of the likelihood function $f(n,N|p)$, giving

$$\hat{p} = \frac{n}{N} = \frac{n_{in}+n_d}{N}$$

Bayesian Estimation In Bayesian theory, the β-factor is considered a random variable and a prior distribution is assumed for it. The beta family of distributions is used for the prior $f(\beta)$, which is conjugate with the binomial family. The prior distribution is updated in the light of data (n_{in}, n_d) to yield the posterior distribution $f(\beta|n_{in}, n_d)$:

$$f(\beta \mid n_{in}, n_d) \propto f(n_{in}, n_d \mid \beta) f(\beta)$$

The posterior distribution for β is again a beta distribution with parameters $A+n_d$ and $B+n_{in}$, where A and B are the parameters of the prior distribution on β.

Similarly, p is considered a random variable and a beta prior $f(p)$ is assumed for it. In the light of data (n,N), the prior is updated to yield the posterior:

$$f(p \mid n,N) \propto f(n,N \mid p) f(p)$$

which is again a beta distribution with parameters $\Gamma+n$ and $\Delta+N-n$, where Γ and Δ are the parameters of the prior distribution on p.

Failure rates

Consider a redundant system of m components. The BF model assumes that failures occur to the system at constant rates. A specific component may fail either independently at rate λ_{in}, or as part of a CCF event affecting all components at rate λ_d. The independent and dependent failures are assumed to occur according to independent homogeneous Poisson processes with rates λ_{in} and λ_d respectively. Consequently, the overall component failure process is a superposition of the two independent Poisson processes with rate λ, and we have

$$\lambda = \lambda_{in} + \lambda_d$$

The fraction of the total failure rate which is due to CCFs is constant, and denoted with β, viz.

$$\beta = \frac{\lambda_d}{\lambda_{in} + \lambda_d} = \frac{\lambda_d}{\lambda}$$

Consequently, the fraction of the total failure rate which is due to independent failures is $1-\beta$, and we have $\lambda_d = \beta\lambda$ and $\lambda_{in} = (1-\beta)\lambda$, for $0 \leq \beta \leq 1$. Thus, it holds

$$T_1 \sim \mathcal{E}(\lambda_{in}) \text{ and } T_m \sim \mathcal{E}(\lambda_d)$$

where T_1 is the time to failure (independently) of component i, $i = 1,...,m$, and T_m is the time to failure of all m components due to a common cause.

Parameter Estimation In a similar fashion as before, the data required for the quantification of each parameter needs to be in the form of component failures. The form of the component-specific data is:

$$(n_{in}, n_d)$$

where n_{in} is the number of independent component failures and n_d is the number of dependent component failures during component exposure time T.

Classical Estimation The estimation of the β-factor is similar to the previous case. The failing state of the component is being modelled as a Bernoulli experiment. The MLE for β is

$$\hat{\beta} = \frac{n_d}{n} = \frac{n_d}{n_{in} + n_d}$$

Consistently with the underlying framework of assumptions, a specific component fails (both dependently and independently) according to a Poisson process with parameter λ. During a specified time interval $[0, T]$, the number of failures has a Poisson distribution with parameter λT. Consequently, the MLE for λ is obtained by maximising the logarithm of the likelihood function of the data

$$f(n \mid \lambda) = \frac{(\lambda \cdot T)^n}{n!} e^{-\lambda \cdot T}$$

and it is

$$\hat{\lambda} = \frac{n}{T} = \frac{n_{in} + n_d}{T}$$

Bayesian Estimation The Bayesian estimation of the β-factor is performed in a similar way as in the model parameterisation in terms of probabilities on demand: a beta prior is defined on β, which is conjugate with the binomial data (n_{in}, n_d).

For the Bayesian estimation of the total failure rate λ, the likelihood function of the data $f(n \mid \lambda, T)$, where $n = n_{in} + n_d$, is modelled with a Poisson distribution. A gamma prior distribution is assumed for λ. Updating the gamma prior with Poisson data yields a gamma posterior again, viz.

$$f(\lambda \mid n) \propto f(n \mid \lambda) f(\lambda) := \mathcal{G}(\Gamma + n, \Delta + T)$$

where Γ and Δ are the gamma parameters of the prior distribution on λ.

Discussion

In terms of assumptions, the Beta Factor model constitutes the simplest of the parametric models developed for the quantification of CCF basic probabilities; not surprisingly, it is also one of the most popular models for practical application. It has two distinctive features: firstly, regardless of the number of components comprising the system, it requires the estimation of only two parameters; secondly, it does not acknowledge CCFs of various multiplicities (subgroups of different sizes), as CCFs always affect all components in the group.

The first implication of the simplicity of the BF model is the fact that it is unable to distinguish between different system architectures. Because CCFs impact on all components, the contribution of CCF events to the overall unavailability of the systems is the same, regardless of the system success logic.

Secondly, the BF model is a conservative approach towards the quantification of CCF events. Since it is assumed that all CCF events are lethal (failing all components in the system), the CCF contribution to risk is always increased. Due to its pessimistic nature, the BF model is often used as a crude cut-off.

2.3.4 The Multiple Greek Letter Model

The Multiple Greek Letter (MGL) model is one of the most well known models for the quantification of CCF basic events (see for example [Apostolakis and Moieni, 1987] and references therein). The MGL model is an extension of the Beta Factor model, developed in an attempt to take into account CCF events of different multiplicities, which occur to systems comprised by more than two components. Similarly to the Beta Factor model, the MGL model is a component-oriented approach; the MGL parameters are defined in terms of conditional probabilities and describe the failure behaviour of a specific component in relation to the rest of the components in the group.

For an m redundant system of identical components, the k-th Greek letter of the model, is defined as

$$\rho_k = P(\text{a } \textit{specific} \text{ component fails dependently with other } k-1 \text{ or more}$$
$$\text{components} \mid \text{it fails dependently with other } k-2 \text{ or more components})$$

for $k = 2, \dots, m$.

Probabilities on demand

In a group of m components, $q_{k/m}$ is defined as the probability that *specific* k components fail. Then, $q_{k/m}$ is the probability that a specific component fails dependently with other *specific* $k-1$ components, which happens in $\binom{m-1}{k-1}$ different ways. On this basis, the probability that the given component fails dependently with other *exactly*

$k-1$ components is

$$\pi_{k/m} = \binom{m-1}{k-1} q_{k/m} \quad \text{for } k = 1,\ldots,m \tag{2.8}$$

and the probability that the given component fails dependently with other *exactly* $k-1$ *or more* components is

$$\sum_{x=k}^{m} \pi_{x/m} = \sum_{x=k}^{m} \binom{m-1}{x-1} q_{x/m} \quad \text{for } k = 1,\ldots,m \tag{2.9}$$

Therefore, the total failure probability of a given component, denoted with p, may be expressed as

$$p = \sum_{x=1}^{m} \binom{m-1}{x-1} q_{x/m} \tag{2.10}$$

and we have

$\rho_k = P($a *specific* component fails dependently with other $k-1$ or more components | it fails dependently with other $k-2$ or more components$)$

$$= \frac{P(\text{a } \textit{specific} \text{ component fails dependently with } k-1 \text{ or more components})}{P(\text{a } \textit{specific} \text{ component fails dependently with } k-2 \text{ or more components})}$$

which yields

$$\rho_k = \frac{\sum_{x=k}^{m} \binom{m-1}{x-1} q_{x/m}}{\sum_{x=k-1}^{m} \binom{m-1}{x-1} q_{x/m}} \quad \text{for } k = 2,\ldots,m \tag{2.11}$$

By solving the system comprised of equations (2.11) and (2.10), it can be shown that the basic probabilities $q_{k/m}$ are given by

$$q_{k/m} = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{j=1}^{k} \rho_j \right) (1 - \rho_{k+1}) p \tag{2.12}$$

where $\rho_1 = 1$, $\rho_2 = \beta$, $\rho_3 = \gamma, \ldots, \rho_{m+1} = 0$. Based on Relationships (2.8) and (2.12), probabilities $\pi_{k/m}$ are expressed in terms of the Greek letters as:

$$\pi_{k/m} = \left(\prod_{j=1}^{k} \rho_j\right)(1-\rho_{k+1})p \tag{2.13}$$

Parameter Estimation Relevant data usually consists of counts of CCF events of different multiplicities, observed from the system when subjected to N demands. The form of the data is:

$$\underline{n} = (n_1, n_2, \ldots, n_m)$$

where n_k is the number of failure events of multiplicity k ($k = 1, \ldots, m$).

Classical Estimation Note that the MGL model is a component-oriented approach, therefore the event-count data must be considered from a component perspective. Therefore, the data set $\underline{n}$ is translated to $N_1 = n_1$ independent component failures, $N_2 = 2n_2$ component failures as part of a CCF affecting two components, and so on. The total number of component failures is $N_T = \sum_{k=1}^{m} kn_k$ out of the $m \cdot N$ component demands. The joint likelihood function of the component-oriented data N_k with $k = 1, \ldots, m$ is a multinomial distribution

$$f\left((N_1, N_2, \ldots, N_m) \mid (\pi_{1/m}, \ldots, \pi_{m/m})\right) \propto \prod_{k=1}^{m} \pi_{k/m}^{N_k} \tag{2.14}$$

Note that the multinomial likelihood implies that the component failures occur independently, even though they occur as part of CCF events.

The MLEs for the Greek Letters ρ_k can be determined by substituting (2.13) into (2.14), taking the logarithm of the resulting expression, setting the partial derivative in terms of ρ_k equal to zero, and solving for ρ_k. We have

$$\hat{\rho}_k = \frac{\sum_{j=k}^{m} j \cdot n_j}{\sum_{j=k-1}^{m} j \cdot n_j}$$

The probability that a component is found unavailable on demand for whatever reason is considered a success in a sequence of Bernoulli trials (component demands). Consequently, the likelihood of the component being unavailable $N_T = \sum_{k=1}^{m} k \cdot n_k$ times out of the $m \cdot N$ component demands is

$$f(N_T, m \cdot N \mid p) = \binom{m \cdot N}{N_T} p^{N_T} (1-p)^{m \cdot N - N_T}$$

and the MLE for p is

$$\hat{p} = \frac{N_T}{m \cdot N} = \frac{\sum_{k=1}^{m} k \cdot n_k}{m \cdot N}$$

Bayesian Estimation In a Bayesian view, $\underline{\pi} = (\pi_{1/m}, \ldots, \pi_{m/m})$ is considered as a vector of random variables and, naturally, the prior on the vector of multinomial parameters is assumed to be a Dirichlet distribution, which is conjugate with the multinomial distribution, viz.

$$f(\underline{\pi}) \propto \pi_{1/m}^{d_1 - 1} \pi_{2/m}^{d_2 - 1} \ldots \pi_{m/m}^{d_m - 1}$$

where $d_1, \ldots, d_m$ are the parameters of the distribution. The prior is updated through Bayes' law to yield the posterior $f((\pi_{1/m}, \ldots, \pi_{m/m}) \mid (N_1, N_2, \ldots, N_m))$, which is again a Dirichlet distribution with parameters $(d_1 + N_1, \ldots, d_m + N_m)$. The marginal posteriors on $\pi_{k/m}$ are determined as

$$f(\pi_{k/m} \mid \underline{N}) = \int_0^1 \ldots \int_0^1 f(\underline{\pi} \mid \underline{N}) \mathrm{d}\pi_{1/m} \ldots \mathrm{d}\pi_{k-1/m} \mathrm{d}\pi_{k+1/m} \ldots \mathrm{d}\pi_{m/m}$$

where $\underline{N} = (N_1, N_2, \ldots, N_m)$. Finally, the posterior on ρ_k is obtained through variable transformation based on Relationships (2.13).

It is suggested ([Apostolakis and Moieni, 1987] and references therein) that omitting to account for correlations amongst the MGL parameters in the estimation process does not necessarily lead to significant errors, at least when the redundancy is small. Alternatively, it is suggested to estimate the epistemic uncertainty on the Greek letters separately, by using a beta prior for ρ_k, which is updated with the binomial data $\left(\sum_{j=k}^{m} N_j, \sum_{j=k-1}^{m} N_j\right)$.

For the estimation of p, a beta distribution is assumed for the prior $f(p)$. The prior is updated with the binomial data

$$f(p \mid N_T, mN) \propto f(N_T, m \cdot N) \mid p) f(p)$$

to yield the posterior on p. The posterior is again a beta distribution with parameters $\Gamma + N_T$ and $\Delta + m \cdot N - N_T$, where Γ and Δ are the parameters of $f(p)$.

Failure rates

Suppose that a given component fails due to a CCF event affecting k components in total. The rate at which specific k components fail out of m is $\lambda_{k/m}$; thus, $\lambda_{k/m}$ is the rate at which the given component fails with other *specific* $k-1$ components, which happens in $\binom{m-1}{k-1}$ different ways. Since the sum of independent Poisson processes is a Poisson process, the rate $l_{k/m}$ at which the given component fails due to a CCF which affects other *exactly* $k-1$ components out of the m is:

$$l_{k/m} = \binom{m-1}{k-1} \lambda_{k/m}.$$

and, the rate of CCF events that fail a given component along with other *exactly* $k-1$ *or more* components out of the m is:

$$L_{k/m} = \sum_{x=k}^{m} l_{x/m} = \sum_{x=k}^{m} \binom{m-1}{x-1} \lambda_{x/m}$$

Given the failure of the given component dependently with other $k-2$ components or more, ρ_k is the probability that the component fails dependently with other $k-1$ components or more. Based on the properties of the Poisson process, it holds that

$$L_{k/m} = \rho_k L_{k-1/m}$$

or

$$\rho_k = \frac{L_{k/m}}{L_{k-1/m}} = \frac{\sum_{x=k}^{m} \binom{m-1}{x-1} \lambda_{x/m}}{\sum_{x=k-1}^{m} \binom{m-1}{x-1} \lambda_{x/m}} \quad \text{for } k = 2, ..., m \tag{2.15}$$

Finally, the failure process of a given component due to both CCFs and independent events is a superposition of the independent Poisson processes with rate

$$\lambda = \sum_{x=1}^{m} \binom{m-1}{x-1} \lambda_{x/m} \tag{2.16}$$

Solving equations (2.15) and (2.16) in terms of the group-specific rates yields:

$$\lambda_{k/m} = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{j=1}^{k} \rho_j \right) (1 - \rho_{k+1}) \lambda \tag{2.17}$$

where $\rho_1 = 1$, $\rho_2 = \beta$, $\rho_3 = \gamma, \ldots, \rho_{m+1} = 0$.

Parameter Estimation As previously, the event-count data needs to be considered from a component perspective. Consequently, the data set

$$\underline{n} = (n_1, n_2, \ldots, n_m)$$

where n_k is the number of CCF events of multiplicity k observed during time T $(k = 1, \ldots, m)$ is transformed to

$$\underline{N} = (N_1, N_2, \ldots, N_m)$$

where $N_k = k \cdot n_k$ is the number that a component fails as part of a CCF event of multiplicity k $(k = 1, \ldots, m)$, recorded during time $m \cdot T$.

Classical Estimation The classical estimation of the Greek letters is similar to the probability on demand case. For the estimation of the total component failure rate λ, the likelihood of observing $N_T = \sum_{i=1}^{m} jn_j$ component failures during the specified interval $[0, mT]$, is described by a Poisson distribution:

$$f(N_T \mid \lambda) = \frac{(\lambda T)^{N_T}}{N_T!} e^{-\lambda \cdot mT}$$

The MLE for the overall component failure rate λ is

$$\hat{\lambda} = \frac{N_T}{mT} = \frac{\sum_{k=1}^{m} k \cdot n_k}{m \cdot T}$$

Bayesian Estimation Bayesian estimation of the Greek letters is performed as in the probability on demand case. For the estimation of the total component failure rate, λ is considered as a random variable, whose prior $f(\lambda)$ is a gamma distribution. If Γ and Δ are the parameters of the gamma prior, then the posterior distribution in the light of N_T failures during fixed time mT is by Bayes theorem

$$f(\lambda \mid N_T) \propto f(N_T \mid \lambda) f(\lambda)$$

and $f(\lambda \mid N_T)$ is again a gamma distribution with parameters $\Gamma + N_T$ and $\Delta + mT$.

Discussion

It is important to note the the MGL model is a component-oriented approach. That implies that the Greek-letter parameters describe the failing behaviour of a given component, in relation to the other components comprising the system. To be more precise, the k-th letter of the model ρ_k is the conditional probability that the given component fails in a certain way. If one wishes to express the conditional probability of k components failing, given that $k-1$ components fail, then the parameters need to be redefined as:

$$\rho_k^* = \frac{\sum_{j=k}^{m} \binom{m}{j} q_j}{\sum_{j=k-1}^{m} \binom{m}{j} q_j} \quad \text{for } k = 1, .., m$$

instead of

$$\rho_k = \frac{\sum_{j=k}^{m} \binom{m-1}{j-1} q_j}{\sum_{j=k-1}^{m} \binom{m-1}{j-1} q_j} \quad \text{for } k = 1,..,m$$

The MGL model is often referred to as a 'ratio model' [Vaurio, 1994b]. The reason for this is the fact that the model parameters are defined in terms of conditional probabilities; therefore, at the failure rate parameterisation of the model, these are expressed in terms of ratios of failure rates. As a result, the estimation of the Greek letters does not require the number of total demands or total system observation time.

Note that the number of Greek-letter parameters that are defined within the MGL framework depends on the size of the system of interest, and the parameter values depend on the overall system redundancy. Finally, the estimation procedures for the MGL parameters are straightforward, provided that there is no uncertainty inherent in the data and that information is available concerning all failure multiplicities.

2.3.5 The Alpha Factor Model

The Alpha Factor (AF) model is one of the most well-known models for the quantification of CCF basic events (see for example [Siu and Mosleh, 1989]). The model describes the dependency conditions existing in the system under study by quantifying the occurrence of failure events that impact on component subgroups of different sizes.

The alpha factors of the model are defined in terms of conditional probabilities; in particular, for an m redundant system of identical components, the k-th alpha factor is the probability that a CCF event fails exactly k components, given that a failure event occurs, viz.

$$\alpha_k = P(\textit{exactly } k \text{ components fail} \mid \text{failure event occurs}) \quad \text{for } k = 1,...,m$$

Probabilities on demand

Consider a system of m components that is subject to demands. Parameters $q_{k/m}$ and $Q_{k/m}$ are related through relationship

$$Q_{k/m} = \binom{m}{k} q_{k/m} \Leftrightarrow q_{k/m} = \frac{1}{\binom{m}{k}} Q_{k/m} \tag{2.18}$$

and the probability that a failure event of any possible multiplicity occurs is expressed as

$$Q_T = \sum_{k=1}^{m} Q_{k/m} = \sum_{k=1}^{m} \binom{m}{k} q_{k/m}$$

A given component may be found unavailable on demand due to either an independent failure (with probability $q_{1/m}$), or due to a CCF event that fails in total k components ($k = 1, ..., m$). In the latter case, the given component fails dependently with other $k-1$ components in the group, which happens in $\binom{m-1}{k-1}$ ways, and each time with the same probability $q_{k/m}$. Therefore, the total failure probability on demand of a given component, p, is:

$$p = \sum_{k=1}^{m} \binom{m-1}{k-1} q_{k/m}$$

Based on the definition of the alpha factors, it is

$$\alpha_k = \frac{P(\textit{exactly } k \text{ components unavailable on demand})}{P(\text{failure event occurs})} = \frac{Q_{k/m}}{Q_T} \tag{2.19}$$

Note that $\sum_{k=1}^{m} \alpha_k = 1$. Moreover, $\sum_{k=1}^{m} k \cdot \alpha_k$ expresses the expected number of components failing, given that a failure event occurs. It holds that

$$\sum_{k=1}^{m} k \cdot \alpha_k = \sum_{k=1}^{m} k \cdot \frac{Q_{k/m}}{Q_T} = \frac{m}{Q_T} \sum_{k=1}^{m} \binom{m-1}{k-1} q_{k/m} = m \frac{p}{Q_T}$$

which leads to

$$Q_T = \frac{mp}{\sum_{k=1}^{m} k \cdot \alpha_k} \tag{2.20}$$

Equations (2.18),(2.19) and (2.20) yield the following expressions for the basic probabilities on demand $q_{k/m}$

$$q_{k/m} = \frac{m\alpha_k}{\binom{m}{k}\sum_{j=1}^{m} j \cdot \alpha_j} p \tag{2.21}$$

Parameter Estimation Relevant data consists of counts of CCF events of each failure multiplicity recorded out of N system demands. The form of the data is:

$$\underline{n} = (n_1, n_2, \ldots, n_m)$$

where n_k is the number CCF events of multiplicity k ($k = 1, \ldots, m$).

Classical Estimation The probability of observing the data is given by the multinomial distribution, viz.

$$f(\underline{n}|\underline{\alpha}) = \frac{n!}{n_1!n_2!\ldots n_m!} \prod_{k=1}^{m} \alpha_k^{n_k} \tag{2.22}$$

where $n = \sum_{k=1}^{m} n_k$. The MLEs of α_k are determined by maximising the logarithm of the likelihood function, under the constraint $\sum_{k=1}^{m} \alpha_k = 1$, and are

$$\hat{\alpha}_k \doteq \frac{n_k}{n}, \quad k = 1, \ldots, m$$

For the estimation of the component failure probability p, the data needs to be counted from a component perspective. Therefore $\underline{n}$ is translated to n_1 times of single component failures, $2 \cdot n_2$ component failures as part of double CCFs, and so on. In total, a single component failed on demand $N_T = \sum_{k=1}^{m} k \cdot n_k$ times out of $m \cdot N$ component demands. The probability that the component is unavailable on demand for whatever reason is described by a Bernoulli trial with probability of success p. Consequently, the data $(N_T, m \cdot N)$ is binomial and

$$f(N_T, mN \mid p) = \binom{N_T}{m \cdot N} p^{N_T}(1-p)^{m \cdot N - N_T}$$

The MLE for p is obtained by maximising the logarithm of the likelihood function, and it is

$$\hat{p} = \frac{\sum_{k=1}^{m} k \cdot n_k}{m \cdot N}$$

Bayesian Estimation Within a Bayesian context, $\underline{\alpha} = (\alpha_1, ..., \alpha_m)$ is a vector of random variables, having a joint prior. A natural choice for the joint prior distribution $f(\underline{\alpha})$ is the Dirichlet distribution, which is the multinomial counterpart of the beta distribution and conjugate with the multinomial distribution; therefore, updating $f(\underline{\alpha})$ in the light of the binomial data $\underline{n}$ through Bayes' theorem:

$$f(\underline{\alpha}|\underline{n}) \propto f(\underline{n}|\underline{\alpha})f(\underline{\alpha})$$

yields again a Dirichlet posterior $f(\underline{\alpha}|\underline{n})$, with parameters $(d_1+n_1, \ldots, d_m+n_m)$, where $(d_1, \ldots, d_m)$ are the parameters of the prior Dirichlet. For the determination of the total component failure probability p, it is typical to assume a beta prior $f(p)$. Recall that the data relevant to p is counted from a component perspective. The posterior on p is obtained through Bayes' theorem:

$$f(p \mid N_T, m \cdot N) \propto f(N_T, m \cdot N \mid p) f(p)$$

The data is described by a Binomial distribution with success probability p and, due to the conjugate properties of the distributions, the posterior $f(p \mid N_T, m \cdot N)$ is Beta again with parameters $\Gamma + N_T$ and $\Delta + m \cdot N - N_T$, where Γ and Δ are the parameters of the prior $f(p)$.

Failure rates

Consider a system of m components. Consistently with the internal symmetry assumption, the process that fails *exactly* k components is the superposition of the group-specific independent Poisson processes, with rate

$$\Lambda_{k/m} = \binom{m}{k} \lambda_{k/m} \tag{2.23}$$

where $\lambda_{k/m}$ is the rate at which *specific* k components fail.

Similarly, all types of failure events occur according to Poisson process with rate

$$\Lambda_T = \sum_{k=1}^{m} \binom{m}{k} \lambda_{k/m}$$

A given component may fail either independently at a rate λ_1, or dependently with other $k-1$ components of the group, each time at a rate λ_k. Then, the total component failure rate considers all possible failure multiplicities, and it is equal to the sum of the superimposed Poisson processes with rate

$$\lambda = \sum_{k=1}^{m} \binom{m-1}{k-1} \lambda_{k/m}$$

Given that a failure occurs, α_k is the probability that k components fail due to a CCF. Based on the properties of the Poisson process, it holds that

$$\Lambda_{k/m} = \alpha_k \Lambda_T$$

or

$$\alpha_k = \frac{\Lambda_{k/m}}{\Lambda_T} = \frac{\binom{m}{k} \lambda_{k/m}}{\sum_{k=1}^{m} \binom{m}{k} \lambda_{k/m}} \tag{2.24}$$

We note that $\sum_{k=1}^{m} \alpha_k = 1$; moreover, $\sum\limits_{k=1}^{m} k \cdot \alpha_k$ expresses the expected number of components failing, given that a failure event occurs. It holds that

$$\sum_{k=1}^{m} k \cdot \alpha_k = \sum_{k=1}^{m} k \cdot \frac{\Lambda_{k/m}}{\Lambda_T} = \frac{m}{\Lambda_T} \sum_{k=1}^{m} \binom{m-1}{k-1} \lambda_{k/m} = m\frac{\lambda}{\Lambda_T}$$

which leads to

$$\Lambda_T = \frac{m\lambda}{\sum_{k=1}^{m} k \cdot \alpha_k} \tag{2.25}$$

Now, the basic rates λ_k may be expressed in terms of the alpha factors as:

$$\lambda_{k/m} = \frac{m\alpha_k}{\binom{m}{k} \sum_{j=1}^{m} j \cdot \alpha_j} \lambda \tag{2.26}$$

Parameter Estimation In a similar fashion as before, the relevant data is of the form

$$\underline{n} = (n_1, n_2, \ldots, n_m)$$

where n_k is the number of failures affecting k components ($k = 1, \ldots, m$), recording during system observation time T.

Classical Estimation The alpha factors α_k ($k = 1, ..., m$) are estimated in a similar way as in the probability on demand case. For the estimation of the total component failure rate λ, the likelihood of observing $N_T = \sum_{i=1}^{m} jn_j$ component failures during the specified interval $[0, mT]$, is described by a Poisson distribution:

$$f(N_T \mid \lambda) = \frac{(\lambda T)^{N_T}}{N_T!} e^{-\lambda \cdot mT}$$

The MLE for the overall rate λ is

$$\hat{\lambda} = \frac{N_T}{mT} = \frac{\sum_{k=1}^{m} k \cdot n_k}{m \cdot T}$$

Bayesian Estimation Bayesian estimation of the alpha factors α_k ($k = 1, ..., m$) is performed as within the probability on demand parameterisation.

For the estimation of the total component failure rate λ, λ is considered as a random variable, whose prior $f(\lambda)$ is modelled with a gamma distribution. If Γ and Δ are the parameters of the gamma prior, then the posterior distribution in the light of the Poisson data (N_T, mT) is by Bayes theorem

$$f(\lambda \mid N_T) \propto f(N_T \mid \lambda) f(\lambda)$$

and $f(\lambda \mid N_T)$ is again a gamma distribution with parameters $\Gamma + N_T$ and $\Delta + mT$.

Discussion

Like the MGL model, the Alpha Factor model is also referred to as a 'ratio' model [Vaurio, 1994b], because the alpha parameters are defined in terms of conditional probabilities or ratios of failure rates.

The alpha factors are expressed in terms of the Basic Parameters as follows:

$$\alpha_k = \binom{m}{k} \frac{q_{k/m}}{1 - q_{0/m}}$$

The difference between the two models is the fact that the estimation of alpha factors, unlike the basic parameters, does not require the number of total system demands or system observation time; counts of CCF events are sufficient.

Finally, the number of alpha parameters depends on the size of the system of interest, and the parameter values depend on the overall system redundancy.

2.3.6 The Binomial Failure Rate Model

The Binomial Failure Rate (BFR) model is one of best known parametric models. First developed by Vesely [Vesely, 1977] and further modified by Atwood [Atwood, 1996], it is based on the Marshall-Olkin model [Marshall and Olkin, 1967]. The model postulates a 'shock' causal mechanism for the failures. In particular, it is assumed that common cause events occur to the system as a result of shocks, that lead to the dependent failure of more than one components simultaneously. The shocks infringe on the system according to Poisson processes, and can potentially lead to failures of all multiplicities. The rate at which CCF shocks hit a component subgroup does not depend on the presence of other components, thus it is considered independent of the total number of the components comprising the system.

Consider a system comprising of m components. Each component in the group fails independently at a rate λ_{in}. Apart from the independent component failures, shocks occur to the system causing CCF events, at a rate μ. It is assumed that at the occurrence of a shock, each component in the group fails independently of the other with probability p. Consequently, the probability that *specific* k components fail, whereas $m-k$ survive, is $p^k(1-p)^{m-k}$; and, the probability that *exactly* k components fail, whereas $m-k$ survive, is given by the binomial distribution:

$$\binom{m}{k} p^k(1-p)^{m-k}, \text{ for } k = 1,...,m$$

Therefore, the rate of CCF events failing *specific* k ($k = 1,...,m$) components, $\lambda_{k/m}$, is determined as the product of the probability that specific k components fail, given the occurrence of a shock, with the rate at which shocks occur, viz.

$$\lambda_{k/m} = p^k(1-p)^{m-k}\mu \quad \text{for } k = 2,...,m \tag{2.27}$$

and the rate of failures affecting *exactly* k components in the system is

$$\Lambda_{k/m} = \binom{m}{k} p^k(1-p)^{m-k}\mu \quad \text{for } k = 2,...,m$$

Consistently with the properties of the Poisson process, failure events of any multiplicity occur according to a Poisson process with rate

$$\Lambda_T = \sum_{k=1}^{m} \Lambda_{k/m} = \sum_{k=1}^{m} \binom{m}{k} p^k(1-p)^{m-k}\mu = (1-(1-p)^m)\mu \tag{2.28}$$

Within the BFR framework, a given component fails individually in two different ways: independently, with rate λ_{in}, or due to single CCF failures, with rate

$p(1-p)^{m-1}\mu$. Consequently, the total rate of single failures for a given component is

$$\lambda_{1/m} = \lambda_{in} + p(1-p)^{m-1}\mu \tag{2.29}$$

and the rate of single failures in the system is

$$\Lambda_{1/m} = m\lambda_{in} + mp(1-p)^{m-1}\mu$$

In case that a given component fails as part of a CCF event of multiplicity k, it fails dependently with other $k-1$ components with probability $p^k(1-p)^{m-k}$ and in $\binom{m-1}{k-1}$ ways. The total probability of the given component failing due to a CCF is

$$\sum_{k=1}^{m} \binom{m-1}{k-1} p^k(1-p)^{m-k} = p$$

Consequently, the total rate of failures of whatever type for a given component is

$$\lambda = \lambda_{in} + p\mu$$

Once the BFR parameters λ_{in}, μ and p are determined, the basic rates λ_k can be determined for any $k = 1,...,m$.

As it has been already mentioned, Atwood is responsible for further adaptations of the original BFR model. In particular, Atwood [Atwood, 1996] suggested a second kind of shocks, those that lead automatically to the failure of all the components comprising the system. These shocks are named lethal, in contrast to the non-lethal shocks, and occur with rate ω. Similar assumptions apply to the lethal shock mechanism: lethal shocks occur independently to non-lethal shocks and independent failures, and infringe on the system according to a Poisson process. Consequently, the individual failure rate of a given component becomes

$$\lambda_{1/m} = \lambda_{in} + p(1-p)^{m-1}\mu + \omega$$

and the rate at which a specific group of k components will fail due to a CCF becomes

$$\lambda_{k/m} = p^k(1-p)^{m-k}\mu + \omega \quad \text{for } k = 2,\ldots,m$$

Parameter Estimation

The relevant for parameter estimation data is in the form of event-count data, i.e.

$$\underline{n} = (n_1, n_2, \ldots, n_m)$$

where n_k is the number CCF events failing k components ($k = 1,\ldots,m$), recorded during system observation time T.

Relationships (2.27) and (2.29) show that the individual failure rate of a given component λ_1 and the group-specific rates $\lambda_{k/m}$, for $k = 2,\ldots,m$, may be determined based on parameters λ_{in}, p and μ. Hence, the interest lies on the estimation of the three aforementioned parameters.

Classical Estimation For the determination of p, let N_k be a random variable expressing the number of CCF events failing k components during system observation time T, for $k = 1,\ldots,m$. Then $\underline{N} = (N_1, N_2, \ldots, N_m)$ is a vector of random variables with a multinomial joint distribution

$$P(N_1 = n_1,\ldots,N_m = n_m) = \frac{n!}{n_1!n_2!\ldots n_m!}\prod_{k=1}^{m} P_{k/m}^{n_k} \tag{2.30}$$

where $(P_{1/m}, P_{2/m}, \ldots, P_{m/m})$ are the parameters of the joint distribution. According to the definition of the multinomial distribution, $P_{k/m}$ is interpreted as the probability that a CCF event of multiplicity k is observed, given that a failure event is observed. Consistently with the fundamental assumptions of the BFR model, failures occur according to a Poisson distribution with rate Λ_T. Based on the properties of the Poisson process, the rate of CCFs failing exactly k components is

$$\Lambda_{k/m} = P_{k/m}\Lambda_T$$

thus,

$$P_{k/m} = \frac{\Lambda_{k/m}}{\Lambda_T} = \binom{m}{k} \frac{p^k(1-p)^{m-k}}{1-(1-p)^m} \tag{2.31}$$

The MLE for p can be determined by substituting (2.31) into (2.30), taking the logarithm of the resulting expression, setting the derivative with respect to p equal to zero, and solving for p.

Unfortunately, the rate of CCF shocks μ cannot be readily estimated from the data; in theory, μ describes shocks that can potentially lead to a failure event, whereas observations carry information regarding actual failures, only. As a result, μ is estimated based on the estimator for the visible shock rate Λ_T.

Let M_k be a random variable expressing the number of CCF events failing k components during system observation time T, for $k = 1,...,m$. According to the BFR framework of assumptions, CCF events of multiplicity k occur according to a Poisson process with rate $\Lambda_{k/m}$, thus $M_1, M_2, ..., M_m$ are independent Poisson distributed random variables. If N_T is the number of failures of any kind, then $M_T = \sum_{k=1}^{m} M_k$ is generated by a process that is the superposition of independent Poisson processes, with rate the sum of the corresponding rates $\Lambda_T = \sum_{k=1}^{m} \Lambda_{k/m}$. Following the MLE standard procedures, we have:

$$\hat{\Lambda}_T = \frac{n_1 + ... + n_m}{T}$$

Using Relationship (2.28), μ is estimated as:

$$\hat{\mu} = \frac{\hat{\Lambda}_T}{1-(1-\hat{p})^m}$$

In a similar fashion, if n_{in} is the number of independent component failures during $[0, T]$, then the MLE for the independent failure rate of a given component is

$$\hat{\lambda}_{in} = \frac{n_{in}}{mT}$$

Bayesian Estimation Consistently with the Bayesian approach, the free parameters of the model λ_{in}, p and Λ_T are random variables, and probability distributions are assumed for them. These distributions are updated in the light of the data.

The number of failures during the pre-specified interval $[0,T]$ is generated according to a Poisson distribution. Specifically, the number of independent failures during fixed component observation time mT is generated by a Poisson process, and the likelihood function of n_{in} is

$$f(n_{in} \mid \lambda_{in}) = \frac{(\lambda_{in} mT)^{n_{in}}}{n_{in}!} e^{-\lambda_{in} \cdot mT}$$

By assuming a gamma prior for λ_{in}, and due to the conjugate properties of the gamma and Poisson distributions, the obtained posterior is again a gamma distribution with parameters $a + n_{in}$ and $b + mT$, where a and b are the parameters of the gamma prior.

In a similar fashion, the total number of failures $n_T = \sum_{k=1}^{m} n_k$ during fixed observation time T are generated from a Poisson process with rate Λ_T, and their likelihood function is:

$$f(n_T \mid \Lambda_T) = \frac{(\Lambda_T \cdot T)^{n_T}}{n_T!} e^{-\Lambda_T \cdot T}$$

It is typical to use a gamma prior for Λ_T, which again yields a gamma posterior with parameters $a + n_T$ and $b + T$, where a and b are the parameters of the gamma prior.

Counting the data set from a component perspective, the event count data corresponds to mn_T visible component shocks, where $n_T = \sum_{k=1}^{m} n_k$, which resulted in $N_T = \sum_{k=1}^{m} k \cdot n_k$ component failures. Considering that the data carries information on observable events only, the likelihood function of observing the aforementioned data is:

$$\begin{aligned} f(N_T \mid p) &= P(N_T \text{ component failures out of } mn_T \text{ component shocks} | \text{visible shock}) \\ &= \frac{P(N_T \text{ component failures out of } mn_T \text{ visible component shocks})}{P(\text{visible shock})} \\ &= \frac{\binom{mn_T}{\nu} p^{\nu}(1-p)^{mn_T - N_T}}{1-(1-p)^m} \end{aligned}$$

Unfortunately, the determination of the posterior distribution on p in the light of data

(N_T, mn_T) requires numerical integration techniques.

Once the distributions on λ_{in}, Λ_T and p, are determined, the distribution of μ, and thus, of the quantities of interest

$$\lambda = \lambda_{in} + p\mu$$

and

$$\lambda_{k/m} = p^k(1-p)^{m-k}\mu \quad \text{for } k = 2, \ldots, m$$

are determined by using numerical approximation techniques. Atwood [Atwood, 1996] suggested an estimation methodology that accounts for the representation of uncertainty, which is referred to as system-to-system and shock-to-shock variability.

Discussion

The BFR model, commonly characterised as the shock model, postulates a clear mechanism for the occurrence of CCF events. In particular, it is assumed that the cause of CCF events is shocks, which infringe on the system according to constant rates, and compel the components to fail either dependently (CCF events) or independently. Within this framework of assumptions, the model allows the possibility of shocks occurring to the system, but without leading to any failures. Consequently, a distinction is made between visible shocks occurring at rate Λ_T and invisible shocks occurring at rate $\mu(1-p)^m$. In a similar fashion, a component could fail independently at a rate λ_{in}, or individually, but as the result of a shock, at a rate $\mu p(1-p)^{m-1}$. In practice it is often difficult to sufficiently identify and estimate the aforementioned differences, especially in cases where the amount of data available for quantification purposes is limited.

The main difference between the BFR model and the rest of CCF models is that the former defines a functional relationship between the basic parameters of the model and the failure rates of different multiplicities. When using the BFR model, independently of the size of the system under assessment, the model parameters that need to be estimated are three: λ_{in}, p and μ. Once the analyst has determined estimators for the aforementioned quantities, it is possible to coherently extrapolate and calculate rates of events of any multiplicity, even those that have not been observed.

Whereas classical estimation of the parameters of interest is relatively straightforward, Bayesian analysis requires certain cumbersome calculations. The reason is that, once the posterior distributions on λ_{in}, p and μ are determined, one needs to use variable transformation techniques to determine the distributions on the quantities of interest $\lambda_{k/m}$, for $k = 1,...,m$.

Finally, describing the failure probability for all components with the same parameter p entails some stringent assumptions. According to the model, the response of all components to shocks is identical, making it difficult to address cases where diversity or separation are present.

2.3.7 Overview of other parametric models

Several of the main parametric models presented earlier have been used as a platform for the development of more sophisticated modelling structures. The aim of this section is to give a brief overview of other models suggested in the literature for the quantification of CCFs.

The Multiple Beta Factor model The Multiple Beta Factor (MBF) model [Hokstad and Corneliussen, 2004; Hokstad et al., 2005] is based on the simple Beta Factor model. The development of the model is based on an attempt to produce a method that, like the BF model, has a sufficiently simple framework for use in practice, whilst, unlike the BF model, manages to distinguish between the performance of different success logics.

Maintaining the 'conditional probability' approach of the ordinary BF model, the MBF model defines multiple betas for a redundant system of components $A_1,...,A_m$ in the following way:

$$\beta_k = P(\text{Component } A_{k+1} \text{ fails} \mid \text{Components } A_k \cap ... \cap A_1 \text{ fail}), \quad k = 1,...,m$$

The β-factor of the ordinary BF model can be directly derived from the MBF model, by assuming that $\beta_k = 1$ for all $k = 2...m$. Under this assumption, CCF events impact on all components of the system with probability $q_{m/m} = \beta_1 p$, where p is the total component failure probability, and β_1 coincides with the ordinary β. Without making this assumption, β_1 coincides with the ordinary β only for systems of two components. For higher redundancy, β is the probability that all components fail, given the failure of a component, whereas β_1 describes the probability that a specific other component is affected, given the failure of a component.

As an extension of the ordinary BF model, which assumes that CCF failures impact on all components of the redundant group, the MBF model manages to distinguish between different failure multiplicities. Indeed, the basic failure rates and probabilities are defined as follows:

$$\lambda_{k/m} = \lambda \cdot \sum_{i=0}^{m-k} (-1)^i \binom{m-k}{i} \prod_{j=1}^{k-1+i} \beta_j$$

or

$$q_{k/m} = p \cdot \sum_{i=0}^{m-k} (-1)^i \binom{m-k}{i} \prod_{j=1}^{k-1+i} \beta_j \quad .$$

On this basis, the contribution of CCF failures to the failure rate or probability of a *MooN* system is of the form $\Lambda_{CCF} = C_{MooN}\beta_1\lambda$ or $P_{CCF} = C_{MooN}\beta_1 p$, where the coefficient C_{MooN} depends on the particular success logic. In other words, the MBF defines a beta factor $\beta_{NooM} = C_{MooN}\beta_1$ that represents the CCF contribution to the unavailability of a system with a particular success logic *NooM*, by adjusting β_1 accordingly.

The MBF model has similarities with the MGL model, which is also an extension of the ordinary BF model. Likewise, it is a component-oriented approach, as the beta factors describe the failure behaviour of a specific component in the redundant group. However, the MBF model assumes that the failure behaviour of subgroups of components does not depend on the presence of other components; therefore, a group of $m-1$ components behaves exactly as a system with m components, and the multiple beta factors apply to subgroups of components of the same size. This is a property that the Multiple Greek Letters do not have.

The main objective of the MBF model is to result in a methodology that is easy to implement and may be applied in cases where little data is available. To this end, generic values for the multiple betas are suggested in [Hokstad and Corneliussen, 2004], based on operational experience. Alternatively, if sufficient observations are available, the multiple betas can be estimated statistically.

The Common Load model The Common Load model [Mankamo and Kosonen, 1992; Mankamo, 1994] is based on a load-resistance analogy for describing the failure mechanism. In particular, the structure of the model postulates a cause-effect interpretation for the occurrence of failures: in an operating environment, load is imposed on a component; the component reacts to the load by manifesting a resistance, and a failure occurs when the resistance is not sufficient to withstand the load. When it comes to redundant systems of components, the load posed to the system is shared by all the components of the system equally, and a failure of certain multiplicity is determined by the number of components whose resistance is exceeded by the load. Both the load and the component resistance are described in terms of random variables, and probability distributions are assumed for them.

Within the Common Load model framework, the dependence that the redundant components manifest in their failing behaviour stems mainly from two factors: the common load infringed on the redundant components, and the identical resistance distributions of the components. The Extended Common Load model involves comparatively complicated computations and numerical analysis, making the use of a computer tool necessary.

Underlying the Common Load model is the assumption of internal symmetry. Symmetry within the group of components implies that the components are identical, and they have resistances that are independent and identically distributed. The probability entities q_k that are obtained from the use of the Extended Common Load model apply to all subgroups of size k, for $k = 1,..,m$. Indeed, the failure probability of specific k components - without taking into account the state of the rest of the components in the group - does not depend on the size of the subgroup:

$$q_{k/m} = \int_{-\infty}^{+\infty} \left(\int_{-\infty}^{x_L} f_R(x_R)\mathrm{d}x_R \right)^k f_L(x_L)\mathrm{d}x_L = q_k$$

The model has a fixed number of basic parameters, independent of the size of the system. Once these parameters are determined, the model can be used to extrapolate or interpolate to all failure multiplicities.

Cases of non-symmetry can be also modelled by removing the assumption of identical distributed components. Moreover, dependencies amongst components may be accounted for, by removing the independence assumption of component resistances.

The Random Probability Shock model A fundamental assumption of the BFR model is that, given the occurrence of a CCF shock, the components of the system fail independently of each other with probability p, which is common for all components. The Random Probability Shock (RPS) model [Hokstad, 1988] is based on the BFR model but attempts to address statistical variation on parameter p, which stems from external factors such as different degrees of vibration caused by different types of shocks (shock-to-shock variability) or from the heterogeneity of data coming from various sources (system-to-system variation).

In a similar fashion as the BFR model, the RPS model assumes that the number of failed components k in a system of m components, given the occurrence of a CCF shock, is a binomially distributed random variable with parameter p. As the name of the PRS model implies, parameter p is a random variable (random probability) that follows a beta distribution, i.e.

$$p \sim \mathcal{B}(r,s)$$

As a result, the number of failed components has now a beta-binomial distribution with parameters r,s. A re-parameterisation is suggested as

$$Q = \frac{r}{r+s} \text{ and } D = \frac{1}{r+s+1}, \quad 0 < D,Q < 1$$

which results in a pair of more convenient parameters. Parameters Q, D describe the system defence against CCF shocks. Parameter Q may be interpreted as the mean probability that a component fails due to a shock, averaged over all possible shocks. Parameter D may be interpreted as a measure of dependence of the outcomes of shocks of various components. Therefore, the RPS model constitutes an intermediate stage of the BF and the BFR model: whereas the BF model assumes complete dependency between components (if one component fails given a CCF shock, then all do) and the BFR model assumes independency (given a CCF shock, each component fails independently and with a probability p), the RPS model allows for various degrees of dependency.

Kvam [Kvam, 1998] suggested a very similar model to the RPS model. Likewise, a beta distribution is defined on the component failure parameter p. Similarly to the BFR model, given p, the number of CCFs of a particular multiplicity is a Poisson distributed random variable; by considering the uncertainty on p, the resulting distribution is a mixture of Poisson distributions, and the model is called 'a parametric mixture model'. The two models are *au fond* equivalent, since both models define p as a random variable following a beta distribution.

The Trinomial Failure Rate (TFR) model The Trinomial Failure Rate (TFR) model [Han et al., 1989] is also a generalisation of the BFR model, but towards a different direction. The majority of parametric models are characterised by a duality in the description of the component states: a component is classified as either failed or operating. The TRF model uses three component states: a component may be failed, operating or in a 'grey' condition. The grey condition describes an intermediate state between failed and operating, and applies to cases where the event reports are vague about the component state, or describe it as partially or potentially failed. Based on similar fundamental assumptions as the BFR model, the TRF model defines parameters p, q and r as the probability of a component being in a failed, grey and operating state respectively, given that a CCF shock occurs to the system. Consequently, the number of failed components, given a CCF shock, is a random variable following the trinomial distribution.

The Coupling model A further modification of the BFR model is the Coupling model [Kreuser and Peschke, 2001; Kreuser et al., 2006]. The model shares the same causal structure as the BFR model, and it attempts to incorporate two additional sources of uncertainty in the modelling process, referred to as translation uncertainty and interpretation uncertainty. Whereas translation uncertainty relates to the transference of CCF data coming from various sources to the system of interest, interpretation uncertainty stems from the analyst's classification of the component failure states across particular classes (failed, degraded, incipient), which is often based on vague event reports and insufficient data.

The Coupling model assumes that different CCF events may have different effects on the particular system of interest. The number of failed components, given the occurrence of a particular CCF shock j, is a random variable that follows a binomial distribution with parameter p_j, multiplied by a probability-filtering factor

$$\frac{T_{CCF_j} f_j}{T_{obs}}$$

where T_{CCF_j} is the failure detection time (test interval), f_j is a factor that expresses the applicability of CCF shock j observed in a different system, to the system of interest, and T_{obs} denotes the total observation time. Factor $\frac{T_{CCF_j} f_j}{T_{obs}}$ may be interpreted as the probability that a multiple failure, caused by CCF event j, can occur to the system of interest (translation uncertainty), but it may be also interpreted as a diagnostic coverage factor: the bigger the test interval is T_{CCF_j}, the less likely is the failure to be prevented, and therefore, the bigger the probability of multiple failures occurring.

The determination of the component failure probability for phenomenon j, denoted by p_j and referred to as 'coupling parameter', is based on a Bayesian approach. Statistical uncertainty on p_j, due to the limited amount of data, is modelled with a beta distribution, which is updated in the light of observations. Interpretation uncertainty is entered into the model through an impact vector, expressing expert judgment on the multiplicity of the event. The resulting posterior on p_j, which considers both statistical and interpretation uncertainties, is a weighted mixture of updated beta distributions.

The Multi-class Binomial Failure Rate model The Multi-class Binomial Failure Rate model (MCBFR) [Hauptmanns, 1996] constitutes an attempt to incorporate additional technical information in the modelling process. The model suggests the classification of observed CCF events according to a technical taxonomy, and apply the BFR formalism to each class. In particular, the model defines class-specific conditional component failure probabilities p_l and failure rates λ_l, where $l \in L$ and L is the set of technical classes, to account for the different kinds of underlying failure mechanisms. The classes are considered probabilistically independent, and the overall results are obtained as superpositions of the corresponding independent processes.

As with the Coupling model, the MCBFR model structure defines additional parameters applying to each observed event, to account for the subjective translation and interpretation of the CCF events. The parameters are an applicability factor, adapting the event to the particular system of interest, and an interpretation factor, expressing uncertainty in determining the multiplicity of the event.

Both the MCBFR and the Coupling model attempt to generalise the BFR model and integrate expert judgment in their framework. However, whereas the Coupling model adopts a Bayesian approach for the estimation of the coupling parameters to account for the inherent uncertainty, the MCBFR model takes a frequentist approach.

The Process-Oriented Simulation (POS) model In principle, the objective of most parametric models is to directly yield estimators of probabilities or rates, by implicitly modelling the impact of CCF events on the system of interest. The Process-Oriented Simulation (POS) model [Berg et al., 2006] is an attempt to develop a more structural model, by explicitly modelling the CCF process. The model adopts a stochastic simulation approach to describe the number of components failing dependently at the occurrence of a CCF event. The process is described from the time of a root cause impact, until the time of detection of component failures. The estimation procedure for the parameters of the model includes approaches of heuristic nature, and further research is on-going.

2.4 Model quantification

The use of a particular parametric model for the quantification of CCF events requires the statistical estimation of the model parameters. As seen in previous sections, estimation techniques suggested for most parametric models require the availability of system-specific data that describes failures of all possible multiplicities. To be more precise, for a system of m components, the data necessary for parameter estimation is of the form

$$\underline{n} = (n_1, \ldots., n_m) \tag{2.32}$$

where n_k is the number of CCF events that involve k components, $k = 1, \ldots, m$, observed out of N system demands or during T observation time. However, the assumptions and requirements of elegantly developed mathematical theories do not always correspond to reality. Especially from a CCF standpoint, the data available hardly comes up to these expectations, different sources of uncertainty exist in the quantification of CCF parameters and expert judgment becomes an essential source of information. This is due to two particular characteristics of CCF events: the fact that CCF events are relatively sparse, and the fact that they are comparatively complex. These issues will now be described in more detail.

2.4.1 Rarity of CCF events

CCF events are in principle rare events. As a result, the number of observations relevant to a particular system or plant is particularly limited [Parry, 1996; Siu and Kelly, 1998; Spitzer, 2006], and the accumulated data is insufficient for definite parameter estimation procedures. The limited availability of CCF data led to the development of efforts towards the construction of generic databases of CCF events. By accumulating event reports from the wider industry, data banks are compiled.

The compilation of data under a standardised scheme is a common approach in reliability [Cooke and Bedford, 2002]. Within the nuclear industry in particular, examples of such initiatives include the Electric Power Research Institute Program [Worledge and Wall, 1989]; the U.S. Nuclear Regulatory Commission (NRC) and the Idaho National Engineering and Environmental Laboratory (INEEL) [Mosleh et al., 1998b,a] database that assimilates CCF-related events that have occurred in U.S. commercial nuclear power plants from 1980 through 1995; the ICDE Project[2] which is an international effort towards the collection and analysis of CCF events; and national initiatives such as Electricité de France [Meslin, 1988], and the German Risk Study for Nuclear Power Plants [Holtschmidt et al., 2006].

Using generic databases for parameter quantification for a particular study involves the creation of a pseudo-database. A database relevant to the system being modelled (target system) is constructed by pooling data from the generic databases and by 'customising' it in relation to the system under assessment. The 'customisation' process relates to the adjustment of the observed CCF events, to account for differences between the system where the event actually occurred and the target system.

To this end, the use of generic databases leads to a considerable amount of uncertainty entering the data analysis, related to the applicability of the generic events to the specific system, and expert judgment becomes an essential source of information. Certain models, like the Coupling model and the MCBFR model, define applicability factors for each event in their structure, in an attempt to incorporate expert judgment and bridge the existing gap between model requirements and data availability.

Additionally, methodologies have been suggested to address quantitative differences between the actual and target system, namely the difference in the sizes of the two systems (levels of redundancy). Statistical techniques called mapping procedures attempt to transform the data so that it represents a system of the same size as the target system. The transformation process is called 'mapping up', when the size of the actual system is smaller than this of the target system, and 'mapping down' when the size of the actual system is larger than this of the target system. The first effort of mapping procedures can be found in [Fleming et al., 1988, 1989], where mapping down rules are presented based on the framework of the BFR model. Vaurio [Vaurio, 1994b] suggests mapping down rules defined directly on CCF rates. Mapping up processes

[2] www.nea.fr/html/jointproj/icde.html

are suggested in [Mosleh et al., 1998c]; nevertheless, they involve additional assumptions and judgment and they are not consistent with the mapping down rules [Vaurio, 2006; Johanson et al., 2003]. In [Vaurio, 2006] and [Kvam, 1996] mapping rules are suggested for both directions.

2.4.2 Complexity of CCF events

CCF events are complex events. Due to this complex structure, event reports are often vague or incomplete [Mosleh et al., 1994]. Thereby, understanding the actual failure mechanism, identifying the potential root causes or the coupling mechanism that propagated the failure amongst redundant components is often a process that involves subjective interpretation of the event description on behalf of the analyst. To this end, lack of sufficient information unavoidably leads to the incorporation of uncertainties in the analysis of CCF events.

Uncertainty also stems from assigning a failure multiplicity to the CCF event. Even though most parametric models describe the status of a given component as failed or operating, in reality intermediate component statuses are observed, characterised by different degrees of degradation. Information on the components statuses is often included in verbal descriptions, which need to be classified accordingly in order to be included in quantitative analysis. This process introduces a considerable amount of uncertainty in the data analysis process, referred to as interpretation uncertainty [Kreuser et al., 2006].

To provide approaches to data analysis that involves the use of insufficient and vague information, Impact Vector methodologies have been suggested. Impact vectors, firstly introduced in [Fleming et al., 1988, 1989], are techniques developed to incorporate expert judgment. The methodologies address issues such as intermediate component statuses, dispersal of component failures in time and uncertainty regarding the existence of a shared cause. Moreover, applicability factors are suggested to account for the transference of a generic event within the particular context [Mosleh et al., 1994]. Within this context quantitative values correspond to qualitative categories given by the analyst. By using appropriate formulae, adjusted CCF event counts are subjectively determined, and 'virtual' numbers of failures are used as an input for the quantification of parametric models.

In the same vein, the use of subjective weights to account for interpretation uncertainties is suggested in [Vaurio, 1994a, 2002]. For CCF event i, a weight is defined as

$$w_i(k/m) = Pr(k \text{ out of } m \text{ components failed in observed event } i)$$

Instead of using 'virtual' numbers of CCF events as an input in estimation formulae, Vaurio suggests the determination of a discrete p.d.f. for the number of observed failures determined based on subjective weights $w_i(k/m)$ $(k = 1, ..., m)$. The discrete p.d.f. is used to determine the posterior distribution on the model parameters.

Similarly, within the context of the Coupling model [Kreuser and Peschke, 2001], subjective probabilities are defined for CCF event i in terms of

$$\begin{aligned} w_i(k/m) = Pr(&k \text{ out of } m \text{ components would fail on an additional demand} \\ &\text{in observed event } i) \end{aligned}$$

based on the event classification used in Impact Vector methodologies. The updated uncertainty distribution on the coupling parameter p_i, in view of the CCF event i, is a mixture of updated beta distributions with weights $w_i(k/m)$. Moreover, in [Kreuser et al., 2006] an aggregation methodology is suggested within the context of the Coupling model, to combine degradation weights given by different experts.

2.4.3 International Common Cause Failure Data Exchange (ICDE) Project

The International Common Cause Failure Data Exchange (ICDE) Project constitutes a structured effort towards the development of a CCF generic database. The project commenced in 1994, when the countries-members of OECD/NEA decided upon an official attempt to encourage and establish a framework for multilateral co-operation in the collection and analysis of data relating to CCF events. The countries-members of the Project at present, and the organisations representing them in the Project group, are given in Table 2.1.

Table 2.1: ICDE participating countries

Country	Organisation
Canada	AECB
Finland	STUK
France	IPSN
Germany	GRS
Japan	JNES
Korea	KAERI
Spain	CSN
Sweden	SKI
Switzerland	HSK
United Kingdom	NII
United States	NRC

Amongst the objectives of the ICDE Project is to improve the understanding of CCF events by generating qualitative insights into root causes and coupling factors, and to quantitatively use the ICDE data in a PSA framework [Johanson et al., 2006].

A general problem that arises when quantitatively using a generic database is the heterogeneity of the accumulated event reports. This problem becomes even more substantial when the event reports are assimilated form across different countries. The reason is that there are usually national guidelines towards CCF event recording and interpretation of data, and that the CCF event reports are written in the native language of the country where the event was observed. Consequently, in order to create a generic database serving for both qualitative and quantitative applications, the issue of data heterogeneity needs to be considered.

In an effort to achieve uniformity of the quantitative data, the ICDE Project developed a common format for coding national CCF data amongst the countries-members [Werner et al., 2004]. Each observed CCF event in the database is reviewed and, a number of features are assigned accordingly, consistently with the ICDE coding guidelines. These features include a root cause and a coupling factor, a degradation status for each component, a time factor, and a shared cause factor. The time factor is a description of the time difference between the component failures. The shared cause factor is a measure of the uncertainty that the components failed indeed due to a shared cause. Each of qualitative description corresponds to a quantitative value, allowing for the use of the information in statistical analysis.

On this basis, the ICDE database constitutes a particularly important advantage towards the availability of CCF data.

2.5 Discussion

Thus far, the main parametric models have been presented in detail, and an overview is given of a number of other CCF models suggested within the literature. This section comments on the CCF models presented in terms of three main facets: data requirements, model properties and model application.

2.5.1 Data requirements

As described in the previous section, the analysis of CCF data involves a considerable amount of uncertainty, and the common feature of all the parametric models is the difficulty in the parameter estimation process [Spitzer, 2006]. Compared to most parametric models, the Beta Factor model, being based on a simple framework of assumptions, has comparatively limited data requirements. This is the reason of its popularity within the scope of reliability analyses.

Except from the Beta Factor model, the data typically required for the quantification of most parametric models given in (2.32) describes failures up to the highest possible multiplicity. The quantification of component-oriented approaches, like the Multiple Greek Letter model, demands the data to be counted from a component-perspective: data $(n_1,....,n_m)$ is translated to $(n_1,2n_2,...,mn_m)$, where kn_k is the number of component failures that occurred as part of an event failing k components in total. The transformed data is expressed by a Poisson or a Binomial distribution, depending on the model parameterisation, which assumes that the failures occur independently. However, these failures have not occurred independently, but rather dependently, and particularly in k-plets, as a result of a CCF event. The consequence is that, when updating a prior distribution in the light of kn_k failures instead of n_k, the variance of the posterior is smaller, implying that the information in the data is stronger. The result of this translation process is to artificially increase the content of the data set [Apostolakis and Moieni, 1987].

The Binomial Failure Rate model assumes the ability to distinguish between independent single component failures and single component failures due to a shock, which could potentially lead to failures of higher multiplicity, but it did not. In addition, Atwood's extension of the model assumes that a failure event involving all components may have occurred due to two different causes: it is either the result of a lethal shock, or it may be caused by a non-lethal shock that coincidentally resulted in the failure of all components. Thus, distinction between those two different events is necessary, and the data required for the quantification of the model's parameters needs to account for this. In the framework of models like the Alpha Factor and the Multiple Greek Letter model, these distinctions are not essential; all shocks are of the same kind and the probability or rate of a specific subgroup of components failing is determined only by the number of the components comprising the subgroup. In other words, a single failure probability or rate is assigned to an event of a specific multiplicity, regardless of the cause that triggered it.

The parameters of the Alpha Factor model and the Multiple Greek Letter model are defined in terms of conditional probabilities. These models are also referred to as 'ratio' models [Vaurio, 1994b]. The advantage of ratio models is the fact that the total number of demands or observation time is not required for the quantification of the model parameters; counts of CCF events are sufficient. However, the MGL model involves comparatively complicated parameter estimation techniques, especially when adopting a Bayesian approach. The alpha-factors may serve as an intermediate stage for the estimation of the Multiple Greek Letters. Indeed,

$$\rho_k = \frac{\sum_{j=k}^{m} \binom{m-1}{j-1} q_{j/m}}{\sum_{j=k-1}^{m} \binom{m-1}{j-1} q_{j/m}} = \frac{\sum_{j=k}^{m} j\alpha_j}{\sum_{j=k-1}^{m} j\alpha_j} \quad \text{for } k = 1,..,m$$

where ρ_k and α_k are the k-th Greek letter and alpha factor respectively.

In general, the statistical analysis performed for parameter estimation of the CCF models involves a number of particularities. In dealing with the 'data-gaps' existing between available observations and model requirements, models have been developed that use expert judgment in either the statistical analysis or the model structure itself. Examples of the latter case are the Coupling model and the Multi-Class Binomial Failure Rate model, which define applicability factors in order to account for existing differences between the system where the event was actually observed and the target system. In addition, the Coupling Model makes use of vectors defined by experts to subjectively describe the multiplicity of a particular CCF event.

2.5.2 Model properties

The construct of each model and the assumptions made within each context assign to the model certain features. An important feature within the CCF context is the 'subgroup invariance' property of the model parameters [Johanson et al., 2003]. When the parameters of a model are subgroup invariant, then these parameters are the same for subgroups of components. In other words, it is assumed that the failure state of a given component does not depend on the failure state of the other components comprising the subsystem, and the model parameters do not depend on the overall size of the system.

As a corollary, the existence of the subgroup invariance property allows for the model to apply the same parameters in case where only part of the system is challenged. To this end, the effect of decreasing the level of multiplicity could be explored, without having to re-estimate the model parameters. In general, parametric models are black-box modelling approaches, with a limited diagnostic value. The parameters of the Binomial Failure model and the Multiple Beta Factor model are subgroup invariant, whereas the Multiple Greek Letter model and the Alpha Factor model lack the subgroup invariance property.

The Binomial Failure model shares a practical advantage. Typically, for most of the parametric models, the number of the model parameters to be estimated is equal to the redundancy level of the system under assessment. The Binomial Failure model defines a functional relationship between the basic parameters and the failure rates of different multiplicities, requiring the estimation of a fixed number of parameters, regardless of the system size. Once these parameters are estimated, it is possible to coherently extrapolate and calculate rates of events of any multiplicity, even for unobserved events. This property is also shared by models that are based on the BFR model, like the Random Probability Shock model, and models that are based on a load-resistance analogy like the Common Load model. Table 2.2 highlights the characteristics of the main parametric models.

Table 2.2: Comparison of main parametric models

Model	Subgroup invariance	Component orientation	System architectures	Single CCFs
BP			√	
BF		√		
BFR	√		√	√
AF			√	
MGL		√	√	

2.5.3 Application

The CCF parametric models are generally applied to redundant systems of similar components. However, certain features render specific models more applicable within particular contexts. In particular, the Beta Factor model does not account for CCFs of various multiplicities, as it assumes that CCFs affect all redundant components in the system. Due to its pessimistic nature, it is usually used as a crude cut-off model in highly redundant systems.

The Basic Parameter model, the Alpha Factor model, the Multiple Greek Letter model, the Binomial Failure Rate model, and the models that are based on these, are generally applicable models. However, the BFR model is not parameterised in terms of probabilities on demand. The causal structure of the model assumes that dependent component failures occur 'simultaneously', or in very close periods of time. The Extended Common Load model accounts for the increasing dependency in the failure behaviour of components that are part of big groups. The additional extreme load probability part allows to model highly redundant structures that demonstrate strong dependence. Therefore, the model is applicable to systems of particularly high redundancy.

2.6 Conclusion

Parametric models constitute an integral part of the quantitative stage of the overall procedural framework for CCF treatment. They are used for the quantification of the impact of CCF events on the system reliability, which is expressed in terms of basic events included in the system logic model. Depending on the application, the CCF basic events may be expressed either in terms of probabilities on demand, or in terms of failure rates. In general, the use of failure rates allows for determining time-dependent unavailability, and take into account the effect of testing schemes, which cannot be defined when using probabilities on demand.

The parameterisation used within the analysis is related to the operational mode of the system. For systems that operate continuously, the CCF quantification is based on failure rates. However, for quantifying the CCF basic events of a system on demand, it is suggested that different parameterisations are used for different failure modes. On the one hand, failure-to-start events are caused by dormant failures and that are only revealed by the demand; in this case, failure rates are considered applicable because time-dependent unavailability can be defined. On the other hand, failure probabilities on demand are more suitable for the quantification of failures that are caused by the demand, which are classified as failure-to-run events.

This chapter provided an overview of models suggested in the literature for CCF quantification. The main parametric models, namely the Basic Parameter model, the Beta Factor model, the Multiple Greek Letter model, the Alpha Factor model and the Binomial Failure Rate model, were presented in detail. Certain CCF models have been suggested initially in terms of either probabilities on demand, or failure rates, determining the area of their application. Essentially, depending on the overall framework of supporting assumptions, most CCF models can be used for both operating modes, provided that necessary changes are made in the definition of some of the model parameters, and, therefore, in part of the estimation procedures. Within this chapter the mathematical structure of the aforementioned parametric models was defined with relevance to two settings: parameterisation in terms of probabilities on demand and parameterisation in terms of failure rates. Moreover, parameter estimation techniques were presented regarding each model parameterisation. Finally, this chapter gave a less detailed overview of other CCF parametric models suggested within the literature, and discussed the presented models in terms of three facets: data requirements, model properties and application.

In general, parametric models are black-box approaches to CCF modelling; CCF mechanisms are not represented explicitly, and the models are mostly characterised by their input, properties and output. The practical use of parametric models relates to a particular issue: the gap that exists between the data requirements of the models and the amount of available information on observed CCFs. This is mainly the reason that methods like the Beta Factor model constitute popular approaches: the simplicity of the model may lead to limited predictive capability, however it also entails limited data requirements. To this end, expert judgment is an essential source of information. The Unified Partial Method (UPM) has a practical advantage: having been initially quantified by experts, UPM can be applied by less knowledgeable analysts by simply calibrating the systems across a set of factors, and yields a beta factor characterising the system under study based on generic scores. The next chapter focuses on UPM. The framework of the methodology is presented, and its advantages and disadvantages are discussed.

Chapter 3

The Unified Partial Method for Common Cause Failure Modelling

3.1 Introduction

Chapter 1 presented the overall framework for the treatment of CCFs as performed in PRAs. In Chapter 2, the quantitative treatment of CCF events was described, and an overview was given of the main parametric models used within this context. The main models were presented in more detail, and others were briefly reviewed. The chapter concluded with a discussion of the parametric models suggested within the literature, which revealed the existing gap between data requirements of the models and data availability. Due to the nature of CCF events, a considerable amount of uncertainty is entered into the data analysis, resulting in expert judgment being an integral part of the process.

The aim of this chapter is to present the Unified Partial Method (UPM) [Brand and Gabbot, 1993] for CCF modelling, which constitutes the most frequently applied method for Common Cause Failure modelling in the UK [Smith, 2000]. UPM is a twofold methodology that employs the structures of the Partial Beta Factor method for component level analysis, and the Cut-Off method for system level analysis. It is a methodology that has been developed within the UK by the AEA Technology, and is an extension of the Rolls Royce and Associates Partial Beta Factor Model [Rolls Royce and Associates, 1986].

The popularity of UPM stems from the fact that it is a methodology which is applicable in cases where available data is particularly limited. By using generic scores and scoring tables, UPM yields a beta factor characterising the vulnerability of the system against CCF events. However, UPM is based on an additive weighting factors scheme. The implications of this feature are highlighted, and its conceptual appropriateness is explored. For this purpose, a connection is drawn between the UPM additive weighting factors scheme and the additive value function approach of Multiattribute Value Theory (MAVT).

This chapter is structured as follows: Sections 3.2 and 3.3 present the Partial Beta Factor (PBF) and the Reliability Cut-Off method respectively, which constitute the platforms on which UPM has been developed. Section 3.4 presents the UPM framework and Section 3.5 discusses its advantages and disadvantages. Section 3.6 explores the additive weighting scheme of UPM. Finally, Section 3.7 concludes the chapter.

3.2 Partial Beta Factor model

Like the Beta Factor model, the Partial Beta Factor (PBF) model has been developed for application at a component level. The model formulation defines a β-factor in an identical way as the ordinary Beta Factor model; that is, as the conditional probability that a specific component fails dependently, given that the component fails on demand or due to a shock. It furthermore assumes that the β-factor is decomposed to a number of partial β-factors (β_j, $j = 1,2,...$) that express contributions from different system features (subfactors). These features are related to design and operational aspects of the system, which are acknowledged as to be able to influence the occurrence of CCF events.

Within the literature, a number of Partial Beta Factor models have been suggested. Some of them determine the overall β-factor according to an additive scheme, whereas

Table 3.1: RRA model subfactors

Design	Operation	Environment
Separation	Procedures	Control
Similarity	Training	Tests
Complexity		
Analysis		

other use a multiplicative scheme [Ansell and Phillips, 1994]:

$$\text{Additive:} \quad \sum_j \beta_j$$

$$\text{Multiplicative:} \quad \prod_j \beta_j$$

The additive model has an advantage over the multiplicative one: the bigger the value that a subfactor receives, the more significant is the contribution to the overall β-factor. Therefore, the model allows the identification of the dominant contributors.

Rolls Royce and Associates (RRA) developed a refinement of the Partial Beta methodology, to result in a model for use with standard systems [Rolls Royce and Associates, 1986]. The RRA Partial Beta Factor model decreases the number of subfactors to eight (See Table 3.1). The methodology requires the analyst to make judgments, based on a set of standard criteria, and assign a level to each sub-factor. Each level corresponds to a score, and the overall β-factor is determined as a function of these scores. The scores used within the methodology are determined in such a way, so that the upper and lower limits of the overall β-factor agree with observations and generally accepted values.

The overall β-factor obtained from the Partial Beta Factor model is defined in exactly the same way as the ordinary β-factor. Thus, it is used in exactly the same way. However, it is worth mentioning that the two factors are estimated in a different way. In particular, the former is determined based on expert judgment, whereas the later is estimated based on observations.

3.3 Reliability Cut-Off

The Reliability Cut-Off method is a system level approach. It aims to assess the reliability of the target system, based on considerations of the vulnerability of the system as a whole, directly, without identifying the partial groups of components that are potentially subject to CCFs. The model yields a direct estimate of the system failure probability on demand for all failures, without distinguishing between dependent and independent ones, based on the assumption that the contribution of dependent failures dominates the result.

Table 3.2: Cut-Off features: + indicates that the particular feature decreases the potential for failure; - indicates that the particular feature increases the potential for failure.

System Features	Assessment
Redundancy/Diversity	+
Fail-safe design	+
Low failure rate technology	+
Unfamiliar/unreliable components	+
Difficult to test	-
Complexity	-
Need for human action	-

The philosophy behind the Cut-Off method is partially similar to this underlying the PBF model, in the sense that it requires the analyst to make assessments across a number of criteria related to particular features of the system [Bourne et al., 1981] (see Table 3.2). The main assumption underlying this methodology is that the unreliability of a system due to CCFs can never exceed some limiting values, determined by the system design. A list is provided of pre-assigned limiting failure probabilities to some specific basic categories of system designs.

The Cut-Off method is usually used when no adequate relevant field data is available. The estimation of the system Cut-Off does not involve system-specific data, but it rather provides a rough indicator of the overall system vulnerability.

3.4 Description of the Unified Partial Method (UPM)

The UPM framework [Brand and Gabbot, 1993] is a refinement and extension of the RRA model, integrating in a single methodology a system level and component level approach. The methodology is two-fold, producing either a Partial Beta factor or a Cut-Off, depending on the particular application. During the implementation of the methodology, the analyst decides which of the two methods to use, depending on the requirements of the reliability assessment and the data available.

As soon as the analyst has decided upon the physical boundaries of the system under investigation, s/he is encouraged to fill in a Pre-Analysis Table. The objective of this step is to identify the available data and the time to be spent on the analysis. At this point a judgement concerning the appropriate level of analysis has to be made, whether Cut-Off or a Beta factor will be used.

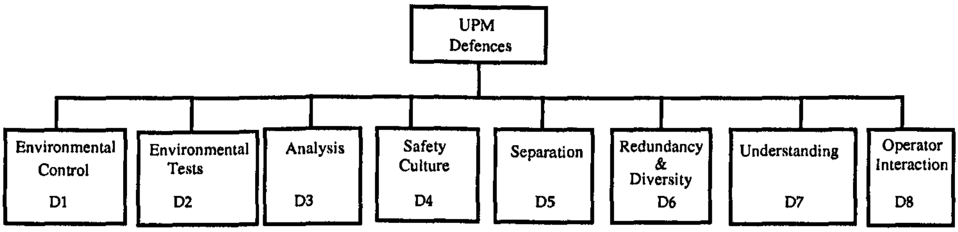


Figure 3.1: UPM subfactors

Regardless of the level of the analysis, at the next step the analyst is required to calibrate the system across a number of subfactors. These subfactors describe different elements of the defence of the system towards CCFs, and are related to design, operational and environmental aspects of the system. In total they count to eight (D_k, for $k = 1,...,8$)(Figure 3.1).

Each subfactor D_k takes one out of five possible levels x_k ($x_k \in \{1,..5\}$) corresponding to levels $A, B, ..., E$ respectively. The analyst decides the level that best describes the target system, by consulting a related table with a set of standard criteria. To each as-

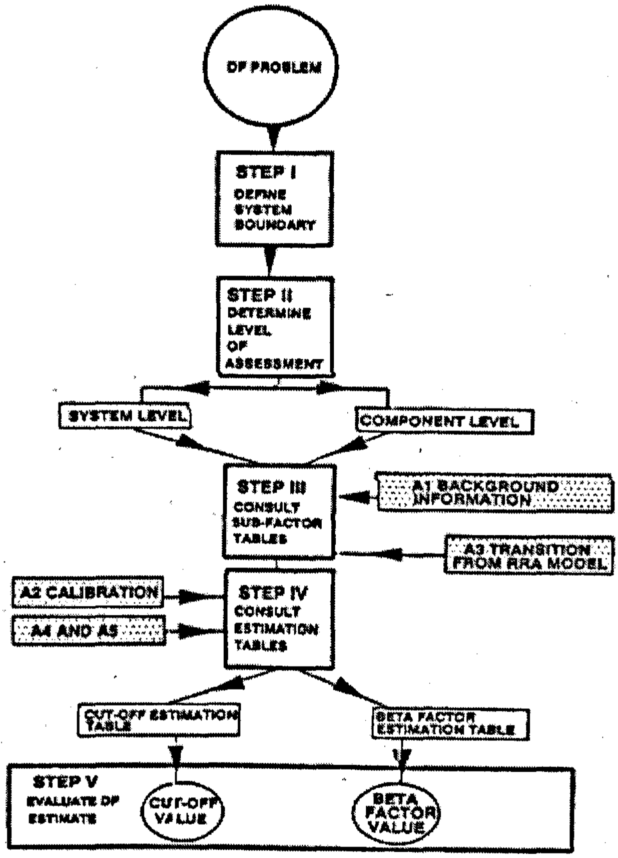


Figure 3.2: UPM structural framework taken from [Brand and Gabbot, 1993]

signed subfactor level corresponds a generic score $s_k(x_k)$, deduced from past research. Finally, the overall cut-off (Q) or partial beta factor (β), is obtained as a linear function of the scores, characterising the (sub)system under assessment:

$$\frac{s_1(x_1)+\ldots+s_8(x_8)}{d} \tag{3.1}$$

where $d \in \mathbb{R}^+$ is a scaling constant. Independently of the level of assessment, whether a beta factor or a cut-off is required, the analyst follows the same procedural steps. The only difference in the framework between the two assessment levels is the category-weighting scheme used, and therefore, the denominator in the linear model described in Relationship (3.1). The ranges of the two obtained estimates are $10^{-2} \leq Q \leq 10^{-6}$ and $0.302 \leq \beta \leq 0.00102$. An overview of the UPM structure is given in Figure 3.2.

The model structure is based on an exponential relationship between the level configuration and the contribution to the β-factor, based on the assumption that improvements on the defence of the system against CCF events become gradually more difficult.

Example Consider a system comprised of three identical components with 2oo3 success logic. The assessment is at a component level, therefore UPM is used to determine a Beta factor. The system is assessed across each sub-factor by consulting the appropriate tables, and categories are assigned accordingly. The classification of the system across each subfactor is decided based on expert judgment, and it is followed by a justification of the choice. The sub-factor categorisation is given in Table 3.3.

Table 3.3: System assessment across UPM subfactors

Sub-factor Judgment	**Sub-factor Category**	**Score**
Redundancy/Diversity	A	1750
Separation	B	580
Understanding	D	25
Analysis	D	25
Operator Interaction	D	40
Safety Culture	D	20
Environmental Control	C	100
Environmental Testing	D	15

The estimator for the β-factor is:

$$\hat{\beta} = \frac{1750+580+25+25+40+20+100+15}{50000} = 0.051 \qquad (3.2)$$

The obtained $\hat{\beta}$ is used in an identical way as the ordinary β factor (See Chapter 2, Section 2.3.3).

3.5 Discussion

At the moment, UPM constitutes the most widely used method within the UK nuclear industry towards the analysis of CCFs[1], and it owes its popularity to a number of distinctive features. In contrast to the other parametric models, UPM incorporates qualitative aspects of the system when assessing its defence level, such as information concerning operator interaction and other system-specific characteristics. During the application process of the model, the analyst gains insight into the potential for CCF events that may indicate possible modifications of the particular defences in order to increase system reliability. Therefore, UPM is a tool that supports the decision-making process.

Moreover, UPM offers a single systematic framework for both system level and component level assessments. It is a step-by-step methodology and its framework is accessible to a non-specialist analyst as well. The application of UPM is based on a standard guide, making it a recordable and reviewable methodology. Finally, the fact that the scoring of subfactor levels is based on a generic table of values allows the UPM Partial Beta to be used when there is limited availability of CCF data, whereas the UPM Cut-Off does not require any system-specific data for its application. However, the implementation of the Cut-Off method has been criticised [Ansell and Phillips, 1994, p.173]. It is argued that the intention of the development of the Cut-Off model has been to result in a tool used for indicative purposes, rather than as a methodology that yields a reliability estimator.

Despite the advantages of UPM, some weak features are identified. The weights used for the different defences were determined based on discussions with engineers [Humphreys, 1987], whereas the actual scores were deduced so that the overall beta-factor and Cut-Off were falling into particular ranges. The extensive use of expert judgment within UPM does not constitute a thorny issue; the nature of CCFs makes it necessary and inevitable. However, the use of expert judgment should be done within a well-documented and structured methodological framework. The output of UPM

[1] Reactor Nuclear Research Index 2005. Technical Area: Probabilistic Safety Analysis. Issue: PSA Methods. Issue Number 11.2. Open Technical Areas. Health and Safety Executive.

consists of a point value, representing the estimated beta factor. In view of the fact that this value has been determined based on expert judgment, the epistemic uncertainty inherent in this assessment is not captured by the model.

Moreover, changes in the design and operation of the system raise the issue of recalibration of the UPM generic scores. Another criticism that UPM has received is being a rather inflexible model, the set of possible model outcomes not being wide enough to correspond to the variation of systems.

UPM is based on the Beta Factor model; thereby, it shares the same fundamental assumptions. According to the Beta Factor model, redundancy is not a defence against failures and different system architectures are not distinguished[2]. Nevertheless, operating experience has proved the practical benefit of redundancy [Edwards and Watson, 1979]. On this basis, UPM defines redundancy in terms of a subfactor, in an attempt to adjust the output of the model in a conceptually consistent manner.

The additive weighting system that UPM uses for the determination of the overall β-factor leads to conceptual inconsistencies in the behaviour of the model. This issue will be further explored in the following section by making a connection between UPM and Multiattribute Value Theory (MAVT).

Finally, the attractive features of UPM have given rise to the development of the BetaPlus model [Smith, 2000]. The latter, based on the UPM form of the Partial Beta Factor model, is an attempt to incorporate a diagnostic coverage aspect. In view of the fact that dependent failures of components do not always occur simultaneously [Walls and Bendell, 1989], the detection and prevention of CCF events for standby systems is related to testing scheme characteristics. While maintaining the main features of UPM, along with the linear weighting of the system defences, the framework of the the BetaPlus model has been further extended to include a category that describes the diagnostic frequency and coverage of the system testing scheme. Other enhancements that the model includes are: a guide of questions to further assist the subjective classification of the system across the defence categories; a differentiation of the checklists and scoring for programmable and non-programmable systems; a recalibration of the

[2] See Chapter 2, Section 2.3.3

scores based on field data; and, a distinction between system defences that protect against failures that can be modulated by increased testing. Similarly to UPM, the construction of the BetaPlus model is largely dependent on expert judgment.

3.6 The UPM additive scheme

3.6.1 Multiattribute Value Theory

Multiattribute Value Theory (MAVT) is a modelling tool that supports the decision-making process. Given a decision problem in the general case, the decision-maker is free to choose from a number of alternatives/actions. For each course of action there is an effect, which has implications across multiple criteria. In the scope of MAVT, it is assumed that the effects/outcomes of each action are well defined, known to the decision-maker with certainty, prior to the choice of action. MAVT is concerned with the definition of a trade-off structure among the different outcomes that reflects the preferences of the decision-maker. A value function is defined, that assigns a value to each set of outcomes consistent with the preference statements of the decision maker. The definition of the preference relation and the value functions should comply with the axioms and conditions of MAVT.

3.6.2 UPM structure within a MAVT context

Within the framework of MAVT, in order to completely describe the outcomes of a specific course of action, each objective is broken down into a number of measurable qualities (attributes) and a hierarchy is formed. Similarly, within the UPM context multiple performance measures are used; the initial objective is the determination of the system's defence level (β-factor), which is broken down to eight different measurable contributions, the different subfactors (system defences) (see Figure 3.1).

When using UPM, the target system is assigned to one category x_k across each subfactor D_k $(k = 1, ..., 8)$, and scores are given accordingly. Thus, a system configuration can be described as a particular 'action', namely the act of accepting the system with these specific categories, that corresponds to the specific outcome of the resulting system configuration. In this fashion, a set of actions $\{b_1, b_2 ...\}$ is defined, where each action $b_i \in \{b_1, b_2 ...\}$ corresponds to an eight-attribute outcome vector $(x_{1i}, ..., x_{8i})$. In other words,

$$\underline{x_i} = (D_1(b_i), ..., D_8(b_i)) = (x_{1i}, ..., x_{8i}) \in V = X_1 \times ... \times X_8$$

where $X_k = \{1, ..., 5\}$ is the range of attribute $D_k(b_i)$, corresponding to the five subfactor levels $\{A, B, \ldots, E\}$.

The actions and attributes in the UPM structure form a matrix in which each row corresponds to an action and each column to an attribute (different performance measures). See Figure 3.3.

Attributes					
Acts	D_1	D_2	D_3	...	D_8
b_1	x_{11}	x_{21}	x_{31}		x_{81}
b_2	x_{12}	x_{22}	x_{32}		x_{82}
⋮	⋮	⋮	⋮	⋮	⋮

Figure 3.3: Acts and attributes in UPM

Definition of the preference structure Recall Relationship (3.1) which yields the estimated $\beta-$ factor for the target system; the formula may be re-written in the form

$$\beta(x_1, ..., x_8) = \sum_{k=1}^{8} \nu_k(x_k) \quad \text{where } \nu_k(\cdot) = \frac{s_k(\cdot)}{d} \tag{3.3}$$

UPM implies the existence of a preference structure as follows:

The smaller the beta factor obtained, the stronger the defence level of the assessed system towards CCFs, and, therefore, the more preferable the action yielding this outcome is

This preference structure can be expressed as a binary relationship $\succcurlyeq$ defined over the outcomes space $V = X_1 \times ... \times X_8$. Note that $\succcurlyeq$ is a negatively oriented relationship, since the lower scores are preferred.

Definition : If $\underline{x}, \underline{y} \in V$,

$$\underline{x} \succcurlyeq \underline{y} \Leftrightarrow -\beta(\underline{x}) \geq -\beta(\underline{y}) \Leftrightarrow \rho(\underline{x}) \geq \rho(\underline{y}) \tag{3.4}$$

where

$$\begin{aligned} \rho(\underline{x_i}) &= -\beta(\underline{x_i}) \\ \rho(\underline{x_i}) &= -\sum_{k=1}^{8} \nu_k(x_{ki}) = \sum_{k=1}^{8} u_k(x_{ki}) \\ u_k(x_{ki}) &= -\nu_k(x_{ki}) \end{aligned} \tag{3.5}$$

for $i \in \mathbb{Z}^+$, $k = 1, ..., 8$.

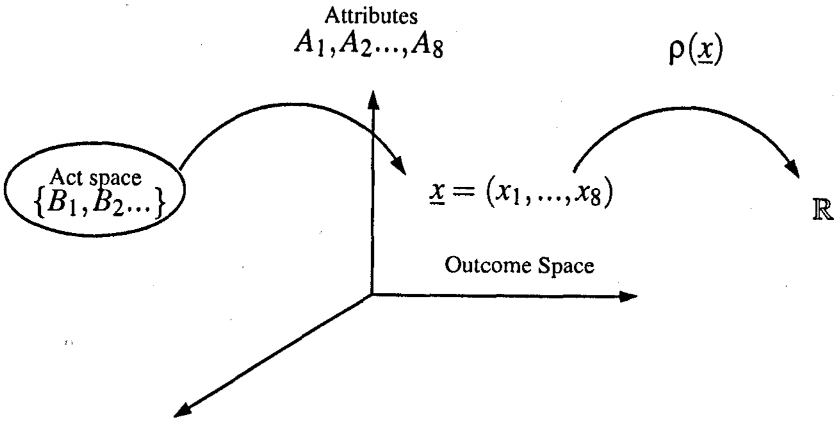


Figure 3.4: The mapping of acts

Relationship $\succcurlyeq$ represents a preference structure, as it obeys the axioms of comparability, transitivity, consistency of indifference and weak preference, and consistency of strict preference and weak preference. A relationship defined on a set for which the above axioms hold is known as a weak order; consequently, set V is a weakly ordered set [French, 1993].

Every element of the act space is mapped to an eight-dimensional outcome space, as equation (3.5) is a function $\rho : V = X_1 \times ... \times X_8 \rightarrow \mathbb{R}$, where $u_k : X_k \rightarrow \mathbb{R}$. See Figure 3.4.

So far, UPM' s preferences are expressed through a weak order $\succcurlyeq$ and a real-value function ρ is defined such that (3.4) holds. Then, we say that ρ is an ordinal value function representing $\succcurlyeq$. The properties below stem from the definitions and assumptions made so far:

1. The smaller the failure rate of an action, the more 'preferable' for a decision maker this action is: For $\underline{x}, \underline{y} \in V$,

$$\underline{x} \succcurlyeq \underline{y} \Leftrightarrow -\beta(\underline{x}) \geq -\beta(\underline{y}) \Leftrightarrow \rho(\underline{x}) \geq \rho(\underline{y})$$

2. (Marginal Orders over sets X_k, $k = 1, ..., 8$). The smaller the score of a category, the more 'preferable' to the decision maker this category is, since it results to a smaller value of β:

$$x_k \succcurlyeq y_k \Leftrightarrow v_k(x_k) \leq v_k(y_k) \Leftrightarrow u_k(x_k) \geq u_k(y_k), \quad k = 1, ..., 8$$

These properties imply that $\rho(\cdot)$ and u_k are monotonic functions[3]. Therefore, ρ is a value function that represents $\succcurlyeq$ and u_k are marginal value functions (single attribute functions) [French, 1993].

3.6.3 Additive form and mutual preferential independence

Equation (3.5) implies that ρ is an additive value function for the preference relation defined in (3.4). However, in MAVT the existence of an additive value function over

[3] If $\phi : X \rightarrow Y$ is monotonic, then for every $x_1, x_2 \in X, x_1 \leq x_2 \Leftrightarrow \phi(x_1) \leq \phi(x_2)$

the set requires that the attributes are *mutually preferentially independent*[4]. This statement says that every subset $Y \subset V$ of attributes is preferentially independent of its complementary set $Z = V - Y$. Or, in other words, the conditional preference structure of the subset Y does not depend on the level of the subset Z; therefore, the trade-offs between the attributes belonging to subset Y do not depend on the level of the attributes belonging to set Z [Keeney and Raiffa, 1976]. Mathematically expressed,

$$\begin{aligned}&\text{If } \underline{y'}, \underline{y''} \in Y,\\ &[(y', z')] \succcurlyeq [(y'', z')] \Rightarrow [(y', z'')] \succcurlyeq [(y'', z'')]\\ &\text{for all } z', z'' \in Z\end{aligned} \tag{3.6}$$

3.6.4 Preferential independence within the context of UPM

The form of the Multiattribute Value Function (3.5) used within the UPM framework makes the assumption of mutual preferential independence. Transferring this notion in the UPM framework implies that a given set of attributes influences the overall beta factor in a fixed way, regardless of the level of the rest of the attributes. However, this may not be conceptually consistent with the behaviour of the model. This inconsistency will be illustrated by considering three hypothetical cases:

Case I: In order to demonstrate this argument, we assume an assessment of a particular system. Typical categories $x'_1, x'_2, x'_5, x'_7, x'_8$ are chosen for all attributes except for Safety Culture (D_4), Redundancy/Diversity (D_6) and Analysis (D_3), which are kept fixed. Next, the preference structure in the subspace $Y = X_3 \times X_4 \times X_6$ will be examined. More precisely, what is going to be examined is the trade-offs between the sub-factors of Redundancy/Diversity and Safety Culture, when modifying the level of Analysis.

First, assume that the target system has been classified to a low category across

[4] Apart from the conditions of weak ordering and mutual preferential independence, there are other necessary conditions for the existence of an additive value. These are restricted solvability, the Archimedean and essentiality conditions (see [French, 1993]). Even though random variable x_{ki}, $k = 1, \ldots, 8$, $i \in \mathbb{Z}$ can take only five values (there are only five categories), we assume that it could be conceptually extended to a continuous random variable with the above conditions met.

the subfactor of Analysis (denoted with x_3^l)[5], to a low category across the subfactor of Redundancy/Diversity (denoted with x_6^l)[6], and to a high category across the subfactor of Safety Culture (denoted with x_4^h)[7]. Redundancy is considered to impact significantly on the defence level of the system; therefore, if the Safety Culture level drops to a low level (denoted with x_4^l), redundancy should significantly increase to a high level (denoted with x_6^h) for the defence of the system to stay at the same level. Mathematically expressed,

$$(x_3^l, x_4^h, x_6^l) \sim (x_3^l, x_4^l, x_6^h) \tag{3.7}$$

Assume now that the configuration of the system in terms of Analysis is high (denoted with x_3^h), meaning that previous analyses have taken place. In this case we can presume that the aspect of redundancy or diversity has been taken into consideration during the previous assessments, and the present design has been recognised as the one that functions better in case of a CCF event. Therefore, the impact of enhancing Redundancy/Diversity on the determination of the overall system defence should be smaller. Then, having a low level of Redundancy/Diversity and a high level of Safety Culture would yield a higher defence level (lower β-factor) than high Redundancy and low Safety Culture. In other words,

$$(x_3^h, x_4^h, x_6^l) \succ (x_3^h, x_4^l, x_6^h) \tag{3.8}$$

However, the UPM structure implies that the preference structure stays the same, regardless of the level of analysis, viz.

$$(x_3^h, x_4^h, x_6^l) \sim (x_3^h, x_4^l, x_6^h) \tag{3.9}$$

which contradicts the expectation about the behaviour of the model.

[5] Category *A* in the attribute of Analysis means that no formal safety assessment has taken place and that there is no design knowledge of dependent failure issues.

[6] Category *A* in the attribute of Redundancy means that there is simple redundancy (1oo2)

[7] Category *D* in the attribute of Safety Culture means that there is simulator training of normal operation AND there is dedicated staff and evidence of good safety culture including systematic training of emergency conditions.

Moreover, an additive value function implies from (3.7) and (3.9) that the range $u_6(x_6^h) - u_6(x_6^l)$ is constant; consequently, the weight of the subfactor of Redundancy/Diversity does not depend on the level of Analysis. This means that the trade-offs between a subset of subfactors do not depend on the categories that the rest of the subfactors have received, fact that is not coherent with intuitive expectations.

Case II : In a similar view, consider the subfactors (system defences) of Analysis D_3 and Understanding D_7; the latter describes the level of understanding of designers, operators and analysts in relation to the system, which depends on the level of technical complexity of the system and the amount of relevant experience on its operation. The impact of the amount of analysis in relation to dependent failures performed on the system design (level of Analysis) is expected to vary depending on the complex characteristics of the system: for a fairly simple and standard system extensive analysis does not strengthen its defence towards CCFs at the same level, as it would do for a comparatively complex and noble system.

Case III : Finally, consider the subfactors (system defences) of Understanding D_7 and Operator Interaction D_8. Let it be that, at a specific assessment, the attribute of Understanding receives a low level. This suggests that the level of understanding of designers, operators and analysts in relation to the system is low. In this case, the quality of the written procedures that are in place and the level of interaction between the operating staff and the system, which is described by the defence of Operator Interaction, should have a stronger impact to the overall system vulnerability towards CCFs, than it would have if the level of understanding of the system were high.

3.7 Conclusion

This chapter has presented the UPM method for CCFs. In particular, the framework of UPM was described, and its advantages and disadvantages were discussed. To be more precise, UPM is a tool that supports the decision-making process, while it requires a limited amount of data. This is a particularly valuable feature of the methodology, since the area of CCF data analysis has in principle a number of problematic issues that stem from the very nature of CCF events. Particular emphasis has been given on the additive weighting scheme of the system defences that UPM uses. It has been shown that the particular system leads to conceptual inconsistencies in the behaviour of the model. In order to argue this particular point, a theoretical connection has been drawn with MAVT, and three hypothetical practical examples were used for demonstration purposes.

In view of the fact that UPM has a number of practical advantages that lead to the popularity of the methodology within the scope of reliability analyses, this research aims to explore the possibilities for further development of UPM, by using alternative mathematical modelling techniques. The next chapter discusses the approach adopted within this context, for pursuing the particular objective and aims discussed in Chapter 1, and justified in Chapters 2 and 3.

Chapter 4

Foundational issues and Bayesian methodology

4.1 Introduction

The overall goal of this research is strongly associated with the assessment of risk posed on complex technological systems. Within this context, a Bayesian approach to risk has been taken. The purpose of this chapter is to justify the particular philosophical position, and within this context, argue and discuss the methodological choices adopted.

The Chapter is structured as follows: Section 4.2 describes the frequentist and subjectivist interpretations of probability, and argues the philosophical approach taken within this thesis; Section 4.3 gives a general overview of the Influence Diagram formalism, and argues the choice of the ID modelling technique for the purposes of this research

4.2 Research Philosophy

The research field that this thesis aims to contribute to is Probabilistic Risk Analysis (PRA). In the broad sense, risk analyses aim to assess the risk involved with the operation of systems. According to Kaplan and Garrick [Kaplan and Garrick, 1981], the term 'risk' involves the set of some scenarios, their likelihood to occur and their consequences. Therefore, measuring risk is tantamount to measuring uncertainty on events related to the system being studied. More specifically, PRAs aim to construct analytical models that produce quantified figures reflecting this uncertainty.

Within the scientific world, it is commonly accepted that probability theory offers a rigorous framework for quantifying uncertainty [Lindley, 2000]. Even though Kolmogorov's axioms of probability are widely accepted as the most appropriate axiomatic framework for uncertainty, within the field of PRA in particular, strong debate exists over the actual meaning of probability [Apostolakis, 1988; Winkler, 1996; Nilsen and Aven, 2003]. The most important interpretations of probability are the frequentist and subjectivist views. *This research adopts the Bayesian paradigm, which complies with the subjective view of probability.* The choice of a specific philosophical position towards probability has major methodological implications, since it defines the type of analysis and relevant data.

In general, the methodological choices made within the scope of a particular research reflect the way the researcher sees the world, and acts within it. Therefore, these choices are shaped through the positions regarding three questions: the ontological, the epistemological and the methodological question [Guba and Lincoln, 1994]. Within the next sections the frequentist and subjectivist views on these fundamental questions are described, and the philosophical position of this research is described.

4.2.1 Ontological Question - What is the form and nature of reality?

The essential difference between frequentists and Bayesians lies in their ontological position. The term ontology derives from the Greek word on (ον), which means being. There are fundamental differences in the assumptions made by the two approaches on the nature of reality and how this is reflected through probability calculus, and thus, through probabilistic models.

A model *sensu lato* is considered to be an approximate representation of reality, built in order to serve a specific purpose. As Pidd more formally defines,

> 'A model is an external and explicit representation of part of reality, as seen by the people who wish to use that model to understand, to change, to manage and to control that part of reality' [Pidd, 2003, p.12]

Within a narrower context, a PRA model aims to estimate the probability, which is a numerical measure of risk, and consequences of events related to a process or system under study [Siu and Kelly, 1998].

On the one hand, frequentists accept that reality exists objectively. Thus, probability as a measure of risk on a particular event is a natural characteristic of the world. According to a frequentist, a PRA model is built in order to predict the 'true', objective value of risk. This type of model uses probability to account for the natural variability of the system (aleatory uncertainty). Thus, aleatory uncertainty represents intrinsic randomness that exists in the natural world, independently of the analyst.

On the other hand, the Bayesian paradigm accepts a subjective (internal) interpretation of probability as a measure of risk. The foundations of subjective probability were placed by Ramsey [Ramsey, 1926], De Finetti [De Finetti, 1974, 1975] and Savage [Savage, 1954] who establishes a link between subjective probability and statistical decision theory. According to the subjective approach, probability is a degree of belief in the occurrence of an event attributed by a given person at a given instant and with a given set of information [De Finetti, 1974]. In this view, subjective probability is a mode of judgment that exists within the mind of the subjects and it is conditional on the knowledge and background information that exists at the point of the definition. Therefore, risk is not an objective characteristic of the system, existing in the real world independently of the analyst, and a risk model is *the analyst's attempt to represent a system in a form that it can be used as an explanatory and exploratory tool* [Parry, 1996, p.120].

4.2.2 Epistemological Question - What is the nature of the relationship between knowledge and the world?

The term epistemology derives from the Greek word episteme (επιστήμη), which for ancient Greeks equates to knowledge. Within the field of philosophy of science, epistemology refers to the process of knowledge acquisition and defines the relationship between the knower and what can be known.

The approach to learning for a frequentist is integrally related to the concept of relative frequencies. Probability is a characteristic of the world, and, in order to learn about this probability, one needs to perform a series of repeatable experiments (trials) in which this event occurs. The probability of the event is the relative frequency of the outcomes of these trials. By increasing the number of the experiments performed, the inference approaches the 'truth'; thus relative frequencies converge to the true values of the probabilities 'in the long run'. In other words, for a sequence of random variables $\{X_1, ..., X_n, ...\}$, for which $X_i = 1$ when an event is observed in a sequence of independent trials, and $X_i = 0$ otherwise

$$P(X=1) = \lim_{n \to \infty} \frac{X_1 + ... + X_n}{n}$$

In view of the fact that, according to frequentists, probability has a single 'true', yet unknown, value, the objective of frequentist epistemology is to produce an estimate of this value, which will be as close to the real value of the parameter as possible. Often, confidence intervals are constructed around the estimator, representing a level of acceptability for the estimation (for more information on the frequentist approach to learning see [Cox and Hindley, 1974]).

The Bayesian epistemological position defines a formal apparatus with two main elements: the first is compliance to the rules of probability as coherent constraints on degrees of belief, and the second is the introduction of the Principle of Conditionalisation, which is a rule of probabilistic inference [Talbott, 2001].

The grounds between conformity and subjective probability are based on the work of Ramsey [Ramsey, 1926] and De Finetti [De Finetti, 1974]. For a measure of uncertainty (degree of belief) to be coherent, it needs to satisfy the laws of probability. By drawing a connection between degrees of belief and individual betting odds, the argument of the *Dutch Book* is formed. A Dutch Book corresponds to a series of bets that result in definite loss. De Finetti has shown that, if a Dutch Book is avoided, the subjective probabilities derived by the individual odds are coherent [Loschi and Wechsler, 2002].

The Bayesian apparatus is a systematic mechanism for viewing the world. In particular, De Finetti's representation theorem offers a platform for constructing an individual's degree of belief regarding particular events. Consider an infinite sequence of random variables $\{X_1, ..., X_n, ...\}$, for which $X_i = 1$ when an event is observed in a sequence of trials, and $X_i = 0$ otherwise; $\{X_1, ..., X_n, ...\}$ is an *exchangeable* sequence of random variables if, for all finite sub-sequences of length n, the probability of the vector of outcomes is unaffected by their order, i.e.

$$P(X_1 = x_1, ..., X_n = x_n) = P(X_1 = x_{\pi(1)}, ..., X_n = x_{\pi(n)})$$

for all permutations π defined over the set $\{1, ..., n\}$ [Bernardo, 1996]. De Finetti' s representation theorem states that if $\{X_1, ..., X_n, ...\}$ is an infinite exchangeable sequence, then the limiting frequency

$$\lim_{n \to \infty} \frac{X_1 + ... + X_n}{n}$$

exists with probability 1, and there exists a probability measure μ supported on $[0, 1]$, for which

$$P(X_1 = x_1, ..., X_n = x_n) = \int_0^1 p^{\sum_i x_i}(1-p)^{n - \sum_i x_i} \mathrm{d}\mu(p)$$

Differently expressed, random variables $X_1, ..., X_n$ are conditionally independent and identically distributed, given p. The essence of De Finetti' s representation theorem is the following:

> '... if future outcomes are viewed as exchangeable, i.e., no pattern is viewed as any more or less likely than any other (with the same num-

> ber of successes), then when an event occurs with a certain frequency in an initial segment of the future, we must, if we are to be consistent, think it likely that that event will occur with approximately the same frequency in later trials...' [Zabell, 2006, pp. 6]

The acceptance of limiting frequencies within the Bayesian canon implies an element of 'objectivity', in the sense that, even though probability is defined as an individual's degree of belief, the probabilities of two different individuals will converge, if they are constructed over the same events [Bedford and Cooke, 2001]. It is interesting to note that 'in the long run' or 'for an infinite sequence of exchangeable events', the subjective probability of a Bayesian will converge to the limiting frequency of a frequentist.

The Principle of Conditionalisation, in epistemological terms, defines the effect of evidence on degrees of belief. It is a two-stage process: if one begins with initial (prior) probabilities, and then acquires an evidentiary statement, then rationality requires that one transforms the initial probabilities in the light of this evidence. The process of revising prior beliefs when new information is obtained is done in Bayesian statistics through Bayes Rule, to finally obtain a set of updated (posterior) beliefs. The Conditionalisation principle establishes an extension of deductive reasoning to include inductive syllogisms. Indeed, Bayes Rule establishes a 'stochastic dependence through an increase in information' [De Finetti, 1974] and defines what one is entitled to say about some future event by the virtue of having acquired relevant information.

4.2.3 Methodological Question - How may the researcher proceed to find what can be known?

The methodological question relates to the nature of data and how it is obtained. From a frequentist's point of view, a given parameter p is an objective characteristic of the system, representing a 'true' entity. Making inferences regarding p requires data to be acquired by observing this system, or by performing controlled experiments in a sufficiently identical to the system environment. Assuming that the data set $\underline{x}$ is generated by a sequence of independent trials from a given population, the likelihood function $f(\underline{x})$ of the data is the analyst's hypothesis for the statistical model of the data-generating process (random sampling from infinite population). As a corollary, parameter estimation for a frequentist restricts to empirical data. From a Bayesian's perspective, the data is a sub-sequence of an exchangeable infinite sequence; the likelihood function of the data $f(\underline{x} \mid p)$ reflects the analyst's degree of belief in the data taking certain values conditionally on certain values of the parameter p.

Whereas both the frequentists and Bayesians define a likelihood function that describes the data in hand, the Bayesian methodology introduces an additional ingredient. The Bayesian ontological thesis considers parameter p as random variable rather than an unknown fixed quantity. The additional ingredient is a probability distribution $f(p)$ assigned to p separately from the relevant data, that reflects the analyst's degree of belief on the values of the parameter, prior to observations (prior distribution). Inductive reasoning allows the analyst to update his/her prior knowledge in the light of relevant information through Bayes Theorem (Conditionalisation principle), to yield the posterior distribution $f(p \mid \underline{x})$:

$$f(p \mid \underline{x}) \propto f(\underline{x} \mid p) f(p)$$

In essence, '...A Bayesian who makes the exchangeability judgment is effectively making the same judgment about data as a frequentist, but with the addition of a probability specification for the parameter' [Lindley, 2000]. On this basis, the Bayesian apparatus allows for the expression of expert judgment through probability theory, which may be updated in the light of observations: the resulting posterior distribution which is an alloy of subjective information and empirical data.

4.2.4 Bayesian paradigm and CCF modelling

Type of uncertainty

In essence, the purpose of risk models is to quantify uncertainty. However, uncertainty may stem from different sources, and it can be therefore distinguished into different kinds. Most frequently, uncertainty is characterised as either aleatory or epistemic [Parry, 1996; Winkler, 1996; Hora, 1996; Bedford and Cooke, 2001]. Aleatory uncertainty results from an inherent variation in the behaviour of a system. Epistemic uncertainty stems from lack of knowledge about the behaviour of a system. Since epistemic uncertainty is defined in a subjective dimension, it can be quantified and further reduced by knowledge of experts. However, even though aleatory uncertainty can be quantified by expert knowledge, it cannot be reduced [Hora, 1996]. Due to this practical difference, distinguishing the type of uncertainty is significant and it constitutes an important part of the modelling process.

Within the literature it is suggested that distinguishing the type of uncertainty does not have a physical dimension [Hora, 1996; Bedford and Cooke, 2001]. Instead, the distinction between aleatory and epistemic occurs for practical, quantification reasons. To this end, uncertainty is characterised in a certain way for the purposes of the particular model; the 'same' uncertainty may be characterised differently in different models with different purposes [Hora, 1996]. Separating aleatory and epistemic uncertainty is useful in clarifying the modelling choices and in determining the quantification process. Moreover, the distinction facilitates the communication between experts, decision-makers and analysts.

As described in Section 1.4.4, the intention of the ID model is to represent the influence of the defence characteristics of the system on its failure behaviour, which is being represented by coupling probabilities and failure rates. More particularly, the intention is to capture the uncertainty on the model parameters, and propagate this uncertainty within the model structure.

When the defence variables of the ID model take particular levels, the coupling probabilities and failure rates describe the failure behaviour of the system with the particular defence configuration. However, given the possible combinations of defence levels, it is possible for certain defence configurations to correspond to fictitious systems. Therefore, the definition of an infinite or large enough population is not always obvious. Within this context, uncertainty cannot result from the inherent heterogeneity in a population, and the concept of aleatory uncertainty cannot be adopted. From a theoretical standpoint, the uncertainty on the model parameters within this context is characterised as epistemic.

From a Bayesian point of view, all uncertainty is characterised as epistemic [Nilsen and Aven, 2003]; to this end, this research adopts the ontological, epistemological and methodological thesis of the Bayesian paradigm in order to capture the uncertainty on the model parameters. Within this context, risk is not viewed as an objective characteristic of the system, which corresponds to a particular population. The ID model is the analyst's attempt to represent a system and use it as an explanatory and exploratory tool. The model, therefore, is a simplified representation of the world and it is based on the available to the analyst information and resources [Apeland et al., 2002]; and the uncertainty represented by the model is associated with the analyst's confidence in the model predictions.

Expert Judgment and CCF modelling

The Bayesian paradigm constitutes a systematic framework for axiomatically expressing expert judgment. As mentioned previously, epistemic uncertainty stems from lack of knowledge, and knowledge regarding an event alters when additional or more complete information is attained. The ability to scientifically elicit expert uncertainty in terms of probabilities, combined with the Bayesian methodology, offers a mechanism for capturing the effect of observations on the uncertainty. Being able to coherently combine subjective (expert judgment) and objective (observations) information is particularly useful within the CCF modelling context, where, due to the rare and complex nature of CCF events, data is sparse and incomplete.

In general, PRA is one of the pioneering sciences that introduced the quantification of expert opinion, and that has the most experience in this field. Even though the frequentist approach to risk is the traditional position adopted within reliability analysis, the Bayesian approach started to emerge over the last thirty years [Apostolakis, 1988]. The reason is that PRA models often deal with the assessment of risks that are associated with rare events, or hypothetical scenarios, or with situations where actual observations are insufficient for model quantification. Therefore, expert judgment becomes an essential source of information.

One of the first applications of lies in the nuclear field, where subjective probabilities where used in the Reactor Safety Study Wash 1400 [Apostolakis 1988 and references therein], albeit in an unstructured way. This fact raised a lot of criticism and led to a formal review of the methodology, which identified a considerable number of deficiencies, but at the same time acknowledged that the use of subjective probabilities is necessary and provides a reasonable input, once it is done in a structured way. This argument formed the basis for the justifiable use of expert judgment within the framework of 'hard sciences', such as reliability analysis.

4.3 Modelling Technique

As stated at the beginning of the thesis, the purpose of this research is to *explore the application of advanced modelling techniques within the framework of UPM, so as to result in a model with a structural and exploratory character, that allows for the representation of epistemic uncertainty and supports the decision-making process.* The modelling technique employed to pursue this purpose is the Influence Diagram (ID) formalism, which is supported by the Bayesian methodology.

Recently, Bayesian Belief Networks (BBNs) and Influence Diagrams (IDs) have found numerous applications within the context of system reliability modelling. General examples include software reliability, maintenance modelling, general reliability modelling of complex systems ([Sigurdsson et al., 2001; Langseth and Portinale, 2005] and references therein). Moreover, BBNs have had real applications in problems of assessment of critical systems [Fenton and Neil, 2004], [Fenton and Neil, 2001].

The BBN formalism has been suggested as a suitable methodology to represent dependencies amongst components in complex systems. The interchangeable use of traditional Fault Trees and BBNs has been studied, and a technique is suggested to map the former to the latter [Bobbio et al., 2001]. The use of BBNs as a more natural environment for modelling dependent failures, such as CCFs, has been also studied in [Toledano and Sucar, 1998], by comparing BBNs to reliability block diagrams. Moreover, Vatn [Vatn, 1997] explores the use of IDs to model the relationships between maintenance actions, system characteristics and preferences.

Lately, the interest for the BBN formalism has been growing in the nuclear area, in particular. In [Celeux et al., 2006] the use of a BBN is considered to model the degradation process of a mechanical system, by using an illustrative example of a reactor coolant sub-component, in order to determine the optimal maintenance strategy. In [Duftoy et al., 2006] the implementation of a BBN for modelling the availability of the cold source system of a nuclear power plant is explored.

Other areas of application include the aerospace safety. In [Kardes and Luxhøj, 2005] a BBN is constructed to evaluate the impact of safety products to maintenance-related aircraft accidents. Their model is a BBN, extended to include decision variables to represent the safety enhancement products. Other examples may be found in [Sachon and Paté-Cornell, 2000] and [Anders et al., 2005].

4.3.1 Influence Diagrams

The model developed within the scope of this research aims to provide a platform for assessing and comparing defence characteristics of the system in terms of the risk involved in relation to CCF events, and support decision-making processes. IDs are extended BBNs [Pearl, 1988] that include decision and value nodes, and allow the representation and comparison of alternative actions and the determination of strategies regarding the decisions involved.

Supported by the Bayesian paradigm, IDs are based on axioms of probability and utility. On the one hand, probability theory provides a coherent framework for representing uncertain relationships, and allows for the representation of human expert knowledge. On the other hand, utility theory offers an axiomatic structure for modelling consequences or outcomes, and the preference relationships for these. In essence, an ID model is a graphical knowledge representation of a decision problem, which allows for reasoning under uncertainty by combining both expert knowledge and quantitative data. Some literature on IDs is given in [Howard, 1990; Matheson, 1990; Lauritzen, 1996; Jensen, 1999].

4.3.2 ID terminology

Like BBNs, an ID model consists of two parts: a qualitative and a quantitative part. The ID model is comprised of a directed acyclic graph (ID network) that displays the decision problem. The graph consists of a set of nodes representing the main features of the problem, and arcs signifying the existence of influence or relevance amongst these features.

The elements of a decision problem fall within three different categories [Morgan and Henrion, 1990]:

Decision variables, represented by square nodes. A decision variable represents a set of alternatives that are available to the decision maker. These variables are under the direct control of the decision maker, thus they are not associated with expressions of uncertainty;

Chance variables, represented by oval nodes. A chance variable represents quantities of the problem that are uncertain. A probability function is associated with each chance variable; this probability function is a set of conditional probabilities describing the strength of the dependency relationship existing between the given variable and the variables that influence it directly (parent variables);

Deterministic variables, represented by double circular nodes. These variables represent deterministic functions of chance or decision variables;

Value variables, represented by diamond nodes. These variables represent the preferences or utilities of the decision maker. In principle, each ID model has one value node.

The arcs of an ID network fall within two categories:

Information arcs, that are directed into decision nodes. Information arcs represent information flow, indicating the type of information that is available at the stage a particular decision needs to be made; and

Influence arcs, that are directed into chance nodes. The absence of an arc between two chance nodes implies that there is no direct influence between the two variables, more precisely, that they are conditionally independent given their parents. The arc from a decision node to a chance node implies that the decision affects the corresponding chance node.

Suppose that two nodes are linked with an arc; the node in which the arc feeds into is called a descendant V, whereas the influencing node (starting point of the arc) is called a parent node, and denoted with Π_V

The network of an ID (or BBN) model portrays the qualitative relationships between the variables of the domain. In particular, the lack of an influence arc between two variables is an expression of probabilistic independence.

Each chance and decision node V is associated a state space $s(V)$; for the chance nodes, $s(V)$ represents the range of possible outcomes outcomes, and for the decision variables, $s(V)$ represents the range of possible options. The uncertainty associated with each chance node is represented by a conditional probability distribution $f(V \mid \Pi_V)$, where Π_V are the parent-nodes of variable V. In principle, value nodes have no descendants.

Like BBNs, an ID uses the conditional probabilistic independencies existing between the variables, so as to decompose the joint probability distribution on a set of variables, and offer a more concise representation. For the simple belief network in Figure (4.1), the joint probability distribution on the model variables is specified as:

$$P(X,Y,Z) = P(X \mid Z)P(Y \mid Z)P(Z)$$

In essence IDs are comprised by two parts: a qualitative part (ID network), and a quantitative part, which relates to the probabilistic configuration of the model.

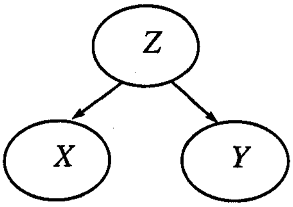


Figure 4.1: Expressions of conditional independence: Variable Z, having no predecessors, is marginally independent. Variable X is conditionally independent of Y, given the common predecessor Z

4.3.3 ID formalism and CCF modelling

In a nutshell, the ID modelling technique has been judged as appropriate for the purposes of this research for the following reasons.

Firstly, this research attempts to extend UPM by representing uncertainty on the model output. IDs are tools for reasoning under uncertainty that are based on the Bayesian canon. Therefore, they allow for the representation of epistemic uncertainty on the elements of the model in terms of probability distributions. Moreover, epistemic uncertainty is coherently propagated through the network to yield an uncertainty distribution on the model output.

Secondly, underlying the ID formalism is the Bayesian methodology. The use of Bayes' theorem is a mechanism for updating expert judgment in the light of observations, to yield coherent posterior probabilities. This information is transmitted through the network of the ID model, to become relevant to events for which observations are not available. This is a key feature of IDs for modelling CCFs in particular, where observations are limited.

Thirdly, this research attempts to extend UPM by developing a model that incorporates root cause and coupling factor taxonomies in its structure. IDs are networks that portray the existing relationships in the problem domain, and give a graphical representation of the influences amongst the system defences, the root cause failure events and the coupling characteristics of the system. The ID formalism allows for a more detailed modelling of CCF events, as it captures the types of CCFs that each defence is able to modulate.

Moreover, IDs allow for the modelling of the existing interactions amongst system defences in the way they impact on the overall system vulnerability towards CCFs, which UPM in its current form fails to do. Finally, IDs permit the effects of interventions to be explored, and what-if analysis to be performed. This structure allows the influence of different defence alternatives on the other variables, and ultimately on the CCF rate, to be monitored, and supports the decision-making process.

4.4 Conclusion

The purpose of this chapter was to outline and clearly justify the methodological approach adopted for the purposes of the particular research. This research adopts a Bayesian view to probability and risk. This chapter described both the frequentist and the Bayesian ontology, epistemology and methodology, and, argued the reasons for choosing the Bayesian apparatus as the most appropriate for accomplishing the purposes of the research. In brief, the key points that justify such a choice are: the axiomatic use of expert judgment, the representation of epistemic uncertainty on the model elements, and the ability to coherently combine subjective opinion with empirical data.

Finally, the choice of the Influence Diagram formalism as the modelling approach adopted was argued. In particular, IDs are based on the Bayesian canon. Moreover, IDs offer a graphical representation of the existing relationships in the modelling domain, allow for the propagation of uncertainty within the model structure, and succeed in modelling the CCF mechanisms at a finer level of detail.

The next chapter introduces the ID model constructed for the purposes of this thesis.

Chapter 5

Theoretical structure of the Influence Diagram Model

5.1 Introduction

In this chapter the theoretical foundations of the Influence Diagram (ID) model for CCF modelling will be presented. To be more precise, the model variables are defined both qualitatively and mathematically. As discussed in Chapter 2, parametric models such as the Multiple Greek Letter model and the Multiple Beta Factor model generalise the simplest Beta Factor model by distinguishing between different levels of failure multiplicities. The UPM model generalises the Beta Factor model in a different direction, by modelling the impact of design, operational and environmental aspects of the system on the CCF measure.

Chapter 4 proposed the development of an ID model. The focus of this chapter is to give the foundations of the ID model. In particular, the present chapter is structured as follows: Section 5.2 illustrates the approach taken for the identification of the ID variables, and describes them both qualitatively and mathematically. The dimensions of the ID variables are initially defined in a general manner; the particular example of EDGs is considered afterwards in Section 5.3. Finally, Section 5.4 concludes the chapter.

5.2 Identification of ID variables

CCF events are defined as the result of two distinct factors: the occurrence of a root cause of failure, that challenges the susceptibility of the components and renders them functionally unavailable, and the existence of a coupling mechanism, that propagates the failure amongst components and compels them to fail dependently rather than independently, [Mosleh et al., 1998c] (Figure 5.1). Research has shown that, in essence, CCF root causes are no different than independent component failure causes [Edwards and Watson, 1979; Fleming et al., 1983]; the additional element, which leads to dependent failures, is the existence of coupling conditions amongst the redundant components [Paula, 1995].

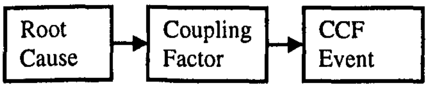


Figure 5.1: CCF definition

On this basis, a defence strategy against CCFs may be separated in three tactics: First, defence actions can be taken aiming to reduce the frequency of the root cause events. This will automatically lead to improved reliability of each component comprising the system in general, without necessarily enhancing the defence of the system towards CCF events in particular. Second, defence actions can be taken against coupling factors. In this case, the objective is to reduce the coupling effect. These actions weaken the conditions that result in multiple failures, without necessarily enhancing the reliability of each component. Third, defence actions can be taken against both root causes and coupling factors.

Based on the above, we can argue that the important elements of the CCF application are: the root causes being the main reason for CCFs, the coupling factors creating the conditions for CCFs to occur, the defence actions taken against CCFs, and a chosen reliability measure. These elements form the problem domain, and need to be expressed in terms of ID variables. The network of the ID model will portray relationships of two types. The first type is the cause-effect relationship between the root causes alongside coupling factors and the CCF performance measure. The second type is the impact of the defence actions to either the root causes, either the coupling factors, or both. What follows is a description of each of the categories of the ID variables.

5.2.1 Defence variables

The first category of variables concerns the defence actions taken against the occurrence of CCF events. These may be described in terms of particular defence factors; these factors are related to operational, design and environmental aspects of the system, and are acknowledged as to be able to influence the occurrence of CCF events. The defence characteristics of a system may be described by ascribing to the system a particular level across each defence factor.

The user of the ID model (assessor) assigns the level that best describes the system across each defence factor. The defence level that a system takes can be controlled and modified; therefore the defence factors are deterministic variables, representing the different decision alternatives.

Let the defence factors be represented by variables D_k $(k = 1,2,...,m)$ and let x_k be the level that defence D_k takes, where $x_k = 1,2,...,m_k$. The defence variables represent a set of mutually exclusive and collectively exhaustive alternatives.

5.2.2 Root Cause variables

The second category of variables concerns the root causes, which describe the basic reasons of failure. The root cause is defined as the most basic reason for components' failure, the most readily identifiable cause [Edwards and Watson, 1979]. Consider a system that operates on demand; suppose that the system is challenged and that a failure is detected. This failure event (dependent or independent) may be attributed to one basic reason, one particular root cause. Within the ID framework this basic reason is described by a root cause category. Equivalently, it is assumed that the root cause categories form mutually exclusive and collectively exhaustive sets of events.

Let T_i be the notional time to failure considered from the moment the system was last activated until a dormant failure due to root cause i occurs ($i = 1, ..., \rho$), that would be observed if all other causes of failure were suppressed. Each failure cause i is assumed to have an exponential distribution for its time of occurrence T_i, viz.

$$f_i(t) = r_i e^{-r_i t}$$

It is assumed that $\{T_i\}$ are mutually independent random variables, given r_i. It is further assumed that in case of a failure, the failed component goes into repair mode and it gets fully restored to its original state, with 'zero' repair time. This means that the mean repair time is assumed to be small compared to the minimum of the mean times of root causes occurrences. The assumption of a homogeneous Poisson process is typical in reliability analyses [Cooke and Bedford, 2002]. Consistently with this assumption, the number of failure events due to root cause i occurs according to Poisson distribution with parameter $r_i T_{obs}$. Failures due to different causes are assumed to occur according to independent Poisson processes.

The rate of failure events occurring to a system that is attributed to a specific root cause is influenced by certain design, environmental and operational characteristics of the system. Abiding by the Bayesian viewpoint, the interest lies in incorporating uncertainty on the value of the rates r_i, stemming from incomplete knowledge of the system (epistemic uncertainty) and of the mechanics of CCF events. In this vein, the root cause rates r_i are uncertain quantities, being represented by chance nodes. Influence arcs from the defence nodes D_k to the root cause nodes r_i signify various defence tactics that the system employs.

Bayesian Inference

Suppose that, during fixed observation time T_{obs}, n_i failure events have been observed, attributed to root cause i. The likelihood function of the data is a Poisson distribution, viz.

$$f(n_i \mid r_i) = \frac{(r_i T_{obs})^{n_i}}{n_i!} e^{-r_i T_{obs}}$$

The uncertainty on r_i, before having observed any failures, is modelled by a prior distribution with p.d.f. $f(r_i)$. A natural choice for $f(r_i)$ is the gamma family of distributions, which is conjugate with the Poisson family. The posterior uncertainty on r_i, in the light of data (n_i, T_{obs}), is by Bayes' law:

$$f(r_i \mid n_i) \propto f(n_i \mid r_i) f(r_i)$$

which is again a gamma distribution.

Suppose that failure data is obtained coming from n different sources, in the form of (n_i^k, T_{obs}), where n_i^k is the number of observed failure events due to root cause i during fixed observation time T_{obs}^k, $k = 1,...,n$. Information from different sources may be combined, and Bayesian inference on r_i is based on the total number of failures $n_i = \sum_{k=1}^{n} n_i^k$ during the total observation time $T_{obs} = \sum_{k=1}^{n} T_{obs}^k$ [Vesely, 1977; Barlow and Proschan, 1986].

Under the model that failures occur according to a homogeneous Poisson process, the gamma family of distributions is a standard choice for modelling uncertainty on failure rates within reliability analyses [Cooke and Bedford, 2002]. The reason for this choice is that, because of the conjugate properties of the gamma and Poisson family of distributions, subsequent analysis is simplified considerably.

5.2.3 Coupling Factor variables

The third category of variables concerns the coupling mechanisms. The concept of coupling mechanism refers to common characteristics of the redundant component; these shared similarities make the redundant components susceptible to the same root cause, and, create the conditions for multiple dependent failures to occur. Within the ID framework it is assumed that a CCF event may be propagated via one only coupling factor category. Equivalently, it is assumed that, given a failure of a certain type, the coupling categories form mutually exclusive and collectively exhaustive sets of events.

Suppose that a failure event occurs to a system that operates on demand due to root cause (rc) i; let p_i be the probability that this event results to a CCF event, viz.

$$p_i = P(\text{CCF event} \mid \text{failure event due to rc } i) \tag{5.1}$$

The probability that the event remains an independent event is

$$q_i = P(\text{independent event} \mid \text{failure event due to rc } i) \tag{5.2}$$

and $q_i = 1 - p_i$.

Denote with p_{ij} the probability that a failure is propagated to all components in the system (CCF event) through coupling factor (cf) j ($j = 1, \ldots, \kappa$), given that a failure occurs due to root cause (rc) $i = 1, \ldots, \rho$. Then

$$\begin{aligned} p_i &= P(\text{CCF} \mid \text{failure due to rc } i) \\ &= \sum_{j=1}^{\kappa} P(\text{CCF through cf }_j \mid \text{failure due to rc } i) \\ &= \sum_{j=1}^{\kappa} p_{ij} \end{aligned}$$

Moreover, from $p_i + q_i = 1$ we have

$$\sum_{j=1}^{3} p_{ij} + q_i = 1 \tag{5.3}$$

The intensity of coupling factor j is described by a vector of parameters

$$\underline{p}_j = (p_{1j}, \ldots p_{\rho j})$$

where

$$p_{ij} = P(\text{CCF through cf } j \mid \text{failure due to rc }_i)$$

Similarly to the root causes, the coupling factor conditions existing in a system are influenced by certain design, environmental and operational characteristics of the system. Therefore probabilities p_{ij} are subject to uncertainty stemming from incomplete knowledge of the system and of the CCF mechanisms (epistemic uncertainty). To this end, coupling probabilities p_{ij} are uncertain quantities, and are represented in the model by chance nodes. Influence arcs from the defence nodes to the coupling factor nodes signify various defence tactics employed by the system.

Bayesian Inference

Suppose that, for a particular system of components, failure data is recorded of the form:

$$\underline{n_i} = (n_{i0}, n_{i1}, n_{i2}, \ldots, n_{i\kappa}) \tag{5.4}$$

where n_{ij} is the number of dependent failures due to root cause i and through coupling factor j, for $j = 1, 2, \ldots, \kappa$ and n_{i0} is the number of independent failures due to root cause i. The joint likelihood function of the data is a multinomial distribution with parameters

$\underline{p_i} = (p_{i0}, p_{i1}, p_{i2}, \ldots, p_{i\kappa})$, where $p_{i0} = q_i$, viz.

$$f(\underline{n_i} \mid \underline{p}) \propto \prod_{j=0}^{\kappa} p_{ij}^{n_{ij}}$$

The conjugate prior for parameter $\underline{p_i} = (p_{i0}, p_{i1}, p_{i2}, \ldots, p_{i\kappa})$ is a Dirichlet distribution, which is the multinomial counterpart of the beta distribution. Let the parameters of the Dirichlet distributions be $\underline{\alpha_i} = (\alpha_{i0}, \alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{i\kappa})$, viz.

$$f(p_{i0}, p_{i1}, p_{i2}, \ldots, p_{i\kappa}) = \frac{\Gamma(\sum_{j=0}^{\kappa} \alpha_{ij})}{\prod_{j=0}^{\kappa} \Gamma(\alpha_{ij})} \prod_{j=0}^{\kappa} p_{ij}^{\alpha_{ij}-1}$$

The means and covariances for parameters p_{ij}, $j = 1, 2, \ldots, \kappa$, are given by [Johnson and Kotz, 1972]:

$$E(p_{ij} \mid \underline{\alpha_i}) = \frac{\alpha_{ij}}{\alpha} \tag{5.5}$$

$$Cov(p_{ik}, p_{il}) = \frac{1}{\alpha+1} \left(\frac{\alpha_{ik}}{\alpha} (\delta_{kl} - \frac{\alpha_{ik}}{\alpha}) \right) \tag{5.6}$$

where $\alpha = \sum_{j=1}^{\kappa} \alpha_{ij}$ and δ_{kl} is the Kronecker delta ($\delta_{kl} = 0$ if $k = l$ and $\delta_{kl} = 1$ otherwise).

Generally, dependent failures are rare events, implying that

$$\sum_{j=1}^{\kappa} p_{ij} << q_i \Rightarrow \sum_{j=1}^{\kappa} p_{ij} << 1 \tag{5.7}$$

Consistently with 5.7, it holds that

$$\sum_{j=1}^{\kappa} E(p_{ij}) << 1 \tag{5.8}$$

which implies that

$$E(p_{ij}) << 1 \Rightarrow \frac{\alpha_{ij}}{\alpha} << 1, \quad \text{for every } j = 1,2,3 \tag{5.9}$$

Based on Relationship (5.6), it follows that

$$Cov(p_{il}, p_{ik}) = -\frac{1}{\alpha+1}\left(\frac{\alpha_{ik}}{\alpha}\frac{\alpha_{ik}}{\alpha}\right) << 1 \quad \text{for } k \neq l$$

implying a weak degree of correlation amongst variables p_{ij}, for $j = 1,2,3$. Therefore, assuming independence of parameters p_{i1}, p_{i2}, p_{i3} constitutes a reasonable approximation. Assumptions of local independence are often employed within the Bayesian methodology [Spiegelhalter and Lauritzen, 1990] to serve as a considerable simplification.

Hence, parameters $p_{i1}, p_{i2}, \ldots, p_{i\kappa}$ may be individually parametrised and updated. The beta family of distributions is used for modelling prior uncertainty on p_{ij}, denoted with $f(p_{ij})$, which shall be updated with data n_{ij}. Within this framework, observed data n_{ij} is assumed to be generated from a binomial distribution with probability p_{ij}, viz.

$$f(n_{ij}, n_i \mid p_{ij}) \propto p_{ij}^{n_{ij}}(1-p_{ij})^{n_i - n_{ij}}, \quad \text{where } n_i = \sum_{j=0}^{\kappa} n_{ij}$$

The posterior distribution $f(p_{ij} \mid n_i)$ is

$$f(p_{ij} \mid n_{ij}, n_i) \propto f(n_{ij}, n_i \mid p_{ij}) f(p_{ij})$$

which is also a beta distribution. When data is obtained from different sources, information may be combined by basing inference on sums of failures of a particular type from different systems.

In principle, any distribution over the interval $[0,1]$ can be used to model uncertainty on probability p_{ij}. Under the model that failures form a Bernoulli process, with probability of success p_{ij}, the beta family of distributions is a standard choice for representing uncertainty on p_{ij} [O'Hagan and Forster, 2004]. The reason lies again on the conjugate properties of the beta and binomial families of distributions, which simplify subsequent analysis.

5.2.4 ID performance measure

This research focuses on systems that are on standby; these systems are idle for a period of time and are only challenged to deliver their intended function periodically, in the case of a true demand or within the context of a testing scheme. As described in Section 2.2.2, a postulated failure of a standby system is classified into two categories: failure revealed by the demand and failure caused by the demand. The ID model built within the scope of this research aims to capture CCF events that belong in the first category; in other words, it aims to capture dependent failures of all components of the system that occurred during its idle period, and rendered it unavailable to operate when challenged.

The main assumption underlying most CCF models is that failures occur according to a Poison process with a constant failure rate [Marshall and Olkin, 1967; Vesely, 1977; Apostolakis and Moieni, 1987]. The Homogeneous Poisson Process model is considered appropriate for the particular purposes for a number of reasons. First, CCFs are rare events and, hence, the rates are not driven by factors such as the aging of the component. Second, the effect of seasonality is considered insignificant; in other words, environmental conditions and other factors related to seasonal effects do not influence the occurrence of CCF events. For CCF events revealed by the demand in particular, it is assumed that the events occur at continuous time during the idle period of the system [Vaurio, 1994b]. On this basis, it is of interest to determine the rate at which CCF events occur within the system, and, more specifically, the output of the ID is chosen to be *the rate of CCF events per unit of time occurring within the system while it is on standby.*

Suppose that failures due to root cause i, where $i = 1,...,\rho$, occur according to a Poisson distribution with parameter r_i. The failure is either an independent failure with probability q_i, or it is propagated to the other components via coupling factor j with probability p_{ij}, where $j = 1,2,...,\kappa$ (Relationship (5.3)). By assuming that probabilities q_i, p_{ij} do not change over time, the overall Poisson process is split into four sub-processes. These sub-processes can be treated as independent Poisson processes. In particular, CCF events occur via coupling factor j and due to root cause i according to a Poisson process with parameter λ_{ij}, where

$$\lambda_{ij} = p_{ij} r_i \tag{5.10}$$

and, independent failures due to root cause i occur according to a Poisson process with parameter λ_{i0}, where

$$\lambda_{i0} = q_i r_i \tag{5.11}$$

Within this set-up, it is assumed that CCF events due to a particular root cause and through the different coupling factors occur according to independent Poisson processes. Therefore, the overall process of CCF events attributed to root cause i, without distinguishing the coupling factor, is a superposition of the independent Poisson processes with rates λ_{ij}, $j = 1,2,...,\kappa$. The rate of the superimposed process is λ_i, where

$$\lambda_i = \sum_{j=1}^{\kappa} p_{ij} r_i = p_i r_i \tag{5.12}$$

Relationship (5.12) implies that the rate of CCF events attributed to root cause i is obtained through the total (both independent and dependent) failure rate due to root cause i, filtered through the coupling factor intensities p_{ij}.

Under the assumption that the root cause categories define mutually exclusive and collectively exhaustive events, the Poisson process of CCFs is a superposition of the root cause Poisson processes; therefore it is

$$\lambda_{CCF} = \sum_{i=1}^{\rho} \lambda_i = \sum_{i=1}^{\rho} r_i p_i = \sum_{i=1}^{\rho} \sum_{j=1}^{\kappa} r_i p_{ij} \tag{5.13}$$

The interest of this research is to capture the epistemic uncertainty on both the model inputs and output; epistemic uncertainty is expressed by subjective probability distributions, and depends on various factors. These factors include design, operational and environmental aspects of the system, which are captured in the model by the system defences. Changing the system features by modifying the defences, in a hypothetical or actual manner, affects the behaviour (and related uncertainty) of the failure parameter. Therefore, λ_{CCF} is an uncertain quantity, being represented in the ID network by a chance node. The aim is to monitor through the ID model the alterations made to the uncertainty distribution on rate λ_{CCF}, induced by the modifications made to the system defences.

Bayesian Inference

Suppose that the system of interest has been observed for fixed time T_{obs}. For standby systems, an observed CCF is characterised as either a failure-to-start, of as a failure-to-run CCF event. Dependent failure events that are revealed by the demand, rather than caused by it, are categorised as fail-to-start CCF events. Thus, this class of events is the one relevant to the ID model.

Now, assume that during fixed time T_{obs}, n_{CCF} dependent failure-to-start events have been recorded. The likelihood function of the data is

$$f\left(n_{CCF} \mid \lambda_{CCF}\right) = \frac{\left(\lambda_{CCF} T_{obs}\right)^{n_{CCF}}}{n_{CCF}!} e^{-\lambda_{CCF} T_{obs}}$$

The uncertainty on λ_{CCF}, before having observed any failures, is modelled by a prior distribution with p.d.f. $f(\lambda_{CCF})$. A natural choice for $f(\lambda_{CCF})$ is the gamma family of distributions, which is conjugate with the Poisson family. The updated uncertainty on λ_{CCF}, in the light of n_{CCF} observations that occurred during fixed time T_{obs}, is by Bayes's law:

$$f(\lambda_{CCF} \mid n_{CCF}) \propto f(n_{CCF} \mid \lambda_{CCF}) f(\lambda_{CCF})$$

which is again a gamma distribution.

Within the Bayesian context, inference concerning λ_{CCF} requires only the total number of event occurrences and the total observation time [Barlow and Proschan, 1986]. Thus, information from n different sources (n^k_{CCF}, T^k_{obs}), $k = 1,...,n$ may be combined by considering that

$$n_{CCF} = \sum_{k=1}^{n} n^k_{CCF}$$

CCF events are observed over time period

$$T_{obs} = \sum_{k=1}^{n} T^k_{obs}$$

5.3 The specific application

The ID model is an application to systems of Emergency Diesel Generators (EDGs) of nuclear power plants, which are standby systems. For this particular example, specific taxonomies for the ID variables are used.

5.3.1 The UPM framework

In order to describe the system defences, the UPM definition of subfactors [Brand and Gabbot, 1993] is used. The definition is preserved from the UPM framework to the ID context for all defences, except for the defence of Redundancy / Diversity. The reason for this distinction is the fact that the ID model is an extension of the UPM approach, which in turn is a generalisation of the Beta Factor model. Thus, both UPM and the ID model share the same fundamental assumptions as the simplest Beta Factor model. The latter allows only two kinds of failures: independent failures and CCF events that impact on all components comprising the system. Consistently with this key assumption, increased redundancy is not a defence against CCF events, since a potential CCF event would impact on all the components, regardless of their number.

Nevertheless, UPM recognises redundancy as a defence against CCF events (subfactor of Redundancy / Diversity). The reason is that operational experience has shown that adding redundancy can actually decrease the likelihood of system failure due to CCF events [Edwards and Watson, 1979]. Therefore, UPM attempts to built-in the defence of Redundancy by adjusting the resulting beta factor accordingly, even though such an argument is opposed to the theoretical set-up of the model.

For purposes of elegance and consistency with the underlying theoretical framework, redundancy is not recognised by the ID model as a defence against CCF events. The ID model is an attempt to further generalise UPM, and thus the beta factor model, by capturing the effect of defence characteristics of the system on its vulnerability towards CCF events. Theoretically, a similar approach can be adopted to generalise models like the Multiple Beta Factor model that *au fond* distinguish between different failure multiplicities. Within this context, the benefit of redundancy shall be recognised and included in the system defences.

On this basis, aspects of redundancy are excluded from the definition of the Redundancy / Diversity subfactor in UPM, with the remaining definition describing only aspects of diversity. Like UPM, the ID model defines eight system defences: Environmental Control, Environmental Testing, Analysis, Safety Culture, Diversity, Separation, Understanding and Op. Interaction. In essence, the ID model captures the impact of the system defences on the uncertainty on the system CCF rate, which may be further updated in the light of system-specific data; to this end, the ID model has more similarities with the Partial Beta Factor method of UPM, rather than with the Cut-Off method. The latter yields a rough estimator of the total probability of system failure by assuming that the unreliability of a system due to CCFs can never exceed some limiting values, without using any actual observations.

Therefore the system defences are represented by variables D_k for $k = 1,...,8$.

Moreover, within UPM each defence is described by five levels, ranging from A to E. Therefore, within the ID framework it holds that for each D_k takes, level x_k takes values from set $\{1,2,3,4,5\}$, corresponding to levels A,B,C,D,E respectively. The definitions of the system defences and the corresponding levels are given in Appendix A.1.

5.3.2 The ICDE coding scheme

Within the particular set-up, a main assumption is that a postulated CCF event is attributed to a single root cause and communicated amongst components via a single coupling factor. Therefore, building the ID model requires a classification scheme for root causes and coupling factors to be adopted.

Several suggestions for classification schemes of CCF events have been found in the literature [Fleming et al., 1988; Mosleh et al., 1998c; Parry, 1991; Werner et al., 2004]. According to some of them, describing a CCF event in terms of a single root cause or coupling factor is considered simplistic [Mosleh et al., 1998c; Parry, 1991]. Alternatively, the CCF classification is based on a more detailed scheme, involving the concepts of proximate cause, conditioning event and trigger event. The proximate cause refers to the condition that is readily identifiable as leading to the failure. The conditioning event refers to conditions that increase the component susceptibility to failure, and the trigger event is an event that activates the failure.

In an effort to establish a mechanism that allows for a structured classification process and reporting of CCFs amongst different countries, coding schemes such as the International Common Cause Failure Data Exchange Project (ICDE)[1]. The countries-members of the Project, are encouraged to document CCF events in terms of a report of standard format, by using common guidance for interpretation of the events [Werner et al., 2004]. Based on the standardised report, the event is classified across certain generic categories, including a root cause and coupling factor characterisation. The root cause is defined as the most basic reason for components' failure, the most readily

[1] See Section 2.4.3

identifiable cause, and, licensees are encouraged to select a single root cause and coupling factor for each event, even in cases where, due to the complex nature of the CCF event, a single root cause is not readily ascribable.

Within the ID model, the root cause and coupling factor categories suggested by the ICDE coding scheme [Werner et al., 2004] particularly for EDGs are used. The reason for the choice of the particular taxonomies is the fact that the ICDE coding guidelines establish a coherent documentation of CCF information, according to a standard format, that allows for collection and analysis of data coming from various countries/members of the project. Thus, the ICDE database incorporates extensive information of a structured form, and by merging the structure of the database with the model structure, a valuable association is created. Moreover, observed CCF events are assigned a single root cause and coupling factor, a fact which aligns with the framework of assumptions of the ID model.

The root cause categories are Environment, Design, Human, Internal, Maintenance and Procedures. The definitions of the root causes are given in Appendix A.2. The coupling mechanisms are assigned to three main categories: hardware based, operation based, and environment based. The definitions of the coupling factors are given in Appendix A.3.

5.3.3 ID variables and graphical representation

In conclusion, the variables of the ID model are

- 8 defence variables, signifying the defence characteristics of the system of components. They are denoted with D_k $(k = 1,...,8)$ and represented by decision nodes, each with set of alternatives $\{1,2,3,4,5\}$;

- 6 root cause variables, signifying the rate of failure events due to a particular root cause per calendar hour. They are denoted with r_i $(i = 1,...,6)$ and represented by chance nodes;

- 3 coupling factor variables, signifying the intensity of the coupling mechanisms in the system. Each coupling factor j ($j = 1,2,3$) is represented by a chance node, and associated with a vector of parameters $\underline{p_j} = (p_{1j},...,p_{6j})$ where

$$p_{ij} = P(\text{CCF through cf }_j \mid \text{failure event due to rc } i)$$

- a CCF rate, signifying the rate of dependent failure-to-start events occurring to the system per calendar hour. It is denoted with λ_{CCF} and represented by a chance node.

The graph in Figure 5.2 illustrates the associational relationships amongst the ID variables. The defence aspects of the system affect the expected behaviour of the root cause and coupling factor variables, which in turn determine the expected behaviour of the CCF rate. These relationships are portrayed in the ID network by arrows. In particular, arrows between defence variables and root cause or coupling factor nodes signify the impact of system features on the occurrence of root cause events and the tendency for coupling behaviour; arrows between the root cause alongside coupling factor variables and the CCF rate variable represent how changes in the uncertainty of the former result in adjustments in the uncertainty of the latter.

The lack of arrows between nodes signifies assertion of a priori conditional independence. To be more precise, it is assumed that the root cause and coupling factor variables are independent. Moreover, in Section 5.2.2 it is assumed that the rates of failures due to different root causes r_i, for $i = 1,...,6$, are independent parameters (assumption of independent Poisson process). In Section 5.2.3, a local independence assumption is made, according to which parameters p_{ij}, for $j = 1,2,3$, are a priori independent.

5.4 Conclusion

This section presented the modelling approach adopted within the particular framework. In particular, the main assumptions have been clearly stated, and the theoretical set-up of the model has been defined. Initially, the important elements of the modelling

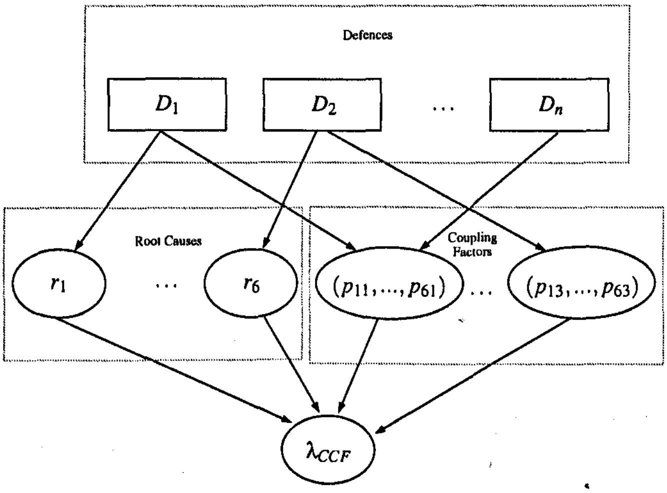


Figure 5.2: Dependency relationships in ID network

domain have been identified and qualitatively defined. Following, a mathematical definition for each element was given.

The ID model considers failures that occurred during the period the system was on standby, and only detected by the demand. The modelling of this type of failure is based on the assumption that CCF events occur at random times during the idle period of the system, and at constant rates [Vaurio, 1994b]. Within the scope of CCF modelling, it is typical to assume that CCF events of different types occur according to independent Homogeneous Poisson Processes [Marshall and Olkin, 1967; Vesely, 1977]. Moreover, the Homogeneous Poisson assumption is considered appropriate because CCF events are rare events, and the occurrence of CCF events is not driven by factors such as the aging of the component or seasonality.

Once the mathematical dimensions of the variables of the ID model are strictly defined, the mathematical structure of the model may be illustrated, and the implying properties presented. This is the aim of the next chapter.

Chapter 6

Mathematical structure of the Influence Diagram Model

6.1 Introduction

This chapter presents the mathematical structure of the Influence Diagram (ID) model for CCF modelling. The ID model extends UPM by reflecting the functional interactions existing amongst the system defences. This is achieved by defining a mathematical formulation which associates the failure behaviour of the system, expressed by the root cause and coupling factor variables, with the defences that are employed by the system. This formulation is referred to as the Geometric Scaling (GS) model. The implied relationships are not graphically portrayed in the model network, but are integral in the mathematical formulation of the ID model.

This setup presents three particularly interesting features. Firstly, the GS model is an operationally useful formulation, because it significantly decreases the amount of information to be elicited from experts. The model associates any root cause and coupling factor variable with the configuration of the system across the influencing defences. For the quantification of the ID, experts need to determine their uncertainty on the parameters of the geometric scaling model, which will then be used in order to determine the subjective distribution on the root cause and coupling factor variable at any defence configuration.

Secondly, the setup allows for quantitative data to be communicated amongst defence levels. Through application of Bayes' theorem, statistical information from one level becomes relevant for making uncertainty statements for other levels. Consequently, updating the prior on a root cause or coupling factor variable at a particular defence configuration, modifies the uncertainty on the variable at any other configuration across the influencing defences.

Thirdly, the model allows for distinguishing between the different types of functional interaction that exist amongst the defence variables that influence a particular failure characteristic of the system.

The chapter is structured as follows: Section 6.2 addresses the issue of existing interactions amongst the defences in the way they impact on the system susceptibility to CCF events. Section 6.3 defines the Geometric Scaling model associating the system failure behaviour with the employed defences, and shows that it succeeds in capturing the structure of the defence domain. In Section 6.4 the process of uncertainty extrapolation to different configuration vectors is presented. Section 6.5 illustrates the process of learning form experience, or Bayesian updating. Section 6.6 determines the uncertainty on the rate of component CCF events. Section 6.7 completes the presentation of the theoretical foundations of the Influence Diagram (ID) model with some general remarks, and Section 6.8 defines the Geometric Scaling model and mathematical configuration within the particular application. Finally, Section 6.9 concludes the chapter.

6.2 Impact of defences

6.2.1 Introduction

The ID model expresses the overall CCF event process in terms of a superposition of root cause processes, filtered through coupling factor intensities[1], i.e.

$$\lambda_{CCF} = \sum_{i=1}^{\rho} \lambda_i = \sum_{i=1}^{\rho} r_i p_i = \sum_{i=1}^{\rho} \sum_{j=1}^{\kappa} r_i p_{ij}$$

where r_i are the root cause rates, and p_{ij} are the coupling factor intensities ($i = 1, ..., \rho$, $j = 1, 2, ..., \kappa$).

Thereby, the ID model introduces intermediate stages in the way the system defences impact on the CCF rate λ_{CCF}, namely the root causes r_i and coupling factors p_{ij} ($i = 1, ..., \rho$ and $j = 1, 2, ..., \kappa$). The impact of the system defences is captured initially on these intermediate elements, which in turn determine the overall λ_{CCF}.

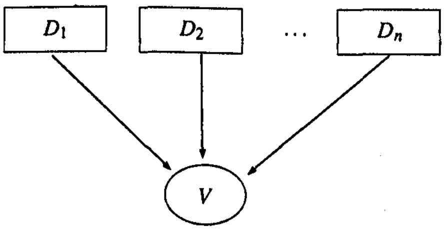


Figure 6.1: Defences $D_1, ..., D_n$ influencing variable V

Suppose that random variable V (root cause or coupling factor variable) is influenced by n system defences $D_1, D_2, \ldots, D_n$ (see Figure 6.1). The system is scored across the n defences, and level x_k is assigned to defence D_k. Let $K = \{1, ..., n\}$ be the set of indices of the influencing defences, and let $\Omega_k = \{1, ..., m_k\}$ be the state space of x_k, so that $k \in K$ and $x_k \in \Omega_k$. The random variable V at configuration vector $(x_1, x_2, \ldots, x_n)$ is denoted with

$$V_{(x_1, ..., x_n)} \quad \text{for} \quad x_k \in \Omega_k, k \in K$$

[1] See Chapter 5, Section 5.2.4

It is assumed that the protection of the system against failures does not become worse as a result of enhancing defence D_i ($i \in K$), from level x_i to level $x_i + 1$ ($x_i, x_i + 1 \in \Omega_i$). This assumption implies a partial ordering of the configuration vectors. For fixed levels of defences D_j for which $i \neq j$ ($i, j \in K$) we have

$$(x_1, \ldots, x_i - 1, 1, x_i + 1, \ldots, x_n) \preceq (x_1, \ldots, x_i - 1, 2, x_i + 1, \ldots, x_n) \preceq \ldots$$
$$\preceq (x_1, \ldots, x_i - 1, 5, x_i + 1, \ldots, x_n)$$

The ordering above induces an (inverse) ordering of random variables $V_{(x_1,\ldots,x_n)}$ at each defence configuration, viz.

$$V_{(x_1,\ldots,x_i-1,1,x_i+1,\ldots,x_n)} \geq V_{(x_1,\ldots,x_i-1,2,x_i+1,\ldots,x_n)}$$
$$\geq \ldots \geq V_{(x_1,\ldots,x_i-1,5,x_i+1,\ldots,x_n)} \qquad (6.1)$$

Let $I_i(x_1, \ldots, x_i, \ldots, x_n)$ be the proportion by which $V_{(x_1,\ldots,x_n)}$ decreases, when the level of D_i changes from x_i to $x_i + 1$, while the levels of the other defences are kept fixed, viz.

$$V_{(x_1,\ldots,x_i+1,\ldots,x_n)} = I_i(x_1, \ldots, x_i, \ldots, x_n) V_{(x_1,\ldots,x_i,\ldots,x_n)} \quad \text{for } x_i \in \Omega_i \qquad (6.2)$$

Relationships (6.1) imply that $0 < I_i(x_1, \ldots, x_n) \leq 1$.

6.2.2 Types of functional interaction

Proportion $I_i(x_1, \ldots, x_i, \ldots, x_n)$ ($i \in K$) expresses the impact of defence D_i on r.v. V, and, ultimately, on the CCF rate, when moving from x_i to $x_i + 1$ whilst the levels of the other defences are kept fixed. In order to describe potential interactions existing amongst D_i and other defences D_j ($j \in K$, $j \neq i$), it suffices to describe the way the other defences influence proportion $I_i(x_1, \ldots, x_n)$.

Let $X_{i,\theta}$ for $\theta = 1, 2, \ldots s_i$ be a partition of Ω_i, that is $\bigcap_{\theta=1}^{s_i} X_{i,\theta} = \emptyset$ and $\bigcup_{\theta=1}^{s_i} X_{i,\theta} = \Omega_i$. When $x_i \in X_{i,\theta}$ and $x_i + 1 \in X_{i,\theta+1}$, for some $\theta \in \{1, 2, \ldots s_i\}$, then it is said that *drastic* changes in the defence of the system occur. Otherwise, *moderate* changes occur.

Within the proposed set-up three types of interaction are distinguished, namely functional independence, functional dependence and threshold functional dependence. It is assumed that between any pair of defences $\{D_i, D_j\}$ $(i, j \in K,\ j \neq i)$ one of these interactions exists. These are defined below.

Functional independence Defence D_i is functionally independent of defence D_j, when the effect on V of improving D_i by one level $(x_i, x_i + 1 \in \Omega_i)$, whilst the levels of the other defences are kept fixed, is the same regardless of the level of D_j. This property is symmetrical, implying that D_j is also functionally independent of D_i. Mathematically expressed,

$$I_i(x_1, \ldots, x_j, \ldots, x_n) = I_i(x_1, \ldots, x_j', \ldots, x_n), \text{ for every } x_j, x_j' \in \Omega_j$$

and

$$I_j(x_1, \ldots, x_i, \ldots, x_n) = I_j(x_1, \ldots, x_i', \ldots, x_n), \text{ for every } x_i, x_i' \in \Omega_i$$

Functional dependence Defence D_i is functionally dependent on D_j, when the effect on V of improving D_i by one level $(x_i, x_i + 1 \in \Omega_i)$, whilst the levels of the other defences are kept fixed, depends on the level of D_j, and vice-versa. This property is symmetrical, implying that D_j is also functionally dependent on D_i. Mathematically expressed,

$$I_i(x_1, \ldots, x_j, \ldots, x_n) = I_i(x_1, \ldots, x_j', \ldots, x_n), \text{ only if } x_j = x_j'$$

with $x_j, x_j' \in \Omega_j$, and

$$I_j(x_1, \ldots, x_i, \ldots, x_n) = I_j(x_1, \ldots, x_i', \ldots, x_n), \text{ only if } x_i = x_i'$$

with $x_i, x_i' \in \Omega_i$.

Threshold functional dependence Defence D_i is threshold functionally dependent on defence D_j, when the effect on V of improving D_i by one level $(x_i, x_i+1 \in \Omega_i)$, whilst the levels of the other defences are kept fixed, depends on θ for which $x_j \in X_{j,\theta}$. Whereas, the effect on V of moderately improving D_j by one level $(x_j, x_j+1 \in X_{j,\theta}$, for some $\theta \in \{1,...,s_j\})$ is the same regardless of the level of D_i. This property is not symmetrical.

Mathematically expressed,

$$I_i(x_1,\ldots,x_j,\ldots,x_n) = I_i(x_1,\ldots,x'_j,\ldots,x_n)$$

if $x_j, x'_j \in X_{j,\theta}$, for some $\theta \in \{1,...,s_j\}$, and for moderate changes (when $x_j, x_j+1 \in X_{j,\theta}$),

$$I_j(x_1,\ldots,x_i,\ldots,x_n) = I_j(x_1,\ldots,x'_i,\ldots,x_n)$$

for every $x_i, x'_i \in \Omega_i$ and constant for all $\theta \in \{1,...,s_i\}$.

6.3 The Geometric Scaling (GS) model

6.3.1 Introduction

The overall goal is to define a model to support uncertainty statements about the failure behaviour of a system employing particular defences, whilst allowing for distinguishing the different types of functional interaction as described above. To achieve this, a functional relationship is assumed between r.v. V [2] and the system configuration vector of the influencing defences $(x_1,...,x_n)$.

Previously, similar set-ups have been proposed within the area of Accelerated Life Testing (ALT). To be more precise, ALT is concerned with the failure behaviour of devices that operate under different levels of stress. Often, the interest lies on stress levels that cannot be reproduced in laboratories, and for which there is no information

[2] V denotes a root cause or coupling factor r.v.

available from tests; thus, it is important to define set-ups that allow making inferences based on the available knowledge, that is tests performed at different stress levels. Within this context, an ordering of the stress levels is assumed, implying an ordering of the parameter of interest, and a relationship is defined between the parameter of interest and the stress level. Within the literature, different types of relationships have been used, such as the power law, the Arrenius model and the Eyring model ([Blackwell and Singpurwalla, 1988] and references therein]), and different methodologies have been explored, both Bayesian [Dorp and Mazzuchi, 2004; Mazzuchi and Soyer, 1996] and frequentist [Singpurwalla, 1971] in order to determine the unknown parameters. In [Mazzuchi and Soyer, 1992] an exponential model is assumed for the system lifetime distribution, and, a power law model is used for describing the stress effect on the failure rate. In [Dorp and Mazzuchi, 2004], an exponential life time distribution is assumed; the ordering of the rates at different levels is preserved by using a multivariate prior distribution defined over an ordered region. The type of model associating the system failure behaviour with the operating conditions depends, in principle, on physical patterns identified in the real world [Mazzuchi and Soyer, 1992].

6.3.2 The model

Structure of the defence domain

For r.v. V being influenced by defences $D_1,...,D_n$ suppose that the structure of the defence domain is defined as follows:

- Let $\{i,j\} \subset K$ be a pair of indices of two functionally independent defences D_i and D_j, $i,j \in K$. Then we define

  $$H_\pi = \{\{i,j\} \mid D_i, D_j \text{ functionally independent}\}$$

  as the set of all the pairs of indices of functionally independent defences, and,

  $$H = \{i \mid i \in \{i,j\} \text{ for some } j \in K, \text{ where } \{i,j\} \in H_\pi\}$$

as the set of indices of all defences that exhibit functional independence with some defence D_k, $k \in K$.

- Let $\{i,j\} \subset K$ be the pair of indices of two functionally dependent defences D_i and D_j, $i,j \in K$. Then we define

$$M_\pi = \{\{i,j\} \mid D_i, D_j \text{ functionally dependent}\}$$

as the set of all the pairs of indices of functionally dependent defences, and,

$$M = \{i \mid i \in \{i,j\} \text{ for some } j \in K, \text{ where } \{i,j\} \in M_\pi\}$$

as the set of indices of all defences that exhibit functional dependence with some defence D_k, $k \in K$.

- We define $Q \subset K$ as the set of indices of threshold functionally dependent defences. For each $q \in Q$, define $L_q \subset K$ as the set of indices of defences on which D_q is threshold functionally dependent. Then

$$L = \{k \mid k \in L_q \text{ for some } q \in Q\}$$

is the set of indices of all defences that are the counterpart of threshold functional dependence with some defence D_k, $k \in K$.

Subsets H, M, Q and L are not necessarily mutually exclusive. A given defence D_k may be functionally independent of defence D_η ($\{k,\eta\} \in H_\pi$), but functionally dependent on defence D_l ($\{k,l\} \in M_\pi$), could be functionally dependent on a second defence $D_{l'}$ ($\{k,l'\} \in M_\pi$ for $l \neq l'$) [3], could be threshold functional dependent on a third defence ($k \in Q$), or the counterpart of threshold dependency of a fourth defence ($k \in L_q$ for some $q \in Q$). Therefore, it is possible that $H \cap M \cap Q \cap L \neq \varnothing$.

[3] Functional dependence is symmetrical but not transitive

Model formula

The following mathematical relationship is assumed, which from now and on will be referred to as the Geometric Scaling (GS) model

$$V_{(x_1,\dots,x_n)} = \prod_{\{i,j\}\in M_\pi} \phi_{ij}^{(x_i-\mu_i)(x_j-\mu_j)} \prod_{k\in K} \Phi_k^{x_k-\mu_k} \cdot V_{(\mu_1,\dots,\mu_n)} \tag{6.3}$$

where $V_{(\mu_1,\dots,\mu_n)}$ is r.v. V when defence D_k receives the medium level $\mu_k \in \Omega_k$, for all $k = 1,\dots,n$, $\phi_{ij} \in \mathbb{R}$ is a cross-term that corresponds to pair $\{i,j\} \in M_\pi$ and Φ_k is a function $\Phi_k : \Omega_{k_1} \times \dots \times \Omega_{k_r} \rightarrow [0,1]$

The form of function Φ_k

The form of function Φ_k is

$$\Phi_k = \begin{cases} \phi_k(x_{k_1}, x_{k_2}, \dots, x_{k_r}) \text{ where } \{k_i \mid i = 1,\dots,r\} = L_k, \text{ if } k \in Q \\ \phi_k, \text{ otherwise} \end{cases}$$

with $0 < \phi_k \leq 1$ and $\phi_k(x_{k_1}, x_{k_2}, \dots, x_{k_r}) : \Omega_{k_1} \times \dots \times \Omega_{k_r} \rightarrow [0,1]$ being a function defined as follows:

If $X_{i,\theta}$ for $\theta = 1,2,\dots,s_i$ is a partition of Ω_i ($i = k_1,\dots,k_r$), then $Y_\eta = X_{\eta_1} \times \dots X_{\eta_r}$ ($\eta_i \in \{1,\dots,s_i\}$) is a partition of $\Omega_{k_1} \times \Omega_{k_r}$ with $\eta = 1,\dots,s_{k_1} \cdot \dots \cdot s_{k_r}$. Formula $\phi_k(x_{k_1}, x_{k_2}, \dots, x_{k_r})$ represents a piecewise function with domain $\Omega_{k_1} \times \dots \times \Omega_{k_r}$, viz.

$$\phi_k(x_{k_1}, x_{k_2}, \dots, x_{k_r}) = \phi_{k,\eta} \text{ when } (x_{k_1}, x_{k_2}, \dots, x_{k_r}) \in Y_\eta$$

with $0 < \phi_{k,\eta} \leq 1$. It is further assumed that for x_{k_j} kept fixed, points $\phi_k(x_{k_1}, \dots, x_{k_l}, \dots, x_{k_r})$, where $j \neq l$ and $j, l \in \{1,\dots,r\}$, are symmetrically distanced.

The general form of the GS model

The GS model may be expressed as

$$V_{(x_1,\ldots,x_n)} = h_v(x_1,\ldots,x_n) \cdot V_{(\mu_1,\ldots,\mu_n)} \tag{6.4}$$

where $h_v(x_1,\ldots,x_n) : \Omega_1 \times \ldots \times \Omega_n \rightarrow \mathbb{R}$ is a log-linear function that relates each configuration vector $(x_1,\ldots,x_n)$ to a real number, and with parameters the proportions Φ_k $(k \in K)$ and ϕ_{ij} $(i,j \in M_{ij})$. Taking the logarithmic transformation of $h_v(x_1,\ldots,x_n)$, the resulting expression is a multivariate polynomial of second degree. The second degree term captures the symmetric dependence between two functionally dependent variables. The piecewise form of the term Φ_k when $k \in Q$, allows to express dependency of defence D_k on a set of defences D_{k_l}, $l = 1,\ldots,r$ $(k_l \in L_k)$, without reciprocating this effect from D_{k_l} to D_k.

The log-linear form of the proposed model reflects the increasing difficulty in enhancing the failure behaviour of the system as the levels of the influencing defences increase. For the dependent failure problem, there is no indication to suggest deviation from a non-linear relationship between the susceptibility of the system and the employed defence levels [Smith, 2000].

Using model (6.3) allows to extrapolate uncertainty from a starting point to any defence level, once the model parameters are determined. Relationship (6.3) suggests $V_{(\mu_1,\ldots,\mu_n)}$ as the starting point, which expresses r.v. V at a medium configuration vector $(\mu_1,\ldots,\mu_n)$, $\mu_k \in \Omega_k$, $k = 1,\ldots,n$. This choice is supported by the fact that it is conceptually easier to elicit information on events that are frequently encountered in practice (systems with medium defences), rather than on extreme situations (systems with exceptionally high or exceptionally low defences).

Below, it is explored whether the GS model succeeds to distinguish between the different types of functional interaction. This property constitutes a model desideratum.

The GS model and functional interactions

Consider defences D_i, D_j for which $i,j \in K$. From (6.2) it follows that,

$$I_i(x_1,\ldots,x_i,\ldots,x_n) = \frac{V_{(x_1,\ldots,x_i+1,\ldots,x_n)}}{V_{(x_1,\ldots,x_i,\ldots,x_n)}} \quad \text{for } x_i = 1,\ldots,4$$

Using Model (6.3), and after removing the common terms from the nominator and the denominator, we have

$$I_i(x_1,\ldots,x_i,\ldots,x_n) = \frac{\Phi_i^{x_i+1-\mu_i} \prod_{\{i,j\}\in M_\pi} \phi_{ij}^{(x_i+1-\mu_i)(x_j-\mu_j)} \prod_{l\in Q, i\in L_l} \phi_l(x_{l_1},\ldots,x_i+1,..x_{l_r})^{x_l-\mu_l}}{\Phi_i^{x_i-\mu_i} \prod_{\{i,j\}\in M_\pi} \phi_{ij}^{(x_i-\mu_i)(x_j-\mu_j)} \prod_{l\in Q, i\in L_l} \phi_l(x_{l_1},\ldots,x_i,..x_{l_r})^{x_l-\mu_l}}$$

$$= \Phi_i \prod_{\{i,j\}\in M_\pi} \phi_{ij}^{x_j-\mu_j} \prod_{i\in L_l} \left(\frac{\phi_l(x_{l_1},\ldots,x_i+1,..x_{l_r})}{\phi_l(x_{l_1},\ldots,x_i,..x_{l_r})}\right)^{x_l-\mu_l}$$

Let

$$C_1 = \prod_{\{i,j\}\in M_\pi} \phi_{ij}^{x_j-\mu_j} \quad \text{and} \quad C_2 = \prod_{l\in Q, i\in L_l} \left(\frac{\phi_l(x_{l_1},\ldots,x_i+1,..x_{l_r})}{\phi_l(x_{l_1},\ldots,x_i,..x_{l_r})}\right)^{x_l-\mu_l}$$

so that

$$I_i(x_1,\ldots,x_i,\ldots,x_n) = \Phi_i \cdot C_1 \cdot C_2 \tag{6.5}$$

Functional independence Suppose that defence D_i is functionally independent of defence D_j, that is $\{i,j\} \in H_\pi$. The impact of defence D_i is given by formula (6.5). Between any two defences only one kind of interaction exists, thus $j \notin L_i$ and Φ_i is not a function of x_j. Moreover, $\{i,j\} \notin M_\pi$ and factor C_1 is not a function of x_j. We will now explore whether C_2 is a function of x_j.

- Assume that there is no $l \in Q$ for which $i,j \in L_l$.

Then, factor C_2 is not a function of x_j either, and proportion

$$I_i(x_1,\ldots,x_i,\ldots,x_n) = \Phi_i \cdot C_1 \cdot C_2$$

does not depend on x_j.

- Assume that there is $l \in Q$, for which $i, j \in L_l$.

Then, for some $m \in \{1,...,r\}$, it holds that $x_{l_m} = x_j$, and $\phi_l(x_{l_1},...,x_{l_r})$ is a function of x_j.

If

$$x_i, x_i + 1 \in X_{i,\theta} \quad \theta \in \{1,...,s_i\}$$

then

$$(x_1,\ldots,x_i,\ldots,x_n), (x_1,\ldots,x_i+1,\ldots,x_n) \in Y_\eta, \eta \in \{1,...,s_{l_1} \cdot \ldots \cdot s_{l_r}\}$$

and

$$\phi_l(x_{l_1},...,x_i+1,..x_{l_r}) = \phi_l(x_{l_1},...,x_i,..x_{l_r})$$

Therefore, $C_2 = 1$ and $I_i(x_1,\ldots,x_i,\ldots,x_n)$ does not depend on x_j.

However, if $x_i \in X_{i,\theta}$ and $x_i + 1 \in X_{i,\theta+1}$ $(\theta \in \{1,...,s_i\})$

$$\phi_l(x_{l_1},...,x_i+1,..x_{l_r}) \neq \phi_l(x_{l_1},...,x_i,..x_{l_r})$$

and C_2 becomes a function of x_j. In this case, *functional independence holds by placing additional conditions on the form of the piecewise function* $\phi_l(x_{l_1},..x_{l_r})$. It is further assumed that

$$\phi_l(x_{l_1},..x_{l_r}) = \prod_{m=1}^{r} \phi_l(x_{l_m}) \tag{6.6}$$

where

$$\phi_l(x_{l_m}) = \phi_{l_m,\theta} \quad \text{when } x_{l_m} \in X_{l_m,\theta}$$

Then,

$$C_2 = \prod_{l \in Q, i \in L_l} \left(\frac{\phi_l(x_i+1)}{\phi_l(x_i)} \right)^{x_l - \mu_l}$$

is not a function of x_j.

Now, in all cases, $I_i(x_1,\ldots,x_i,\ldots,x_n)$ does not depend on x_j, and

$$I_i(x_1,\ldots,x_j,\ldots,x_n) = I_i(x_1,\ldots,x_j',\ldots,x_n) \text{ for any } x_j, x_j' \in \Omega_j$$

implying that D_i is functionally independent of D_j.

In a similar fashion it may be shown that

$$I_j(x_1,\ldots,x_j,\ldots,x_n) = \Phi_j \cdot C_1 \cdot C_2$$

where factors Φ_j, C_1, C_2 do not depend on x_i, and that

$$I_j(x_1,\ldots,x_i,\ldots,x_n) = I_\eta(x_1,\ldots,x_i',\ldots,x_n) \text{ for any } x_i, x_i' \in \Omega_i$$

Thus, the formulation agrees with the mathematical expression of functional independence.

Functional dependence Suppose that defences D_i and D_j are functionally dependent, i.e., $\{i,j\} \in M_\pi$. The impact of defence D_i is given by formula (6.5).

Based on the assumption that between any two defences only one kind of interaction exists, it holds that $j \notin L_i$, and Φ_i is not a function of x_j. Moreover, C_1 may be re-written as

$$C_1 = \prod_{\{i,j\} \in M_\pi} \phi_{ij}^{x_j - \mu_j} = \phi_{ij}^{x_j - \mu_j} \prod_{\{i,j'\} \in M_\pi, j \neq j'} \phi_{ij'}^{x_{j'} - \mu_{j'}}$$

and

$$C_2 = \prod_{l \in Q, i \in L_l} \left(\frac{\phi_l(x_{l_1},\ldots,x_i+1,..x_{l_r})}{\phi_l(x_{l_1},\ldots,x_i,..x_{l_r})} \right)^{x_l - \mu_l} = \prod_{l \in Q, i \in L_l} \left(\frac{\phi_l(x_i+1)}{\phi_l(x_i)} \right)^{x_l - \mu_l}$$

Proportion $I_i(x_1,\ldots,x_i,\ldots,x_n)$ now becomes

$$I_i(x_1,\ldots,x_i,\ldots,x_n) = \Phi_i \phi_{ij}^{x_j - \mu_j} C$$

where factors Φ_i, C do not depend on x_j. Similarly, one finds that

$$I_j(x_1,\ldots,x_j,\ldots,x_n) = \Phi_j \phi_{ij}^{x_i - \mu_i} C$$

where factors Φ_j, C do not depend on x_i. Therefore, if $x_j \neq x'_j$, then

$$I_i(x_1,\ldots,x_j,\ldots,x_n) \neq I_i(x_1,\ldots,x'_j,\ldots,x_n)$$

and, if $x_i \neq x'_i$, then

$$I_j(x_1,\ldots,x_i,\ldots,x_n) \neq I_j(x_1,\ldots,x'_i,\ldots,x_n)$$

Thus, Model (6.3) agrees with the mathematical expression of functional dependence.

In addition, the effect on $I_i(x_1,\ldots,x_n)$, with respect to the level of D_j, is symmetrical to the effect on $I_j(x_1,\ldots,x_n)$, with respect to the level of D_i.

The two defences may present either a *compensating* or an *aggravating* effect. A compensating effect implies that improving the defence characteristics of the system concerning one defence becomes less effective when the other defence is strong. An aggravating effect implies that improving the defence characteristics of the system concerning one defence becomes more effective when the other defence is strong. The range of ϕ_{ij} determines the nature of interaction between defences D_i and D_j. Indeed, $0 < \Phi_i, \Phi_j < 1$, and for $\phi_{ij} > 1$ we have

$$\Phi_i \phi_{ij}^{x_j - \mu_j} < \Phi_j \phi_{ij}^{x_j + 1 - \mu_j} \quad \text{and} \quad \Phi_j \phi_{ij}^{x_i - \mu_i} < \Phi_j \phi_{ij}^{x_i + 1 - \mu_i}$$

which imply that improving one defence is less effective for higher levels of the other defence (compensating effect). In a similar fashion, for $0 < \phi_{ij} < 1$ we have

$$\Phi_i \phi_{ij}^{x_j - \mu_j} > \Phi_i \phi_{ij}^{x_j + 1 - \mu_j} \quad \text{and} \quad \Phi_j \phi_{ij}^{x_i - \mu_i} > \Phi_j \phi_{ij}^{x_i + 1 - \mu_i}$$

which imply that improving one defence is more significant for higher levels of the other defence (aggravating effect).

Threshold functional dependence Suppose that defence D_i is threshold functionally dependent on defence D_j, i.e. $i \in Q$ and $j \in L_i$. The impact of defence D_i is given by formula (6.5).

Based on the assumption that between any two defences only one kind of interaction exists, it holds that $\{i,j\} \notin M_\pi$, which implies that C_1 is not a function of x_j. Moreover, $i \notin L_j$, and C_2 is not a function of x_j, either. Therefore,

$$I_i(x_1,\ldots,x_i,\ldots,x_n) = \Phi_i \cdot C$$

where

$$\Phi_i = \phi_i(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) \quad \text{for } i_m \in L_i, m = 1, \ldots, r$$

Consistently with (6.6), we have

$$I_i(x_1,\ldots,x_i,\ldots,x_n) = \Phi_i \cdot C = \phi_i(x_j) \prod_{m, i_m \neq j} \phi_i(x_{i_m}) \cdot C$$

where C is not a function of x_j. Therefore, if $x_j, x_j' \in X_{j,\theta}$, then $\phi_i(x_j) = \phi_i(x_j')$ and $I_i(x_1,\ldots,x_j,\ldots,x_n) = I_i(x_1,\ldots,x_j',\ldots,x_n)$.

In a similar fashion, according to (6.5) the impact of D_j is given by

$$I_j(x_1,\ldots,x_j,\ldots,x_n) = \Phi_j \cdot C_1 \cdot C_2$$

where

$$C_1 = \prod_{\{i,j\} \in M_\pi} \phi_{ij}^{x_i - \mu_i} \quad \text{and} \quad C_2 = \prod_{l \in Q, j \in L_l} \left(\frac{\phi_l(x_{l_1}, \ldots, x_j + 1, ..x_{l_r})}{\phi_l(x_{l_1}, \ldots, x_j, ..x_{l_r})} \right)^{x_l - \mu_l}$$

Threshold functional dependence is not a symmetric property. Therefore, defence D_j, which is the counterpart of threshold dependence of defence D_i ($j \in L_i$), cannot be threshold dependent on defence D_i ($i \notin L_j$). Moreover, based on the fact only one type of interaction exists between two defences, defences D_i and D_j cannot be functionally dependent ($\{i,j\} \notin M_\pi$). Thus, Φ_j, C_1 are not functions of x_i, and

$$C_2 = \left(\frac{\phi_i(x_j + 1)}{\phi_i(x_j)} \right)^{x_i - \mu_i} \prod_{j \in L_l, l \neq i} \left(\frac{\phi_l(x_j + 1)}{\phi_l(x_j)} \right)^{x_l - \mu_l}$$

The impact of D_j is now expressed as

$$I_j(x_1,\ldots,x_j,\ldots,x_n) = \Phi_j \left(\frac{\phi_i(x_j+1)}{\phi_i(x_j)}\right)^{x_i-\mu_i} \cdot C \tag{6.7}$$

where C is not a function of x_i. For moderate modifications of x_j, i.e., $x_j, x_j+1 \in X_{j,\theta}$ we have $\phi_i(x_j) = \phi_i(x_j+1)$ and (6.7) becomes

$$I_j(x_1,\ldots,x_j,\ldots,x_n) = \Phi_j \cdot C$$

which implies that

$$I_j(x_1,\ldots,x_i,\ldots,x_n) = I_j(x_1,\ldots,x_i',\ldots,x_n)$$

for every $x_i, x_i' \in \Omega_i$, and constant for all $\theta \in \{1,...,s_j\}$. Therefore, Model (6.3) agrees with the definition of threshold functional dependence.

However, when drastic modifications occur, then $\phi_i(x_j) \neq \phi_i(x_j+1)$ and $I_j(x_1,\ldots,x_i,\ldots,x_n)$ depends on the level of D_i. Suppose that the effect of D_j on D_i is compensating, implying that enhancing D_i is more effective when D_j is assigned to a lower lever, i.e.

$$\phi_i(x_j+1) > \phi_i(x_j) \Leftrightarrow \frac{\phi_i(x_j+1)}{\phi_i(x_j)} > 1$$

and

$$\left(\frac{\phi_i(x_j+1)}{\phi_i(x_j)}\right)^{x_i-\mu_i} > 1 \quad \text{for } x_i > \mu_i \quad \text{and} \quad \left(\frac{\phi_i(x_j+1)}{\phi_i(x_j)}\right)^{x_i-\mu_i} < 1 \quad \text{for } x_i < \mu_i$$

Based on Relationship (6.7), and for $x_j \in X_{j,\theta}$, $x_j+1 \in X_{j,\theta+1}$ ($\theta \in \{1,...,s_j\}$), we have

$$I_j(x_1,\ldots,x_i,\ldots,x_n) > I_j(x_1,\ldots,x_i',\ldots,x_n) \quad \text{for } x_i > x_i'$$

which implies that for drastic changes in the level of D_j, the higher the level of D_i is, the less efficient enhancing the level of D_j becomes.

In a similar fashion, when the effect of D_j on D_i is aggravating and for drastic modifications of D_j, the higher the level of D_i is, the more efficient enhancing the level of D_j becomes.

6.4 Extrapolation of uncertainty

The GS model defined in Section 6.3 allows the specification of the uncertainty on r.v. $V_{\underline{x}}$ at any configuration vector $\underline{x}$. In performing uncertainty analysis on Model (6.3) a joint distribution on the proportion parameters ϕ_ι ($\iota = 1,...,m$)[4] and variable $V_{\underline{\mu}}$ is required, where $\underline{\mu} = (\mu_1,...,\mu_n)$ is the 'base-level' configuration vector. Within the particular framework, a number of key assumptions are made. In particular, it is assumed that

1. variables ϕ_ι and $V_{\underline{\mu}}$ are *a priori* independent. This assertion implies that the proportions of decrease induced on $V_{\underline{\mu}}$ by modifying a particular defence depend exclusively on the environment in which the system operates, and not on the actual value of $V_{\underline{\mu}}$;

2. proportion variables ϕ_ι are mutually *a priori* independent;

3. the uncertainty distribution on variable $r_{i,\underline{x}}$ is a gamma density[5] with parameters $a_{i,\underline{x}}$ and $b_{i,\underline{x}}$, i.e.

$$r_{i,\underline{x}} \sim \mathcal{G}\left(a_{i,\underline{x}}, b_{i,\underline{x}}\right), \quad \text{for all } i = 1,...,\rho$$

4. the uncertainty distribution on variable $p_{ij,\underline{x}}$ is a beta density[6] with parameters $\gamma_{ij,\underline{x}}$ and $\delta_{ij,\underline{x}}$, i.e.

$$p_{i,\underline{x}} \sim \mathcal{B}\left(\gamma_{ij,\underline{x}}, \delta_{ij,\underline{x}}\right) \quad \text{for all } i = 1,...,\rho,\ j = 1,...,\kappa$$

5. the uncertainty distribution on variable ϕ_ι is a lognormal density with parameters

[4] With ϕ_ι we denote all the proportion variables ϕ_{ij} ($\{ij\} \in M_\pi$) and $\Phi_k (k \in K)$

[5] See Chapter 5, Section 5.2.2

[6] See Chapter 5, Section 5.2.3

μ_ι and σ_ι, i.e.

$$\phi_\iota \sim \Lambda(\mu_\iota, \sigma_\iota) \quad \text{for all } \iota$$

Function $h_v(\underline{x})$ in the GS model given in (6.4) is a log-linear function of proportions ϕ_ι. In view of the fact that products of lognormal variables are themselves lognormally distributed, the choice of a lognormal distribution for the prior on ϕ_ι leads to simple and elegant calculations. Moreover, assumptions of local independence also significantly simplify uncertainty analysis, and thus are often made within the context of Bayesian graphical models [Spiegelhalter and Lauritzen, 1990]. Figure 6.2 embodies these assumptions, which are not graphically represented in the network of the ID model, but are integral into its mathematical structure .

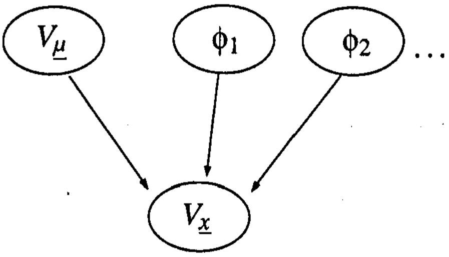


Figure 6.2: A priori dependency relationships in the GS model

The case where V is a root cause variable, and the case where V is a coupling factor variable will be considered separately.

6.4.1 Root Cause Variables

As defined previously, each root cause is expressed in the ID by a random variable r_i representing the rate of events due to the particular root cause i ($i = 1, ..., \rho$). Let $\underline{\phi_i} = (\phi_{i,1}, ..., \phi_{i,m_i})$ be the proportion parameters related to r_i.

The uncertainty distribution on the 'base-level' r.v. $r_{i,\underline{\mu}}$ is a gamma density with shape parameter a_i and scale parameter b_i, viz.

$$r_{i,\underline{\mu}} \sim \mathcal{G}(a_i, b_i)$$

According to Model (6.4) it holds that

$$r_{i,\underline{x}} = h_i(\underline{x}) \cdot r_{i,\underline{\mu}} \tag{6.8}$$

where $\underline{x} = (x_1,...,x_n)$ and $h_i(\underline{x}) : \Omega_1 \times \ldots \times \Omega_n \to \mathbb{R}$ is a log-linear function of $\phi_{i,\iota}$, $\iota = 1,...,m_i$. By using variable transformation techniques consistently with model (6.8) and for given $\phi_{i,\iota}$ ($\iota = 1,...,m_i$), one obtains the prior distribution on $r_{i,\underline{x}}$, which is again a gamma density, viz.

$$f(r_{i,\underline{x}} \mid \underline{\phi_i}) := \mathcal{G}\left(a_i, \frac{b_i}{h_i(\underline{x})}\right) \quad . \tag{6.9}$$

and on the grounds of the GS model (6.8), the prior distribution on $r_{i,\underline{x}}$ is

$$f(r_{i,\underline{x}}) = \int_{-\infty}^{+\infty} f(r_{i,\underline{x}} \mid \underline{\phi_i}) f(\underline{\phi_i}) \mathrm{d}\underline{\phi_i}$$

Parameters $\phi_{i,\iota}$, for $\iota = 1,...,m_i$, are *a priori* mutually independent random variables, and the joint prior is

$$f(\underline{\phi_i}) = f_1(\phi_{i,1}) \ldots f_{m_i}(\phi_{i,m_i}) \quad .$$

where f_ι is the marginal distribution of $\phi_{i,\iota}$.

Thus, $f(r_{i,\underline{x}})$ is a continuous version of a mixture of priors. Mixture priors are frequently used in reliability; Diaconis and Ylvisaker [Diaconis and Ylvisaker, 1985] showed that any prior can be satisfactorily represented as a 'mixture prior', whereas Youngblood and Atwood [Youngblood and Atwood, 2005] defined mixture priors to model different performance states of a component.

The joint prior distribution of rates due to root cause i is

$$\begin{aligned} & f(r_{i,(1,\ldots,1)}, \ldots, r_{i,(x_1,\ldots,x_n)}, \ldots) = \\ & = \int_{-\infty}^{+\infty} f(r_{i,(1,\ldots,1)}, \ldots, r_{i,(x_1,\ldots,x_n)}, \ldots \mid \underline{\phi_i}) f(\underline{\phi_i}) \mathrm{d}\underline{\phi_i} \\ & = f(r_{i,(\mu_1,\ldots,\mu_n)}) \prod_{x_1 \neq \mu_1,\ldots,x_n \neq \mu_n} \int_{-\infty}^{+\infty} f(r_{i,(x_1,\ldots,x_n)} \mid \underline{\phi_i}) f(\underline{\phi_i}) \mathrm{d}\underline{\phi_i} \end{aligned}$$

6.4.2 Coupling Factor Variables

Recall that each coupling factor is described by a vector of parameters

$$\underline{p_i} = (p_{i1}, p_{i2}, ..., p_{i\kappa}) \quad \text{for every } i = 1, ..., \rho,$$

where

$$p_{ij} = P(\text{CCF through coupling factor } j \mid \text{failure due to root cause } i), \quad j = 1, 2, ..., \kappa$$

Let $\underline{\varphi_{ij}} = (\phi_{ij,1}, ..., \phi_{ij,m_{ij}})$ be the proportion parameters related to p_{ij}. According to the GS model (6.4),

$$p_{ij,\underline{x}} = h_{ij}(\underline{x}) \cdot p_{ij,\underline{\mu}} \tag{6.10}$$

where $\underline{x} = (x_1, ..., x_n)$ is the system's configuration vector and $h_{ij}(\underline{x}) : \Omega_1 \times \ldots \times \Omega_n \rightarrow \mathbb{R}$ is a log-linear function of $\varphi_{i,\iota}$, $\iota = 1, ..., m_{ij}$.

Random variable $p_{ij,\underline{\mu}}$ is a beta distributed variable, therefore it is restricted within the interval $[0, 1]$. However, for large enough values of $h_{ij}(\underline{x})$, the transformed variable $p_{ij,\underline{x}}$ of Relationship (6.10) may in principle take values outside this interval. Thus, the distribution obtained analytically through the variable transformation is no longer a beta distribution. However, CCF events are by nature rare, and variables $p_{ij,\underline{x}}$ essentially take particularly small values. This fact allows to approximate the distribution of $p_{ij,\underline{x}}$ by a beta distribution, without significant loss of information.

Numerically, this approximation is performed by assuring that the first two moments of $p_{ij,\underline{x}}$ agree with (6.10), i.e.

$$E(p_{ij,\underline{x}}) = h_{ij}(\underline{x}) E(p_{ij,\underline{\mu}}) \tag{6.11}$$

$$Var(p_{ij,\underline{x}}) = h_{ij}(\underline{x})^2 Var(p_{ij,\underline{\mu}}) \tag{6.12}$$

Let

$$p_{ij,\underline{\mu}} \sim \mathcal{B}(\gamma_{ij}, \delta_{ij}) \quad \text{and} \quad p_{ij,\underline{x}} \sim \mathcal{B}(\gamma_{ij,\underline{x}}, \delta_{ij,\underline{x}})$$

Now, specifying the prior on $p_{ij,\underline{x}}$ reduces to the task of determining the beta parameters $\gamma_{ij,\underline{x}}$ and $\delta_{ij,\underline{x}}$ such that Relationships (6.11) and (6.12) are met, leading to the system of equations

$$\frac{\gamma_{ij,\underline{x}}}{\gamma_{ij,\underline{x}}+\delta_{ij,\underline{x}}} = h_{ij}(\underline{x})\frac{\gamma_{ij}}{\gamma_{ij}+\delta_{ij}} \tag{6.13}$$

$$\frac{\gamma_{ij,\underline{x}}\delta_{ij,\underline{x}}}{(\gamma_{ij,\underline{x}}+\delta_{ij,\underline{x}})^2(\gamma_{ij,\underline{x}}+\delta_{ij,\underline{x}}+1)} = h_{ij}(\underline{x})^2\frac{\gamma_{ij}\delta_{ij}}{(\gamma_{ij}+\delta_{ij})^2(\gamma_{ij}+\delta_{ij}+1)} \tag{6.14}$$

The system provides a closed form solution for $\gamma_{ij,\underline{x}}$ and $\delta_{ij,\underline{x}}$, and let

$$\gamma_{ij,\underline{x}} = s_1(\underline{x}) \quad \text{and} \quad \delta_{ij,\underline{x}} = s_2(\underline{x})$$

be the solutions of the system, where

$$s_1 : \Omega_1 \times \ldots \times \Omega_n \to (0,\infty) \quad \text{and} \quad s_2 : \Omega_1 \times \ldots \times \Omega_n \to (0,\infty)$$

are functions with parameters φ_ι $(\iota = 1,...,m_{ij})$. A similar approach of moment-fitting is explored in [Mazzuchi and Soyer, 1992].

Now, the prior distribution on $p_{ij,\underline{x}}$ is a continuous mixture of prior distributions. In particular,

$$f(p_{ij,\underline{x}}) = \int_{-\infty}^{+\infty} f(p_{ij,\underline{x}} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) \mathrm{d}\underline{\varphi_{ij}}$$

where

$$f(p_{ij,\underline{x}} \mid \underline{\varphi_{ij}}) := \mathcal{B}(\gamma_{ij,\underline{x}}, \delta_{ij,\underline{x}})$$

Parameters $\varphi_{ij,\iota}$, for $\iota = 1,...,m_{ij}$, are considered as independent random variables with joint prior:

$$f(\underline{\varphi_{ij}}) = f_1(\varphi_{ij,1})\cdots f_{m_{ij}}(\varphi_{ij,m_{ij}})$$

where f_ι is the marginal distribution of $\varphi_{ij,\iota}$.

The joint prior distribution of r.v.'s expressing the intensity of coupling factor j

related to root cause i, is

$$\begin{aligned}
&f(p_{ij,(1,\ldots,1)},\cdots,p_{ij,(x_1,\ldots,x_n)},\cdots) = \\
&= \int_{-\infty}^{+\infty} f(p_{ij,(1,\ldots,1)},\cdots,p_{ij,(x_1,\ldots,x_n)},\cdots \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) \mathrm{d}\underline{\varphi_{ij}} \\
&= f(p_{ij,(\mu_1,\ldots,\mu_n)}) \prod_{x_1 \neq \mu_1,\ldots,x_n \neq \mu_n} \int_{-\infty}^{+\infty} f(p_{ij,(x_1,\ldots,x_n)} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) \mathrm{d}\underline{\varphi_{ij}}
\end{aligned}$$

6.5 Bayesian Update

6.5.1 Introduction

The process of learning from experience, as it occurs within the GS model, is now illustrated. Suppose that data regarding a variable at a particular level configuration becomes available. Through the GS model the additional information becomes relevant to variables at other configuration levels, allowing for revision of inferences.

Root cause and coupling factor variables will be explored separately. For the purposes of simplification, the indices denoting the category of root cause or coupling factor will be omitted.

6.5.2 Root Cause Variables

The dependency relationships amongst the parameters of the GS model *prior* any update are depicted in Figure 6.3. When information for a particular defence configuration level $\underline{x} = (x_1,\ldots,x_n)$ becomes available, this the information is propagated through the arcs of Figure 6.3 to the rest of the levels, allowing to revise the uncertainty on $r_{\underline{x}}$, for any x_i, $i = 1,\ldots,n$.

Form of data

The information relevant to $r_{\underline{x}}$ comprises of the number of failures attributed to the particular root cause $n_{\underline{x}}$, recorded during the fixed observation time of $T_{\underline{x}}$ units, from a

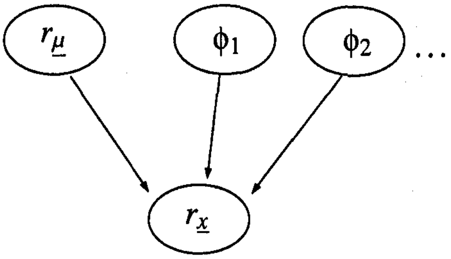


Figure 6.3: A priori dependency relationships for root cause variables r_i.

system with defence configuration vector $\underline{x} = (x_1, ..., x_k)$[7]. Let

$$d_{\underline{x}} = (n_{\underline{x}}, T_{\underline{x}}) \quad \text{where } T_{\underline{x}} \text{ is fixed}$$

with likelihood represented by the Poisson distribution

$$f(d_{\underline{x}} \mid r_{\underline{x}}) = \frac{(r_{\underline{x}} T_{\underline{x}})^{n_{\underline{x}}}}{n_{\underline{x}}!} e^{-r_{\underline{x}} T_{\underline{x}}}, \quad n_{\underline{x}} = 0, 1, 2, ..., \; r_{\underline{x}} \in (0, +\infty)$$

Evidence on base-level $r_{\underline{\mu}}$

Suppose that data relates to $r_{\underline{\mu}}$, denoted with $d_{\underline{\mu}} = (n_{\underline{\mu}}, T_{\underline{\mu}})$. Prior uncertainty on $r_{\underline{\mu}}$ is represented by the subjective distribution $f(r_{\underline{\mu}})$. Let

$$f(r_{\underline{\mu}}) := \mathcal{G}(a, b)$$

The posterior uncertainty on $r_{\underline{\mu}}$, in the light of data $d_{\underline{\mu}}$, is by Bayes' law:

$$f(r_{\underline{\mu}} \mid d_{\underline{\mu}}) \propto f(d_{\underline{\mu}} \mid r_{\underline{\mu}}) f(r_{\underline{\mu}})$$

Due to the conjugate properties of the Poisson and the gamma families of distributions, $f(r_{\underline{\mu}})$ is again a gamma, viz.

$$f(r_{\underline{\mu}} \mid d_{\underline{\mu}}) := \mathcal{G}(a + n_{\underline{\mu}}, b + T_{\underline{\mu}})$$

[7] See Chapter 5, Section 5.3.2

Once uncertainty on the 'base-level' rate is updated, information is propagated through the arcs of the graph as depicted in Figure 6.4. The uncertainty on $r_{\underline{x}}$ alters to

$$f(r_{\underline{x}} \mid d_{\underline{\mu}}) = \int_{-\infty}^{\infty} f(r_{\underline{x}} \mid d_{\underline{\mu}}, \underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi}$$

where $f(r_{\underline{x}} \mid d_{\underline{\mu}}, \underline{\phi})$ is the uncertainty on $r_{\underline{x}}$ determined through the GS model by considering the updated uncertainty on the base-level variable $f(r_{\underline{\mu}} \mid d_{\underline{\mu}})$, viz.

$$f(r_{\underline{x}} \mid d_{\underline{\mu}}, \underline{\phi}) := \mathcal{G}\left(a + n_{\underline{\mu}}, \frac{b + T_{\underline{\mu}}}{h(\underline{x})}\right)$$

where $r_{\underline{x}} = h(\underline{x}) r_{\underline{\mu}}$ and $h(\underline{x})$ is log-linear with parameters ϕ_ι $(\iota = 1, ..., m)$.

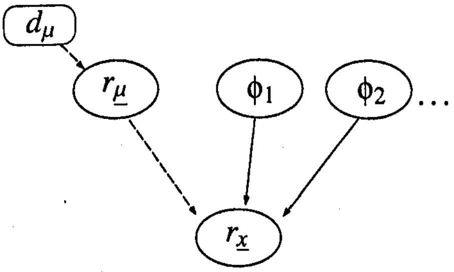


Figure 6.4: When base-level rate is updated, information is transmitted through the dotted arc

Evidence at configuration level $\underline{x}^*$

Suppose that data $d_{\underline{x}^*} = (n_{\underline{x}^*}, T_{\underline{x}^*})$ becomes available regarding variable $r_{\underline{x}^*}$, where $\underline{x}^* = (x_1^*, ..., x_n^*)$ and $x_i^* \neq \mu_i$, $i = 1, ..., n$. The objective is to specify the updated uncertainty on $r_{\underline{x}^*}$, in view of data $d_{\underline{x}^*}$. Consistently with the GS model we have

$$r_{\underline{x}^*} = h(\underline{x}^*) r_{\underline{\mu}}$$

where $h : \Omega_1 \times \ldots \times \Omega_n \to \mathbb{R}$ is a function with parameters ϕ_ι ($\iota = 1,\ldots,m$); thereby, the prior on $r_{\underline{x}^*}$ is a mixture prior, viz.

$$f(r_{\underline{x}^*}) = \int\limits_{-\infty}^{+\infty} f(r_{\underline{x}^*} \mid \underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi}$$

where

$$f(r_{\underline{x}^*} \mid \underline{\phi}) := \mathcal{G}\,(a, \frac{b}{h(\underline{x}^*)})$$

The updated uncertainty on $r_{\underline{x}^*}$ is obtained by averaging over all the values of $\underline{\phi}$:

$$\begin{aligned} f(r_{\underline{x}^*} \mid d_{\underline{x}^*}) &= E_{\underline{\phi}}\left[f(r_{\underline{x}^*} \mid d_{\underline{x}^*}, \underline{\phi})\right] \\ &= \int\limits_{-\infty}^{+\infty} f(r_{\underline{x}^*} \mid d_{\underline{x}^*}, \underline{\phi}) f(\underline{\phi} \mid d_{\underline{x}}^*) \mathrm{d}\underline{\phi} \end{aligned}$$

Due to the conjugate properties of the Poisson and gamma families of distributions, the updated uncertainty $f(r_{\underline{x}^*} \mid d_{\underline{x}^*}, \underline{\phi})$ is again a gamma distribution, and in particular

$$f(r_{\underline{x}^*} \mid d_{\underline{x}^*}, \underline{\phi}) := \mathcal{G}\,(a + n_{\underline{x}^*}, \frac{b}{h(\underline{x}^*)} + T_{\underline{x}^*})$$

So, the interest lies in specifying the updated joint uncertainty $f(\underline{\phi} \mid d_{\underline{x}^*})$. By Bayes' law

$$f(\underline{\phi} \mid d_{\underline{x}^*}) = \frac{f(\underline{\phi}) f(d_{\underline{x}^*} \mid \underline{\phi})}{\int\limits_{-\infty}^{+\infty} \left\{ f(\underline{\phi}) f(d_{\underline{x}^*} \mid \underline{\phi}) \right\} \mathrm{d}\underline{\phi}} \tag{6.15}$$

Integrating over the range of $r_{\underline{x}^*}$ gives

$$f(d_{\underline{x}^*} \mid \underline{\phi}) = E_{r_{\underline{x}^*}}\left[f(d_{\underline{x}^*} \mid \underline{\phi}, r_{\underline{x}^*})\right] = \int\limits_{0}^{+\infty} f(d_{\underline{x}^*} \mid \underline{\phi}, r_{\underline{x}^*}) f(r_{\underline{x}^*} \mid \underline{\phi}) \mathrm{d}r_{\underline{x}^*} \tag{6.16}$$

and (6.15) becomes

$$f(\underline{\phi} \mid d_{\underline{x}^*}) = \frac{f(\underline{\phi}) \int\limits_{0}^{+\infty} f(d_{\underline{x}^*} \mid r_{\underline{x}^*}, \underline{\phi}) f(r_{\underline{x}^*} \mid \underline{\phi}) \mathrm{d}r_{\underline{x}^*}}{\int\limits_{-\infty}^{+\infty} \left\{ f(\underline{\phi}) \int\limits_{0}^{+\infty} f(d_{\underline{x}^*} \mid r_{\underline{x}^*}) f(r_{\underline{x}^*} \mid \underline{\phi}) \mathrm{d}r_{\underline{x}^*} \right\} \mathrm{d}\underline{\phi}} \tag{6.17}$$

For the implementation of model (6.15), the distribution $f(d_{\underline{x}^*} \mid \underline{\phi})$ is analytically determined through Relationship (6.16), and more specifically it is

$$f(d_{\underline{x}^*} \mid \underline{\phi}) \propto \frac{(T_{\underline{x}^*})^{n_{\underline{x}^*}}}{\left(T_{\underline{x}^*} + \frac{b}{h(\underline{x}^*)}\right)^{n_{\underline{x}^*}+a}} \left(\frac{b}{h(\underline{x}^*)}\right)^{a} \tag{6.18}$$

However, the integral implicit (6.15) may not be analytically solvable; consequently, subsequent analysis requires the use of computational methods.

Propagation of evidence to base-level rate

Once $r_{\underline{x}^*}$ is updated, the propagation of evidence is accomplished through the 'arc reversal' transformation [Shachter, 1986], representing Bayes' theorem (Figure 6.5).

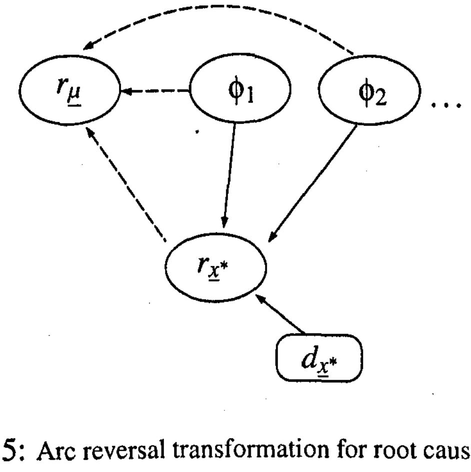


Figure 6.5: Arc reversal transformation for root cause variables

In the particular case, the arc reversal represents the inverse variable transformation

$$r_{\underline{\mu}} = \frac{1}{h(\underline{x}^*)} r_{\underline{x}^*} = h(\underline{x}^*)^{-1} r_{\underline{x}^*}$$

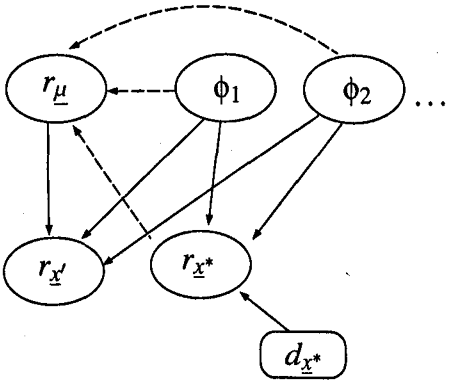


Figure 6.6: Information transmission from base-level rate to the rest of the defence level configurations

which leads to

$$f(r_{\underline{\mu}} \mid d_{\underline{x}^*}) \propto \int_{-\infty}^{+\infty} f(\underline{\phi} \mid d_{\underline{x}^*}) \cdot f(r_{\underline{\mu}} \mid d_{\underline{x}^*}, \underline{\phi}) \mathrm{d}\underline{\phi} \tag{6.19}$$

where

$$f(r_{\underline{\mu}} \mid d_{\underline{x}^*}, \underline{\phi}) := \mathcal{G}(a + n_{\underline{x}^*}, b + h(\underline{x}^*) T_{\underline{x}^*}) \tag{6.20}$$

Note that after the arc reversal process, arrows are added from $\underline{\phi}$ to $r_{\underline{\mu}}$. This implies that after updating, the aforementioned variables are not independent. This is consistent with relationships (6.19) and (6.24).

Propagation of evidence to other configuration levels

Now, due to the updated uncertainty on the base-level rate and proportion parameters, the distribution on $r_{\underline{x}'}$ for $\underline{x}' \neq \underline{x}^*, \underline{\mu}$ is revised as well (see Figure 6.6).

For

$$r_{\underline{x}'} = h(\underline{x}') r_{\underline{\mu}}$$

it is

$$f(r_{\underline{x}'} \mid d_{\underline{x}^*}) \propto \int_{-\infty}^{+\infty} f(r_{\underline{x}'} \mid d_{\underline{x}^*}, \underline{\phi}) \cdot f(\underline{\phi} \mid d_{\underline{x}^*}) \mathrm{d}\underline{\phi} \tag{6.21}$$

where

$$f(r_{\underline{x}'} \mid d_{\underline{x}^*}, \underline{\phi}) := \mathcal{G}\left(a + n_{\underline{x}^*}, \frac{b}{h(\underline{x}')} + \frac{h(\underline{x}^*)}{h(\underline{x}')} T_{\underline{x}^*}\right) \tag{6.22}$$

Acquisition of data at multiple levels

Suppose that data becomes available regarding rate r at different configuration levels $\underline{x_1}$ and $\underline{x_2}$, for which

$$r_{\underline{x_1}} = h(\underline{x_1}) r_{\underline{\mu}} \quad \text{and} \quad r_{\underline{x_2}} = h(\underline{x_2}) r_{\underline{\mu}}$$

Then, the update uncertainty of r at any configuration level $\underline{x}$, for which

$$r_{\underline{x}} = h(\underline{x}) r_{\underline{\mu}}$$

in the light of data $d_{\underline{x_1}} = (n_1, T_1)$ and $d_{\underline{x_2}} = (n_2, T_2)$, is

$$f(r_{\underline{x}} \mid d_{\underline{x_1}}, d_{\underline{x_2}}) \propto \int_{-\infty}^{+\infty} f(r_{\underline{x}} \mid \underline{\phi}, d_{\underline{x_1}}, d_{\underline{x_2}}) \cdot f(\underline{\phi} \mid d_{\underline{x_1}}, d_{\underline{x_2}}) \mathrm{d}\underline{\phi} \tag{6.23}$$

where

$$f(r_{\underline{x}} \mid \underline{\phi}, d_{\underline{x_1}}, d_{\underline{x_2}}) := \mathcal{G}\left(a + n_1 + n_2, \frac{b}{h(\underline{x})} + \frac{h(\underline{x_1})}{h(\underline{x})} T_1 + \frac{h(\underline{x_2})}{h(\underline{x})} T_2\right) \tag{6.24}$$

and

$$f(\underline{\phi} \mid d_{\underline{x_1}}, d_{\underline{x_2}}) \propto f(\underline{\phi}) f(d_{\underline{x_1}} \mid \underline{\phi}) f(d_{\underline{x_2}} \mid d_{\underline{x_1}}, \underline{\phi}) \tag{6.25}$$

Distribution $f(d_{\underline{x_1}} \mid \underline{\phi})$ is specified through the model given in (6.16), and distribution $f(d_{\underline{x_2}} \mid d_{\underline{x_1}}, \underline{\phi})$ is the likelihood of data $d_{\underline{x_2}}$.

In general, suppose that data set d is divided into different part $d = (d_1, d_2, ..., d_m)$. Applying Bayes' theorem sequentially with data $d_1, d_2, ...$ is equivalent to applying it a single time with data $d = d_1 + d_2 + ...$ In this fashion, the posterior distribution on $\underline{\phi}$ given in (6.25) may be viewed as the result of a single application of Bayes' theorem in the light of the 'transformed' data

$$d = (n_1 + n_2, \frac{h(\underline{x_1})}{h(\underline{x})} T_1 + \frac{h(\underline{x_2})}{h(\underline{x})} T_2)$$

Summary

Table 6.1 summarises the updating process for root cause variables

6.5.3 Coupling Factor Variables

The dependency relationships amongst the parameters of the GS model *prior* any update are depicted in Figure 6.7. Suppose that information for a particular defence configuration level $\underline{x} = (x_1, ..., x_n)$ becomes available; the information is propagated through the arcs of Figure 6.7 to the rest of the levels, allowing to revise the uncertainty on $p_{\underline{x}}$, for any x_k, $k = 1, ..., n$.

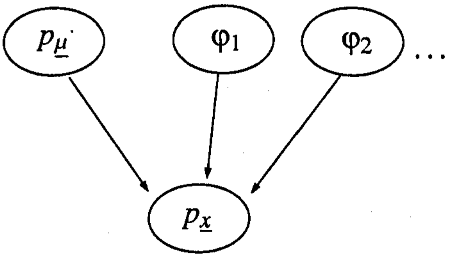


Figure 6.7: A priori dependency relationships for coupling factor variables p_{ij}

The information relevant to $p_{\underline{x}}$ comprises of the number of failures $n_{\underline{x}}$ that resulted in a CCF via the particular coupling mechanism j, observed out of $m_{\underline{x}}$ failures due to a particular root cause i, at a system with configuration vector $\underline{x} = (x_1, ..., x_k)$[8]. Let

$$d_{\underline{x}} = (n_{\underline{x}}, m_{\underline{x}})$$

[8] See Chapter 5, Section 5.2.3

Table 6.1: Updating root cause variables

Data:

$$d_{\underline{x}} = (n, T)$$

Likelihood function:

$$f(d_{\underline{x}} \mid r_{\underline{x}}) = \frac{(r_{\underline{x}} T)^n}{n!} e^{-r_{\underline{x}} T}$$

GSM:

$$r_{\underline{x}} = h(\underline{x}) r_{\underline{\mu}}$$

Prior Distribution	Posterior Distribution
$f(r_{\underline{\mu}}) := \mathcal{G}(a, b)$	$f(r_{\underline{\mu}} \mid d_{\underline{x}}, \underline{\phi}) := \mathcal{G}(a+n, b+h(\underline{x})T)$
$f(r_{\underline{x}} \mid \underline{\phi}) := \mathcal{G}(a, \frac{b}{h(\underline{x})})$	$f(r_{\underline{x}} \mid d_{\underline{x}}, \underline{\phi}) := \mathcal{G}(a+n, \frac{b}{h(\underline{x})} + T)$
$f(\underline{\phi}) = \prod_{\iota} f_{\iota}(\phi_{\iota})$	$f(\underline{\phi} \mid d_{\underline{x}}) = \frac{f(\underline{\phi}) \int f(d_{\underline{x}} \mid r_{\underline{x}}, \underline{\phi}) f(r_{\underline{x}} \mid \underline{\phi}) \mathrm{d}r_{\underline{x}}}{\int_{-\infty}^{+\infty} \left\{ f(\underline{\phi}) \int f(d_{\underline{x}} \mid r_{\underline{x}}) f(r_{\underline{x}} \mid \underline{\phi}) \mathrm{d}r_{\underline{x}} \right\} \mathrm{d}\underline{\phi}}$
$f(r_{\underline{x}^*} \mid \underline{\phi}) := \mathcal{G}(a, \frac{b}{h(\underline{x}^*)})$	$f(r_{\underline{x}^*} \mid d_{\underline{x}}, \underline{\phi}) := \mathcal{G}(a+n, \frac{b}{h(\underline{x}^*)} + \frac{h(\underline{x})}{h(\underline{x}^*)} T)$

with likelihood represented by the binomial distribution

$$f(d_{\underline{x}} \mid p_{\underline{x}}) \propto p_{\underline{x}}^{n_{\underline{x}}}(1-p_{\underline{x}})^{m_{\underline{x}}-n_{\underline{x}}} \quad m_{\underline{x}}, n_{\underline{x}} = 0,1,2,\ldots,\ p_{\underline{x}} \in [0,1]$$

Evidence on base-level $p_{\underline{\mu}}$

Suppose that the information relates to $p_{\underline{\mu}}$, that is $d_{\underline{\mu}} = (n_{\underline{\mu}}, m_{\underline{\mu}})$. The prior uncertainty on $p_{\underline{\mu}}$ is represented by the subjective distribution $f(p_{\underline{\mu}})$. Let

$$f(p_{\underline{\mu}}) := \mathcal{B}(\gamma, \delta)$$

The posterior uncertainty on $p_{\underline{\mu}}$, in the light of data $d_{\underline{\mu}}$, is by Bayes' law:

$$f(p_{\underline{\mu}} \mid d_{\underline{\mu}}) \propto f(d_{\underline{\mu}} \mid p_{\underline{\mu}}) f(p_{\underline{\mu}})$$

Due to the conjugate properties of the binomial and the beta family of distributions, $f(p_{\underline{\mu}})$ is again a beta distribution, viz.

$$f(p_{\underline{\mu}} \mid d_{\underline{\mu}}) := \mathcal{B}(\gamma + n_{\underline{\mu}}, \delta + m_{\underline{\mu}} - n_{\underline{\mu}})$$

Once $f(p_{\underline{\mu}})$ is updated, the new evidence is propagated through the arcs of the graph, as depicted in Figure 6.8, to update the uncertainty on $p_{\underline{x}}$:

$$f(p_{\underline{x}} \mid d_{\underline{\mu}}) = \int_{-\infty}^{\infty} f(p_{\underline{x}} \mid d_{\underline{\mu}}, \underline{\varphi}) f(\underline{\varphi}) \mathrm{d}\underline{\varphi}$$

where $f(p_{\underline{x}} \mid d_{\underline{\mu}}, \underline{\varphi})$ is the uncertainty on $p_{\underline{x}}$, obtained through the GS model by considering the updated uncertainty on the base-level variable, $f(p_{\underline{\mu}} \mid d_{\underline{\mu}})$. In particular,

$$f(p_{\underline{x}} \mid d_{\underline{\mu}}, \underline{\varphi}) := \mathcal{B}(\gamma_{\underline{x}}, d_{\underline{x}})$$

where parameters $\gamma_{\underline{x}}$ and $\delta_{\underline{x}}$ are the solutions of System

$$\frac{\gamma_{\underline{x}}}{\gamma_{\underline{x}}+\delta_{\underline{x}}} = h(\underline{x})\frac{\gamma+n_{\underline{\mu}}}{\gamma+\delta+m_{\underline{\mu}}}$$

$$\frac{\gamma_{\underline{x}}\delta_{\underline{x}}}{(\gamma_{\underline{x}}+\delta_{\underline{x}})^2(\gamma_{\underline{x}}+\delta_{\underline{x}}+1)} = h(\underline{x})^2\frac{(\gamma+n_{\underline{\mu}})(\delta+m_{\underline{\mu}}-n_{\underline{\mu}})}{(\gamma+\delta+m_{\underline{\mu}})^2(\gamma+\delta+m_{\underline{\mu}}+1)}$$

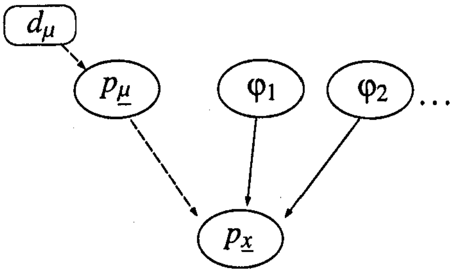


Figure 6.8: When base-level coupling probability is updated, information is transmitted through the dotted arc

Evidence at configuration level $\underline{x}^*$

Suppose that data $d_{\underline{x}^*} = (n_{\underline{x}^*}, m_{\underline{x}^*})$ becomes available regarding variable $p_{\underline{x}^*}$, where $\underline{x}^* = (x_1^*, \ldots, x_n^*)$ and $x_i^* \neq \mu_i$, $i = 1, \ldots, n$ for which

$$p_{\underline{x}^*} = h(\underline{x}^*)p_{\underline{\mu}}$$

The prior distribution on $p_{\underline{x}^*}$ is a mixture prior, viz.

$$f(p_{\underline{x}^*}) = \int_{-\infty}^{+\infty} f(p_{\underline{x}^*} \mid \underline{\varphi}) f(\underline{\varphi}) \mathrm{d}\underline{\varphi}$$

where

$$f(p_{\underline{x}^*} \mid \underline{\varphi}) := \mathcal{B}(\gamma_{\underline{x}^*}, \delta_{\underline{x}^*})$$

with parameters

$$\gamma_{\underline{x}^*} = s_1(\underline{x}^*) \quad \text{and} \quad \delta_{\underline{x}^*} = s_2(\underline{x}^*)$$

that are solutions of the system

$$\begin{aligned}\frac{\gamma_{\underline{x}^*}}{\gamma_{\underline{x}^*}+\delta_{\underline{x}^*}} &= h(\underline{x}^*)\frac{\gamma}{\gamma+\delta}\\ \frac{\gamma_{\underline{x}^*}\delta_{\underline{x}^*}}{(\gamma_{\underline{x}^*}+\delta_{\underline{x}^*})^2(\gamma_{\underline{x}^*}+\delta_{\underline{x}^*}+1)} &= h(\underline{x}^*)^2\frac{\gamma\delta}{(\gamma+\delta)^2(\gamma+\delta+1)}\end{aligned}$$

Following similar steps as in Section 6.5.2, one concludes that the updated uncertainty on $p_{\underline{x}^*}$ is

$$\begin{aligned}f(p_{\underline{x}^*}\mid d_{\underline{x}^*}) &= E_{\underline{\varphi}}\left[f(p_{\underline{x}^*}\mid d_{\underline{x}^*},\underline{\varphi})\right]\\ &= \int_{-\infty}^{+\infty} f(p_{\underline{x}^*}\mid d_{\underline{x}^*},\underline{\varphi})f(\underline{\varphi}\mid d_{\underline{x}^*})\mathrm{d}\underline{\varphi}\end{aligned}$$

Due to the conjugate properties of the binomial and beta families of distributions, the updated uncertainty $f(p_{\underline{x}^*}\mid d_{\underline{x}^*},\underline{\varphi})$ is again a beta distribution, and in particular

$$f(p_{\underline{x}^*}\mid d_{\underline{x}^*};\underline{\varphi}) := \mathcal{B}\left(\gamma_{\underline{x}^*}+n_{\underline{x}^*}, d_{\underline{x}^*}+m_{\underline{x}^*}-n_{\underline{x}^*}\right)$$

and the updated joint uncertainty $f(\underline{\varphi}\mid d_{\underline{x}^*})$ is given by

$$\begin{aligned}f(\underline{\varphi}\mid d_{\underline{x}^*}) &= \frac{f(\underline{\varphi})f(d_{\underline{x}^*}\mid\underline{\varphi})}{\int_{-\infty}^{+\infty}\left\{f(\underline{\varphi})f(d_{\underline{x}^*}\mid\underline{\varphi})\right\}\mathrm{d}\underline{\varphi}}\\ &= \frac{f(\underline{\varphi})\int_0^1 f(d_{\underline{x}^*}\mid p_{\underline{x}^*},\underline{\varphi})f(p_{\underline{x}^*}\mid\underline{\varphi})\mathrm{d}p_{\underline{x}^*}}{\int_{-\infty}^{+\infty}\left\{f(\underline{\varphi})\int_0^1 f(d_{\underline{x}^*}\mid p_{\underline{x}^*})f(p_{\underline{x}^*}\mid\underline{\varphi})\mathrm{d}p_{\underline{x}^*}\right\}\mathrm{d}\underline{\varphi}}\end{aligned} \qquad (6.26)$$

As previously, $f(d_{\underline{x}^*}\mid\underline{\varphi})$ is analytically determined, and more particularly

$$f(d_{\underline{x}^*}\mid\underline{\varphi}) \propto \frac{\Gamma(m_{\underline{x}^*}-n_{\underline{x}^*}+\delta_{\underline{x}^*})\Gamma(n_{\underline{x}^*}+\gamma_{\underline{x}^*})}{B(\gamma_{\underline{x}^*},\delta_{\underline{x}^*})\Gamma(m_{\underline{x}^*}+\gamma_{\underline{x}^*}+\delta_{\underline{x}^*})}$$

whereas the specification of the normalising constant in (6.26) requires to numerically approximate the implicit integral.

Propagation of evidence to base-level coupling variable

Once $p_{\underline{x}^*}$ is updated, propagation of information is accomplished through the 'arc reversal' transformation [Shachter, 1986], representing Bayes' theorem (Figure 6.9).

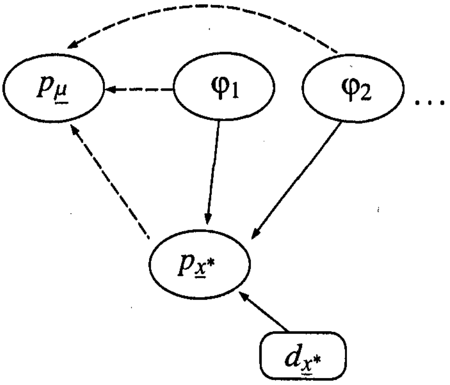


Figure 6.9: Arc reversal transformation for coupling factor variables

The arc reversal represents the inverse variable transformation

$$p_{\underline{\mu}} = \frac{1}{h(\underline{x}^*)} p_{\underline{x}^*} = h(\underline{x}^*)^{-1} p_{\underline{x}^*} \tag{6.27}$$

The uncertainty distribution on $p_{\underline{\mu}}$ is again a mixture of distributions, viz.

$$f(p_{\underline{\mu}} \mid d_{\underline{x}^*}) \propto \int_{-\infty}^{+\infty} f(\underline{\varphi} \mid d_{\underline{x}^*}) \cdot f(p_{\underline{\mu}} \mid d_{\underline{x}^*}, \underline{\varphi}) \mathrm{d}\underline{\varphi} \tag{6.28}$$

For given the proportion parameters $\underline{\varphi}$, let

$$f(p_{\underline{\mu}} \mid d_{\underline{x}^*}, \underline{\varphi}) := \mathcal{B}(\gamma', \delta')$$

The parameters of $f(p_{\underline{\mu}} \mid d_{\underline{x}^*}, \underline{\varphi})$ are obtained by matching

$$E(p_{\underline{\mu}}) = h(\underline{x}^*)^{-1} E(p_{\underline{x}^*}) \tag{6.29}$$

$$Var(p_{\underline{\mu}}) = h(\underline{x}^*)^{-2} Var(p_{\underline{x}^*}) \tag{6.30}$$

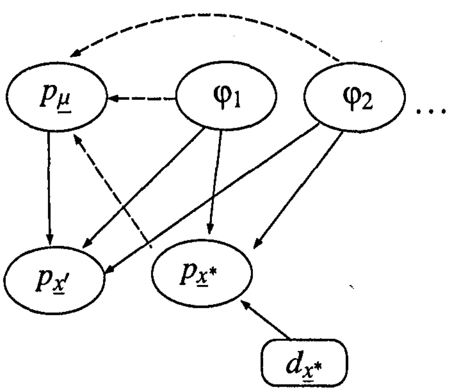


Figure 6.10: Information transmission from base-level coupling probability to the rest of the defence level configurations

and γ', δ' are the solution of the system of equations

$$\frac{\gamma'}{\gamma'+\delta'} = \frac{1}{h(\underline{x}^*)}\frac{\gamma_{\underline{x}^*}+n_{\underline{x}^*}}{\gamma_{\underline{x}^*}+\delta_{\underline{x}^*}+m_{\underline{x}^*}}$$

$$\frac{\gamma'\delta'}{(\gamma'+\delta')^2(\gamma'+\delta'+1)} = \frac{1}{h(\underline{x}^*)^2}\frac{(\gamma_{\underline{x}^*}+n_{\underline{x}^*})(\delta_{\underline{x}^*}+m_{\underline{x}^*}-n_{\underline{x}^*})}{(\gamma_{\underline{x}^*}+\delta_{\underline{x}^*}+m_{\underline{x}^*})^2(\gamma_{\underline{x}^*}+\delta_{\underline{x}^*}+m_{\underline{x}^*}+1)}$$

Note that during the arc reversal process, an arrow is added from $\underline{\phi}$ to $r_{\underline{\mu}}$. This implies that after updating, the aforementioned variables are no longer independent.

Propagation of evidence to other configuration levels

Now, due to the updated uncertainty on the base-level variable $p_{\underline{\mu}}$ and proportion parameters $\underline{\varphi}$, the uncertainty on $p_{\underline{x}'}$ for $\underline{x}' \neq \underline{x}^*, \underline{\mu}$ is revised, as well (see Figure 6.10).

For

$$p_{\underline{x}'} = h(\underline{x}')p_{\underline{\mu}}$$

the uncertainty on $p_{\underline{x}'}$ becomes

$$f(p_{\underline{x}'} \mid d_{\underline{x}^*}) = \int_{-\infty}^{+\infty} f(p_{\underline{x}'} \mid \underline{\varphi}, d_{\underline{x}^*}) f(\underline{\varphi} \mid d_{\underline{x}^*}) \mathrm{d}\underline{\varphi}$$

where

$$f(p_{\underline{x}'} \mid \underline{\varphi}, d_{\underline{x}^*}) := \mathcal{B}(\gamma_{\underline{x}'}, \delta_{\underline{x}'})$$

and

$$\gamma_{\underline{x}'} = s_1(\underline{x}') \quad \text{and} \quad \delta_{\underline{x}'} = s_2(\underline{x}')$$

are solutions of the system

$$\begin{aligned} \frac{\gamma_{\underline{x}'}}{\gamma_{\underline{x}'} + \delta_{\underline{x}'}} &= h(\underline{x}')\frac{\gamma'}{\gamma' + \delta'} \\ \frac{\gamma_{\underline{x}'}\delta_{\underline{x}'}}{(\gamma_{\underline{x}'} + \delta_{\underline{x}'})^2(\gamma_{\underline{x}'} + \delta_{\underline{x}'} + 1)} &= h(\underline{x}')^2 \frac{\gamma'\delta'}{(\gamma' + \delta')^2(\gamma' + \delta' + 1)} \end{aligned}$$

where γ' and δ' have been determined earlier by solving the system of equations following from (6.29) and (6.30).

Summary

Tables 6.2 and 6.3 summarises the updating process for coupling factor variables

6.6 Rate of CCF events

The issue of interest, following logically at this stage, is the determination of the subjective distribution on rate λ_{CCF} at level configuration $\underline{x} = (x_1, ..., x_k)$. For purposes of simplification, the notation $\underline{x}$, signifying the configuration vector of the system, is omitted. It is thus assumed that all variables describe failure characteristics of the system of components operating under defence environment $\underline{x} = (x_1, ..., x_k)$.

The rate of CCF events occurring to a system is expressed as

$$\lambda_{CCF} = \sum_{i=1}^{\rho} \sum_{j=1}^{\kappa} p_{ij} r_i = \sum_{i=1}^{\rho} \lambda_i \tag{6.31}$$

Table 6.2: Updating coupling factor variables (1)

Data:

$$d_{\underline{x}} = (n,m)$$

Likelihood function:

$$f(d_{\underline{x}} \mid p_{\underline{x}}) = \binom{m}{n} p_{\underline{x}}^{n} (1 - p_{\underline{x}})^{m-n}$$

GSM:

$$p_{\underline{x}} = h(\underline{x}) p_{\underline{\mu}}$$

Coupling intensity $p_{\underline{\mu}}$, where $\underline{x}^{*} \neq \underline{x}$

Prior Distribution

$$f(p_{\underline{\mu}} \mid \underline{\varphi}) := \mathcal{B}(\gamma, \delta)$$

Posterior Distribution

$$f(p_{\underline{\mu}} \mid \underline{\varphi}, d_{\underline{x}}) := \mathcal{B}(\gamma', \delta')$$

where parameters γ', δ' are obtained by solving the system

$$\frac{\gamma'}{\gamma' + \delta'} = \frac{1}{h(\underline{x})} \frac{\gamma_{\underline{x}} + n}{\gamma_{\underline{x}} + \delta_{\underline{x}} + m}$$

$$\frac{\gamma' \delta'}{(\gamma' + \delta')^2 (\gamma' + \delta' + 1)} = \frac{1}{h(\underline{x})^2} \frac{(\gamma_{\underline{x}} + n)(\delta_{\underline{x}} + m - n)}{(\gamma_{\underline{x}} + \delta_{\underline{x}} + m)^2 (\gamma_{\underline{x}} + \delta_{\underline{x}} + m + 1)}$$

Proportion parameters $\underline{\varphi}$

Prior Distribution

$$f(\underline{\varphi}) := \prod_{\iota} f_{\iota}(\varphi_{\iota})$$

Posterior Distribution

$$f(\underline{\varphi} \mid d_{\underline{x}}) \frac{f(\underline{\varphi}) \int f(d_{\underline{x}} \mid p_{\underline{x}}, \underline{\varphi}) f(p_{\underline{x}} \mid \underline{\varphi}) \mathrm{d}p_{\underline{x}}}{\int_{-\infty}^{+\infty} \left\{ f(\underline{\varphi}) \int f(d_{\underline{x}} \mid p_{\underline{x}}) f(p_{\underline{x}} \mid \underline{\varphi}) \mathrm{d}p_{\underline{x}} \right\} \mathrm{d}\underline{\varphi}}$$

Table 6.3: Updating coupling factor variables (2)

Coupling intensity $p_{\underline{x}}$

Prior Distribution

$$f(p_{\underline{x}} \mid \underline{\varphi}) := \mathcal{B}(\gamma_{\underline{x}}, \delta_{\underline{x}})$$

where parameters $\gamma_{\underline{x}}, \delta_{\underline{x}}$ are obtained by solving the system

$$\frac{\gamma_{\underline{x}}}{\gamma_{\underline{x}} + \delta_{\underline{x}}} = h(\underline{x}) \frac{\gamma}{\gamma + \delta}$$

$$\frac{\gamma_{\underline{x}} \delta_{\underline{x}}}{(\gamma_{\underline{x}} + \delta_{\underline{x}})^2 (\gamma_{\underline{x}} + \delta_{\underline{x}} + 1)} = h(\underline{x})^2 \frac{\gamma\delta}{(\gamma + \delta)^2 (\gamma + \delta + 1)}$$

Posterior Distribution

$$f(p_{\underline{x}} \mid \underline{\varphi}, d_{\underline{x}}) := \mathcal{B}(\gamma_{\underline{x}} + n, \delta_{\underline{x}} + m - n)$$

Coupling intensity $p_{\underline{x}^*}$, where $\underline{x}^* \neq \underline{x}$

Prior Distribution

$$f(p_{\underline{x^*}} \mid \underline{\varphi}) := \mathcal{B}(\gamma_{\underline{x^*}}, \delta_{\underline{x^*}})$$

where parameters $\gamma_{\underline{x}^*}, \delta_{\underline{x}^*}$ are obtained by solving the system

$$\frac{\gamma_{\underline{x}^*}}{\gamma_{\underline{x}^*} + \delta_{\underline{x}^*}} = h(\underline{x}^*) \frac{\gamma}{\gamma + \delta}$$

$$\frac{\gamma_{\underline{x}^*} \delta_{\underline{x}^*}}{(\gamma_{\underline{x}^*} + \delta_{\underline{x}^*})^2 (\gamma_{\underline{x}^*} + \delta_{\underline{x}^*} + 1)} = h(\underline{x}^*)^2 \frac{\gamma\delta}{(\gamma + \delta)^2 (\gamma + \delta + 1)}$$

Posterior Distribution

$$f(p_{\underline{x}^*} \mid \underline{\varphi}, d_{\underline{x}}) := \mathcal{B}(\gamma_{\underline{x}^*}, \delta_{\underline{x}^*})$$

where parameters $\gamma_{\underline{x}^*}, \delta_{\underline{x}^*}$ are obtained by solving the system

$$\frac{\gamma_{\underline{x}^*}}{\gamma_{\underline{x}^*} + \delta_{\underline{x}^*}} = h(\underline{x}^*) \frac{\gamma'}{\gamma' + \delta'}$$

$$\frac{\gamma_{\underline{x}^*} \delta_{\underline{x}^*}}{(\gamma_{\underline{x}^*} + \delta_{\underline{x}^*})^2 (\gamma_{\underline{x}^*} + \delta_{\underline{x}^*} + 1)} = h(\underline{x}^*)^2 \frac{\gamma'\delta'}{(\gamma' + \delta')^2 (\gamma' + \delta' + 1)}$$

where r_i is the rate of total failure events due to root cause i,

$$p_{ij} = P(\text{CCF through cf } j \mid \text{failure due to rc } i)$$

and, λ_i is the rate of CCF events due to root cause i.

Let $\underline{p_i} = (p_{i1}, p_{i2}, ..., p_{i\kappa})$; Figure 6.11 portrays the dependency relationships inherent in model 6.31.

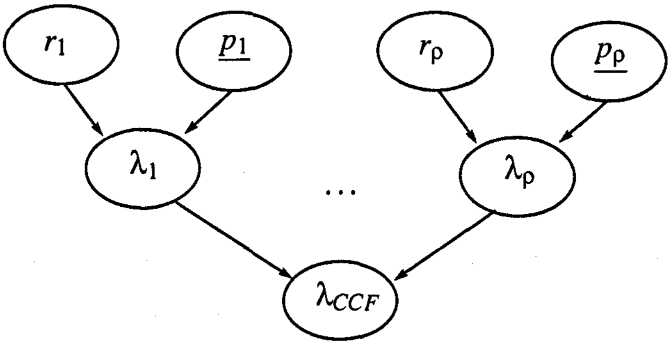


Figure 6.11: Rate of CCF events

As described in Chapter 5, failures due to different root causes are assumed to occur according to independent Poisson processes. Therefore, r.v.'s λ_i ($i = 1, ..., \rho$) are *conditionally* mutually independent. The first two moments of $f(\lambda_i)$ may be determined as:

$$E(\lambda_{CCF}) = \sum_{i=1}^{\rho} E(\lambda_i) \tag{6.32}$$

$$Var(\lambda_{CCF}) = \sum_{i=1}^{\rho} Var(\lambda_i) \tag{6.33}$$

One can estimate the first two moments of λ_{CCF}, on the grounds of the first two moments of λ_i, for $i = 1, ..., \rho$.

Uncertainty on λ_i

Based on Relationship (6.31), the rate of CCF events due to root cause i is equal to

$$\lambda_i = \sum_{j=1}^{\kappa} p_{ij} r_i \tag{6.34}$$

Based on the GS model, the uncertainty distribution on rate r_i is a mixture of gamma distributions

$$f(r_i) = \int_{-\infty}^{+\infty} f(r_i \mid \underline{\phi_i}) f(\underline{\phi_i}) \mathrm{d}\underline{\phi_i}$$

where

$$f(r_i \mid \underline{\phi_i}) := \mathcal{G}\,(a_i, \frac{b_i}{h_i(\underline{\phi_i})}) \tag{6.35}$$

with a_i, b_i being the shape and scale parameters respectively of the gamma distributed base-level rate $r_{i,\underline{\mu}}$, and $h_i(\underline{\phi_i})$ being a log-linear function of the proportion parameters $\underline{\phi_i}$[9]. Moreover, p_{ij}, where $j = 1,2,\ldots,\kappa$, are beta distributed variables with parameters that are functions of proportions $\underline{\varphi_{ij}}$. In particular, let

$$f(p_{ij} \mid \underline{\varphi_{ij}}) := \mathcal{B}\,(\gamma(\underline{\varphi_{ij}}), \delta(\underline{\varphi_{ij}}))$$

As described in Chapter 5, the correlation between variables p_{ij}, $j = 1,2,3$ is weak, making the assumption of *local* independence of parameters p_{ij} a reasonable approximation. Thus,

$$f(\underline{p_i} \mid \underline{\varphi_{ij}}) = f(p_{i1} \mid \underline{\varphi_{ij}}) f(p_{i2} \mid \underline{\varphi_{ij}}) \ldots f(p_{i\kappa} \mid \underline{\varphi_{ij}})$$

Variable transformation rules on the basis of relationship (6.34) imply that

$$f(\lambda_i \mid \underline{\phi_i}) = \int_{-\infty}^{+\infty} \int_0^1 f(\lambda_i \mid \underline{p_i}, \underline{\phi_i}) f(\underline{p_i} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) \mathrm{d}\underline{p_i} \mathrm{d}\underline{\varphi_{ij}}$$

[9] Thus far the log-linear function h has been denoted as $h(\underline{x})$. At this point there is no need to make reference to vector $\underline{x}$, but it is of interest to refer to $\underline{\phi_i}$

where

$$f(\lambda_i \mid \underline{p_i}, \underline{\phi_i}) := \mathcal{G}\left(a_i, \frac{b_i}{\sum_{j=1}^{\kappa} p_{ij} h_i(\underline{\phi_i})}\right) \qquad b_i, a_i \in [0, +\infty) \tag{6.36}$$

Averaging over all the possible values of $\underline{\phi_i}$ gives

$$f(\lambda_i) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \int_{0}^{1} f(\lambda_i \mid \underline{p_i}, \underline{\phi_i}) f(\underline{p_i} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) f(\underline{\phi_i}) \mathrm{d}\underline{p_i} \mathrm{d}\underline{\varphi_{ij}} \mathrm{d}\underline{\phi_i} \tag{6.37}$$

Moments of $\underline{\lambda_i}$

The $k-$th moment of λ_i is obtained by

$$E(\lambda_i^k) = \int_0^{+\infty} \lambda_i^k f(\lambda_i) \mathrm{d}\lambda_i$$

Based on (6.37), it is

$$\begin{aligned}
&E(\lambda_i^k) = \\
&= \int_0^{+\infty} \lambda_i^k \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \int_0^1 f(\lambda_i \mid \underline{p_i}, \underline{\phi_i}) f(\underline{p_i} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) f(\underline{\phi_i}) \mathrm{d}\underline{p_i} \mathrm{d}\underline{\varphi_{ij}} \mathrm{d}\underline{\phi_i} \mathrm{d}\lambda_i \\
&= \int_0^1 \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \left(\int_0^{+\infty} \lambda_i^k f(\lambda_i \mid \underline{p_i}, \underline{\phi_i}) \mathrm{d}\lambda_i \right) f(\underline{p_i} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) f(\underline{\phi_i}) \mathrm{d}\underline{p_i} \mathrm{d}\underline{\varphi_{ij}} \mathrm{d}\underline{\phi_i}
\end{aligned}$$

By considering (6.36),

$$\begin{aligned}
&E(\lambda_i^k) = \\
&= \int_0^1 \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{1}{b_i^k} \prod_{l=0}^{k-1} (a_i + l) \left(\sum_{j=1}^{\kappa} p_{ij} \right)^k h^k(\underline{\phi_i}) f(\underline{p_i} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) f(\underline{\phi_i}) \mathrm{d}\underline{p_i} \mathrm{d}\underline{\varphi_{ij}} \mathrm{d}\underline{\phi_i} \\
&= \frac{1}{b_i^k} \prod_{l=0}^{k-1} (a_i + l) \int_0^1 \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \left(\sum_{j=1}^{\kappa} p_{ij} \right)^k h^k(\underline{\phi_i}) f(\underline{p_i} \mid \underline{\varphi_{ij}}) f(\underline{\varphi_{ij}}) f(\underline{\phi_i}) \mathrm{d}\underline{p_i} \mathrm{d}\underline{\varphi_{ij}} \mathrm{d}\underline{\phi_i}
\end{aligned}$$

These calculations cannot be determined analytically. The determination of the $k-$th moment of λ_i for $i = 1, \ldots, 6$ requires the use of numerical approximation techniques and appropriate computational tools.

6.7 Uncertainty analysis

6.7.1 Prior distributions

Let V be a root cause or a coupling factor variable. The *prior* distribution on V is

$$f(v) = \int_{-\infty}^{+\infty} f(v \mid \underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi} \tag{6.38}$$

where $\underline{\phi} = (\phi_1, ..., \phi_m)$ is a vector of parameters expressing the effect of the influencing defences on r.v. V. Distribution $f(v)$ may be considered as a continuous mixture of distributions $f(v \mid \underline{\phi})$. A key assumption within the particular set-up is that parameters $\phi_\iota, \iota = 1, ..., m$ are *a priori* mutually independent. Thus,

$$f(\underline{\phi}) = \prod_{\iota=1}^{m} f(\phi_\iota)$$

The moments of $f(v)$ are:

$$E(v^m) = \int_0^{+\infty} \int_{-\infty}^{+\infty} v^m f(v \mid \underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi} \mathrm{d}v$$

It is assumed that distribution $f(v \mid \underline{\phi})$ belongs to a particular family of distributions. In particular, for rates it is assumed that

$$f(v \mid \underline{\phi}) := \mathcal{G}(a, b/h(\underline{\phi}))$$

with raw moments given by

$$\mu'_m = \frac{\Gamma(a+m)}{b^m \Gamma(a)} h(\underline{\phi})^m$$

For coupling probabilities it is assumed that

$$f(v \mid \varphi) := \mathcal{B}(s_1(\underline{\phi}), s_2(\underline{\phi}))$$

where $s_1(\underline{\phi}), s_2(\underline{\phi})$ are the solutions of the corresponding system of equations, with raw moments given by

$$\mu'_m = \frac{\Gamma(s_1(\underline{\phi})+s_2(\underline{\phi}))\Gamma(s_1(\underline{\phi})+m)}{\Gamma(s_1(\underline{\phi})+s_2(\underline{\phi})+m)\Gamma(s_1(\underline{\phi}))}$$

Consequently,

$$\begin{aligned} E(v^m) &= \int_{-\infty}^{+\infty} f(\underline{\phi}) \left(\int_0^{+\infty} v^m f(v \mid \underline{\phi}) f(\underline{\phi}) \mathrm{d}v \right) \mathrm{d}\underline{\phi} \\ &= \int_{-\infty}^{+\infty} f(\underline{\phi}) \frac{\Gamma(a+m)}{b^m \Gamma(a)} h(\underline{\phi})^m \mathrm{d}\underline{\phi} = \frac{\Gamma(a+m)}{b^m \Gamma(a)} \int_{-\infty}^{+\infty} h(\underline{\phi})^m f(\underline{\phi}) \mathrm{d}\underline{\phi} \end{aligned}$$

or

$$\begin{aligned} E(v^m) &= \int_{-\infty}^{+\infty} f(\underline{\phi}) \left(\int_0^{+\infty} v^m f(v \mid \underline{\phi}) f(\varphi) \mathrm{d}v \right) \mathrm{d}\underline{\phi} \\ &= \int_{-\infty}^{+\infty} f(\underline{\phi}) \frac{\Gamma(s_1(\underline{\phi})+s_2(\underline{\phi}))\Gamma(s_1(\underline{\phi})+m)}{\Gamma(s_1(\underline{\phi})+s_2(\underline{\phi})+m)\Gamma(s_1(\underline{\phi}))} \mathrm{d}\underline{\phi} = \int_{-\infty}^{+\infty} g(\underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi} \end{aligned}$$

Moments of the uncertainty distribution on V may be analytically computed, allowing for the articulation of probabilistic statements.

6.7.2 Posterior distributions

Suppose that data d is acquired, relevant to V. The posterior distribution on V, in the light of the new evidence, is

$$f(v \mid d) = \int_{-\infty}^{+\infty} f(v \mid \underline{\phi}, d) f(\underline{\phi} \mid d) \mathrm{d}\underline{\phi} \tag{6.39}$$

The posterior distribution $f(v \mid d)$ may be considered as a weighted average of the posterior conditional distributions $f(v \mid \underline{\phi}, d)$, using as weights the posterior probabilities $f(\underline{\phi} \mid d)$, which are given by

$$f(\underline{\phi} \mid d) = \frac{f(d \mid \underline{\phi}) f(\underline{\phi})}{\int_{-\infty}^{+\infty} f(d \mid \underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi}} \tag{6.40}$$

The distribution $f(d \mid \underline{\phi}, v)$ implicit in (6.40) is the likelihood of the data, given $V$and it is obtained by integrating over the parameter space of V, i.e.

$$f(d \mid \underline{\phi}) = \int_0^{+\infty} f(d \mid \underline{\phi}, v) f(v \mid \underline{\phi}) \mathrm{d}v \tag{6.41}$$

Within the particular set-up, the data is generated by either a Poisson or a binomial process. In both cases, the integral in (6.41) can be evaluated analytically. Indeed,

$$f(d \mid \underline{\phi}) \propto \frac{T^n}{\left(T + \frac{b}{h(\underline{\phi})}\right)^{n+a}} \left(\frac{b}{h(\underline{\phi})}\right)^a .$$

where $d = (n, T)$ and $n \sim P(vT)$, or

$$f(d \mid \underline{\phi}) \propto \frac{\Gamma(m - n + s_2(\underline{\phi}))\Gamma(n + s_1(\underline{\phi}))}{B(s_1(\underline{\phi}), s_2(\underline{\phi}))\Gamma(m + s_1(\underline{\phi}) + s_2(\underline{\phi}))}$$

when $d = (n, m)$ and $\mathrm{v} \sim B_p(n \mid m)$. In cases where the integral in (6.41) is not analytically tractable, computational techniques are required. A useful family of techniques based on asymptotic approximations of integrals is the Laplace method [Tierney and Kadane, 1986]. In cases were the dimensionality is high, Markov Chain Monte Carlo methods may be appropriate [Evans and Swartz, 1995].

In any case, the integral implicit in (6.40) cannot be carried out analytically. Computational methods are required to approximate the normalising constant, and thus to specify the posterior distribution $f(\underline{\phi} \mid d)$.

Within the ID framework, the uncertainty distribution on V is always represented by a continuous mixture of distributions. Moreover, model $f(v \mid d)$ is decomposed to two sub-models: the elegant, analytically tractable sub-model $f(v \mid \underline{\phi}, d)$, and the numerically determined sub-model $f(\underline{\phi} \mid d)$.

6.8 The specific application

This thesis is an application example of the suggested methodology. The research focuses on the CCF modelling of EDGs of nuclear power plants, and the ID model merges features of the UPM methodology with the structure of the ICDE database.

Within this context, the definition of the system defences represented by the ID model is preserved from the UPM framework[10]. Thus, the number of system defences counts to eight, and the number of levels of each defence is five. In other words,

$$x_k \text{ is the level of defence } D_k, \text{ where } k = 1, \ldots, 8 \text{ and } x_k \in \Omega = \{1, ..., 5\}$$

Therefore, it holds that $\Omega_k = \Omega$ for every k. Within the particular framework, Ω is partitioned to low, medium and high levels; viz. $s_k = 3$ for every k and

$$X_{k,1} = X_1 = \{1,2\}, \; X_{k,2} = X_2 = \{3\}, \; X_{k,3} = X_3 = \{4,5\} \quad \text{for } k = 1, \ldots, 8$$

On this basis, the medium level for any defence D_k is 3, and for every k it holds that $\mu_k = \mu = 3$. The Geometric Scaling model is now written as

$$V_{(x_1,\ldots,x_n)} = \prod_{\{i,j\} \in M_\pi} \phi_{ij}^{(x_i-3)(x_j-3)} \prod_{k \in K} \Phi_k^{x_k-3} \cdot V_{(3,\ldots,3)} \tag{6.42}$$

where $V_{(3,\ldots,3)}$ is r.v. V when all influencing defences receive the medium level, $\phi_{ij} \in \mathbb{R}$ is a cross-term that corresponds to pair $\{i, j\} \in M_\pi$ and Φ_k is a function $\Phi_k : \Omega^r \to [0, 1]$

Moreover, the definition of function

$$\phi_k(x_{k_1}, x_{k_2}, \ldots, x_{k_r}) \text{ where } \{k_i \mid i = 1, ..., r\} = L_k \text{ for } k \in Q$$

[10] See Chapter 5, Section 5.3.1

which is found in the GS model given in (6.42), is simplified. In particular, $\phi_k(x_{k_1}, x_{k_2}, \dots, x_{k_r})$ is a piecewise function with

$$\phi_k(x_{k_1}, x_{k_2}, \dots, x_{k_r}) : \Omega^r \rightarrow [0,1]$$

and

$$\phi_k(x_{k_1}, x_{k_2}, \dots, x_{k_r}) = \phi_{k,\eta} \text{ when } (x_{k_1}, x_{k_2}, \dots, x_{k_r}) \in Y_\eta$$

with $0 < \phi_{k,\eta} < 1$, where $Y_\eta = X_{\eta_1} \times \dots \times X_{\eta_r}$ with $\eta = 1, ..., 3^r$ and $\eta_1, ..., \eta_r \in \{1,2,3\}$. Now, consistently with the assumption according to which for fixed x_{k_j} with $j \neq l$ and $j,l = 1, ..., r$, points $\phi_k(x_{k_1}, \dots, x_{k_l}, \dots, x_{k_r})$ are symmetrically distanced, we have

$$\phi_k(x_{k_1}, ..., x''_{k_l}, ..., x_{k_r}) = \left(\phi_k(x_{k_1}, ..., x'_{k_l}, ..., x_{k_r}) \cdot \phi_k(x_{k_1}, ..., x'''_{k_l}, ..., x_{k_r})\right)^{\frac{1}{2}} \qquad (6.43)$$

where $x''_{k_l} \in X_2$, $x'_{k_l} \in X_1$ and $x'''_{k_l} \in X_3$.

The association between the ICDE database and the ID model is achieved by using the taxonomy for the root causes and coupling factors as defined within the ICDE coding guidelines[11]. Within this context $\rho = 6$ and $\kappa = 3$; now Relationship (6.31) becomes

$$\lambda_{CCF} = \sum_{i=1}^{6} (p_{i1} + p_{i2} + p_{i3}) r_i = \sum_{i=1}^{6} \lambda_i \qquad (6.44)$$

6.9 Conclusion

Within this section, the mathematical foundations of the ID model have been presented. In particular, the elements of the model have been qualitatively specified and quantitatively defined as probabilistic variables. Moreover, the mathematical framework of the ID model has been described, which distinguishes between different types of functional interactions existing amongst the system defences. Finally, the Geometric Scaling (GS) model has been proposed, which has a threefold functionality: first, it decreases the amount of information required for the specification of the prior distri-

[11] See Section 5.3.2

butions on the ID variables, offering a pragmatic approach to the ID building process; second, it allows for the propagation of evidence within the ID variables; and, third, it allows for the classification of the defence interactions across different categories.

Once the theoretical and mathematical set-up of the model is grounded, the basis is set to allow for a comprehensive description of the building process of the ID model.

Chapter 7

Qualitative Stage of the Influence Diagram Building Process

7.1 Introduction

The previous chapter described the theoretical foundations of the ID model. At this stage, the building process of the model will be described. Essentially, there are three main steps in building an ID model: problem structuring (qualitative stage), instantiation (quantitative stage) and inference [van der Gaag, 1996; Sigurdsson et al., 2001].

The aim of this chapter is to describe the first stage of the ID building process, namely the qualitative stage (Figure 7.1).

Once the basic elements of the ID model are defined and expressed as variables, the construction of the network of the ID model takes place. In most applications, the construction of the network is usually performed with expert judgment elicitation. 'Expert judgment elicitation' refers to the extraction of domain knowledge by means of a formal, structured process [Cooke, 1991]. The term 'expert' *sensu lato* refers to 'any individual entrusted with providing specific inputs to an analysis, including not only those with formal training in analysis, but also untrained individuals with unique knowledge needed for the analysis' [Fischhoff, 1989]. Within this stage of the application, experts are individuals that are able to identify the topology of the network,

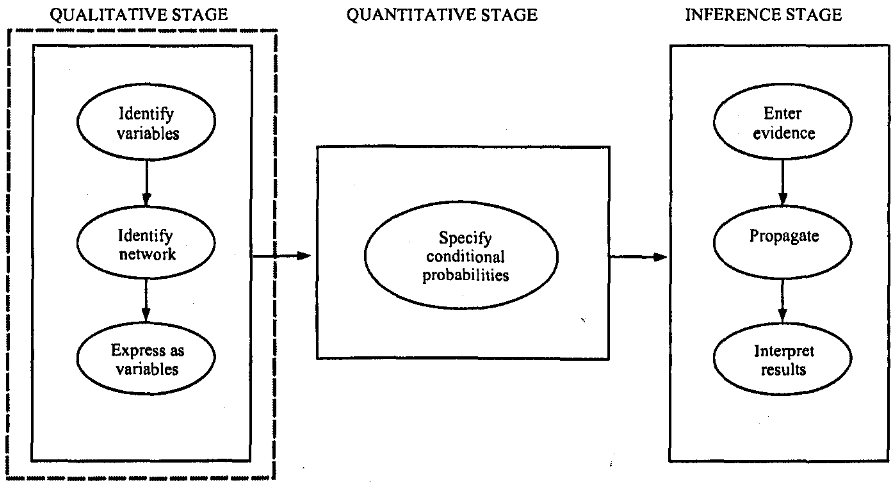


Figure 7.1: Qualitative stage of ID building process

based on concepts of relation, causality and influence.

The chapter is structured as follows: Section 7.2 describes the overall protocol designed for the purposes of building the ID model. Section 7.3 focuses on the qualitative stage of the model building, describes the elicitation process used for this purpose, and presents the results. Section 7.4 reflects on the process and discusses on the insights gained. Finally, Section 7.5 concludes this chapter.

7.2 Expert judgment elicitation

A particular characteristic of models built for PRA purposes is the fact that they are intended to be used in settings such as quantitative policy analysis and regulatory decision-making [Melchers, 2001]. Clearly, decisions of such large scale have implications to the large public sector. Strictly speaking, the Bayesian paradigm applies to individual decision makers [French, 1986]. However, in large-scale decision problems, it is of high importance to combine the opinions of multiple experts in a scientifically justifiable manner. The term scientifically justifiable means that the expert judgment methodology adopted for the quantification of the model should conform to the norms of scientific research and it should aim to consensus. As Cooke argues, 'were science to abandon its commitment to rational consensus, then its potential contribution to rational decision-making should be compromised' [Cooke, 1991, p. 80].

The aim of the methodological framework designed within the context of this research is to use expert judgment both qualitatively and quantitatively, within a scientifically structured approach. The desiderata of a scientifically robust framework for expert judgment elicitation are summarised as [Cooke and Goosens, 2000]:

- Scrutability: all data and models used are documented and open to peer review, the process is reproducible;
- Neutrality: the method for combining/evaluating expert judgment should encourage experts to state their true judgments.
- Fairness: all experts are treated equally, prior to processing the results of observations.

7.2.1 Protocol for expert judgment elicitation

A general protocol for expert judgment elicitation is The Standford Research Institute (SRI) assessment protocol [Morgan and Henrion, 1990; Merkhofer, 1987; Spetzler and von Holsteins, 1975]. The SRI protocol comprises of the following stages: 1. motivating, 2. structuring, 3. conditioning, 4. encoding, and 5. verifying.

The objective of *motivating* is to establish rapport between the experts and the analyst. This is achieved by providing to the expert panel information on the project in hand, explaining the role of expert judgment within the particular context, and presenting the methods used for expert judgment elicitation. It is important to clarify that the objective of the process is to measure the experts' degree of belief regarding certain quantities, rather than to test their knowledge on the particular subject. During this stage, motivational biases, which are either conscious or subconscious adjustments on the experts' responses stemming from various rewards for particular responses [Spetzler and von Holsteins, 1975], are identified and controlled.

The second stage of *structuring* aims to clarify the objects and events that are the subjects of the elicitation process. During this stage, the variables are defined unambiguously, along with the corresponding state spaces. In order to ensure a clear understanding of the modelling situation, a list of assumptions underlying the modelling approach is given.

Conditioning is the stage where it is explained to the experts how to coherently assess their degree of belief. In order to reduce the effect of cognitive biases in assessments, insight is provided into the different types of bias that experts are susceptible to. These biases involve: representativeness, which usually appears when subjects are requested to assess the probability of an object or event belonging to a particular class or process, and describe situations where the same factors of assessing similarity are used to asses probability [Tversky, 1974]; availability, which describes the tendency to assess probabilities of events based on familiarity and salience. Events that are easier recallable, are assigned higher probabilities [Cooke, 1991]; and anchoring, which refers to the tendency of making an assessment by setting a starting point or an initially value, and work out the assessment by adjusting this value [Tversky, 1974]. Anchoring may be caused either by the formulation of the problem, or due to incomplete computations of the expert.

The stage of *encoding* is where the actual expert judgment elicitation occurs. During this stage, experts are encouraged to provide numerical assessments of their uncertainty regarding particular variables (elicitation variables). Finally, the stage of *verifying* aims to ensure that the assessments made by the experts reflect their true belief, and check the quality of the results of the probability encoding process.

These stages constitute the building blocks of the protocol designed for the purposes of this research. The overall protocol has been slenderly modified to accommodate the particular objectives. It is summarised in Figure 7.2.

7.2.2 Expert Panel Selection

Within the scope of the specific research, a resource expert is defined as a person with detailed and deep knowledge of a particular area, issue, aspects and particular methodologies. Resource experts are acknowledged as being suitable to give the appropriate input for the accomplishment of the research objectives.

Expert Judgment Elicitation Protocol

1. Identification and selection of experts
2. Motivating
3. Structuring
4. Qualitative elicitation
5. Verifying
6. Probability training - Conditioning
7. Probability encoding
8. Data analysis
9. Verifying

Figure 7.2: Protocol used within the scope of the research

The identification and selection of the resource experts (step 1 of the protocol) was carried out with the help of UK Health and Safety Executive (HSE). Experts are selected who have knowledge of the EDG system, expertise in CCF modelling issues, and were available within the time framework of the research. The final panel consists of six nuclear experts. Out of the six experts, three have experience in Probabilistic Safety Assessment; two have experience in failure data analysis and specifically for diesels; and one has experience in common cause failure modes.

The intention that the expert panel selection needs to fulfil is twofold: it needs to ensure that the experts carry the appropriate expertise to properly respond to the requirements of the research, whilst opinion variability is included in the panel. The appropriate candidates for the expert panel are people that are involved in the nuclear industry and they have one or more of the kinds of expertise mentioned above.

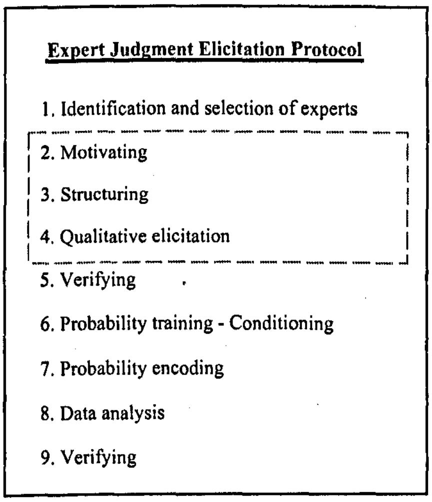
7.3 Expert Judgment Workshop

The elicitation of the necessary qualitative information was performed by means of a workshop with the expert panel. The major part of the workshop had the format of a group decision-making exercise, the outcome of which was the network of the ID model and the existing functional interactions amongst the system defences. In order to practically reach agreement on these two issues, the concept of moderate consensus decision-making [Ness and Hoffman, 1998] was used. Whereas traditionally consensus implies the unanimous agreement of all the members of a group, moderate consensus implies that a majority have reached a given decision, and that the minority who opposed this decision have had a reasonable opportunity to influence this choice. The final decision is approved by the majority, and not objected by the minority. The rule of moderate decision-making has been chosen because, in practice, experts agree completely very rarely.

The workshop took place on September 29, 2004 at the Atkins Nuclear, Aztec West, Bristol, between 9am and 5pm.

7.3.1 Objectives of the Workshop

Essentially, the workshop was designed in order to conduct Steps 2 to 4 of the Expert Judgment Elicitation Protocol (Figure 7.3).



Expert Judgment Elicitation Protocol

1. Identification and selection of experts
2. Motivating
3. Structuring
4. Qualitative elicitation
5. Verifying
6. Probability training - Conditioning
7. Probability encoding
8. Data analysis
9. Verifying

Figure 7.3: Steps of the protocol accomplished during the workshop

The specific elicitation goals of the workshop are summarised as:

- Verification of model assumptions;
- Structuring the ID network;

- Identification of functional interactions amongst system defences.

7.3.2 Introduction to the workshop

Prior to the workshop, the expert panel received an introductory document. The document outlined the project scope and the important features of the problem addressed. The purpose of the document was to prepare the panel for the elicitation process. Receiving the document before the workshop provided the panel with time to reflect on the background of the project and on the relevant information before the actual elicitation took place.

At the opening of the workshop, a presentation was given to the expert panel. During the presentation the experts were briefed in more detail on the project, on the purpose of the elicitation workshop, and on their role within this context. The aim of the presentation was to familiarise experts with the objectives of the workshop and create rapport between the analysts and the expert panel.

The objectives of the workshop included structuring the network of an Influence Diagram (ID) model. IDs are advanced mathematical modelling tools; therefore, it was not expected from the experts to be familiar with the concepts involved. Nevertheless, familiarising the panel with the ID formalism was imperative for meeting the objectives of the workshop. For this purpose a tutorial on IDs was given before the structuring phase.

More precisely, the aim of the tutorial was to introduce concepts that were necessary for the graph elicitation. To this end, only two types of nodes where described (namely decision nodes and chance nodes), and the attention was focused on the concept of causality rather than the concept of conditional independence. To facilitate the acquaintance of the panel with IDs, a simple example of an ID model was given. The example was taken from the area of reliability. During the tutorial, the panel did not show any particular problems in understanding the concept of cause and effect, or influence, and how this is represented by an ID model. This observation was confirmed afterwards, during the actual elicitation, when experts tackled the exercise with a particular ease.

After the tutorial on the ID formalism, a second presentation was given. The aim of the presentation was to provide information on the issue of expert judgment. More particularly, the importance of using expert judgment as a source of information for the purposes of PRA in general, and for modelling CCFs in particular was highlighted. The purpose of expert judgment elicitation was defined, and the role of experts and their required input within the particular framework was clearly described (motivating stage).

At the end of the presentations and tutorials, it was important to ensure that the expert panel had gained a good understanding of the elements of the domain whose network was to be elicited. In the effort to establish clear and unambiguous definitions on the elements of the model and the component boundaries (EDG), discussion was generated amongst the members of the panel. During intense discussion, disagreement arose regarding the definition of some of the elements of the problem. The disagreement was resolved during the discussion and interaction amongst the members of the panel. This was a critical stage of the elicitation process: this disagreement, if not resolved, could have lead to significant misunderstandings and raise problems in the actual elicitation. The discussion resulted in the definitions of the elements of the modelling domain to be refined, and the framework of model assumptions to be indirectly verified (structuring phase).

7.3.3 Eliciting the ID network

Once the model assumptions and the definitions of the elements of the domain were verified and refined, the expert panel was ready to proceed with the actual elicitation of the ID network. The overall process of eliciting the network is given in Figure 7.5. This section describes the steps taken in more detail. Structuring the ID network entails the determination of the influencing relationships amongst the system defences and the root causes and coupling factors. More particularly, the root causes and/or coupling factors that each defence variable is able to modulate need to be identified. These modulating relationships between the defence variables and the root cause/coupling factor variables are depicted in the network by arcs from the former to the latter. In order to identify these arcs, an exercise was designed for the expert panel.

The exercise

For the purposes of the exercise, each expert was handed an acetate containing the variables of the model represented by the appropriate nodes, but without the arcs representing modulating relationships (Figure 7.4). The experts were requested to identify these relationships from the defences to the root causes and coupling factors, and draw arcs from the defences to the appropriate nodes. The panel was given roughly half an hour to perform this task individually.

The aim of the next step of the process was to structure the panel's responses, and reach consensus on the form of the network. Once the experts' conclusions were obtained, a matrix C_{jk} was drawn on a flipchart, the rows $j = 1,..8$ representing the defences, and the columns $k = 1,..,9$ representing the root causes and coupling factors. Element c_{jk} denoted the number of experts claiming that defence D_j may modulate variable V_j (coupling factor or root cause), therefore, should this number include the majority of experts, an arc from D_j to V_k should be drawn in the network. Discussion was facilitated amongst the panel over the 'debatable' arcs, in order to reach a conclusion for each case. The process lasted for nearly two hours. The overall process was recorded to be further analysed. In areas where unanimous agreement was not reached, the analyst had to make some further judgments; the reasoning underlying these judgments was described in detail in a feedback document, which was sent to the expert panel. Comments were requested from the experts, to ensure that the final ID network does not lead to conceptual inconsistencies and that there are no members of the panel opposing to the inclusion of particular modulating relationships. This way, it was ensured that decision-making consensus was reached.

Figure 7.6 depicts the resulting network of the ID model. The relationships portrayed in the model network are verbally described in Appendix B.

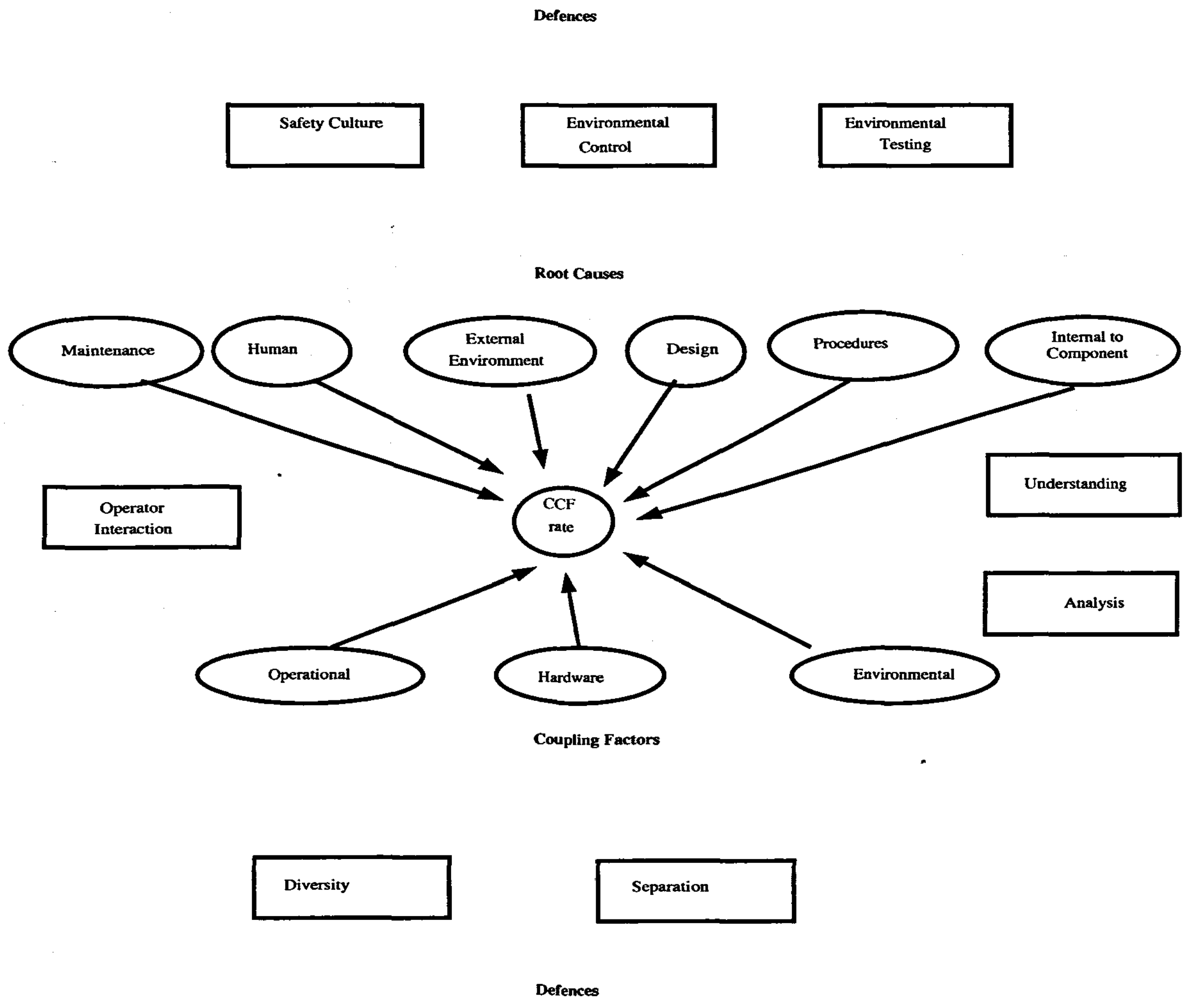


Figure 7.4: Acetate handed to each member of the panel

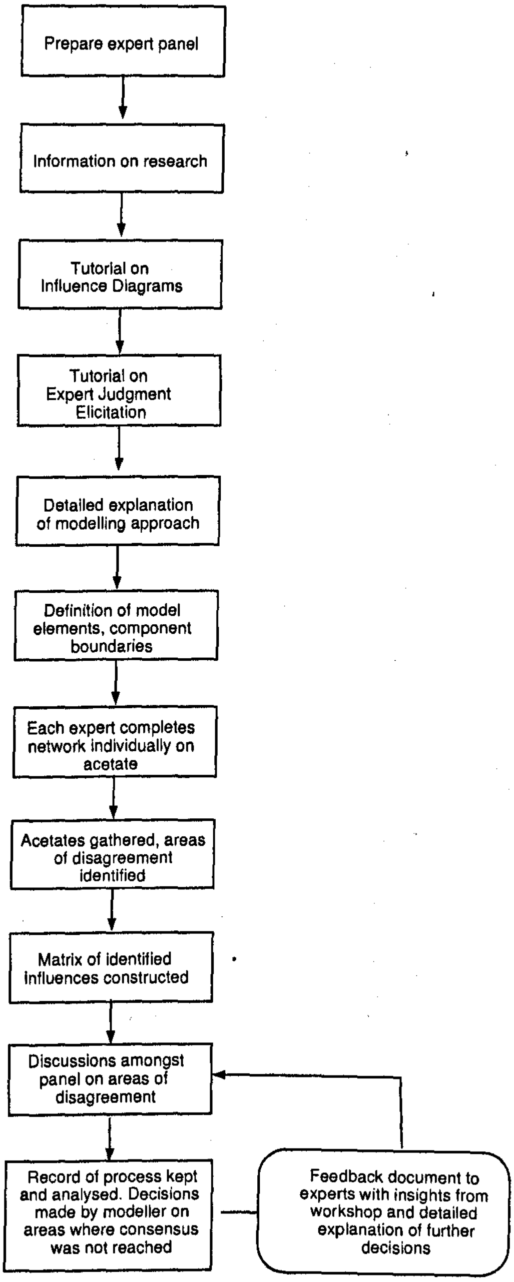

Prepare expert panel
Information on research
Tutorial on Influence Diagrams
Tutorial on Expert Judgment Elicitation
Detailed explanation of modelling approach
Definition of model elements, component boundaries
Each expert completes network individually on acetate
Acetates gathered, areas of disagreement identified
Matrix of identified influences constructed
Discussions amongst panel on areas of disagreement
Record of process kept and analysed. Decisions made by modeller on areas where consensus was not reached
Feedback document to experts with insights from workshop and detailed explanation of further decisions

Figure 7.5: Elicitation of ID network

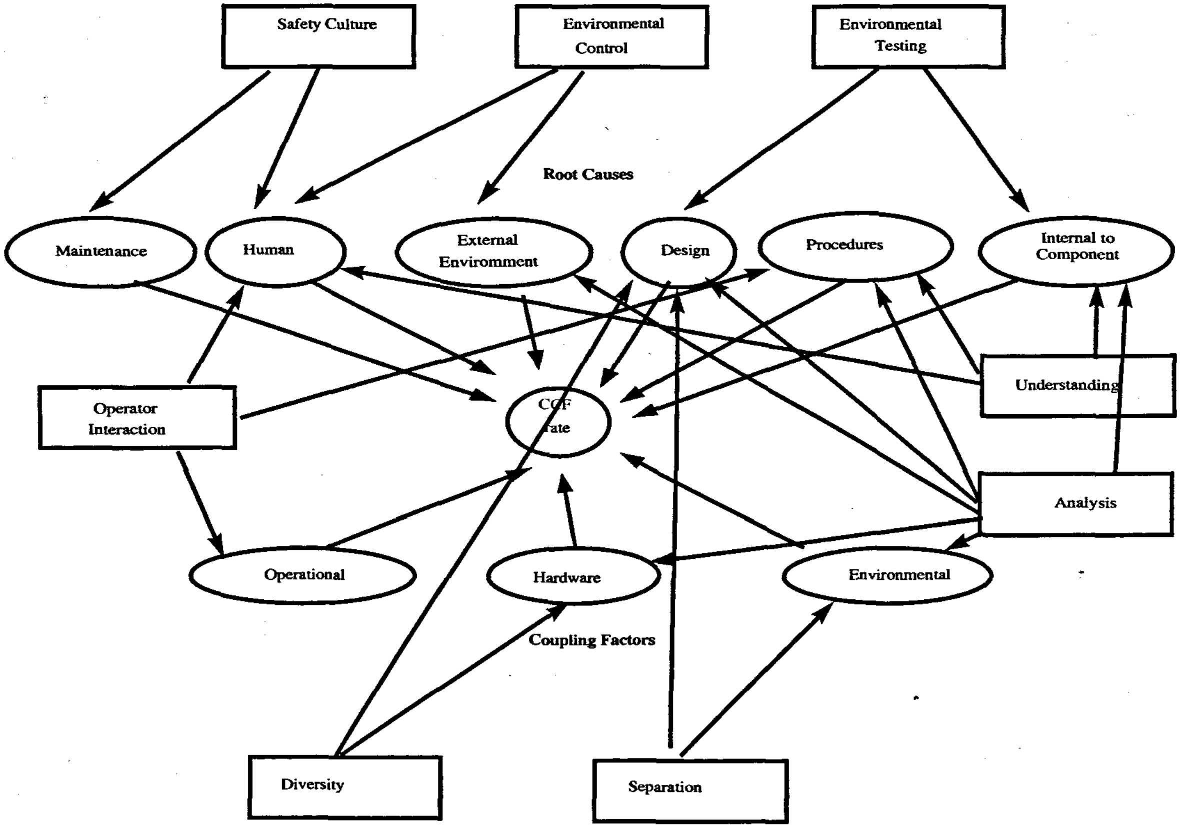


Figure 7.6: Network of the ID model

Response to the exercise

As previously stated, the panel showed no difficulty in understanding the concept of cause and effect, and how this is represented in a ID network. Experts could easily reason in terms of which defences influence which failure characteristics of the system (root causes or / and coupling factors), and present related examples to support their arguments. Nevertheless, identifying the significance of these relationships, and deciding which ones should be included in the model, proved to be rather problematic.

A model is a simplification of reality, built in order to understand, manage and control this part of reality [Pidd, 2003]. To this end, not all relationships existing in reality and relevant to the situation can be incorporated in the model. This is an aspect that one feels comfortable with, given that they have previous experience in model-building; however, the members of the panel had limited experience in the actual construction of models, resulting in the identification and representation in the network of any possible modulating relationship, regardless of its significance. As a consequence, when the acetates with the networks completed by the experts were gathered, they included such a large amount of information, that it was extremely difficult to decipher.

In order to tackle this development, it was imperative to explain to the panel the fact that a model is only an approximation of reality, and to urge experts to include only the relationships for which they could retrieve practical examples. Once these points were addressed, a considerable number of arcs was retrieved from the acetates, and the analysis of the information became possible by using the matrix.

7.3.4 Eliciting the functional interactions

After constructing the network, the functional interactions amongst the defences that influence the same element (root cause or coupling factor) were elicited. The elicitation process is summarised in Figure 7.7. This section elaborates on this process in more detail.

During the construction of the ID network described previously, the defences that influence the same model element (root cause or coupling factor variable) had been

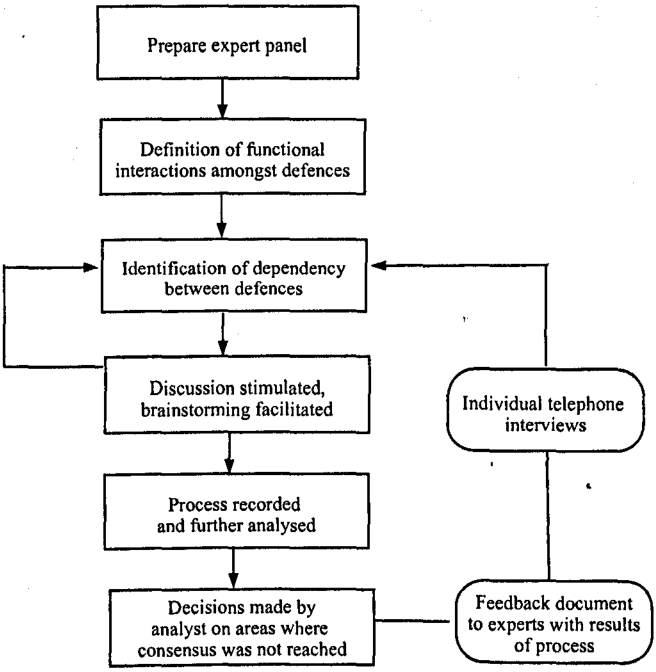

Prepare expert panel
Definition of functional interactions amongst defences
Identification of dependency between defences
Discussion stimulated, brainstorming facilitated
Process recorded and further analysed
Decisions made by analyst on areas where consensus was not reached
Individual telephone interviews
Feedback document to experts with results of process

Figure 7.7: Elicitation of Functional Interactions

identified, forming particular subgroups of defences. The intention was to identify the nature of interaction between each pair of defences belonging to the same subgroup.

Before the actual elicitation, a presentation was given to prepare the panel accordingly . A simple example was used for this purpose, according to which two defences D_m and D_n ($m, n \in \{1, ..., 8\}$) influencing a particular failure characteristic (root cause or coupling factor). With the help of the example the different types of functional interaction existing between the two defences were clearly defined, in the way they influence the defence characteristic of the system. Once it was ensured that the panel was feeling comfortable with these definitions, the actual elicitation proceeded.

An exercise was designed in order to identify the functional interactions of interest. The main component of the exercise was the identification of the type of functional interaction that exists between two defences D_m and D_n. For this purpose, questions of the following form were used

> Suppose that defence D_m is at a low level, and defence D_n is at level Y.
> You are thinking of spending an amount of money to enhance D_n by one

level (to $Y+1$). If you were told that the level of D_m is high instead of low, would you be prepared to spend the same amount of money?

In principle, a positive response implies that the impact of enhancing the level of D_n is independent of the level of D_m.

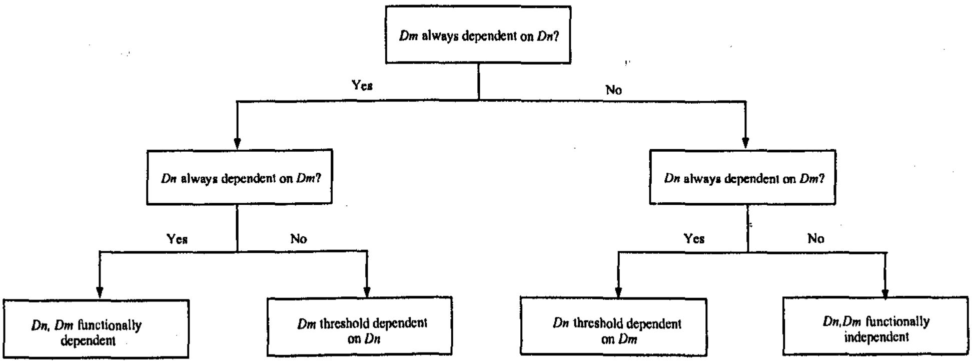

Dm always dependent on *Dn*?
Yes
No
Dn always dependent on *Dm*?
Yes
No
Dn always dependent on *Dm*?
Yes
No
Dn, *Dm* functionally dependent
Dm threshold dependent on *Dn*
Dn threshold dependent on *Dm*
Dn,*Dm* functionally independent

Figure 7.8: Assessing type of functional interaction

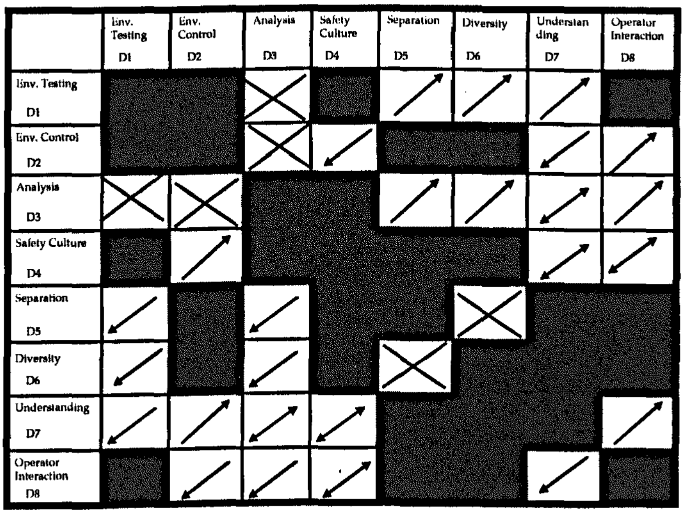
In order to identify the type of functional interaction, a combination of questions was used according to the logic given in Figure 7.8. The exercise was based on the assumption that only one type of functional interaction exists between any pair of defences, and on the non-symmetric property of threshold functional dependence. Moreover, the term 'always' refers to both moderate and drastic modifications of the level of the corresponding defence.

To this end, two negative answers imply functional independency, whereas two positive answers imply functional dependency. Threshold dependency is implied when the effect of the one defence is dependent on the level of the other defence, whereas the reverse does not always hold. Indeed, the counterpart of threshold dependency manifests a dependency only for drastic modifications.

The exercise designed for the expert panel in order to identify the functional interactions inherent amongst the system defences has similarities with a focus group exercise. In particular, specific questions were addressed to the expert panel, stimulating brainstorming and discussion amongst the members. In case of disagreement, experts were encouraged to make use of specific engineering examples to support their arguments.

The whole process was recorded for further analysis. In most cases, the expert panel shared similar opinions regarding the particular questions. In few cases, where disagreement was not resolved through discussion, the facilitator had to make further judgments based on the engineering information given during the debate. In a similar fashion as earlier, the rationale behind these judgments was described in detail in a feedback report, documenting the results of the exercise. The report was sent to the expert panel and individual telephone meetings with each of the experts were arranged, in order to provide feedback on the conclusions reached during the workshop. The panel as a whole ensured that the final results of the qualitative data do not lead to conceptual inconsistencies, and that decision-making consensus is reached.

The results of the process are given in Figure 7.9.



	Env. Testing D1	Env. Control D2	Analysis D3	Safety Culture D4	Separation D5	Diversity D6	Understanding D7	Operator Interaction D8
Env. Testing D1	▨	▨	✕	▨	↗	↗	↗	▨
Env. Control D2	▨	▨	✕	↙	▨	▨	↙	↗
Analysis D3	✕	✕	▨	▨	↗	↗	⤢	↗
Safety Culture D4	▨	↗	▨	▨	▨	▨	⤢	⤢
Separation D5	↙	▨	↙	▨	▨	✕	▨	▨
Diversity D6	↙	▨	↙	▨	✕	▨	▨	▨
Understanding D7	↙	↗	⤢	⤢	▨	▨	▨	↗
Operator Interaction D8	▨	↙	↙	⤢	▨	▨	↙	▨

In position (i,j): ✕ implies that *Di* and *Dj* are functionally independent

↗ implies that *Dj* is threshold functionally dependent on *Di*

↙ implies that *Di* is threshold functionally dependent on *Dj*

⤢ implies that *Di* and *Dj* are functionally dependent

Figure 7.9: Functional interactions between defences

7.4 Reflections on the elicitation process

The elicitation process described in the previous sections was used for the particular industrial example of EDGs in nuclear power plants. This section reflects on the application of the process, with respect to the stated goals of the elicitation workshop. Verifying the assumptions of the modelling approach is an integral part of the elicitation process. In order to achieve this task, a semi-structured discussion was used amongst the expert panel, preceding the network-elicitation exercise. Creating a common basis of agreement on the fundamental components of the model not only creates rapport, but also ensures consistency in the elicitation process and compatibility of results. Distributing handouts to the experts describing the framework of assumptions facilitates the identification of the arguable points, and assists their further clarification and resolution.

During the initial stages of the elicitation of the ID network, much disagreement arose amongst the panel members regarding the influences existing between the elements of the modelling domain. Naturally, some disagreement was expected, as different people share different viewpoints; disagreement is even in some cases welcomed, as it helps to gain a more complete appreciation of the problem. However, in some cases difference in opinion may stem from other reasons rather than different perspectives, and this option should be examined. In the particular application, we considered each area of debate separately, and we encouraged discussion. The discussion process revealed that the most significant part of disagreement stemmed from difference in the background of the members of the panel. To be more precise, members interpreted the model elements differently, according to their personal experience. Furthermore, the process revealed overlaps and ambiguity in some definitions of the system defences, which were adopted from the UPM framework. It is worth mentioning that once the panel agreed on common element definitions, disagreement tended to resolve.

The identification of the non-linear structure of the modelling domain required the form and sequence of questions used to be such that it allowed experts to reason comfortably. The elicitation of functional interactions was performed in terms of preferences and trade-offs, which created an intuitive environment that helped the experts to make assessments more naturally. The sequence of questions used was according to a stepwise logic, which involved pairwise comparisons between defences. Overall, it is believed that the experts did not encounter any significant problems in reasoning and making assessments within the particular context.

7.5 Conclusion

This chapter illustrated the elicitation process and the results obtained used for the purposes of the qualitative stage of the ID building process. During this stage, in particular, the model assumptions have been verified, the network of the model was structured, and the types of functional interaction between the system defences were identified.

The protocol presented within this section is not application- specific. To be more precise, the process for the elicitation of the ID network and of the non-linear structure of the domain depends neither on the number of defences, root causes and coupling factors incorporated in the model, nor on their physical dimensions. The exercise designed for the structuring of the ID network can be essentially used for any problem domain; the exercise for eliciting the functional interactions between the system defences depends on preferences and trade-offs and does not depend on the physical definition of the defences.

The next chapter describes the second part of the ID building process, namely the Quantitative stage.

Chapter 8

Quantitative Stage of the Influence Diagram Building Process

8.1 Introduction

The previous chapter presented the Qualitative stage of the model building process. In particular, the chapter described the protocol used for: 1) the construction of the model network and and 2) the identification of the functional interactions amongst the system defences, and presented the results obtained.

The aim of this chapter is to describe the second stage of the ID building process, namely the quantitative stage (model instantiation) (Figure 8.1). The chapter is structured as follows: initially, the role of expert judgment within the instantiation context is explained. Afterwards, the probability encoding technique used within this context is described, and the elicitation strategy is presented. Finally, a brief description of the analysis of the results obtained from the process is given.

8.2 The role of Expert Judgment

Influence diagrams (IDs), like Bayesian Belief Networks (BBNs), decompose the joint probability distribution on the modelling domain by using conditional independency

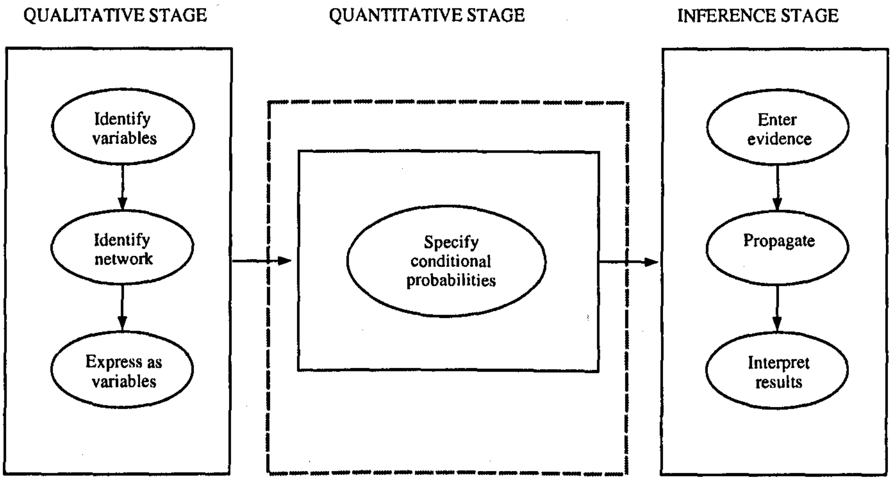


Figure 8.1: Quantitative stage of ID building process

relationships inherent amongst the model elements. The conditional (in)dependency structure of the modelling domain is encoded in the network of the ID model; hence, the overall joint probability distribution is expressed as a product of marginal conditional distributions, defined on the basis of the network.

The marginal conditional distributions are related to the chance nodes of the ID model. To be more precise, each chance node is associated with a set of conditional distributions, describing uncertainty on the node's random variable, for each combination of values of the influencing nodes (parent nodes). Instantiation of the ID model involves the determination of these sets of marginal conditional distributions, describing variable uncertainty prior any statistical information. In principle, these conditional distributions may be learned from data [Chickering et al., 1995], or, especially in expert systems, defined on the basis of expert judgment [Max et al., 1991].

Regarding the particular application, CCFs are particularly rare events; they cannot be studied experimentally and observational procedures yield relatively limited observations [Mosleh et al., 1994; Parry, 1991; Paula, 1995]. Hence, the quantification of the ID network on the basis of statistical data proves to be problematic. As a result, all necessary priors on the model variables need to obtained from expert judgment elicitation[1].

[1] The term 'expert judgment elicitation'refers to the extraction of qualitative and quantitative domain

8.3 The determination of prior distributions

Instantiation of the ID diagram requires the quantification of two types of chance nodes: the root cause nodes, and, the coupling factor nodes. Let r.v. V denote a root cause variable r_i or a coupling factor variable p_{ij} ($i = 1,...,6$ and $j = 1,2,3$), and $D_1,...,D_n$ be the parent defences of r.v. V. The objective at this stage is, for each r.v. V, to specify prior distributions for every configuration of the influencing defences $D_1,...,D_n$, based on expert judgment.

Given the fact that each defence D_k ($k = 1,..,n$) may be assigned to one out of five states, denoted by x_k ($x_k \in \{1,...,5\}$), the set of distributions that need to be determined, associated with V only, comprises of 5^n distributions. In view of the total number of chance nodes that need to be quantified, the number of distributions to be elicited is unmanageably large. The Geometric Scaling (GS) model presented in Chapter 6 proves to be an operationally useful methodology for quantification purposes. In particular, the GS model defines a functional relationship between r.v. V and the configuration vector $\underline{x} = (x_1,...,x_n)$ of the system, viz.

$$V_{\underline{x}} = h(\underline{x})V_{\underline{3}} \tag{8.1}$$

where $h(\underline{x})$ is a log-linear function with parameters $\underline{\phi} = (\phi_1,...,\phi_m)$, and, $V_{\underline{3}}$ is the variable of interest at the 'base-level' $\underline{3} = (3,...,3)$. Based on (8.1), the marginal distribution $f(V_{\underline{x}})$ is decomposed to a product of marginal conditional distributions, i.e.

$$f(V_{\underline{x}}) = \int f(V_{\underline{x}} \mid \underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi}$$

Now, for the determination of $f(V_{\underline{x}})$, for every x_k, $k = 1,...,n$, it suffices to determine the joint distribution on the parameters of the GS model, $f(\underline{\phi})$, and the prior on the 'base-level' variable, $f(V_{\underline{3}})$. As a result of the assumption of 'prior independence' of

knowledge by means of a formal, structured process the proportion parameters (Section 5.5), it is

$$f(\underline{\phi}) = f(\phi_1)...f(\phi_m)$$

and the variables that need to be quantified from expert judgment (target variables) reduce to

- ϕ_ι, for $\iota = 1,..,m$, and
- $V_{\underline{3}}$

8.4 Probability encoding within the ID framework

The elicited distributions represent judgement of knowledgeable individuals (experts), and reflect epistemic uncertainty regarding particular variables. The process used for the determination of the probability distributions of interest is referred to as probability encoding. Many techniques have been suggested for completing probability encoding [Kadane and Wolfson, 1998; Meyer and Booker, 1991; Morgan and Henrion, 1990; Merkhofer, 1987]. In the particular application, the approach adopted is parametric. .

According to the parametric probability encoding approach, specific families of probability distributions are presupposed for the target variables. On this basis, experts are requested to make predictions regarding probabilities or values of the variable, that allow the determination of the parameters of the distributions of interest indirectly. Given that there are analytic relationships that link the experts' assessments regarding a variable with the parameters of its uncertainty distribution, on the grounds of the parametric assumptions made, one is required to solve an analytic problem in order to determine the parameters of interest.

For the specific application, the following classes of distributions have been presupposed for the target variables[2].

- When V is a root cause variable (r_i, for $i = 1,...,6$), the uncertainty distribution

[2] See Chapter 6, Section 6.4

on V belongs to the gamma family viz.

$$f(r_i) = \frac{\beta^\alpha}{\Gamma(a)} r_i^{\alpha-1} e^{-\beta r_i} \quad \alpha, \beta > 0$$

for $r_i \in [0, +\infty]$.

- When V is a coupling factor variable (p_{ij}, for $i = 1,...,6$ and $j = 1,2,3$), the uncertainty distribution of V belongs to the beta family of distributions, viz.

$$f(p_{ij}) = \frac{1}{B(\gamma, \delta)} p_{ij}^{\gamma-1} (1 - p_{ij})^{\delta-1} \quad \gamma, \delta > 0$$

for $p_{ij} \in [0, 1]$.

- The uncertainty distribution on proportion variable ϕ_ι belongs to the lognormal family of distributions, viz.

$$f(\phi_\iota) = \frac{1}{\phi_\iota \sigma \sqrt{2\pi}} e^{-(\ln \phi_\iota - \mu)^2 / 2\sigma^2} \quad \mu \in [-\infty, +\infty], \sigma > 0$$

for $\phi_\iota \in [0, +\infty]$.

Approximating subjective distributions

In principle, the elicitation techniques for determining continuous distributions that are a priori identified to belong into specific families, relies on the determination of points on the cumulative distribution function (CDF) or on the probability density function (PDF). The number of elicited quantities should be in principle equal to the number of family parameters to be determined, so that a system of as many equations as the number of unknowns is obtained, which may be algebraically solved. Once the family parameters are determined, the uncertainty distribution on the variable of interest is fully specified.

However, in practice it is often infeasible to determine closed form solutions for the parameters, especially in cases where calculations involve integrals of the incomplete beta function. In these cases, numerical approximations are required by the analysis. Within the particular framework, the methodology adopted is based on a parametric approach. Particular families of distributions are assumed for the elicitation variables, and the expert is requested to provide numerical estimates for three fractiles of the uncertainty distribution on the variable, namely the median, the 0.5% and the 0.95% fractile (fixed probability technique). Note that, although the prior distributions on the variables are approximated by two-parameter families (gamma, beta or lognormal), the number of elicited quantities for each variable is one too many for a unique solution. Hence, the technique results in a minimisation problem, rather than in a system of equations. The minimisation problem aims to determine the parameters of the distribution so that the fractiles are as close as possible to the subjective assessments made by the expert. Following, the steps of the techniques are described.

Suppose that the interest lies in assessing the prior on V, which is approximated by a probability distribution with p.d.f. $f(v)$. An expert is requested to make assessments regarding V, according to the following steps

Step 1 The subject is requested to state a 'best estimate' for the variable of interest. The 'best estimate' is a value such that there is equal probability (0.5) that the actual value of the variable is smaller than this value, as that it is higher; it is mathematically translated to the median $v_{0.5}$ of the variable, viz.

$$Pr(V \leq v_{0.5}) = 0.5 \Leftrightarrow \int_0^{v_{0.5}} f(v)\mathrm{d}v = 0.5 \tag{8.2}$$

Step 2 The subject is requested to state a 'lower value' for the variable of interest. The 'lower value' is defined as the value for which there is only 0.05 probability that the variable is less than that; it is mathematically translated to the 5% percentile $v_{0.05}$ of the variable, viz.

$$Pr(V \leq v_{0.05}) = 0.05 \Leftrightarrow \int_0^{v_{0.05}} f(v)\mathrm{d}v = 0.05 \tag{8.3}$$

Step 3 The subject is requested to state an 'upper value' for the variable of interest. The 'upper value' is defined as the value for which there is only 0.05 probability that the variable is higher than that; it is mathematically translated to the 95%

percentile $v_{0.95}$ of the variable, viz.

$$Pr(V \leq v_{0.95}) = 0.95 \Leftrightarrow \int_0^{v_{0.95}} f(v)\mathrm{d}v = 0.95 \tag{8.4}$$

The expert's responses are denoted by v_1 (median), v_2 (lower bound) and v_3 (upper bound). The problem is identified as the determination of the parameters of $f(v)$, so that $f(v)$ agrees as much as possible with the information obtained from the expert. Note that f belongs to a two-parameter family and let these parameters take particular values θ_1 and θ_2. Assuming that $f(v)$ is the 'expert' distribution, one can obtain the 'expert' quantiles p_1, p_2 and p_3 that correspond to the expert's responses through Relationships (8.2), (8.3) and (8.4). It holds that

$$\begin{aligned}
\int_0^{v_1} f(v \mid \theta_1, \theta_2)\mathrm{d}v &= p_1 \\
\int_0^{v_2} f(v \mid \theta_1, \theta_2)\mathrm{d}v &= p_2 \\
\int_0^{v_3} f(v \mid \theta_1, \theta_2)\mathrm{d}v &= p_3
\end{aligned}$$

In order to fit the most appropriate distribution on the obtained quantiles v_1, v_2 and v_3, the mean squared error between the expert probabilities p_1, p_2, and p_3 and the theoretical probabilities $q_1 = 0.05$, $q_2 = 0.5$, and $q_3 = 0.95$ is minimised. The mean squared error is a measure of how close are the subjective and theoretical probabilities. Conceptually (Figure 8.2), the squared error $(p_j - q_j)^2$ corresponds to the square of the Euclidean distance d_j between points $(0, p_j)$ and $(0, q_j)$. By minimising the average squared length of the paths between $(0, p_j)$ and $(0, q_j)$, for $j = 1, 2, 3$, the distance between the subjective and theoretical distributions is reduced.

Thus, the problem of determining the parameters of $f(v)$ reduces to finding the optimal values of θ_1, θ_2 according to the following minimisation problem:

$$\text{minimise } \frac{1}{3}\sum_{j=1}^{3}\left(\int_0^{v_j} f(v \mid \theta_1,\theta_2)\mathrm{d}v - q_j\right)^2$$

subject to

$$\theta_1 \in [x_1,y_1]$$

$$\theta_2 \in [x_2,y_2]$$

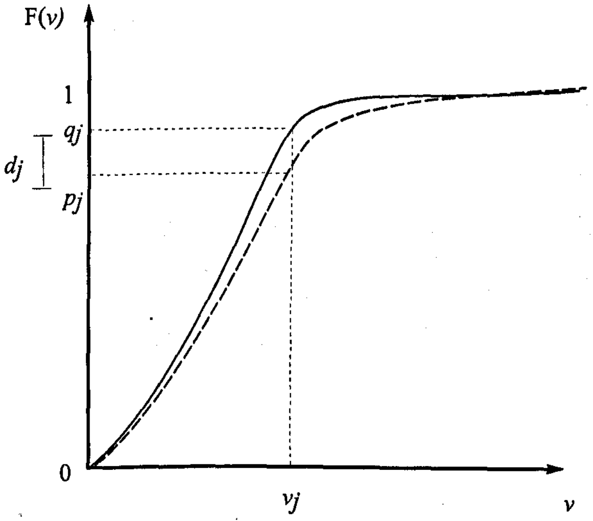


Figure 8.2: By minimising the distance between the subjective and theoretical quantiles, the distance between the corresponding distributions is conceptually minimised

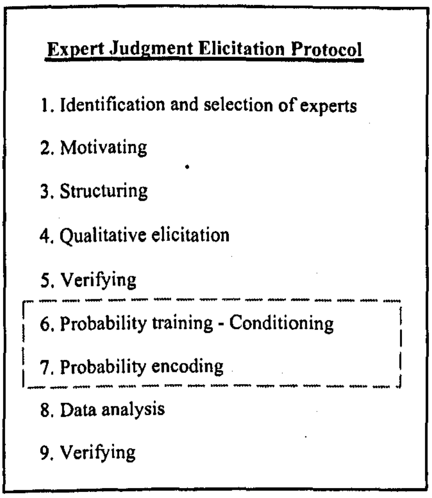
8.5 Elicitation Strategy

The elicitation process, designed in order to extract the information required for the ID instantiation, is in the form of a questionnaire. In practice, it is often difficult for experts to assess the target variables directly. Alternatively, it is considerably more straightforward to assess quantities that are somehow related to the target variables. The uncertainty on the target variables is subsequently determined based on this information. These intermediate quantities are referred to as elicitation variables. At each elicitation variable corresponds a question, which requests to provide a lower value, best estimate, and upper value for the particular variable.

The choice of the particular format for the elicitation exercise is based on two main reasons

- The subject is free to consult other sources of information (past data, event reports, etc), in order to form an assessment they felt comfortable with
- There are no strict restrictions imposed on the time frame of the exercise; the subject has the freedom to adjust the time required to respond to the questions, within logical constraints.

Essentially, the questionnaire was designed in order to conduct Steps 6 and 7 of the Expert Judgment Elicitation Protocol (Figure 8.3). The questionnaire is comprised of three main parts: an Introductory part, a Root Cause part, and a Coupling Factor part. Note that the Questionnaire respondent (subject) has been present during the problem structuring stage of the ID building process, thus, is already familiar with the project scope and objectives.



Expert Judgment Elicitation Protocol

1. Identification and selection of experts
2. Motivating
3. Structuring
4. Qualitative elicitation
5. Verifying
6. Probability training - Conditioning
7. Probability encoding
8. Data analysis
9. Verifying

Figure 8.3: Steps of the protocol accomplished by the questionnaire

8.5.1 Introductory Part

The purpose of the Introductory part of the Questionnaire is three-fold; in particular, the introduction aimed to 1) serve as a reminder of the information provided during the structuring phase by giving information on the particular problem, modelling approach, and problem elements 2) present the results obtained by the qualitative exercise that took place during the expert workshop, and, 3) give explicit instructions on the questionnaire, along with virtual examples for purposes of illustration, in order to facilitate the process of completing the Questionnaire.

8.5.2 Root Cause Part

The Root Cause part of the elicitation questionnaire serves as a means to elicit expert knowledge for determining the prior distributions over the Root Cause variables ($r_{i,\underline{x}}$, for $i = 1,...,6$ at any configuration vector $\underline{x}$). The particular part was comprised of two types of assessment questions. .

The first type of question aims to elicit uncertainty on the 'base-level' variable, r_i (see Relationship (8.1)); the format of the questions used for this purpose is given in Table 8.1.

Table 8.1: Assess uncertainty on root cause 'base-level' rate r_i

A system of EDGs is assessed at the medium level (C) across the influencing defences. Give your percentiles for the failure rate of events attributed to **Root Cause i** (per calendar hour).	5%	50%	95%
Defence D_1: C ... Defence D_k: C ... Defence D_n: C			

The aim of the second type of question is to determine the uncertainty on the proportion variables $\underline{\phi} = (\phi_1,...,\phi_m)$ of the GS model given in Relationship (8.1). Specifying the parameters of the GS model allows the extrapolation of the 'base-level' uncertainty to any configuration vector $\underline{x} = (x_1, ..., x_n)$, for $x_k \in \Omega$, $k \in K$. The series of questions used for this purpose aim to assess the impact of a particular defence on the 'base-level' root cause rate, by taking into account the different kinds of interactions existing amongst the influencing defences.

Functional independence For defence D_k that is functionally independent ($k \in H$), the interest lies in determining the uncertainty on variable ϕ_k. The respondent is requested to assess the impact of modifying the particular defence characteristic by one level on the 'base' root cause rate r_i. The format of questions used for this purpose is given in Table 8.2.

Table 8.2: Assess uncertainty on the impact of modifying defence D_i on the root cause 'base-level' rate

The system's defence regarding Defence D_k is enhanced to level D (while the levels of the rest defences stay at the same level). Consider the ratio of decrease in the failure rate due to Root Cause i. Give your percentiles for this ratio.	5%	50%	95%
Defence D_1: C Defence D_1: C ... Defence D_k: C → Defence D_k: D ... Defence D_n: C Defence D_n: C			

Functional dependence For defences D_m and D_l that are functionally dependent ($\{m, l\} \in M_\pi$), the interest lies in determining the uncertainty on variables ϕ_m, ϕ_l and on the cross-term ϕ_{ml}. For eliciting uncertainty on each ϕ_k, $k = m, l$, the respondent is requested to assess the impact of modifying defence D_k by one level. The questions used for this purpose, similarly to the previous case, request from the respondent to assess the impact on the root cause rate r_i of modifying the particular defence characteristic by one level (see Table 8.2).

For eliciting uncertainty on cross-term ϕ_{ml}, the respondent is requested to evaluate the interaction between the two defences, by assessing the impact of modifying *both* defences D_m and D_l by one level. The format of questions used for this purpose is given in Table 8.3.

Table 8.3: Assess interaction between functionally dependent defences D_m and D_l

The system's defence regarding Defence D_i is enhanced to level D (while the levels of the rest defences stay at the same level). Consider the ratio of decrease in the failure rate due to Root Cause i. Give your percentiles for this ratio.	5%	50%	95%
Defence D_1: C Defence D_1: C ... Defence D_m: C → Defence D_m: D Defence D_l: C → Defence D_l: D ... Defence D_n: C Defence D_n: C			

Threshold functional dependence For defence D_q that is threshold functionally dependent on defences D_t ($t \in L_q$, $q \in Q$), the interest lies in determining the uncertainty on the components of the piecewise function $\phi_q(x_{q_1},...,x_{q_r})$, where

$$\phi_q(x_{q_1},...,x_{q_r}) = \phi_{q,\kappa} \quad \text{when} \quad (x_{q_1},...,x_{q_r}) \in Y_\kappa$$

and Y_κ is a partition of Ω^r.

Initially, the respondent is requested to assess the uncertainty on the impact on r_i of modifying defence D_q by one level, conditionally on the fact that all defences D_t ($t \in L_q$) receive low levels, i.e., $x_t \in X_1$ (Table 8.4). In order to facilitate reasoning, the respondent is then requested to consider whether defence D_q is more or less significant when the defences D_t, $t \in L_q$, are assigned to high levels, i.e., $x_t \in X_3$ (see Table 8.5). Afterwards, the respondent is requested to assess, consistently with the previous response, the uncertainty on the impact of modifying defence D_q, by one level, conditionally on defences D_t being high (Table 8.6).

Table 8.4: Assess the impact of modifying defence D_q on the root cause rate, whilst defence D_t is low.

Suppose that the system is assessed at a *low* level across D_t and that the level of defence Defence D_q is enhanced from C to level D (while the levels of the rest defences stay at the same level). Consider the ratio of decrease in the failure rate due to Root Cause i. Give your percentiles for this ratio.	5%	50%	95%
Defence D_1:C Defence D_1: C ... Defence D_q: C $\rightarrow$ Defence D_q: D Defence D_t: A or B Defence D_t: A or B ... Defence D_n: C Defence D_n: C			

Table 8.5: Facilitating question

Now, suppose that the system is assessed at *high* levels across defence D_t (D or E) and that the level of D_q moves from C to D. Consider the ratio of decrease in the root cause rate r_i. Compared to the previous case where D_t was low, will this ratio

i. Increase (less significant impact of D_q) □
ii. Decrease (more significant impact of D_q) □
iii. Stay the same □

Within the particular application, the set L_q comprises of one or two indices, corresponding to one or two defences. In the case where the counterpart of threshold dependence is one only defence D_t, then the information elicited from Questions 8.4 and 8.6 is sufficient to determine $\phi_q(x_q)$. Indeed, due to the symmetric form of the piecewise function, it is

$$\phi_{q,2} = \sqrt{\phi_{q,1} \cdot \phi_{q,3}} \tag{8.5}$$

where parameters $\phi_{q,1}$ and $\phi_{q,3}$ correspond to Questions 8.4 and 8.6 respectively.

Table 8.6: Assess the impact of modifying defence D_q on the root cause rate, whilst defence D_t is high.

Suppose that the system is assessed at a *high* level across D_t and that the level of defence Defence D_q is enhanced from C to level D (while the levels of the rest defences stay at the same level). Consider the ratio of decrease in the failure rate due to Root Cause i. Give your percentiles for this ratio.			5%	50%	95%
Defence D_1:C ... Defence D_q: C Defence D_t: D or E ... Defence D_n: C	 →	Defence D_1: C Defence D_q: D Defence D_t: D or E Defence D_n: C			

In the case where D_q is threshold dependent on two defences D_{t_1} and D_{t_2}, it is of interest to perform a check regarding the additional conditions placed on the form of function $\phi_q(x_{t_1}, x_{t_2})$[3], namely

$$\phi_q(x_{t_1}, x_{t_2}) = \phi_q(x_{t_1}) \cdot \phi_q(x_{t_2}) \tag{8.6}$$

For this purpose, two additional questions are included in the questionnaire. The first question (see Table 8.7) requests from the respondent to assess the impact of enhancing D_q by one level, given that D_{t_1} has a low level ($x'_{t_1} \in X_1$) and D_{t_2} has a high level ($x'_{t_2} \in X_3$). The second question (see Table 8.8) requests the respondent to assess the same event, this time given that the reverse occurs ($x''_{t_1} \in X_3$ and $x''_{t_2} \in X_1$). If the assessments for variables $\phi_q(x'_{t_1}, x'_{t_2})$ and $\phi_q(x''_{t_1}, x''_{t_2})$, for $x'_{t_1}, x''_{t_2} \in X_1$ and $x''_{t_1}, x'_{t_2} \in X_3$ are close, then (8.6) is a reasonable assumption.

[3] See Chapter 6, Section 6.3.2

Table 8.7: Checking additional condition on piecewise function - Question 1

Suppose that the system is assessed at a *low* level across D_{t_1} and at a *high* level across D_{t_2}. The level of defence Defence D_q is enhanced from C to level D (while the levels of the rest defences stay at the same level). Consider the ratio of decrease in the failure rate due to Root Cause *i*. Give your percentiles for this ratio.	5%	50%	95%
Defence D_1:C Defence D_1: C ... Defence D_q: C → Defence D_q: D Defence D_{t_1}: A or B Defence D_{t_1}: A or B Defence D_{t_2}: D or E Defence D_{t_2}: D or E ... Defence D_n: C Defence D_n: C			

8.5.3 Coupling Factor Part

The Coupling Factor part of the questionnaire serves as a means to elicit the expert judgment required for the quantification of the Coupling Factor nodes. The coupling factors describe the similar characteristics of a system that propagate a failure event due to a particular root cause amongst several components, compelling them to fail dependently rather than independently. Depending on the nature of the root cause event, certain coupling factor mechanisms may be more significant in propagating the root cause event, than others.

The elicitation burden imposed on the Expert may be reduced by taking advantage of the weak association existing amongst particular root causes and coupling factors. The respondent is initially requested to assess the association of each root cause to each coupling factor. The format of the questions serving the particular purpose is given in Table 8.9.

Consider root cause i ($i = 1,...,6$) and coupling factor j ($j = 1,2,3$). If the associ-

Table 8.8: Checking additional condition on piecewise function - Question 2

Suppose that the system is assessed at a *low* level across D_{t_1} and at a *high* level across D_{t_2}. The level of defence Defence D_q is enhanced from C to level D (while the levels of the rest defences stay at the same level). Consider the ratio of decrease in the failure rate due to Root Cause *i*. Give your percentiles for this ratio.	5%	50%	95%
Defence D_1:C Defence D_1: C ... Defence D_q: C → Defence D_q: D Defence D_{t_1}: D or E Defence D_{t_1}: D or E Defence D_{t_2}: A or B Defence D_{t_2}: A or B ... Defence D_n: C Defence D_n: C			

ation between them is evaluated as irrelevant, then it is assumed that

$$p_{ij} = 0$$

and the variable is not quantified (link between root cause i and coupling factor j is omitted from the model). If the association between them is evaluated as significant, then

$$p_{ij} \neq 0$$

and the respondent is encouraged, by being referred to the appropriate section of the questionnaire, to proceed with a range of questions aiming to assess the uncertainty on p_{ij}.

The probability encoding questions designed for eliciting uncertainty on the coupling factor variables p_{ij} comprised of two types of assessment questions.

The first type of questions are designed in order to elicit uncertainty on the 'base-level' coupling factor intensity, $p_{ij,\underline{3}}$ (see Relationship 8.1); the format of the questions is given in Table 8.10.

Table 8.9: Assess association between a particular root cause and different coupling factors

Suppose that a failure event occurs attributed to **Root Cause *i*.** Identify the coupling factors that are IRRELEVANT in propagating the specific root cause event to multiple components of the (sub)system, thus, resulting in a CCF event rather than an independent failure. For each coupling factor, tick the appropriate box.

	IRRELEVANT	RELEVANT	If RELEVANT ticked, fill in section
Coupling Factor 1	□	□	A1
Coupling Factor 2	□	□	B1
Coupling Factor 3	□	□	C1

Table 8.10: Assess uncertainty on coupling factor 'base-level' intensity

A system of EDGs is assessed at the medium level across the influencing defences, i.e. Defence 1 and Defence 2. Suppose that a failure occurs due to Root Cause *i*. Give the percentiles for the probability that the event will result to a CCF via Coupling Factor *j*.	5%	50%	95%
Defence 1: C Defence 2: C Defence 3: C			

The second type of question is designed in order to elicit uncertainty on proportion variables $\varphi_{ij,1},\ldots,\varphi_{ij,m}$. The series of questions used for this purpose aim to assess the impact of a particular defence on the 'base-level' coupling intensity, by taking into account the different kinds of interactions existing amongst the influencing defences, and they are similar to the type of questions used in the Root Cause Part of the questionnaire.

8.6 Elicitation Exercise

Whereas the qualitative stage of the ID building process is strongly dependent on the interaction between the members of the expert panel, the quantitative stage is in the form of a questionnaire that is individually completed by the experts. In view of the fact that the aim of this research is not to produce a definitive industry model, but rather to explore the feasibility of the proposed methodology within the particular context, the elicitation exercise has been conducted with the help of one expert, thereafter referred to as the Expert.

In principle, the questionnaire designed for probability encoding purposes may be completed by various experts. In this case, the results of the elicitation exercise are sets of subjective distributions over the elicitation variables. By using aggregation techniques, the various subjective distributions are mathematically combined to yield overall priors on the model variables [Genest and Zidek, 1986; Thorpe and Williams, 1992; Clemen and Winkler, 1999; Hora, 2004].

The Root Cause Part of the elicitation questionnaire was sent to the participating Expert by mail. Note that the Expert participated in the structuring phase of the model building process, thus he was already aware of the particular problem and modelling approach. Shortly after, a telephone meeting was arranged. The purpose of the meeting was to ensure that the Expert was feeling comfortable with the tasks that he was requested to conduct. In order to achieve this objective, analyst and Expert interactively went through the instructions of the questionnaire, in a stepwise manner. The Expert was provided with a time frame, within which he was encouraged to complete and send the questionnaire to the analyst.

On receipt of the questionnaire, the responses of the Expert were analysed. Probabilistic distributions were fitted on the elicited fractiles, and on the grounds of the GS model, the Expert's uncertainty on the 'base-level' rates was extrapolated to all the defence levels.

In order to verify that the responses of the Expert reflected his true beliefs, an individual meeting was arranged. During the meeting, graphical aids were used to visually project the encoded distributions to the expert, along with the extrapolated distributions obtained through the GS model. The Expert was given the opportunity to reflect on the results and potentially make further adjustments on his initial responses. Given the extensive number of the encoded distributions, it was not possible to request feedback on the whole range of distributions. Instead, a manageable set of distributions was chosen to serve as a sample.

The individual meeting was also an introductory session to the second part of the questionnaire, namely the Coupling Factor Part. The purpose of the particular section of the questionnaire was explained, along with instructions on the completion of the tasks involved. The particular assumptions implied by the theoretical structure of the model were described and elicitation examples were visually illustrated to the Expert, by using interactive plotting means. Having gained a comprehensive view on the second part of the Questionnaire, the Expert was provided with a time frame, during which he was encouraged to complete the Questionnaire, and send it to the analyst via mail.

After analysis of the Expert's assessments on the Coupling Factor section, received via mail, a telephone meeting was arranged with the Expert. The purpose of the meeting was to receive feedback on the assessments made by the Expert regarding the coupling factor variables, and perform any adjustments when requested. Prior the meeting, an excel file was sent illustrating the results of the analysis, in order to prepare the Expert and allow a margin of time to be used for consideration.

The overall expert judgment elicitation process used for the determination of the aforementioned priors is portrayed in Figure 8.4.

8.7 Analysis of the results of the elicitation exercise

This section aims to describe the analysis involved in the determination of the subjective distributions on the root cause and coupling factor variables of the model based on the information extracted from the elicitation exercise.

The methodology is described by using a particular variable as an illustrative example, this of the Internal to Component root cause rate. Detailed computations for this particular variable, and the rest of the variables of the ID model, may be found in Appendix C.

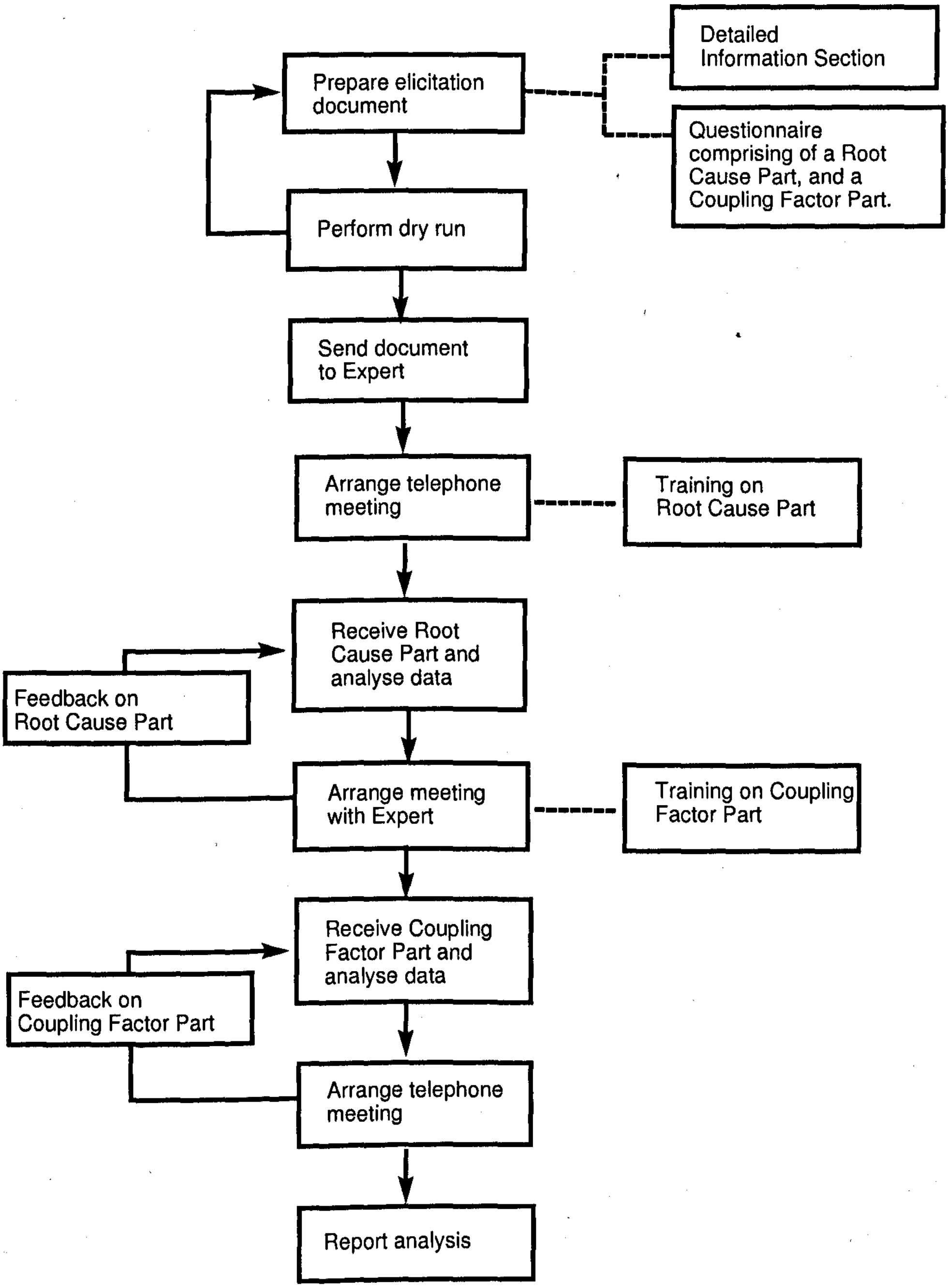

Detailed Information Section
Prepare elicitation document
Questionnaire comprising of a Root Cause Part, and a Coupling Factor Part.
Perform dry run
Send document to Expert
Arrange telephone meeting
Training on Root Cause Part
Receive Root Cause Part and analyse data
Feedback on Root Cause Part
Arrange meeting with Expert
Training on Coupling Factor Part
Receive Coupling Factor Part and analyse data
Feedback on Coupling Factor Part
Arrange telephone meeting
Report analysis

Figure 8.4: Instantiation process

8.7.1 Target and elicitation variables

The rate of failure events due to Internal to Component causes occurring to a system with defence configuration

$$\underline{x} = (x_1, x_3, x_7), \quad \text{where } x_k \in \{1,...,5\} \text{ and } k = 1,3,7$$

is represented by random variable $r_{3,\underline{x}}$. The defences that are targeted against the occurrence of this type of failures are Environmental Testing (D_1), Analysis (D_3), and, Understanding (D_7). The identified functional interactions existing amongst these defences are: Analysis (D_3) and Understanding (D_7) are functionally dependent; Understanding (D_7) is threshold dependent on Env. Testing (D_1).

Consistently with the GS model defined in Chapter 6, this rate is given by:

$$r_{3,(x_1,x_3,x_7)} = \phi_1^{x_1-3}\phi_3^{x_3-3}\phi_7(x_1)^{x_7-3}\phi_{37}^{(x_3-3)(x_7-3)}r_{3,(3,3,3)} \tag{8.7}$$

where $\phi_1, \phi_3, \phi_{37}, \phi_7(x_1) \in (0,1]$ are the proportion variables, and $r_{3,(3,3,3)}$ is the 'base-level' rate at defence configuration $\underline{x} = (3,3,3)$. Note that $\phi_7(x_1)$ is a piecewise function, viz.

$$\phi_7(x_1) = \phi_{7,\theta} \quad \text{when } x_1 \in X_\theta,\ \theta = 1,2,3$$

and $X_1 = \{1,2\}, X_2 = \{3\}$ and $X_3 = \{4,5\}$.

Performing uncertainty analysis on model (8.7) requires the determination of the uncertainty on the 'base-level' rate and the proportion variables. These constitute the uncertain quantities of interest and referred to as the *target* variables, which will be determined through the use of elicitation variables. Each question of the questionnaire extracts sufficient information to assess the uncertainty on a particular elicitation variable. The part relevant to the Internal to Component root cause rate consists of six questions. Let e_n denote the elicitation variable associated with the n-th question, $n = 1,...,6$.

The first question relates to the assessment of the uncertainty on the 'base-level' rate $r_{3,(3,3,3)}$, which is assessed directly. Therefore,

$$e_1 = r_{3,(3,3,3)}$$

The following questions aim to assess the uncertainty on the proportion variables, which are related to the impact of enhancing a particular defence on the rate. The relationships associating the elicitation with the target variables are

$$e_2 = \phi_1 \qquad e_3 = \phi_3 \tag{8.8}$$

$$e_4 = \phi_3\phi_{37}\phi_{7,2} \qquad e_5 = \phi_{7,1} \tag{8.9}$$

$$e_6 = \phi_{7,3} \tag{8.10}$$

In order to elicit the uncertainty on the cross-term ϕ_{37}, which expresses the dependency between the two functionally dependent variables D_3 and D_7, the expert is requested to assess the impact on the rate induced by enhancing both dependent defences at the same time by one level, whilst keeping the rest fixed at the medium level. This quantity corresponds to elicitation variable e_4. Moreover, the uncertainty on $\phi_{7,2}$ is determined based on the symmetry assumption

$$\phi_{7,2} = \sqrt{\phi_{7,1}\phi_{7,3}} \tag{8.11}$$

Therefore, assessing the uncertainty on the elicitation variables is sufficient for the determination of the uncertainty on the target variables. The subsequent analysis is significantly simplified by making two key assumptions: firstly, it is assumed that the proportion variables are *a priori* independent, and secondly, it is assumed that the proportion variables are lognormally distributed[4]. Therefore, by applying log-transformations on relationships (8.8), (8.9), (8.10) and (8.11) one gets linear transformations of independent normally distributed variables.

[4] See Chapter 6, Section 6.4

8.7.2 Conditions on target variables

According to the theoretical setup of the model, the target variables need to meet two types of conditions. Firstly, it is assumed that the vulnerability of the system does not become worse as a result of enhancing the defence characteristics of the system. In the particular example, for functionally dependent variables D_3 and D_7, the impact proportion of the defences is expressed by

$$\phi_3\phi_{37}^{x_7-3} \text{ and } \phi_7(x_1)\phi_{37}^{x_3-3}$$

For the defence enhancement to be beneficial, the respective rate should decrease, implying the associated impact proportion should take values in the interval $(0,1]$, viz.

$$0 < \phi_3\phi_{37}^{x_7-3}, \phi_7(x_1)\phi_{37}^{x_3-3} \leq 1 \quad \text{for every } x_1, x_3, x_7 \in \{1,...,5\} \tag{8.12}$$

Secondly, when a defence interaction is identified as compensating, enhancing one defence becomes less effective for higher values of the other defence. In this case D_7 is threshold functionally dependent on D_1, and the following needs to hold

$$\phi_{7,1} \leq \phi_{7,2} \leq \phi_{7,3} \tag{8.13}$$

Within the particular framework, the following relaxation of Conditions (8.12) and (8.13) is applied: let ν_{pi,ϕ_ι} be the $p_i \cdot 100\%$ fractile of the distribution F on ϕ_ι, for $p_1 = 0.05, p_2 = 0.5, p_3 = 0.95$, viz.

$$F(\nu_{pi,\phi_\iota}) = p_i,\ i = 1,2,3$$

it is then requested that

$$0 < F(\nu_{p_i,\phi_m\phi_{ml}^{x_l-3}}), F(\nu_{p_i,\phi_l\phi_{ml}^{x_m-3}}) < 1, \quad i = 1,2,3,\ x_m, x_l = 1,...,5 \tag{8.14}$$

and

$$F(\nu_{p_i,\phi_q(x_t)}) \leq F(\nu_{p_i,\phi_q(x_t')}) \quad \text{for } x_t < x_t' \tag{8.15}$$

During the analysis of the encoding results, there may be cases where conditions 8.14 and 8.15 are not met. In order to avoid violation of these conditions, minimisation problems are solved for the parameters of the subjective distributions subject to conditions 8.14 and 8.15. The details are given in Appendix C.

8.8 Conclusion

This chapter described the methodological steps employed in order to obtain the information required for the quantification of the ID model. In particular, the probabilistic configuration (prior distributions) of the ID model is determined based on probability encoding, which was conducted with the help of one participating expert. Through probability encoding, the Expert was encouraged to provide numerical assessments of his uncertainty in terms of quantiles of random variables. These assessments constitute summaries of the prior distributions, and the expert priors are then specified by choosing distributions that conform to the conditions posed by the summaries.

Within this particular application, it is assumed that the expert prior distributions belong to particular families, namely the gamma, beta and lognormal families. These modelling choices have been made on the grounds of both common practice and convenience. As discussed in Chapter 5, particular families of distributions constitute standard choices within reliability analyses; moreover, they simplify subsequent analysis because of the conjugate properties of these families. In addition, the particular selection has been verified during the feedback sessions with the Expert, where it was ensured that the fitted distributions reflected adequately his uncertainty on a sample of variables. Retrospectively, the particular families of distributions seem to fit sufficiently well to the expert summaries: the mean squared error between the corresponding expert probabilities and the theoretical probabilities is in most cases low.

Moreover, the chapter described the analysis of the results that this process yielded in order to determine the priors, by using a practical example. It is interesting to remark that, in this practical example, the checks performed on the additional condition placed on the form of the piecewise function

$$\phi(x_1, \ldots, x_r) = \prod_{m=1}^{r} \phi(x_m)$$

showed that this is a reasonable assumption.

In principle, the probability encoding process described in this chapter is not application-specific. The same process may be used to determine the probabilistic specification on the ID variables, regardless of their number and their physical dimensions. Moreover, the same protocol may be repeated with the help of more experts. By using mathematical techniques to combine the assessments of more than one experts, the results will be representing aggregated field knowledge.

The next chapter describes the validation process employed within this thesis. Firstly, sensitivity analysis is performed on the probability specifications of the ID variables; secondly, the behaviour of the ID model is compared to this of UPM; thirdly, the behaviour of the ID model is generally explored.

Chapter 9

Model Validation

9.1 Introduction

The purpose of this chapter is to discuss the concept of verification and validation within the context of this research. The concepts of verification and validation are central not only to Probabilistic Safety Assessment (PSA), but also to any other discipline that is concerned with modelling. Only when a model is verified and validated, it can stand up to scrutiny and it is accepted by the scientific community as a sound and legitimate piece of scientific work. Therefore, confirming the quality of a model is a key aspect of the modelling process and should be given the appropriate attention.

The concept of validation is often used interchangeably with the concept of verification. Nevertheless, the two concepts are not equivalent. Normally, the concept of verification refers to checking the conformity of a model to some well-defined specification, while the concept of validation normally refers to assessing that the model is suitable for its intended purpose [Kristensen, 2004]. The main difference between the two concepts is the fact that, while verification is related to a set of objective standards, validation is closely related to the particular situation and methodological approach in hand.

This Chapter is structured as follows: Section 9.2 defines the set of quality criteria and conditions used for model evaluation, with reference to the model definition and the philosophical position of the research, and Section 9.3 describes the validation process used within the context of the ID model. Section 9.4 presents the sensitivity analysis performed on the model. The ID model is compared to UPM in Section 9.5, and the overall behaviour of the model is explored in Section 9.6. Finally, Section 9.7 concludes the chapter.

9.2 Validation Criteria

Whereas model verification is achieved by comparing the model against scientifically acceptable specifications and assumptions, model validation is in principle established based on the pragmatic criterion. The pragmatic criterion is based on comparison with 'objective' values [Aven, 2003] and it is achieved by exploring how close to observations the predictions of the model lie. Within a Bayesian context, data-based diagnostics can be computed in order to explore how well the model predictions fit the observed data [O'Hagan and Forster, 2004]. However, in many cases sufficient data is not available and the specification of 'objective' probability is philosophically inconsistent. Thus, scientific acceptance is often achieved through agreed formalisms and 'peer' reviews, rather than comparison with an objective reality [Melchers, 2001].

Within the particular scope, the pragmatic criterion is not relevant. The reason is that this research does not seek to produce a definitive tool for performing risk assessments within the industry; instead, the feasibility of the proposed methodology is explored. This aim can be achieved by performing the model quantification with the participation of a single expert. To this end, model predictions are of a highly subjective nature, and it is not appropriate to assess the quality of the model in an absolute way, to accept or refute it on the basis of 'right' or 'wrong', or on the basis of how accurate to reality the outputs of the model are. Instead, it is of key importance to confirm that the model is consistent, meaning that the probability assignments abide by the laws of probability (syntactic criterion) and they are the outcome of a formal encoding process (semantic criterion)[Aven, 2003].

Moreover, the concept of validation cannot be defined outside the scope of the objectives of the model. A model may be consistent and with a strong predictive ability, however, if it fails to fulfill its intended purposes, it is of no use. In general, a PRA model can be described as the analyst's attempt to represent the system in a form that can be used as an explanatory and exploratory tool [Parry, 1996]. Within the particular context, the ID model attempts to serve as an exploratory tool by capturing the impact of the system characteristics on its vulnerability towards CCF events and permitting to explore postulated modifications; the ID model intends to serve as an explanatory tool by providing a detailed understanding of the CCF mechanisms through root causes and coupling factors. Therefore, validating the model based on its predictive ability would address the issue only partially. A comprehensive model validation should involve attaining credibility in terms of the construction of the model, and assurance that it sufficiently represents and communicates the relationships existing within the modelling domain.

During the model building process, assumptions are stated and modelling decisions are made. To achieve verification, it is important to ensure that these choices are appropriate within the particular context, or that they abide by generally accepted standards. Clear documentation of the mathematical assumptions of the methodology renders the modelling choices admissible to peer review. To achieve validation, we seek to *assure that the model is consistent and useful for its intended purpose.*

9.3 Validation process

Validating the ID model as a whole equates to validating the components comprising the model. In order to identify how credibility of these components may be achieved, it is important to define the nature of what is being assessed.

The ID model is comprised of a qualitative and a quantitative part. The qualitative part is the network of the model, which portrays the important features of the modelling domain and the inherent relationships amongst these features. The network of the model is constructed during the qualitative stage of the model building process.

The quantitative part of the model comprises of probabilistic expressions relevant to each feature, describing the impact of the influencing features. These probabilistic specifications are determined during the quantitative stage of the model building process.

Finally, the model yields quantified figures related to the vulnerability of the system towards the occurrence of CCFs. These figures are obtained and interpreted during the inference stage of the model building process.

Therefore, model validation is defined with reference to the following three components

- Model network (Qualitative stage)
- Probability specifications (Quantitative stage)
- Model outputs (Inference stage)

Overall, model validation is an ongoing process, that takes place during the different stages of the model-building process. The overall validation process adopted within the particular framework is portrayed in Figure 9.1.

STAGE	COMPONENT	VALIDATION
Qualitative	Model network	Validate assumptions and modelling principles Feedback on model network
Quantitative	Probability specifications	Formal elicitation protocol Frequent feedback
Inference	Model output	Sensitivity Analysis Comparison of behaviour of the model with UPM

Figure 9.1: Validation process

9.3.1 The model network

The model network describes the structure of the modelling situation from a conceptual perspective. Validating the model structure involves ensuring that the model is a meaningful representation of the particular situation. This is achieved by certifying that the assumptions, simplifications and limitations used are valid within the particular context, and that the network consistently portrays the inherent relationships.

Validation of the model structure is achieved by ensuring that the modelling approach is perceived as reasonable by the people that have a thorough understanding of the modelling domain. At a first stage, an extensive presentation was given (Gartmore, Gloucester) at the early stages of the model building process, to a group of people that are involved in risk analysis within the nuclear industry. The group comprised of assessors, regulators and analysts. During the presentation, the modelling approach was described in detail. Particularly, the ID formalism was explained, the elements of the ID were identified, and the modelling approach towards CCF treatment in terms of system defences, root causes and coupling factors was presented. Relevant feedback certified that the particular approach is sensible for achieving the model's intended purpose.

The construction of the model network is based on expert judgment and was completed during the workshop with the expert panel. Validation of the model network relates to ensuring that the resulting graph captures the inherent dependencies in the modelling domain and does not lead to any conceptual inconsistencies. This is achieved by requesting frequent feedback from the expert panel, both during the elicitation exercise and afterwards, by providing a clear documentation of the process and the results obtained (see Figures 7.5 and 7.7 in Chapter 7).

9.3.2 Probability specifications

Within the model's context, the uncertainty on the elements of the model is captured through probabilistic expressions. Specifically within the particular application, expert judgment is the major source of data. Validation of the quality of the elicited information occurs in two facets. Firstly, it needs to be ensured that expert judgment was elicited through a formal process, in an axiomatic and structured way that minimises inherent biases. Within the particular context, this is achieved by constructing a comprehensive elicitation protocol for expert judgment that meets the desiderata of scrutability, neutrality and fairness[1]. Secondly, it is necessary to assure that the information elicited succeeds to sufficiently reflect the actual beliefs of experts, and that the elicitation results are conceptually consistent. This is achieved by requesting frequent feedback from the participating experts, during and after the completion of each elicitation exercise (see Figure 8.4 in Chapter 8).

9.3.3 Model outputs

In principle, validation of the outputs of a Bayesian Belief Network, in particular, is supported by two types of analysis: sensitivity analysis, and comparison of the behaviour of the model with well-known scenarios [Langseth and Portinale, 2005].

The probabilistic specification of the model is based on expert judgment. Encoding the expert's degrees of belief is not just a simplification of reality, it is 'a simplification of the expert's perception of reality' [Pradhan et al., 1996]. Therefore, the resulting probability distributions are inevitably inaccurate. In order to ensure that these inaccuracies do not influence significantly the reliability of the model's output, one needs to explore the extent to which deviations from the determined probability distributions influence the model output. "The study of how the uncertainty in the output of a model can be apportioned to different sources of uncertainty in the model input" is achieved by performing sensitivity analysis [Saltelli, 2002]. The purpose behind sensitivity analysis is twofold: it serves as a means for understanding the robustness of the inferences obtained by the model, and, as a method for identifying the areas that are more influential of the model output.

Moreover, it needs to be ensured that the model serves its intended purpose. In the particular case, the ID model is an extension of UPM, seeking to address particular

[1] See Chapter 7, Section 7.2

features. In particular, the ID model attempts to capture the dependencies existing amongst the system defences, something that the linear weighting system of UPM fails to do. Thus, the behaviour of the model is explored in relation to the behaviour of UPM.

The validation process of the model outputs is presented in the following sections.

9.4 Sensitivity Analysis

For a mathematical model, sensitivity analysis relates to exploring the effect of input inaccuracies on the model output, and it is achieved by systematically varying the model's parameters [Morgan and Henrion, 1990]. For a Bayesian Belief Network in particular, sensitivity analysis is achieved by investigating the effect of inaccuracies in the probability specifications of the model variables on a probability of interest [Coupé and van der Gaag, 2002; Laskey, 1995]. This is achieved by varying the network's parameters. The simplest technique to perform sensitivity analysis involves varying directly one parameter of the model at a time, while keeping the other parameters fixed, and exploring the effects of these changes on the probabilities of interest.

In principle, there are two approaches towards performing sensitivity analysis: the brute-force approach and the analytical approach. Brute-force sensitivity analysis is achieved by examining directly the effect of a number of deviations from the parameter in question [Kjærulff and van der Gaag, 2000]. Such an approach, even in principle the simplest, is particularly cumbersome when used for graphical models, as it requires numerous network evaluations. Analytical sensitivity analysis establishes an analytical function between expressing the probability on a parameter in terms of the parameters under study. For instance, sensitivity values may be obtained by computing partial derivatives of a marginal probability with respect to the parameters of study [Laskey, 1995]. This method yields a first order approximation of the effect of varying a particular parameter on an uncertainty distribution, and defines sensitivity measures analytically. Alternatively, in [Kjærulff and van der Gaag, 2000] and [Coupé and van der Gaag, 2002] a given probability is expressed as a polynomial over the parameter under study. By analytically determining the coefficients of the polynomial, one is able to determine the effect of varying the parameters of interest. Analytical treatment of sensitivity analysis is an automated technique, and the computational cost involved is significantly reduced in comparison to the direct variation approach.

The ID model decomposes the overall structure on the modelling domain to smaller structures. The chance node of the ID model that represents either a root cause or a coupling factor variable, generally denoted with V, is expressed through the GS model in terms of a 'base-level' variable $V_{(3,\dots,3)}$, and proportion variables ϕ_ι, through a geometric scaling model, viz.

$$V_{(x_1,\dots,x_n)} = h_v(x_1,\dots,x_n) \cdot V_{(3,\dots,3)} \tag{9.1}$$

where $\underline{x} = (x_1, x_2, \dots, x_n)$ is the configuration vector and $h_v(x_1,\dots,x_n) : \Omega^n \rightarrow \mathbb{R}$ is also a function of the proportion variables $\underline{\phi} = (\phi_1,\dots,\phi_m)$.

The quantification of the root cause/coupling factor nodes requires the determination of the probability distributions on variables $V_{(3,\dots,3)}$ and proportion variables ϕ_ι $(\iota = 1,\dots,m)$; the latter are elicited from expert judgment. Performing sensitivity analysis locally regarding each sub-model (9.1) allows us to identify the variables with the most impact on output $V_{\underline{x}}$.

9.4.1 Method

The approach adopted for performing sensitivity analysis on the ID model exploits the mathematical structure of the model, resulting in an analytical approach to sensitivity analysis. First order sensitivity measures are used to explore the relative contribution of distributions of parameters on the distribution of the target variable.

Within the particular framework, a model variable v is linked to its influencing or parent variables, denoted by v_π, through a mathematical function (Relationship (9.1)), viz.

$$v = f(v_\pi)$$

Suppose that v_π is a vector of n random variables, i.e.

$$v_\pi = (v_{\pi,1}, \ldots, v_{\pi,n})$$

Consider a nominal scenario, v_π^0, where all the parent variables take their expected values, i.e.

$$v_\pi^0 = (E[v_{\pi,1}], \ldots, E[v_{\pi,n}])$$

yielding

$$v^0 = f(v_\pi^0)$$

The interest lies in exploring the deviations of the output from the nominal scenario. By considering a Taylor expansion of $v - v^0$ and assuming that the expected value of the deviation in v is zero, i.e.

$$E[v - v^0] = 0$$

one can obtain a *first order approximation* for the variance of the model output as

$$\begin{aligned} var[v] \approx & \sum_{\iota=1}^{n} var[v_{\pi,\iota}] \left[\frac{\partial v}{\partial v_{\pi,\iota}}\right]_{v^0}^{2} \\ & + 2 \sum_{\iota=1}^{n} \sum_{\kappa=\iota+1}^{n} cov[v_{\pi,\iota}, v_{\pi,\kappa}] \left[\frac{\partial v^2}{\partial v_{\pi,\iota} \partial v_{\pi,\kappa}}\right]_{v^0} \end{aligned} \qquad (9.2)$$

A key assumption of the ID theoretical structure is the fact that the input variables in Relationship (9.1) are *a priori* independent. Relationship (9.2) is simplified to

$$var[v] \approx \sum_{\iota=1}^{n} var[v_{\pi,\iota}] \left[\frac{\partial v}{\partial v_{\pi,\iota}}\right]_{v^0}^{2} \qquad (9.3)$$

Relationship (9.3) offers an analytic means to determine the relative contribution of each parent variable to the uncertainty on the output. In particular, the contribution of variable $v_{\pi,\iota}$ to the variation of v is

$$\left(\sigma_{\pi,\iota}\left[\frac{\partial v}{\partial v_{\pi,\iota}}\right]_{v0}\right)^2$$

Relationship (9.3) may be rewritten as

$$1 \approx \sum_{\iota=1}^{n} \frac{var[v_{\pi,\iota}]}{var[v]} \left[\frac{\partial v}{\partial v_{\pi,\iota}}\right]_{v0}^{2} \tag{9.4}$$

Hence, the quantities

$$C_{\pi,\iota} = \frac{var[v_{\pi,\iota}]}{var[v]} \left[\frac{\partial v}{\partial v_{\pi,\iota}}\right]_{v0}^{2} \tag{9.5}$$

for $\iota = 1,\ldots,n$, rank the parameters of the model according to the fraction of the total variation of the model output due to small variations in the parameter values, taken one at a time. Measures $C_{\pi,\iota}$ consider both sensitivity and uncertainty aspects [Morgan and Henrion, 1990]: $C_{\pi,\iota}$ is the product of the sensitivity of $v_{\pi,\iota}$,

$$S_{\pi,\iota} = \left[\frac{\partial v}{\partial v_{\pi,\iota}}\right]_{v0}^{2}$$

which is the squared rate of change of v with respect to variation of $v_{\pi,\iota}$, and the relative uncertainty in $v_{\pi,\iota}$,

$$U_{\pi,\iota} = \frac{var[v_{\pi,\iota}]}{var[v]}$$

so that

$$C_{\pi,\iota} = S_{\pi,\iota} \times U_{\pi,\iota}$$

Note that within the particular framework, function $f(\cdot)$ is log-linear; by applying a lognormal transformation on v, it becomes

$$\ln[v] = \sum_{\iota=1}^{n} \alpha_\iota \ln[v_{\pi,\iota}]$$

Consequently, the variance approximations are exact, given that the inputs are independent, with finite means. The partial derivatives are now

$$\left[\frac{\partial \ln v}{\partial \ln v_{\pi,\iota}}\right]_{\ln v^0} = \frac{\partial \ln v}{\partial \ln v_{\pi,i}} = \alpha_\iota$$

which are independent of the nominal scenario v^0. Consequently, the uncertainty measure $C_{\pi,\iota}$ considers scenarios distant from the nominal scenario. $C_{\pi,\iota}$ is a measure to assess the relative importance of input factors (parameters) in the presence of uncertainty. Under the assumption that variance is a measure of uncertainty, $C_{\pi,\iota}$ is assessing the contribution of the uncertainty of each factor to the overall uncertainty of the output.

9.4.2 Root Cause variables

This section presents results from the sensitivity analysis performed on the root cause variables of the model r_i ($i = 1,...,6$). Recall that the root cause rate r_i at configuration vector $(x_1,...,x_n)$ is given by the GS model[2], viz.

$$r_{i,(x_1,...,x_n)} = h_i(x_1,...,x_n) \cdot r_{i,(3,...,3)} \tag{9.6}$$

where

$$h_i(x_1,...,x_n) = \prod_{\{i,j\}\in M_\pi} \phi_{ij}^{(x_i-3)(x_j-3)} \prod_{k\in K} \Phi_k^{x_k-3}$$

and $0 < \Phi_k \leq 1$ for every $k \in K$. By applying a log transform to (9.6), a linear relationship is established between $r_{i,(x_1,...,x_n)}$ and parameters ϕ_ι[3] and $r_{i,(3,...,3)}$, i.e.

$$\ln r_{i,(x_1,...,x_n)} = \sum_{\{i,j\}\in M_\pi} (x_i-3)(x_j-3)\ln\phi_{ij} + \sum_k (x_k-3)\ln\Phi_k + \ln r_{i,(3,...,3)} \tag{9.7}$$

The importance measures for proportion parameters $\ln(\phi_\iota)$ are given in Table 9.1. It may be seen that the sensitivity of parameter $\ln(\phi_\iota)$ depends on the level x_ι of the associated defence: the further x_ι is from the base level 3, the more sensitive the distribution

[2] See Chapter 6, Section 6.3

[3] With ϕ_ι we denote all the proportion variables ϕ_{ij} and Φ_k, for $i,j \in M_{ij}$ and $k \in K$

of $\ln\phi_\iota$ is to the distribution of parameter $\ln r_{(x_1,\ldots,x_n)}$.

Table 9.1: Formulae for importance measures of parameters influencing the root cause rate r_i

Parameter	$S_{\pi,\iota}$	$U_{\pi,\iota}$	$C_{\pi,\iota}$
$\ln(\phi_\iota)$	$(x_\iota-3)^2$	$\frac{var[\ln\phi_\iota]}{var[\ln r_{(x_1,\ldots,x_n)}]}$	$(x_\iota-3)^2\frac{var[\ln\phi_\iota]}{var[\ln r_{(x_1,\ldots,x_n)}]}$

The relative importance of each parameter is investigated in relation to two extreme scenarios: the first scenario $\underline{x}^-$ considers the lowest possible defence configuration, and the second scenario $\underline{x}^+$ considers the highest possible defence configuration i.e.

$$\underline{x}^- = (1,\ldots,1) \text{ and } \underline{x}^+ = (5,\ldots,5)$$

The importance measures $C_{\pi,\iota}$ for the two scenarios are given in Figure 9.2. The values measure the contribution of the assessed uncertainty on the decrease induced to the root cause rate by modifying a particular defence.

Note that for the base level rates $\ln r_{i,(3,\ldots,3)}$ $(i=1,\ldots,6)$, the coefficients of parame-. ters $\ln\phi_\iota$ are zero for all ι; this is expected as $\ln r_{i,(3,\ldots,3)}$ is a parent node of $\ln r_{i,(x_1,\ldots,x_n)}$. Moreover, the importance measures $C_{\pi,\iota}$ for a particular root cause rate do not always sum up to unity. The reason is that the cross-terms ϕ_{ij} $(\{i,j\}\in M_\pi)$ are also contributors to the uncertainty on the root cause rate $\ln r_{i,(x_1,\ldots,x_n)}$. However, their contribution is relatively very small resulting in small deviations from unity, and are thus omitted. Moreover, the contribution of the base rates $\ln r_{i,(3,\ldots,3)}$ is comparatively insignificant. Finally, the importance measure of the impact of Safety Culture on the Maintenance root cause rate ($\ln\phi_4$) is 1, because the latter is the only defence that is able to modulate the particular type of failures.

From the values in Figure 9.2 it may be seen that for scenario $\underline{x}^-$, the proportion of decrease by modifying Env. Control is the dominant contributor to the uncertainty of the Design root cause ($C=0.66$), with the impact of Diversity and Separation being relatively unimportant for both scenarios. Env. Control is also a significant contributor to the uncertainty of the Internal root cause rate ($C=0.31$), but only for scenario $\underline{x}^+$.

Root Cause														
Design		Human		Internal		Maintenance		Procedures		External		*Average*		**Defence**
x-	x+	x-	x+	x-	x+	x-	x+	x-	x+	x-	x+	x-	x+	
0.66	0.77			0.08	0.31							0.37	0.54	E. Control
		0.24	0.32							0.06	0.06	0.15	0.19	E. Testing
0.10	0.12			0.09	0.36			0.18	0.43	0.94	0.94	0.33	0.46	Analysis
		0.11	0.18			1	1			0.06	0.06	0.08	0.12	S. Culture
0.10	0.09											0.10	0.09	Separation
0.13	0.02											0.13	0.02	Diversity
		0.24	0.41	0.82	0.32			0.21	0.49			0.42	0.41	Understanding
		0.42	0.08					0.60	0.05			0.51	0.07	Op. Interaction

Figure 9.2: Importance measures $C_{\pi,\iota}$ for root cause rates

The impact of Env. Testing is an important contributor to the uncertainty on the Human root cause rate, whereas it is an insignificant contributor to the uncertainty of the External root cause rate.

The impact of Analysis is almost entirely responsible for the uncertainty on the External root cause rate ($C = 0.94$) for both scenarios, and a significant contributor to the uncertainty on the root cause rates of Internal ($C = 0.36$) and Procedures ($C = 0.43$) for scenario $\underline{x}^+$.

The impact of Safety Culture is comparatively limited, for both scenarios $\underline{x}^+$ and $\underline{x}^-$.

The uncertainty on the Internal root cause rate is almost entirely attributed to impact of Understanding ($C = 0.82$) for scenario $\underline{x}^-$, whereas for scenario $\underline{x}^+$ the impact of the influencing defences are almost equally responsible. Assessing the impact of Understanding contributes significantly to the uncertainty on the Procedures root cause rate ($C = 0.49$), on the Human root cause rate ($C = 0.41$) and on the Internal root cause rate (0.32).

Finally, the impact of Op. Interaction appears to be a significant contributor to the uncertainty of Human and Procedures root cause rates, however only for the low-level scenario $\underline{x}^-$.

Overall, for scenario $\underline{x}^-$ assessing the impact of Env. Control, Analysis, Understanding and Op. Interaction are the main contributors to the uncertainty on the root cause rates as a whole. For scenario $\underline{x}^+$, the contribution of the impact of Op. Interaction decreases significantly, whereas the contributions of the other three defences remain approximately at the same level.

9.4.3 Coupling Factor variables

This section presents results of the sensitivity analysis performed on the coupling factor variables of the model p_{ij} ($i = 1,...,6$ and $j = 1,2,3$). Recall that coupling factor variable p_{ij} at configuration vector $(x_1,...,x_n)$ is given by the GS model, viz.

$$p_{ij,(x_1,\ldots,x_n)} = h_{ij}(x_1,\ldots,x_n) \cdot p_{ij,(3,\ldots,3)} \tag{9.8}$$

where

$$h_{ij}(x_1,\ldots,x_n) = \prod_{i,j \in M_{ij}} \varphi_{ij}^{(x_i-3)(x_j-3)} \prod_{k \in K} \Phi_k^{x_k-3}$$

and $0 < \Phi_k \leq 1$ for every $k \in K$.

By applying a log transform to (9.8), a linear relationship is established between $p_{ij,(x_1,\ldots,x_n)}$ and parameters φ_ι and $p_{ij,(3,\ldots,3)}$. In a similar fashion as previously, the importance measures $C_{\pi,\iota}$ for the two scenarios $\underline{x}^-$ and $\underline{x}^+$ are given in Figure 9.3. The values measure the contribution of the assessed uncertainty on the decrease induced to the root cause rate by modifying a particular defence.

	Environmental Coupling Factor				**Hardware Coupling Factor**			
Scenario	x-		x+		x-		x+	
	Analysis	Separation	Analysis	Separation	Analysis	Diversity	Analysis	Diversity
Design	0.04	0.96	0.50	0.50	0.08	0.92	0.11	0.89
Human	0.88	0.12	0.93	0.07				
Internal	0.07	0.93	0.51	0.49	0.08	0.92	0.11	0.89
Maintenance	0.06	0.94	0.06	0.94	0.49	0.51	0.52	0.48
Procedures					0.11	0.89	0.22	0.78
External	0.00	1.00	0.22	0.78	0.39	0.61	0.88	0.12
Average	**0.21**	**0.79**	**0.44**	**0.56**	**0.23**	**0.77**	**0.37**	**0.63**

Figure 9.3: Importance measures $C_{\pi,\iota}$ for coupling factor variables

Note that for the base level rates $\ln p_{ij,(3,\ldots,3)}$ for ($i = 1,\ldots,6$ and $j = 1,2,3$), the coefficients of parameters $\ln \varphi_\iota$ are zero for all ι; this is expected as $\ln p_{ij,(3,\ldots,3)}$ is a parent node of $\ln p_{ij,(x_1,\ldots,x_n)}$.

From the values in Figure 9.3 it may be seen that for scenario $\underline{x}^-$, the uncertainty on the Environmental coupling intensities is almost entirely attributed to the impact of Separation: for all root causes apart from Human, the impact of Separation is responsible for over the 90% of the uncertainty on the coupling factor intensity. The contribution of the impact of Separation is less important for scenario $\underline{x}^+$, but still remains dominant.

A similar pattern may be identified for the Hardware coupling intensities. Here, the main contributor to the uncertainty of the coupling probabilities is the impact of Diversity, for all root causes apart form Maintenance, where the contribution is almost equally distributed between the impact of Analysis and Diversity. This holds for both scenarios and in relevance to all root causes, except from the External root cause; here, the main contributor at scenario $\underline{x}^+$ is the impact of Analysis.

9.4.4 Restrictions on parameter variations

The structure of the ID model poses a number of restrictions on the model parameters. To be more precise, the proportion variables ϕ_ι comprising sub-models (9.1) need to meet a set of conditions in order to be conceptually consistent. In particular, the impact of any defence D_k ($k = 1,...,8$), denoted with $I_k(x_1,...,x_n)$ needs to take values within the interval $[0,1]$. These restrictions pose stringent conditions on the proportion variables, forbidding unrestricted variations on their values. During the analysis of the results that were obtained from the probability encoding exercise, there were cases where these fundamental assumptions were violated (see Chapter 8). In order to avoid these violations, small minimisation problems were employed. Within this context, cross-terms ϕ_{ij} ($\{i,j\} \in M_\pi$) have been forced to have low variation. This fact is reflected in the Sensitivity Analysis, where cross-terms receive particularly low importance measures.

9.5 Comparison to UPM

9.5.1 Functional Interactions

Both the ID model and UPM are methods for assessing the vulnerability of the system under study towards dependent failures. However, the two methods use different performance indicators. On the one hand, the output of UPM is a beta factor (β), which is defined as the probability that a component in the system fails dependently, given that it fails. On the other hand, the output of the ID model is a rate λ_{CCF}, which represents the rate of failure-to-start CCF events that occur to the system.

According to the fundamental assumptions of the Beta Factor model[4], β is the fraction of the total component failure rate λ that is associated to CCFs, denoted with λ_d viz.

$$\lambda_d = \beta\lambda$$

A CCF event results in the dependent failure of all components comprising the system. Therefore, λ_d corresponds to the rate of system CCFs. If the rate λ represents failure-to-start component failures per unit of time, then λ_d coincides with the rate of system CCF failure-to-start events λ_{CCF}, which is the output of the ID model.

As described in Chapter 3, UPM uses a linear scheme to capture the impact of system defences on the β factor, and, thus, on the rate λ_d, viz.

$$\lambda_d = \sum_{k=1}^{8} s_k(x_k) \cdot \lambda$$

where s_k is the score related to defence D_k that receives level x_k, where $k = 1,...,8$ and $x_k \in \{1,...,5\}$. It may be seen that the change induced by modifying the level of defence D_l from x_l to x_l' is

$$(\sum_{k \neq l}^{8} s_k(x_k) + s_l(x_l)) \cdot \lambda - (\sum_{k \neq l}^{8} s_k(x_k) + s_l(x_l')) \cdot \lambda = (s_l(x_l) - s_l(x_l')) \cdot \lambda$$

This change is constant, implying that the impact of a particular defence on the system vulnerability is independent of the level of any other defence; in other words UPM does no recognise any interactions amongst the defences.

In contrast, the ID model attempts to distinguish between three types of defence interactions, namely functional dependency, functional independency and threshold functional dependency. In order to demonstrate the different approaches of ID and UPM, three cases are considered. Each case describes an identified interaction, and has been used in Chapter 3 to demonstrate the conceptual fallacies that the UPM linear model falls into.

For illustration purposes, a particular value for λ is considered to determine the

[4] See Chapter 2, Section 2.3.2

failure rate λ_d based on β. The value of λ is of no particular importance, since the interest lies in the pattern of change induced in this rate, rather than the absolute values.

Case I: Interaction between Analysis and Diversity

The defence of Analysis describes the amount of analysis that has been done on the design of the system, and the degree of awareness of the designers of the dependent failures issue. For a high level of Analysis, one can presume that diversity issues have been considered during previous assessments and appropriate feedback has been given to designers. Thus, the present design is recognised as the one that functions better in case of a CCF event. Therefore, improving or degenerating the level of diversity when comprehensive analysis has been performed (Analysis has a high level) should have a smaller effect compared to the case when a limited amount of analysis has been performed on the design of the system (Analysis receives a low level).

Figure 9.4 illustrates the change in λ_d induced by modifying the level of Diversity, whilst the rest of the defences are fixed at the medium level, as captured by UPM. It may be seen that, regardless of whether the level of Analysis is fixed at a high or at a low level, the change in λ_d is constant. Within the ID model, the defence of Diversity is threshold functionally dependent on the defence of Analysis. Figure 9.5 illustrates the change induced in λ_{CCF} for the same scenario, as captured by the ID model. Now, it may be seen that when Analysis is fixed at a high level, the change induced in λ_{CCF} takes smaller values, implying that the effect of enhancing Diversity is less significant.

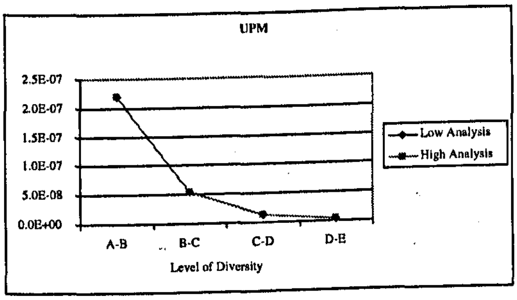


Figure 9.4: Change in λ_d as captured by UPM

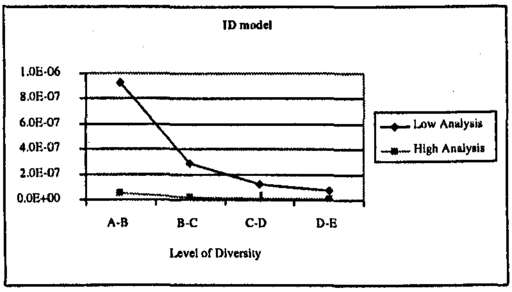


Figure 9.5: Change in $E[\lambda_{CCF}]$ as captured by the ID model

Case II: Interaction between Analysis and Understanding

Consider the defences of Analysis and Understanding. Conceptually, the positive effect of improving the amount of analysis conducted during the design phase of the system (level of Analysis) is not as substantial when the system is fairly simple (high level of Understanding), as when the system is complex or novel (low level of Understanding). Thus, one can argue that the effectiveness of Analysis depends on the level of Understanding. In reverse, aiming for a high level of Understanding (trade-offs between experience, complexity and novelty of the system) is more important when the amount of analysis on the design of the system conducted is limited (low level of Analysis), rather than when significant analysis is undertaken an extensive knowledge on dependent failures issues exists (high level of Analysis). Similarly, one can argue that the effectiveness of Understanding depends on the level of Analysis.

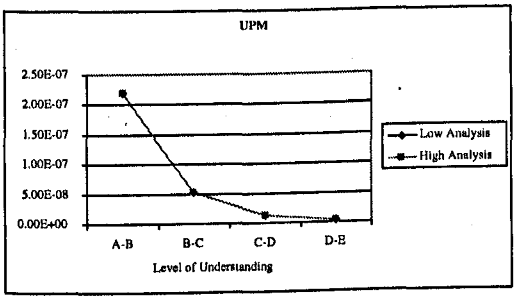


Figure 9.6: Change in λ_d as captured by UPM

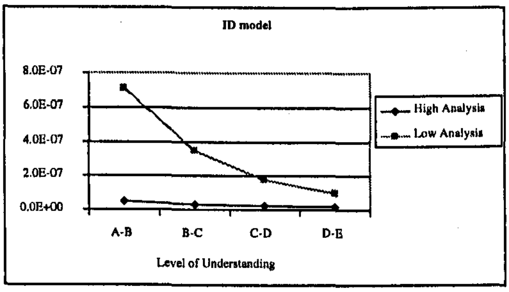


Figure 9.7: Change in $E[\lambda_{CCF}]$ as captured by the ID model

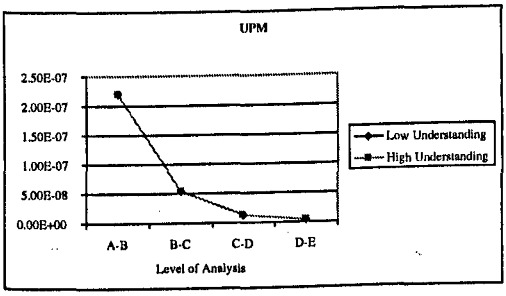


Figure 9.8: Change in λ_d as captured by UPM

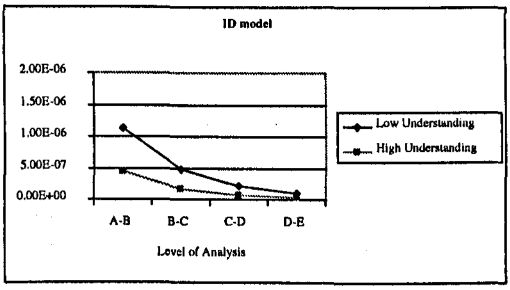


Figure 9.9: Change in $E[\lambda_{CCF}]$ as captured by the ID model

Figures 9.6 and 9.8 illustrate the change induced in the failure rate by changing one of the two defences, while the other is fixed at a high and at a low level respectively, as modelled by UPM. It may be seen that the impact of the one defence is the same regardless of the level of the other defence. Within the ID model, the defences of Analysis and Understanding are identified as being functionally dependent. The effect of modelling this functional interaction is illustrated in Figures 9.7 and 9.9. It may be seen that, unlike within UPM, the impact of Analysis is different for a high and low level of Understanding, and vice-versa. To be more precise, a compensating effect is exhibited, where the change induced by modifying one defence is smaller for higher levels of the other defence.

Case III: Interaction between Op. Interaction and Understanding

Similar conclusions can be drawn for the defences of Op. Interaction and Understanding. Consider a system for which no written procedures are in place (low level of Op. Interaction), leaving high margin for interpretation and decision by the staff. It is of interest to distinguish between two different cases: the case of not having written procedures as a reasonable decision, as the system is familiar or simple enough and detailed procedures are redundant; and the case where no written procedures in place is an omission that has negative effects. Similarly, the effectiveness of having detailed procedures in place (high level of Op. Interaction) should be limited for a system that is simple or familiar, compared to the case of a complicated or noble system. This implies that the impact of Op. Interaction depends on the level of Understanding, which describes the level of understanding of designers, operators and analysts in relation to the system.

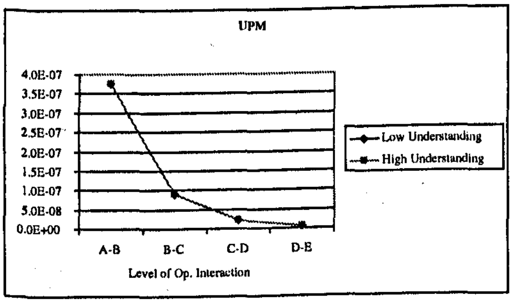


Figure 9.10: Change in λ_d as captured by UPM

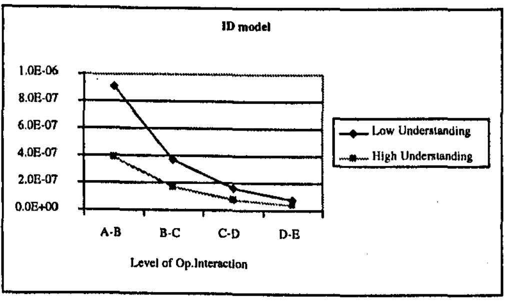


Figure 9.11: Change in $E[\lambda_{CCF}]$ as captured by the ID model

Figure 9.11 shows that UPM does not capture the dependence of Op. Interaction on Understanding - the effect of enhancing Op. Interaction is the same regardless of the level of Understanding. However, by identifying that Op. Interaction is threshold functionally dependent on Understanding, the ID model addresses this issue. The change in the CCF rate induced by enhancing the level of Op. Interaction takes smaller values for high levels of Understanding, entailing that this defence becomes less effective (Figure 9.11).

Discussion

For both the ID model and UPM, the change induced in the rate by enhancing a particular defence decreases exponentially with the level at which the enhancement occurs. This implies that, as the system defences are enhanced, it becomes gradually more difficult to improve the defence of the system towards CCF events.

Moreover, it may be seen that, for Cases I and II, the change induced by modifying the defences of Analysis, Diversity and Understanding, as captured by UPM, is identical. The ID model not only considers a broader range for the defence impacts, but it also captures different intensities of defence interaction. For example, the change induced by modifying the level of Diversity differentiates significantly between high and low levels of Analysis (see Figure 9.5); whereas, the change induced by modifying the level of Op. Interaction differentiates far less between high and low levels of Understanding (see Figure 9.11).

Overall, the ID model is a more flexible approach in terms of capturing the impact of the defence characteristics of the system on the CCF rate.

9.5.2 Ranking of defences

It is of interest to explore the relative effect that the action of enhancing each defence has on the overall system vulnerability to CCFs, as represented within the two models.

For this purpose, consider the following hypothetical scenario: a system receives the lowest level configuration $\underline{x}^{-}$, implying that it has generally very poor defence characteristics against dependent failures. Then, a particular defence at a time is enhanced to the maximum level, whilst keeping the rest of the defence levels fixed. For the ID model, the performance indicator for the impact of each defence is considered to be the ratio of decrease of the expected value of λ_{CCF}, induced by the defence enhancement. Within the UPM framework, the performance indicator is the ratio of decrease induced to β, which corresponds to the proportion of decrease induce to λ_d. The results are shown in Table 9.2.

System Defence	ID model	UPM
	Decrease in CCF rate	Decrease in beta factor
Diversity	0.69	0.88
Separation	0.77	0.84
Understanding	0.22	0.88
Analysis	0.43	0.88
Op. Interaction	0.54	0.80
Saf. Culture	0.57	0.90
Env. Control	0.75	0.88
Env. Testing	0.54	0.92

Table 9.2: Performance indicators for each defence within the UPM and ID framework

Firstly, it may be seen that the ID model represents a stronger effect of enhancing the system defences on the system vulnerability towards CCF events, compared to UPM. Whereas the resulting ratios within the ID framework range between 0.26 and 0.91, within UPM the respective ratios range within a much narrower interval, taking values between 0.84 and 0.92.

In terms of relative strength, within the ID framework the most potent defence is Understanding: increasing the particular defence from the lowest to the highest configuration, whilst keeping the rest defences at a minimum defence level, results in the expected value of the CCF rate to reduce to nearly the 20% of its initial value. Within UPM, Understanding has a comparatively medium impact on the beta factor, equivalent to the ones of Diversity, Analysis and Env. Control. The least potent defences within the ID framework seem to be Separation and Env. Control. Within UPM on the other hand, Separation is the first defence in the impact ranking. Finally, the defence of Env. Testing is the least potent defence within the UPM framework, whereas within the ID model is a relatively strong defence, inducing the expected value of the overall CCF rate to decrease to the 54% of its initial value.

9.6 Behaviour of the ID model

9.6.1 Impact of system defences

The ID model captures the impact of the defence characteristics on the overall vulnerability of the system to CCFs by using root cause rates and coupling factor intensities as intermediate variables in the modelling process. This feature allows to explore the impact of the defences initially on the intermediate variables, and afterwards on the rates of CCF events.

Certain of the system defences protect against CCFs by impeding the occurrence of both dependent and independent failures. Others, by alleviating the coupling tendency of the failures that occur to the system. Finally, there are defence characteristics that are targeted against both the occurrence of total failures, and their capacity to propagate amongst components.

In order to investigate the impact of a particular defence on a root cause and coupling factor variable (denoted generally with V), the following hypothetical scenario is used: consider a system that employs generally poor defences against failures, i.e. receives the minimum configuration vector $\underline{x}^-$, where

$$\underline{x}^- = (x_1, \ldots, x_8), \quad \text{where } x_k = 1 \text{ for every } k = 1, \ldots, 8$$

Enhancing a particular defence D_l to the maximum level, whilst keeping the rest at a minimum level of defence, viz.

$$\underline{x}^l = (x_1, \ldots, x_l, \ldots x_8), \quad \text{where } x_l = 5, x_k = 1 \text{ for every } k \neq l \text{ and } k, l \in \{1, \ldots, 8\}$$

impacts on the uncertainty of a given variable V. The interest lies in exploring the impact on the model variables caused by the particular enhancement. An indicator of this impact is the ratio of decrease in the expected value of variable V

$$I_l = \frac{E[V_{\underline{x}^l}]}{E[V_{\underline{x}^-}]}$$

The smaller this ratio is, the stronger is the impact on V by enhancing D_l. When for a given defence the ratio is 1, then this defence does not influence the particular variable.

Root cause rates

Ratios I_l

Defence D_l	Diversity	Separation	Understanding	Analysis
Root Cause				
Design	0.239	0.408	1	0.311
Human	1	1	0.140	1
Internal	1	1	0.029	0.114
Maintenance	1	1	1	1
Procedures	1	1	0.082	0.044
External	1	1	1	0.062

Defence D_l	Op. Interaction	Saf. Culture	Env. Control	Env. Testing
Root Cause				
Design	1	1	1	0.097
Human	0.192	0.005	0.406	1
Internal	1	1	1	0.057
Maintenance	1	0.002	1	1
Procedures	0.237	1	1	1
External	1	1	0.410	1

Table 9.3: Ratio of change for the root cause rates, induced by enhancing one defence at a time, from the lowest to the highest level

Table 9.3 shows the ratios I_l ($l = 1,...,8$) for the root cause rates r_i ($i = 1,...,6$).

It may be seen that the more dominant influence on the **Design** root cause rate comes from the Env. Testing characteristics of the system. The rest three design-related defences of Analysis, Separation and Diversity have approximately equivalent impact, with Separation subtly being the less effective defence against this type of failures.

The Safety Culture defence seems to be able to considerably modulate the **Human** root cause rate. The defences of Op. Interaction and Understanding also have a strong impact, whereas enhancing Env. Control seems to be comparatively less efficient in impeding this type of failures.

The defence that is most capable to modulate failures due to the **Internal to Component** root cause appears to be Understanding. Env. Testing and Analysis are also potent defences against this type of failures.

The failure rate due to **Maintenance** causes is influenced exclusively by the Safety Culture characteristics of the system. However, enhancing the particular defence has drastic impact on the rate, as the corresponding ratio is particularly low.

The **Procedures** root cause rate is mostly influenced by the defence of Analysis. Understanding is an important defence against this type of failures, and Op. Interaction has a smaller, but still substantial impact on the Procedures root cause rate.

Finally, the **External Environment** root cause rate is modulated by the defences of Analysis and Environmental Control. Analysis has the most impact, while the defence of Environmental Control has considerably less impact on the particular type of failures.

Coupling factor intensities

Table 9.4 shows the ratios I_l $(l = 1,...,8)$ for coupling probabilities p_{ij} $(j = 1,2,3$ and $i = 1,...,6)$. For the coupling mechanisms that do not have effect at the occurrence of particular root cause events, there is no ratio.

The **Operational** coupling probabilities p_{i2}, $i = 1,...,5$, are influenced only by the defence of Operator Interaction. The impact of this defence is the same for all probabilities p_{i2}, regardless of the root cause event.

The defence of Analysis is targeted against both **Environmental** and **Hardware** coupling probabilities. Enhancing the level of Analysis seems to have the most impact on the coupling tendency of Design and Internal to Component CCF events, propagated through environmental and hardware similarities. The least impact appears to be on the coupling tendency of Maintenance CCF events, through both coupling mechanisms. The defence of Separation is targeted against environmental coupling characteristics, and is more effective in relation to Design, Internal to Component and External Envi-

Table 9.4: Ratio of change for the coupling probabilities, induced by enhancing one defence at a time, from the lowest to the highest level

Ratio I_l

Defence	Analysis			Separation		
Coupling Factor	Environ.	Hardware	Operational	Environ.	Hardware	Operational
Root Cause						
Design	0.17	0.22	1	0.06	1	1
Human	0.37	—	1	0.66	—	1
Internal	0.18	0.22	1	0.13	1	1
Maintenance	0.81	0.46	1	0.52	1	1
Procedures	—	0.48	1	—	1	1
External	0.22	0.32	—	0.13	1	—

Defence	Diversity			Op. Interaction		
Coupling Factor	Environ.	Hardware	Operational	Environ.	Hardware	Operational
Root Cause						
Design	1	0.01	1	1	1	0.13
Human	1	—	1	1	—	0.13
Internal	1	0.01	1	1	1	0.13
Maintenance	1	0.41	1	1	1	0.13
Procedures	—	0.24	1	—	1	0.13
External	1	0.41	—	1	1	—

ronment CCFs. Finally, the defence of Diversity is targeted against hardware coupling mechanisms, and has the most drastic effect on the coupling tendency of Design and Internal to Component CCFs.

Different types of CCF rates

By being targeted against certain root cause rates and coupling factors, defences are able to modulate particular types of CCF events. In a similar fashion as earlier, each defence is enhanced to the maximum level, whilst the rest defences remain fixed to the minimum level, and the resulting ratios of decrease in the CCF rates due to the a particular root cause are determined, viz.

$$I_l = \frac{E[\lambda_{i,\underline{x}^l}]}{E[\lambda_{i,\underline{x}^-}]}$$

The expected values of rates λ_i $(i = 1,...,6)$ at configuration vectors $\underline{x}^-$ and $\underline{x}^l$ $(l = 1,...,8)$ are given in Table 9.5, along with the ratios of decrease I_l.

It may be seen that CCF events due to **Design** causes are mostly impeded by the de-

Table 9.5: Decrease induced in CCF rate by enhancing one defence at a time, distributed across the root causes.

	Lowest Configuration	**Different Scenarios**			
Root Cause	Expected Value of CCF rate	Expected Value	Decrease	Expected Value	Decrease
		Diversity		**Separation**	
Design	3.47E-06	2.98E-07	0.09	9.95E-07	0.29
Human	2.15E-05	2.15E-05	1.00	2.12E-05	0.98
Internal	2.47E-05	1.18E-05	0.48	1.62E-05	0.66
Maintenance	2.86E-06	2.65E-06	0.93	2.78E-06	0.97
Procedures	1.74E-06	8.51E-07	0.49	1.74E-06	1.00
External	2.56E-06	2.20E-06	0.86	8.70E-07	0.34
Overall	5.69E-05	3.93E-05	0.69	4.38E-05	0.77
		Understanding		**Analysis**	
Design	3.47E-06	3.47E-06	1.00	2.48E-07	0.07
Human	2.15E-05	3.01E-06	0.14	2.09E-05	0.97
Internal	2.47E-05	7.24E-07	0.03	7.46E-07	0.03
Maintenance	2.86E-06	2.86E-06	1.00	2.64E-06	0.92
Procedures	1.74E-06	1.42E-07	0.08	5.01E-08	0.03
External	2.56E-06	2.56E-06	1.00	3.90E-08	0.02
Overall	5.69E-05	1.28E-05	0.22	2.46E-05	0.43
		Op. Interaction		**Safety Culture**	
Design	3.47E-06	3.36E-06	0.97	3.47E-06	1.00
Human	2.15E-05	6.98E-07	0.03	2.15E-05	0.005
Internal	2.47E-05	2.30E-05	0.93	2.47E-05	1.00
Maintenance	2.86E-06	8.21E-07	0.29	2.86E-06	0.002
Procedures	1.74E-06	2.93E-07	0.17	1.74E-06	1.00
External	2.56E-06	2.56E-06	1.00	2.56E-06	1.00
Overall	5.69E-05	3.08E-05	0.54	5.69E-05	0.57
		Env. Control		**Env. Testing**	
Design	3.47E-06	3.47E-06	1.00	3.37E-07	0.10
Human	2.15E-05	8.75E-06	0.41	2.15E-05	1.00
Internal	2.47E-05	2.47E-05	1.00	1.40E-06	0.06
Maintenance	2.86E-06	2.86E-06	1.00	2.86E-06	1.00
Procedures	1.74E-06	1.74E-06	1.00	1.74E-06	1.00
External	2.56E-06	1.05E-06	0.41	2.56E-06	1.00
Overall	5.69E-05	4.26E-05	0.75	3.04E-05	0.54

fence of Analysis, which is targeted against Design, Procedures, Internal and External failures and their capability to propagate amongst components. Diversity and Separation also protect the system from two fronts: the occurrence of Design total events, and the coupling capability of this type of failures. Finally, Env. Testing is a strong defence against Design failures by having a substantial impact on the occurrence of Design and Internal total failures.

CCFs due to **Human** factors are mostly modulated by the Safety Culture and Operator Interaction. Understanding constitutes a strong defence against this type of CCFs, followed by Environmental Control. These defences are targeted against the occurrence of failure events, rather than the alleviation of coupling mechanisms.

Internal to Component CCF events appear to be substantially impeded by the defences of Understanding, Analysis and Env. Testing. Diversity and Separation are also targeted against this type of failures.

The most efficient defences against CCF events due to **Maintenance** causes are Safety Culture and Operator Interaction. Whereas the former impacts on the rate of total events due to this cause, the latter is effective by removing the conditions responsible for failure propagation.

Procedures CCF events are modulated by the defences of Understanding, Op. Interaction and Analysis. The two first are targeted against the occurrence of both dependent and independent failures, while Analysis is also able to modulate the propagation tendency of this type of failures amongst all components.

Finally, **External Environment** CCF events are impeded by enhancing Analysis, Separation and Env. Control. The most efficient defence is Analysis, which has a strong impact not only on the occurrence of total failures, but also on their propagation through environmental and hardware coupling mechanisms.

9.6.2 Limiting scenarios

The expected rates of CCF events due to the different root causes are presented in relation to two extreme scenarios: the 'low-level' scenario $\underline{x}^-$, which describes the setting where the system under study receives the minimum possible configuration across all defences, and the 'high-level' scenario $\underline{x}^+$, which describes the setting where the system receives the maximum possible configuration across all defences, viz.

$$\underline{x}^- = (x_1, ..., x_8), \quad \text{where } x_k = 1 \text{ for every } k = 1, ..., 8$$

and

$$\underline{x}^+ = (x_1, ..., x_8), \quad \text{where } x_k = 5 \text{ for every } k = 1, ..., 8$$

'Low-level' CCF rate This scenario implies that the system is particularly poorly equipped against the occurrence of dependent failure events. The expected values of the comprising root cause rates are given in Figure 9.12. For the lowest defence configuration, the overall CCF rate is dominated by failures due to the Internal to Component and Human root causes, with expected rates $2.5 \cdot 10^{-5}$ and $2 \cdot 10^{-5}$ per calendar hour respectively. Design failures are a considerable contributor to the overall CCF rate (expected rate $3.5 \cdot 10^{-6}$ per calendar hour), and Maintenance and External root causes are almost equivalent, with expected rates at approximately $2.5 \cdot 10^{-6}$ per calendar hour. Finally, CCFs due to Procedures are the least significant contributor, with expected value of the corresponding rate of approximately $1.7 \cdot 10^{-6}$ per calendar hour.

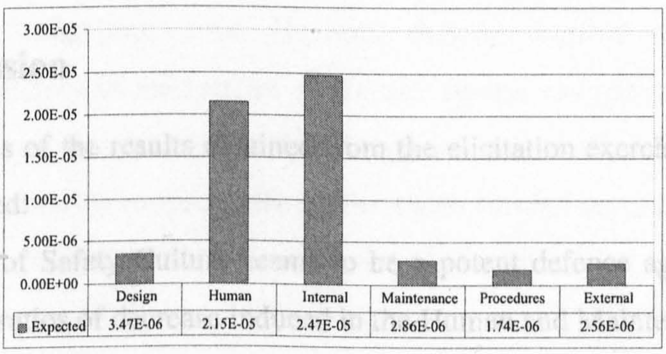


Figure 9.12: Expected values of the 'low-level' CCF rate (per calendar hour) across the different root causes

‘High-level’ CCF rate

This scenario implies that the system is mostly equipped against the occurrence of dependent failures. The distribution of the expected CCF rates across the different root causes is summarised in Figure 9.13. It may be seen that External events constitute the main contributor to the overall CCF rate (expected rate of $9 \cdot 10^{-9}$ per calendar hour), whereas Internal CCFs are still expected to occur at a relatively high rate ($4 \cdot 10^{-9}$ per calendar hour). Human root cause events are expected to decrease to a rate of approximately $2 \cdot 10^{-9}$ per calendar hour, whereas Maintenance causes constitute the least threatening source of CCFs (expected rate of $7.6 \cdot 10^{-10}$ per calendar hour).

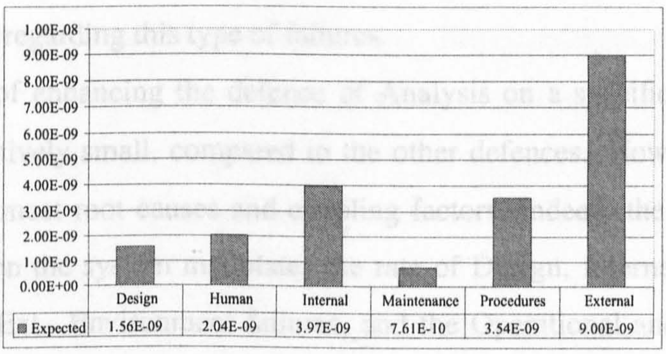


Figure 9.13: Expected value of the ‘high-level’ CCF rate (per calendar hour) across the different root causes

9.6.3 Discussion

From the analysis of the results obtained from the elicitation exercise, the following insights are gained:

The defence of Safety Culture seems to be a potent defence against root cause events, since the ratios of decrease induced in the Human and Maintenance root cause rates by enhancing Safety Culture are overall the lowest ones. This effect is demonstrated in the comparison of the two extreme scenarios $\underline{x}^{-}$ and $\underline{x}^{+}$. For a system that lacks defences, Human failures are expected to occur at a particularly high rate; however, when the defences are enhanced to the maximum, Human failures tend to constitute one of the weakest expected threats to the system. Similarly, the Maintenance root cause rate is the second failure rate to decrease by the highest proportion after the Human one.

For a system that overall lacks defence characteristics, Internal to Component failures constitute the most significant threat to the system vulnerability to CCF events. When all the defences are enhanced to the highest level, internal causes remain the second most significant source of CCF events.

Failures due to procedural faults occur at a particularly low rate to a system with the lowest levels across the system defences, compared to the rest types of failures, this type of failures occur at a comparatively significant rate to a system with the highest configuration across the system defences. This fact implies that the system defences are overall weak regarding this type of failures.

The impact of enhancing the defence of Analysis on a specific type of failures seems to be relatively small, compared to the other defences. However, Analysis is targeted against most root causes and coupling factors; indeed, the amount of analysis performed on the system modulates the rate of Design, Internal to Component, Procedures and Ext. Environment failures, and the Operational and Hardware coupling factors. Therefore, overall, Analysis proves to be a comparatively potent defence against dependent failures.

The defences of Separation and Diversity influence the occurrence of total failures due to only the Design root cause. However, they are targeted mostly against the coupling characteristics of the system: the former against environmental similarities, and the latter against hardware similarities. It may be seen that the defence of Diversity has a drastic impact on the coupling effect of hardware similarities of the system mostly in relation to Design and Internal to Component failure events.

9.7 Conclusion

This chapter described the validation process within the scope of this research. The behaviour of the ID model is explored across two facets: sensitivity analysis and comparison with UPM.

Sensitivity analysis aims to identify the dominant sources of uncertainty that contribute to the determination of the probabilistic specification of the model's root cause and coupling factor nodes. This type of analysis allows to gain insight in the properties of the model, and to draw the attention on areas that manifest the highest sensitivity. For the purposes of the analysis, two scenarios are considered: the minimum level configuration $\underline{x}^-$ and the maximum level configuration $\underline{x}^+$ across the system defences. An interesting point is that often significant differences are identified in the contribution of the impact of a particular defence to the overall uncertainty on a root cause or coupling factor (target) variable between the two scenarios. This difference is attributed to the effect of threshold functional dependency. In particular, suppose that defence D_q is threshold functionally dependent on defence D_t. The quantification of the ID model requires the determination of the uncertainty on the proportion of decrease of the target variable induced by modifying defence D_q with relevance to two settings: when D_t receives a high level, and when defence D_t receives a low level. Considerable difference in the importance factor $C_{\pi,q}$ between scenarios $\underline{x}^-$ and $\underline{x}^+$ implies that there is a substantial difference in the confidence with which the impact of D_q has been assessed within the two aforementioned settings.

The second part of the analysis explores the behaviour of the model in terms of the impact of the defence characteristics of the system on the overall system vulnerability. The approach compares the behaviour of the ID model with UPM. Whereas UPM does not make any distinction between the interactions existing amongst the defences in the way they impact on the overall system unavailability, with the impact of each defence being independent of the configuration across the rest of defences, the ID model succeeds to represent a range of functional interactions. This is shown by considering the three cases used for illustration purposes in Chapter 3.

Finally, the behaviour of the model has been explored. By incorporating a root cause and coupling factor classification, the model allows to explore which types of failure the system defences are more capable to modulate. This allows a more detailed modelling of CCF events.

Chapter 10

Discussion

10.1 Introduction

The aim of this final chapter is to discuss the application of the ID formalism within the context of CCF modelling.

The chapter will proceed as follows: Section 10.2 will discuss the goal, aims and objectives of this research and will identify the extent to which they have been fulfilled. Section 10.3 will discuss the features of the proposed methodology that bring theoretical and practical value. Section 10.4 will discuss the limitations identified during the implementation of the ID formalism within the particular application. In relation to these limitations, areas of future research are identified. This chapter will conclude with Section 10.5.

10.2 Review of goal and objectives of the research

10.2.1 Goal

The overall goal of this thesis has been to explore the feasibility of the application of advanced modelling techniques within the framework of UPM, so as to result in a model with a structural and exploratory character, that allows to represent epistemic uncertainty and support the decision - making process. Within this context, an Influence Diagram (ID) has been constructed to model CCF events on systems, and applied to EDGs in nuclear power plants.

The application of the proposed methodology seeks to maintain the strong features of UPM, and at the same time, to address those that are identified as weak. The aim is not to produce a definitive model for the modelling of CCFs within the industry; it is to explore the feasibility of the proposed methodology, by identifying the benefits and limitations of the application, and provide a documentation of this process.

10.2.2 Objectives

This section reviews the objectives of this research as described at the beginning of the thesis[1], and explores the extent to which they have been fulfilled.

A desideratum of the proposed model is the incorporation of qualitative aspects into the CCF modelling process (Objective 1). This constitutes the strong feature of UPM, which the ID model seeks to maintain. The output of UPM (beta factor) is determined by calibrating the system under study across design, operational and environmental characteristics. The ID model has been built on the same structure: the system defences have been taken exactly from UPM for all defences except for Redundancy[2], and represented in the model network by decision variables. The output of the ID model (uncertainty distribution on the system failure rate) is determined on the basis of states given to the defence variables by the user of the model. Moreover, by changing the states of the defence variables, the changes induced onto the other elements of the model are identified. On this basis, the effects of interventions in the defence aspects of the system are explored without making actual changes on the system, and what-if analysis may be in principle performed. Thereby, the ID model succeeds in capturing the effect of design, operational and environmental aspects of the system to its susceptibility to CCF events, and supports the decision-making process.

A second advantage of UPM is the fact that, having been initially quantified by

[1] See Table 1.1 in Chapter 1

[2] Redundancy characteristics have been removed from the definition, and the resulting defence describes only diversity aspects of the system. See Chapter 5.

experts, can be applied by less knowledgable analysts by simply scoring the system across the defences. Analysts making use of UPM do not use their expert judgment during the modelling process, apart from deciding on the system configuration, based on a set of standard criteria; the defence categories are generically defined, along with the scores corresponding to each category. In a similar fashion, the ID model uses expert judgment in a quantitative manner. The process of expert judgment elicitation is applied during the model construction. Being based on the Bayesian methodology, it is possible to update the expert judgment in the light of observations. The updating process involves relatively cumbersome calculations, requiring a standard knowledge of probability theory. The updated model may be used by analysts within the context of standard risk analyses, who are not required to have the same level of insight in dependent failures as the experts used for the quantification of the model, or the same knowledge of probability theory as the analysts that performed Bayesian update on the model. Thus, the ID model maintains this practical advantage of UPM (Objective 2).

UPM captures the effect that system defences have on its susceptibility to CCFs. The ID model expands this feature by incorporating intermediate stages between the system defences and the model output. These are rates of total failures attributed to particular root causes, and intensities of coupling mechanisms existing in the system. On this basis, the system defences are distinguished in terms of whether they reduce the occurrence of different types of failures, whether they alleviate certain coupling conditions, or whether they achieve both. Therefore, the ID model offers a more detailed modelling of CCF events, by identifying the types of failure events that each defence aspect of the system is able to modulate, and extends UPM to a finer causal level (Objective 3).

UPM uses a linear weighting system to capture the effect of system defences on its susceptibility to CCF events. This implies that the effect of enhancing a particular defence aspect is independent of the level of any other defence aspect of the system. However, interactions exist amongst defences, that render the effect of modifying the system more or less beneficial, depending on the level of certain existing system characteristics. For example the effect of improving the safety culture of the operating staff on the system vulnerability depends on the degree of the existing man-machine interaction[3]. Although not portrayed in the network of the ID model, within the mathematical formulation of the model different types of functional interaction amongst defences are represented[4], which are elicited from experts[5]. Thus, the ID model succeeds in capturing the non-linearity of the defence domain, something that UPM does not to address (Objective 4).

From a decision-making perspective, it is often of interest not only to determine the amount by which the vulnerability of the system is modified by performing certain actions, but also to provide indicators of the uncertainty involved in this prediction. This aspect is central in the area of CCF modelling which, due to the rare and complex nature of CCF events, is characterised by considerable uncertainty. By adopting a Bayesian approach to risk, the ID model allows for the quantitative use of expert judgment and the coherent expression of epistemic uncertainty (Objective 5). Moreover, information is propagated through the structure of the ID model, to support uncertainty statements regarding quantities on which information is not available[6].

Finally, the last objective is to associate the ID model with the ICDE generic database of CCF events. As described in Chapter 2, the International Common-Cause Failure Data Exchange (ICDE) Project is an international effort to collect CCF events from various sources, so as to create a generic CCF data bank. In order to achieve a consistent format of the data, general ICDE coding guidelines [Werner et al., 2004] are used by the participating operators. According to the guidelines, a root cause and coupling factor is assigned to each failure event, amongst other characteristics. The definition of the root cause and coupling factor variables in the ID model has been taken exactly from the ICDE guidelines. Therefore, the ID model associates the structure of the database with the model structure, nevertheless not in a way that will presently allow the use of the ICDE data for model update (Objective 6).

[3] See Chapter 3

[4] See Chapter 6 and 8

[5] See Chapter 7

[6] See Chapter 6

10.3 Benefits of the proposed methodology

The ID model proposed in this thesis bears features of both theoretical and practical value. This section discusses the two main novelties of the model, namely the definition of the defence interactions and the Geometric Scaling (GS) model.

10.3.1 Functional interactions

To capture the non-linear structure of the defence domain, the ID model distinguishes between three different types of functional interaction: functional independence, functional dependence and threshold functional dependence[7]. Functional independence represents the case where the impact of modulating particular characteristics of the system stays unaffected by any other characteristic; this situation corresponds to UPM. The modelling of functional dependence and threshold functional dependence to express the existing interactions amongst the related defences is a new feature.

The main difference between functional dependence and threshold functional dependence is the fact that the former is symmetric, whereas the latter is asymmetric. In functional dependence, the impact of enhancing one defence differentiates for every level of the other defence, and vice-versa. Threshold functional dependence implies that dependency is exhibited only between certain sets of level configuration, and not within: the impact of a defence that is threshold dependent on a second defence always depends on whether the level of the second defence is at a low, medium or high level. However, the impact of the second defence exhibits a dependency on the level of the first defence only when it changes between low, medium, or high levels (drastic modifications). For modifications within these sets (moderate modifications), no dependency is exhibited. For example, the effect of increasing separation depends on the amount of analysis performed on the system design; however, the effect of increasing analysis depends on the degree of separation employed by the system only for drastic changes; this effect is the same if the level of analysis remains within the same configuration set after the modification.

[7] See Chapter 6

Succeeding to express the functional interactions amongst defences has been a desired property of the GS model. In order to fulfill this property, an additional assumption has been placed on the form of the piecewise function expressing the impact of a threshold dependent defence[8]. In particular,

$$\phi_k(x_{k_1},....,x_{k_r}) = \prod_{l=1}^{r} \phi_k(x_{k_l}), \quad \text{where } k \in Q, k_l \in L_k \text{ for } l = 1,...,r \tag{10.1}$$

During the probability encoding exercise, additional questions have been used as a means of checking the validity of this assumption[9]. It is interesting to remark that this assumption has been intuitively met by the expert in many cases. This fact implies that (10.1) is a reasonable assumption to make.

Within the ID framework, the state space of the defence variables is comprised of five levels. Levels A and B constitute low levels, level C constitutes the medium level, and levels D and E constitute the high levels. This categorisation is relatively fine, with the defined sets consisting of two, or even of one level. Due to this feature, the effect of threshold dependence is not exhibited clearly and the two types of functional interaction tend to be close, however not equivalent.

10.3.2 The Geometric Scaling model

The quantification of the ID model requires the determination of prior distributions on the model root cause and coupling factor variables, for each configuration of the influencing defences. Given that each defence may receive one out of five levels, and that a particular variable may be influenced by one up to eight defences, the number of distributions that need to be determined becomes significantly increased. This results into an unmanageable amount of information to be elicited from experts by means of probability encoding. Problems arise because firstly, the availability of experts is within particular limits, and, secondly, subjecting an expert to a long and particularly demanding elicitation exercise may affect the results of the process.

[8] See Chapter 6, Section 6.3

[9] See Chapter 8, Section 8.5

Therefore, it has been imperative to adopt a pragmatic approach, which will allow for reducing the requirements posed on the participating experts, and for gathering the information necessary without setting unrealistic demands on them, both in terms of time availability and their actual ability to respond. This has been achieved by associating the root cause and coupling factor variables with the levels of the influencing defences, through a mathematical relationship. This relationship is referred to as the Geometric Scaling (GS) model.

The GS model is an operationally useful methodology that reduces the computational burden of the quantification process in the following way: instead of eliciting a probability distribution on a target variable for each combination of configuration levels of the influencing defences, one needs to determine a probability distribution on the target variable at a base configuration, and assess the effect of modifying the levels of the influencing defences. This relationship supports uncertainty statements about the variable of interest at levels where no information has been elicited from experts. The GS model decreased the number of elicitation variables to a manageable size, allowing for the instantiation of the ID model to be completed by means of an elicitation questionnaire[10].

The definition of the GS model has an additional advantage. Defining a functional relationship between the variable of interest and the defence levels of the system creates a framework that allows for the communication of information amongst different defence levels. Through the GS model, statistical data is propagated amongst different levels. Thereby, observations regarding a particular defence configuration become relevant to configurations on which there is no available information[11].

Moreover, the GS model creates a structured framework for uncertainty analysis. The uncertainty distribution on a variable is expressed as a weighted average of conditional distributions, viz.

$$f(v) = \int f(v \mid \underline{\phi}) f(\underline{\phi}) \mathrm{d}\underline{\phi}$$

Through Bayes' theorem, the weighted average $f(v)$ is updated in the light of data d,

[10] See Chapter 8

[11] See Chapter 6

to yield a posterior distribution, viz.

$$f(v \mid d) = \int f(v \mid \underline{\phi}, d) f(\underline{\phi} \mid d) \mathrm{d}\underline{\phi}$$

The posterior distribution is again a weighted average of conditional distributions, with weights the updated weights of the prior distribution $f(\underline{\phi} \mid d)$. The theoretical set-up of the GS model is based on gamma-Poisson and beta-binomial models. This allows for the analytical determination of the conditional distributions $f(v \mid \underline{\phi}, d)$. However, the normalising constants implicit in the posterior weights $f(\underline{\phi} \mid d)$ are not analytically tractable. Within the GS set-up, the inference problem is divided to simple, analytically solvable subproblems, and subproblems that require numerical approximation techniques.

10.4 Limitations of the proposed methodology and further research

This chapter proceeds with the limitations of the proposed methodology. These are issues that arose during the implementation of the protocol, creating room for further research.

10.4.1 Model boundaries

The ID model constitutes an application on Emergency Diesel Generators (EDGs) of nuclear power plants. The application characteristics of the model are summarised in Table 10.1.

The ID model is comprised of two parts: the model network and the probabilistic specification of the model. The application boundaries of the ID model are defined by exploring which components are generalised, and to what extent.

Table 10.1: Application characteristics of the ID model

Application characteristics
1. The model is a system-oriented approach. It is built for carrying out assessments of the vulnerability of systems of Emergency Diesel Generators to dependent failures.
2. Emergency Diesel Generators are stand-by systems.
3. The output of the model is a failure rate of CCF events per calendar hour.
4. The ID model captures failure events that occur during the idle period of the system, and are revealed by the demand (failure-to-start mode).

Model Network

The theoretical definition of the ID variables has been based on two recognised frameworks[12]. In particular, the system defences and respective levels have been defined as within UPM, and the coupling factor and root cause features of the ID model are defined exactly as in the ICDE Project. UPM is a generic methodology for dependent failure assessment on standard systems. Similarly, the ICDE taxonomies are defined for application in any event report included in the database, regardless of the contributing system. Therefore, the definition of the ID variables is not system-specific. Moreover, the relationships portrayed by the model network are conceptually coherent interactions existing amongst the model elements. On this basis, the ID model network is not focused on EDGs specifically, but is generalisable to standard systems.

Probability specification

The mathematical definition of the ID variables[13] seeks to capture failure events that occur to systems of EDGs during standby, and only revealed when the systems were

[12] See Chapter 5, Section 5.2

[13] See Chapter 5, Section 5.3

challenged to deliver their intended function. These failures are classified as failure-to-start events. On this basis, the output of the model is a system failure-to-start rate. For the model instantiation, the amount and type of the information to be elicited on experts has been based on the GS model, and the probability encoding has been achieved through the means of a questionnaire[14]. In view of the fact that the GS model is not accommodating a specific system, the elicitation methodology and questionnaire are applicable to any standard system. Thus, even though the numerical results obtained from the expert judgment elicitation process are EDG specific, the process itself is generalisable to failure-to-start events occurring in any standard system.

A similar approach may be used for capturing failure-to-run events. Failure-to-run events are typically described by probabilities on demand. For accommodating this type of events, the theoretical foundations of the model need to be modified accordingly.

A parameterisation of the ID model is possible in terms of probabilities on demand. In this case, the output of the model would describe the probability of the system failing on demand due to a CCF, viz.

$$p_{CCF} = Pr(\text{system fails on demand due to a CCF})$$

Given that the root cause taxonomy describes mutually exclusive and collectively exhaustive events, it holds that

$$\begin{aligned} p_{CCF} &= \\ &= \sum_{i=1}^{6} Pr(\text{CCF} \mid \text{ system fails due to root cause } i) Pr(\text{ system fails due to root cause } i) \\ &= \sum_{i=1}^{6} Pr(\text{CCF} \mid \text{ system fails due to root cause } i) \cdot q_i \end{aligned}$$

Based on the assumption that a CCF event is propagated to more than one components

[14] See Chapter 8, Section 8.5

via one out of the three defined coupling mechanisms, it holds that

$$Pr(\text{CCF} \mid \text{system fails due to root cause } i)$$
$$= \sum_{j=1}^{3} Pr(\text{CCF via coupling factor } j \mid \text{system fails due to root cause } i) = \sum_{j=1}^{3} p_{ij}$$

Finally, the failure probability on demand due to a CCF is expressed as

$$p_{CCF} = \sum_{i=1}^{6} \sum_{j=1}^{3} p_{ij} \cdot q_i$$

Table 10.2 portrays the ID variables for each parameterisation. For the parameterisation of the system in terms of probabilities on demand, the variables that need to be adjusted are the model output and the root cause variables.

Table 10.2: Parameterisation of ID model in terms of probabilities of failure on demand and failure rates

	Parameterisation	
Model elements	Probability on demand	Failure rate (per calendar hour)
Output	p_{CCF} = Pr(CCF on demand)	λ_{CCF} := rate of CCFs
Root causes i = 1,...,6	q_i = Pr(failure due to root casue i)	r_i := rate of failure events due to root cause i
Coupling factors j=1,2,3	p_{ij} = Pr(CCF via coupling factor j | failure due to root cause i)	p_{ij} = Pr(CCF via coupling factor j | failure due to root cause i)

For the parameterisation of the ID model in terms of probabilities on demand, the probability distributions need to be re-determined. The expert elicitation process may be adjusted to accommodate the new parameterisation of the model. However, the main structure of the strategy and the elicitation techniques remain the same.

10.4.2 Expert judgment elicitation

The ID building process is separated into a qualitative and a quantitative part. In this application, both parts were completed by using expert judgment.

The objective of the qualitative stage is to construct the network of the model, and has been completed during a workshop with six participating experts[15].

The objective of the quantitative part of the ID building process is to determine the probability specification on the model variables. Due to limited amount of available CCF data, this part was completed through a probability encoding exercise. The exercise was designed to extract uncertainty distributions from the participating expert.

To increase confidence in the results of the quantitative part, the exercise is in principle repeated to a number of participating experts, generating a set of uncertainty distributions for each elicitation variable. Subsequently, the elicited distributions are mathematically combined by using aggregation techniques [Genest and Zidek, 1986; Thorpe and Williams, 1992; Clemen and Winkler, 1999; Hora, 2004], to yield an overall prior on the elicitation variable. However, the aim of this research is not to produce a definitive tool for CCF modelling, readily used within the industry. Rather, it is to explore the feasibility of the proposed methodology. Insights can be gained from applying the process once, and practical issues can be identified without repeating the methodology to a number of experts. On these grounds, in the particular application the quantitative part has been completed with the help of a single expert.

10.4.3 Restrictions on elicitation variables

The probability encoding exercise was achieved by means of a questionnaire, which was completed by the participating expert. During subsequent analysis, the uncertainty on the elicitation variables was determined, and the GS model was used to extrapolate this uncertainty to variables for which assessments were not directly made (target variables).

The GS model results in a relatively complex mathematical structure. Based on

[15] See Chapter 7

the fundamental assumption that the vulnerability of the system to failures does not become worse as a result of enhancing the level of a defence, particular restrictions on the uncertainty distributions are posed. These restrictions apply both to the variables the uncertainty on which has been assessed directly (elicitation variables), and to the variables the uncertainty on which has been derived indirectly (target variables). On this basis, it needs to be ensured that the subjective distributions do not lead to conceptual inconsistencies, by violating these assumptions.

Avoiding violation of the fundamental assumptions proves to be a comparatively straightforward task when it comes to elicitation variables. During the structuring phase, the participating expert is informed on the conditions that conceptually need to hold, and encouraged to keep these into consideration when making assessments. Within the particular application, contradictions in the experts' assessments on elicitation variables have been rare.

However, a number of incoherences arose related to the uncertainty distributions of target variables that are assessed indirectly. The reason is that, during the probability encoding exercise, experts are not aware of the extrapolation techniques and the computational processes involved in the determination of the uncertainty on the target variables, nor they are expected to. Therefore, no tangible indication is available to them to check the coherency of the assessments when extrapolated to other variables, and adjust them respectively. This problem is addressed by two means. Firstly, the 'problematic' assessments were reviewed during the arranged feedback sessions. By using visual aids like plots and spreadsheets the reasons of violation of the conditions were explored. It has been crucial at this point to ensure that the analyst does not lead the expert, and that the expert's assessments, even when adjusted, do not cease to reflect their true beliefs. Secondly, minimisation problems were used to 'tune' the parameters of the subjective distributions of target variables (mostly cross-terms), so that violations of conditions are avoided[16].

[16] See Chapter 6

10.4.4 Use of data for update

ID data requirements

As described in Chapter 5, the data required for updating the priors on the root cause variables r_i and coupling factor variables p_{ij} ($i = 1,...,6$ and $j = 1,2,3$) at configuration vector $(x_1,...,x_8)$ is of the following form (see Table 10.3):

Table 10.3: Format of data required for updating the root cause and coupling factor variables of the ID model

For system with defence configuration $\underline{x}=(x_1,...,x_8)$					
Observation time: T_{obs} years		**Coupling Factors**			
		CF$_1$	**CF$_2$**	**CF$_3$**	Independent failures
Root Causes	**R$_1$**	n_{11}	n_{12}	n_{13}	n_{10}
	R$_2$	n_{21}	...		
	R$_3$	⋮			
	R$_4$				
	R$_5$				
	R$_6$	n_{61}	n_{62}	n_{63}	n_{60}

- For root cause variables r_i, the relevant data is (n_i, T_{obs}) where $n_i = \sum_{j=0}^{3} n_{ij}$ is the number of failures attributed to root cause i that are recorded during time T_{obs}, from a system with configuration vector $(x_1,...,x_8)$.
- For coupling factor variables p_{ij}, the relevant data is (n_{ij}, n_i) where n_{ij} is the number of CCFs propagated through coupling factor j, out of n_i failures attributed to root cause i, from a system with configuration vector $(x_1,...,x_8)$.

As mentioned, the ID model integrates the structure of the ICDE database. Each observed CCF event in the database is reviewed and, a number of features are assigned accordingly, consistently with the ICDE guidelines. These features include a root cause and a coupling factor. The observed CCF events from all contributing systems are accumulated, and classified according to system size. Relevant data from the ICDE database is illustrated in Table 10.4.

Table 10.4: Format of relevant to the ID variables data incorporated in the ICDE database

Contributing system of size m				
Observation time: T_{obs} years		**Coupling Factors**		
		CF_1	**CF_2**	**CF_3**
Root Causes	**R_1**	n_{11}	n_{12}	n_{13}
	R_2	n_{21}	...	⋮
	R_3	⋮		
	R_4			
	R_5			
	R_6	n_{61}	...	n_{63}

The root cause and coupling factor ID variables are defined as within the ICDE guidelines, and in principle the ICDE data can be used for model update. Nevertheless, there are two main drawbacks that make the use of ICDE data within the framework of the ID model presently unfeasible. Firstly, the ICDE event reports do not include information on the configuration of the contributing system across defences D_k, $k = 1, ..., 8,$ apart from the system size. Therefore, the data contained in the database comes from a combination of defence configurations, and it is not relevant to a specific variable $r_{i,\underline{x}}$ or $p_{ij,\underline{x}}$. Secondly, the ICDE database does not always include information on the number of independent failures that occurred to the system, classified across the root causes. Therefore, the total number of failures due to a particular root cause n_i cannot be determined.

Even though the ID model creates a context for using the information incorporated in such a generic database, this information cannot be used at its present form. However, it can be potentially used in the future, provided that a documentation scheme is developed for ICDE. This scheme should allow for the incorporation in the event reports of: firstly, the system configuration across defences D_k; secondly, the number of independent failures classified across the root causes. Given such a development, the use of the ICDE data in a quantitative way can be achieved, rather than as a means for gaining insight into the relevant failure mechanisms.

10.4.5 Definition of system defences

Like UPM, the ID model is based on the basic Beta Factor model. Within this framework, CCF events of different multiplicities are not recognised, as a CCF event fails all components, despite the size of the system. Therefore, according to the underlying assumptions, aspects of redundancy do not constitute a defence against dependent failures.

Using the Beta Factor model as a platform is inevitably a conservative approach to CCF modelling. Operating experience has proved the practical benefit of redundancy [Edwards and Watson, 1979]. Defining redundancy as a system defence is an attempt of UPM to 'correct' the output of the model accordingly, even though the fundamental assumptions of the model are violated.

For purposes of consistency, the ID model does not include redundancy amongst the system defences. Thus, the defence variables D_k ($k = 1, ..., 8$) defined within the context of the ID model, along with the corresponding five levels x_k ($x_k = 1, ..., 5$) have been accurately taken from the UPM framework for all defences, apart from the Redundancy and Diversity defence. For this particular defence, the aspects that describe redundancy characteristics of the system have been excluded, and only characteristics of diversity are described. Although a limitation, addressing this issue has not been an objective of the particular research. In principle, a similar methodology may be used to generalise models such as the Multiple Greek Letter model[17], which considers CCFs of different multiplicities. This research explores the feasibility of this methodology, and provides a documentation of the particular application, which may provide a platform for further research and future applications.

Another limitation concerns the original definition of the system defences. During interactions with the expert panel, the extent to which the UPM definitions of the system defences as a whole capture the system vulnerability has been criticised. Firstly,

[17] See Chapter 2

the panel felt that the sub-factor of Safety Culture is very narrowly defined within the UPM framework. The experts were uncomfortable with the fact that the definition focuses entirely on the training of the operators and that it does not include the aspect of safety culture in a more general fashion. Secondly, the panel argued that the design characteristics of Redundancy and Diversity should not be described be a single defence. They ultimately describe different design aspects of the system, thus, they should be describes by different defences.

These insights raise the question of whether the defence definitions should be developed further, and modified in order to represent the system under study in a more comprehensive manner. Re-defining the defence characteristics and their classification has not been an objective of this research. However, insights have been gained through the process that motivate further research.

10.5 Conclusion

This thesis is an application of the ID formalism on the CCF modelling of EDGs in nuclear power plants.

Within this research, UPM has played a particular role: it constituted the platform on which the ID model has been constructed. As stated in the objectives of this research, maintaining the strong features of UPM has been a desideratum. Apart from capturing the effect of system defences and using expert judgment in a quantitative way, UPM has another advantage: it constitutes a structured, well-documented methodology for CCF modelling.

The ID model partly maintains this feature in its current form. The checklists used within the UPM framework in order to guide and document the calibration of the system against the defences have been preserved within the ID framework, along with the defence definitions and corresponding levels. However, based on a Bayesian methodology, the ID model involves cumbersome numerical calculations compared to UPM, requiring standard knowledge of probability theory. On this basis, developing a standardised algorithm and a user-friendly interface by means of appropriate computer tools constitutes an interesting potential that would increase the practical value of the ID model.

The modelling approach presented in this thesis is an attempt to merge aspects of the qualitative treatment of CCF failures with quantitative analysis. In particular, root cause and coupling factor issues are expressed in the model quantitatively, as intermediate stages of the modelling process. The purpose behind this modelling choice is to allow for the use of qualitative insights regarding root cause and coupling factor characteristics of CCF events at a quantitative level. Combined with the modelling of defence characteristics of the system that have been acknowledged as relevant, the ID model offers a more detailed representation of CCF events and their mechanisms. This aspect of the proposed model emphasizes its use as a decision-making tool, with a strong structural and exploratory character.

Within a decision-making context, the interest lies not only in the model predictions, but also in the uncertainty related to these predictions. The ID model allows to coherently express the uncertainty related to the assessment of the risk contribution to the system. Gaining insight in this uncertainty allows control of certain outcomes in restricting them within a particular tolerance envelope. Moreover, based on the Bayesian methodology, the ID model allows to propagate uncertainty within the model structure, and support uncertainty statements regarding events for which information is not available.

The Geometric Scaling model defines a functional relationship that associates failure characteristics of the system with the defence characteristics that it employs. This relationship allows to extrapolate information and the related uncertainty to any defence configuration within the particular context, provided that the parameters of the model are determined. Moreover, the mathematical format of the GS model allows for the distinction of the functional interactions existing amongst the system defences, in the way they impact on the overall system susceptibility to failures. Finally, the use of the Geometric Scaling model offered a pragmatic approach to address the expert judgment elicitation process. Problems that demand a particularly large amount of information to be elicited from experts are frequently encountered in practice. The proposed methodology offers a way to tackle this problem.

This thesis explored the application of a methodology that approaches CCF modelling from a structural and exploratory viewpoint. The insights gained throughout this process suggest the feasibility of such a methodology and set the grounds for further research towards this direction.

Bibliography

Anders, D. M., Loxhøj, J. T., and Coit, D. W. (2005). Modelling of human-system risk and safety: aviation case studies and exemplars. *Human Factors and Aerospace Safety*, 5(2):137–167.

Ansell, J. I. and Phillips, M. J. (1994). *Practical Methods for Reliability Data Analysis*. Oxford University Press.

Apeland, S., Aven, T., and Nilsen, T. (2002). Quantifying uncertainty under a predictive, epistemic approach to risk analysis. *Reliability Engineering and System Safety*, 75:93–102.

Apostolakis, G. (1988). The interpretation of probability in probabilistic safety assessments. *Reliability Engineering and System Safety*, 23:247–252.

Apostolakis, G. and Moieni, P. (1987). The foundations of models of dependence on probabilistic safety assessment. *Reliability Engineering*, 18:177–195.

Atwood, C. (1996). The Binomial Failure Rate common cause model. *Technometrics*, 28(2):139–148.

Aven, T. (2003). *Foundations of Risk Analysis: a knowledge and decision-oriented perspective*. John Wiley and Sons Ltd.

Aven, T. and Kvaløy, J. T. (2002). Implementing the Bayesian paradigm in risk analysis. *Reliability Engineering and System Safety*, 78:195–201.

Barlow, R. and Proschan, F. (1986). Inference for the exponential life distribution. In Serra, A. and Barlow, R., editors, *Theory of Reliability*, pages 143–164. North-Holland, Amsterdam.

Bedford, T. and Cooke, R. (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press.

Berg, H. P., Görtz, R., Schimetschka, E., and Kesten, J. (2006). The process-oriented simulation model for common cause failures: recent progress. *Kerntechnik*, 71(1-2):54–59.

Bernardo, J. M. (1996). The concept of exchangeability and its applications. *Far East J. Mathematical Sciences*, 4:111–121.

Blackwell, L. M. and Singpurwalla, N. D. (1988). Inference from accelerated life tests using filtering in coloured noise. *Journal of the Royal Statistical Society. Series B, Methodology*, 50(2):281–292.

Bobbio, A., Portinale, L., Minichino, M., and Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and System Safety*, 71:249–260.

Bourne, A., Edwards, G., Hunns, D., Poulter, D., and Watson, I. (1981). Defences against common-mode failures in redundancy systems. Technical report, UKAEA Safety and Reliability Directorate.

Brand, P. V. and Gabbot, D. (1993). Unified Partial Method for dependent failures assessment. Technical Report AEA Technology, AEA Project Reference Number: GNSR/PSA/6, NSMRU Project Reference Number: PSA/GNSR/11., AEA Technology.

Celeux, G., Corset, F., Lannoy, A., and Ricard, B. (2006). Designing a Bayesian network for preventive maintenance from expert opinions in a rapid and reliable way. *Reliability Engineering and System Safety*, 91(7):849–856.

Chickering, D. M., Geiger, D., and Heckerman, D. (1995). Learning Bayesian networks: The combination of knowledge and statistical data. *Machine Learning*, 20:197–243.

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

Cooke, R. (1991). *Experts in Uncertainty: Opinion and Subjective Probability in Science*. Oxford University Press.

Cooke, R. and Bedford, T. (2002). Reliability databases in perspective. *IEEE Transactions on Reliability*, 51(3):294–310.

Cooke, R. M. and Goosens, L. J. H. (2000). Procedures guide for structured expert judgment. Technical Report EUR 18820, Nuclear Science and Technology, European Commision.

Coupé, V. M. H. and van der Gaag, L. C. (2002). Properties of sensitivity analysis of Bayesian Belief Networks. *Annals of Mathematics and Artificial Intelligence*, 36(4):323 – 356.

Cox, D. and Hindley, D. (1974). *Theoretical Statistics*. Chapman and Hall.

De Finetti, B. (1974). *Theory of Probability: A Critical Introductory Treatment*, volume 1. John Wiley, New York.

De Finetti, B. (1975). *Theory of Probability: A Critical Introductory Treatment*, volume 2. John Wiley, New York.

Diaconis, P. and Ylvisaker, D. (1985). Quantifying prior opinion. In Bernardo, M., Degroot, M. H., Lindley, D. V., and Smith, A. F. M., editors, *2nd Valencia Int'l Meeting*, pages 133–156, North-Holland, Amsterdam.

Dorp, J. R. V. and Mazzuchi, T. A. (2004). A general Bayes inference model for accelerated life testing. *Journal of Statistical Planning and Inference*, 119:55–74.

Duftoy, A., Pierplot, S., and Deleuze, G. (2006). An innovating application of Bayesian Networks. Presented in The First International Conference on Availabilty, Reliability and Security (ARES 2006), Vienna, Austria.

Ebeling, C. E. (1997). *An Introduction to Reliability and Maintainability Engineering*. The McGraw-Hill Companies, Inc.

Edwards, G. T. and Watson, I. A. (1979). A study of common-mode failures. Technical Report SRD R 146, Safety and Reliability Directorate, United Kingdom Atomic Energy Authority, Wigshaw Lane, Culcheth Warrington, WA3 4NE.

Fenton, N. and Neil, M. (2001). Making decisions: using Bayesian nets and MCDA. *Knowledge-Based Systems*, 14:307–325.

Fenton, N. and Neil, M. (2004). Combining evidence in risk analysis using bayesian networks. *Safety Critical Systems Club Newsletter*, 13(4):8–13.

Fischhoff, B. (1989). Eliciting knowledge for analytical representation. *IEEE Transactions on Systems, Man, and Cybernetics*, 19(3):448–459.

Fleming, A. M. K., Parry, G., Paula, H., Worledge, D., and Rasmuson, D. (1988). Procedures for treating common cause failures in safety and reliability studies. Technical Report NUREG/CR-4780, EPRI NP-5613, U.S. Nuclear Regulatory Commission and Electric Power Research Institute. Vol 1.

Fleming, A. M. K., Parry, G., Paula, H., Worledge, D., and Rasmuson, D. (1989). Procedures for treating common cause failures in safety and reliability studies. Technical Report NUREG/CR-4780, EPRI NP-5613, U.S. Nuclear Regulatory Commission and Electric Power Research Institute. Vol 2.

Fleming, K. N. (1975). A reliability model for common mode failure in redundant safety systems. In *Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation*, pages 23–25. General Atomic Report GA-A13284.

Fleming, K. N., Mosleh, A., and Kelley, A. P. (1983). On the analysis of dependent failures in risk assessment and reliability evaluation. *Nuclear Safety*, 24(5):637–657.

French, S. (1986). *Decision Theory: An Introduction to the Mathematics of Rationality*. Ellis Horwood Limited, Chichester.

Genest, C. G. and Zidek, J. V. (1986). Combining probability distributions: A critique and annotated bibliography. *Statistical Science*, 1(1):114–135.

Guba, E. G. and Lincoln, Y. (1994). Competing paradigms in qualitative research. In Denzin, N. K. and Lincoln, Y. S., editors, *Handbook in Qualitative Research*, pages 105–117. Sage.

Han, S. G., Yoon, W. H., and Chan, S. H. (1989). The trinomial failure rate model for treating common mode failures. *Reliability Engineering and System Safety*, 25(2):131–146.

Hanks, B. J. (1998). An appreciation of common cause failures in reliability. *Proc Instn Mech Engns*, 212(Part E):31–35.

Hauptmanns, U. (1996). The multi-class binomial failure rate model. *Reliability Engineering and System Safety*, 53:85–90.

Hirschberg, S. and Pulkkinen, U. (1985). Common cause failure data: Experience from diesel generator studies. *Nuclear Safety*, 26(3):305–313.

Hokstad, P. (1988). A shock model for common-cause failures. *Reliability Engineering and System Safety*, pages 127–145.

Hokstad, P. and Corneliussen, K. (2004). Loss of safety assessment and the IEC 61508 standard. *Reliability Engineering and System Safety*, 83:111–120.

Hokstad, P., Maria, A., and Tomis, P. (2005). Estimation of common cause factors from systems with different numbers of channels. To appear in IEEE transactions on Reliability.

Høland, A. and Rausand, M. (1994). *System Reliability Theory: Models and Statistical Methods*. Wiley Series in Probability and Mathematical Statistics. John Wiley and Sons Inc.

Holtschmidt, H., Kreusur, A., and Verstegen, C. (2006). Extension of the German database for common cause failure events. *Kerntechnik*, 71(1-2):22–28.

Hora, S. C. (1996). Aleatory and epistemic uncertainty in probability elicitation with an example from hazardous waste management. *Reliability Engineering and System Safety*, 54:217–223.

Hora, S. C. (2004). Probability judgments for continuous quantities: linear combinations and calibration. *Management Science*, 50(5):597–604.

Howard, R. (1990). From influence to relevance to knowledge. In R.M., O. and Q., S. J., editors, *Diagrams, Belief Nets and Decison Analysis*, pages 3–23. John Wiley and Sons, Chichester.

Humphreys, R. A. (1987). Assigning a numerical value to the beta factor common cause failure evaluation. In *Proceeding of Reliability '87*. Rolls Royce and Associates Ltd. Paper 2C/5.

Jensen, F. N. (1999). *An introduction to Bayesian Belief Networks*. UCL Press Limited, London.

Johanson, G., Kreuser, A., Pyy, P., Rasmuson, D., and Werner, W. (2006). OECD/NEA International Common Cause Failure Data Exchange project - insights and lessons learnt. *Kerntechnik*, 71(1-2):13–16.

Johanson, G., Mankamo, T., and Knochenhauer, M. (2003). Summary report of the Nordic Working Group on Common Cause Failure Analysis. Technical Report NAFCS-PR21, Nordisk Arbetsgrupp før CCF studier.

Johnson, N. L. and Kotz, S. (1972). *Distributions in Statistics: Continuous Multivariate Distributions*. John Wiley and Sons, New York.

Kadane, J. B. and Wolfson, L. J. (1998). Experiences in elicitation. *The Statistician*, 47(1):3–19.

Kaplan, S. and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1:11–27.

Kardes, E. and Luxhøj, J. T. (2005). A hierarchical probabilistic approach for risk assessments of an aviation safety product portofolio. *Air Traffic Control Quarterly*, 13(3):279–308.

Kjærulff, U. and van der Gaag, L. C. (2000). Making sensitivity analysis computationally efficient. In *Proceedings of the 16th Conference on Uncertainty in Artificial Intelligence (UAI)*, pages 317–325, San Francisco, California. Morgan Kaufmann Publishers.

Kreuser, A. and Peschke, J. (2001). Coupling model: a common-cause-failure model with consideration of interpretation uncertainties. *Reactor Safety*, 136:255–260.

Kreuser, A., Peschke, J., and Stiller, J. C. (2006). Further development of the coupling model. *Kerntechnik*, 71(1-2):50–53.

Kristensen, V. (2004). A proposal to a holistic framework for validation of risk analysis. Submitted for publication in Reliability Engineering and System Safety.

Kvam, P. (1998). A parametric mixture model for common-cause failure data. *IEEE Transactions on Reliability*, 47(1):30–34.

Kvam, P. H. (1996). Estimation techniques for common cause failure data with different system sizes. *Technometrics*, 38(4):382–388.

Langseth, H. and Portinale, L. (2005). Bayesian networks in reliability. Technical Report TR-INF-2005-04-01-UNIPMN, Dipartimento di Informatica, Universitá Degli Studi del Piemonte Orientale "A. Avogadro".

Laskey, K. (1995). Sensitivity analysis for probability assessments in Bayesian Networks. *IEEE Transactions on Systems, Man, and Cybernetics*, 25(6):901–909.

Lauritzen, S. (1996). *Graphical Models.* Clarendon Press, Oxford.

Lindley, D. V. (2000). The philosophy of statistics. *The Statistician*, 49(3):293–337.

Loschi, R. and Wechsler, S. (2002). Coherence, Bayes theorem and posterior distributions. *Brazilian Journal of Probability and Statistics*, 16:169–185.

Mankamo, T. (1994). Extended Common Load Model, a tool for dependent failure modeling in highly redundant structures. Technical Report SKI Report 94:3, Swedish Nuclear Power Inspectorate. Publication manuscript, 1990, NKS/SIK-1(92)3, 26 p. Published as part of "Supporting Documentation for Safety Evaluation by Living Probabilistic Safety Assessment".

Mankamo, T. and Kosonen, M. (1992). Dependent failure modelling in highly redundant structures - application to BWR safety valves. *Reliability Engineering and System Safety*, 35:235–244.

Marshall, A. W. and Olkin, I. (1967). A multivariate exponential distribution. *Journal of the American Statistical Association*, 62(317):30–44.

Martz, H., Kvam, P., and Abramson, L. (1996). Empirical Bayes estimation of the reliability of nuclear power plant emergency diesel generators. *Technometrics*, 38(1):11–24.

Matheson, J. E. (1990). Using influence diagrams to value information and control. In Oliver, R. and Smith, J. Q., editors, *Diagrams, Belief Nets and Decison Analysis*, pages 25–48. John Wiley and Sons, Chichester.

Max, H., John, B., and Eric, H. (1991). Decision analysis and expert systems. *Artificial Intelligence*, pages 64–91.

Mazzuchi, T. A. and Soyer, R. (1992). A dynamic general linear model for inference from accelerated life tests. *Naval Research Logistics*, 39:757–773.

Mazzuchi, T. A. and Soyer, R. (1996). A Bayesian perspective on some replacement strategies. *Reliability Engineering and System Sàfety*, 51:295–303.

Melchers, R. E. (2001). On the ALARP approach to risk management. *Reliability Engineering and System Safety*, 71:201–208.

Merkhofer, M. W. (1987). Quantifying judgmental uncertainty: methodology, experiences and insights. *IEEE Transactions on Systems, Man, and Cybernetics*, 17(5):741–752.

Meslin, T. (1988). Analysis and quantification of common-cause failures on the basis of operating experience. *Nuclear Safety*, 84:239–246.

Meyer, M. A. and Booker, J. M. (1991). *Eliciting and Analysing Expert Judgment: A Practical Guide.* American Statistical Association and the Society of Industrial and Applied Mathematics.

Mitchell, G. (1993). *The Practice of Operational Research.* John Wiley and Sons, Chichester.

Morgan, M. G. and Henrion, M. (1990). *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis.* Cambridge University Press.

Mosleh, A., Fleming, K. N., Parry, G. W., Paula, H. M., Worledge, D., and Rasmuson, D. M. (1987). Procedures for treating common cause failures in safety and reliability studies. volume 1: Procedural framework and examples. Technical Report NUREG/CR-4780-Vol.1;EPRI-NP-5613-Vol.1, U.S. Nuclear Regulatory Commission and Electric Power Research Institute.

Mosleh, A., Parry, G. W., and Zikria, A. F. (1994). An approach to the analysis of common cause failure data for plant-specific application. *Nuclear Engineering and Design*, 150:25–47.

Mosleh, A., Rasmuson, D., and Marshal, F. (1998a). Common cause failure database and analysis: System software reference manual. Technical Report NUREG/CR-6268, U.S. Nuclear Regulatory Commission. Volume 4.

Mosleh, A., Rasmuson, D., and Marshal, F. (1998b). Common cause failure database and analysis: System/overview. Technical Report NUREG/CR-6268, U.S. Nuclear Regulatory Commission. Volume 1.

Mosleh, A., Rasmuson, D., and Marshal, F. (1998c). Guidelines on modeling common-cause failures in probabilistic risk assessment. Technical Report NUREG/CR-5485, INEEL/EXT-97-01327, U.S. Nuclear Regulatory Commission.

Ness, J. and Hoffman, C. (1998). *Putting Sense Into Consensus: Solving the Puzzle of Making Team Decisions.* VISTA Associates, Tacoma, Wash.

Nilsen, T. and Aven, T. (2003). Models and model uncertainty in the context of risk analysis. *Reliability Engineering and System Safety*, 79:309–317.

O'Hagan, A. and Forster, J. (2004). *Kendall' s Advanced Theory of Statistics, Volume 2B: Bayesian Inference.* Arnold, London, second edition.

Parry, G. W. (1991). Common cause failure analysis: a critique and some suggestions. *Reliability Engineering and System Safety*, 34:309–326.

Parry, W. G. (1996). The characterisation of uncertainty in probabilistic risk assessments of complex systems. *Reliability Engineering and System Safety*, 54:119–126.

Paula, H. (1995). Technical note: on the definition of common-cause failures. *Nuclear Safety*, 36(1):53–57.

Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference.* Morgan Kaufmann Publishers Inc, San Mateo, CA.

Pidd, M. (2003). *Tools for Thinking: Modelling in Management Science.* Wiley and Sons Ltd., England, second edition.

Pradhan, M., Henrion, M., Provan, G., Favero, B. D., and Huang, K. (1996). The sensitivity of belief networks to imprecise probabilitites: an experimental investigation. *Artificial Intelligence*, 85:363–397.

Ramsey, F. P. (1926). Truth and probability. In Braithwaite, R. B., editor, *Foundations of Mathematics and Other Logical Essays*, pages 156–198. Kegan Paul.

Roberts, N. H., Vesely, W. E., Haasl, D. F., and Goldberg, F. F. (1981). Fault tree handbook. Technical Report NUREG-0492, US Nuclear Regulatory Commission.

Rolls Royce and Associates (1986). Numerical values for beta factor common cause failure evaluation. Technical Report RRA/7692.

Sachon, M. and Paté-Cornell, E. (2000). Delays and safety in airline maintenance. *Reliability Engineering and System Safety*, 67:301–309.

Saltelli, A. (2002). Sensitivity analysis for importance assessment. *Risk Analysis*, 22(3):579–590.

Savage, L. J. (1954). *The Foundations of Statistics*. John Wiley, New York.

Shachter, R. D. (1986). Evaluating influence diagrams. *Operations Research*, 34(6):871–882.

Sigurdsson, J. H., Walls, L. A., and Quigley, J. (2001). Bayesian Belief Nets for managing expert judgment and modelling reliability. *Quality and Reliability Engineering International*, 17:181–190.

Singpurwalla, N. D. (1971). Inference from accelerated life tests when observations are obtained from censored samples. *Technometrics*, 13(1):161–170.

Siu, N. and Mosleh, A. (1989). Treating data uncertainties in common-cause failure analysis. *Nuclear Technology*, 84:265–281.

Siu, N. O. and Kelly, D. L. (1998). Bayesian parameter estimation in probabilistic risk assessment. *Reliability Engineering and System Safety*, 62:89–116.

Smith, D. J. (2000). *Developments in the use of failure rate data and reliability prediction methods*. Isbn: 09516562 6 0, DELFT University of Technology.

Spetzler, C. S. and von Holsteins, C.-A. S. S. (1975). Probability encoding in decision analysis. *Management Science*, 22(3):340–358.

Spiegelhalter, D. J. and Lauritzen, S. L. (1990). Sequential updating of conditional probabilities on directed graphical structures. *Networks*, 20:579–605.

Spitzer, C. (2006). CCF treatment in PSA: insights and recommendations from reviewing procedures. *Kerntechnik*, 71(1-2):35–40.

Talbott, W. (2001). *Bayesian Epistemology.* The Stanford Encyclopedia of Philosophy, fall 2001 edition. Edward N. Zalta (ed.), URL = http://plato.stanford.edu/archives/fall2001/entries/epistemology-bayesian/.

Thorpe, M. C. and Williams, M. M. R. (1992). A review of expert judgment techniques with reference to nuclear safety. *Progress in Nuclear Energy*, 27(2-3):91–223.

Toledano, J. G. T. and Sucar, L. E. (1998). Bayesian networks for reliability analysis of complex systems. *Lecture Notes in Artificial Intelligence*, 1484:195–206.

Tversky, A. (1974). Assessing uncertainty. *Journal of the Royal Statistical Society. Series B, Methodology*, 36(2):148–159.

van der Gaag, L. C. (1996). Bayesian Belief Networks: odds and ends. *The Computer Journal*, 39(2):97–113.

Vatn, J. (1997). Maintenance optimisation from a decision theoretical point of view. *Reliability Engineering and System Safety*, 58:119–126.

Vaurio, J. (1994a). Estimation of common cause failure rates based on uncertain event data. *Risk Analysis*, 14(4):383–387.

Vaurio, J. (1994b). The theory and quantification of common cause shock events for redundant standby systems. *Reliability Engineering and System Safety*, 43(3):289–305.

Vaurio, J. (1995). The probabilistic modeling of external common cause failure shocks in redundant systems. *Reliability Engineering and System Safety*, 50:97–107.

Vaurio, J. K. (2002). Extensions of the uncertainty quantification of common cause failure rates. *Reliability Engineering and System Safety*, 78:63–69.

Vaurio, J. K. (2006). Is mapping a part of common cause failure quantification? *Kerntechnik*, 71(1-2):41–49.

Vesely, W. E. (1977). Estimating common cause failure probabilities in reliability and risk analysis: Marshall-olkin specializations. In Fussell, J. B. and Burdick, G. R., editors, *Nuclear Systems Reliability Engineering and Risk Assessment*, Society for Industrial and Applied Mathematics, page 314Ű341. Philadelphia.

Walls, L. A. and Bendell (1989). Exploring field reliability data for potential dependent failures. In *UK Reliability Symposium, Reliability 89*. Paper 4Ab/3.

Werner, W., Johanson, G., and Concepcion, M. (2004). International common-cause failure data exchange general coding guidelines. Technical Report NEA/CSNI/R(2004)4, Nuclear Energy Agency.

Wierman, T. E., Rasmuson, D. M., and Marshall, F. M. (2000). ICDE project report on collection ans analysis of common-cause failures of emrgency diesel generators. Technical Report NEA/CSNI/R(2000)20, Nuclear Energy Agency, France.

Winkler, R. (1996). Uncertainty in probabilistic risk assessment. *Reliability Engineering and System Safety*, 54:127–132.

Worledge, D. H. and Wall, I. B. (1989). Overview of the electric power research institute - research programme on common cause failures. *Nuclear Technology*, 84:256–259.

Youngblood, R. W. and Atwood, C. L. (2005). Mixture priors for Bayesian performance monitoring 1: fixed-constituent model. *Reliability Engineering and System Safety*, 89(2):151–163.

Zabell, S. L. (2006). Symmetry and its discontents: Essays on the history of inductive probability. In *Cambridge Studies in Probability, Induction and Decision Theory.* Cambridge University Press.

Zitrou, A. (2002). Common cause failure modelling. Master's thesis, Department of Management Science, University of Strathclyde, Glasgow, UK.

Appendix A

Variables of the ID model

A.1 Defence variables

A.1.1 Diversity

This defence describes the diverse characteristics of the system.

A	No diversity
B	Similar items with small differences in manufacturing/design
C	Diverse items which achieve the same purpose/function i.e. same method and principle of operation
D	Different items which achieve the same principle of operation and redundancy exists below diversity
E	Two entirely diverse independent redundant sub-systems

A.1.2 Separation

This defence describes the degree of segregation of the redundant components by an appropriate form of barrier. The categorisation below describes increasing levels of segregation which must be interpreted appropriately for the type of system being assessed.

Level 1 Appropriate wall or barrier (e.g. for blast or flooding protection) within the same room

Level 2 Separate cubicle or room (implies separate physical environment)

Level 3 Separate buildings or possibly well separated rooms.

A	Redundant identical items separation level less than Level 1
B	Redundant identical items separation Level 1
C	Redundant identical items, adjacent separation Level 2
D	Redundant identical items, adjacent separation Level 3
E	Redundant identical items in separate rooms

A.1.3 Understanding

This defence is a general measure of the vulnerability of the system to "unknown" dependent failure threats. It describes the level of understanding of designers, operators and analysts in relation to the system.

The Understanding defence levels are described in terms of four factors:

1. The factor of *experience* describes the amount of available experience with the system either from operational experience or from data coming from similar systems

2. The factor of *novelty* describes the degree to which the system uses new ideas (principles of operation, configuration). It is seen as increasing the uncertainty regarding possible dependent failure modes and causes.

3. The factor of *complexity* describes the complexity of the system.

4. The factor of *specific design* refers to the extent to which the equipment has been designed specifically for the application.

Limited experience (< 10 years)				
	Novelty	Complexity	Specific Design	
A	Big	Big	Small	OR software in system
B	Big	Big	Big	OR
	Big	Small	Small	OR
	Big	Big	Small	
C	Big	Small	Big	OR
	Small	Big	Big	OR
	Small	Small	Small	
D	Small	Small	Big	
E				

Level E not permitted for limiting experience

Extensive experience (< 10 years)				
	Novelty	Complexity	Specific Design	
A				
B	Big	Big	Small	
C	Big	Big	Big	OR
	Big	Small	Small	OR
	Small	Big	Small	
D	Big	Small	Big	OR
	Small	Big	Big	OR
	Small	Small	Small	
E	Small	Small	Big	

Level A not permitted for extensive experience

A.1.4 Analysis

This defence refers to the amount of analysis that has been done on the design/system and to the degree of awareness of the designers of the dependent failures issue.

A	No formal safety assessment. No design knowledge of dependent failures issues.
B	High level study (perhaps FMEA) or designer has general knowledge of dependent failure issues (demonstrated in the design).
C	Previous reliability assessment and evidence on feedback or designer has specific guidelines and knowledge of dependent failure issues (demonstrated in design).
D	Previous reliability assessment and evidence on feedback or designer has specific guidelines and knowledge of dependent failure issues (demonstrated in design) plus evidence of management support for feedback from assessment to design/operations.
E	Previous reliability assessment with clear evidence of results feedback and management support AND evidence of designer knowledge of dependent failure issues.

A.1.5 Operator Interaction

This defence refers to the degree of interaction with the operation of the item and whether there are written procedures or not that minimise the requirement for interpretation and decision by the staff.

A	No written procedures - Normal operator interaction
B	No written procedures - Minimal operator interaction OR Written procedures - Normal operator interaction
C	Written procedures - minimal operator interaction
D	Checklist procedures - Minimal operator interaction
E	Checklist procedures and evidence that procedures are followed - Minimal operator interaction

A.1.6 Safety Culture

This defence considers the training of the staff; such training is particularly relevant to emergency operations. Training relates to how well trained and what experience the person operating, maintaining and repairing the system has. Also, an active safety culture and a dedicated staff should be considered.

A		On the job training
B		Systematic regular training covering general and emergency operations
C		Simulator training of normal operations
	OR	Dedicated staff and evidence of good safety culture including a systematic training programme
D		Simulator training of normal operations
	AND	Dedicated staff and evidence of good safety culture including systematic training of emergency conditions
E		Simulator training of normal and emergency conditions. Clear safety policy/culture

A.1.7 Environmental Control

This defence relates to the control exercised over the environment in which the system is installed. The worst case might be represented by installation in an area in which other major processes, not related to the system are present. The potential dangers result from the unlimited access of people with no knowledge of the system. The dependent failure effect may be direct, or may simply cause the operator to leave his post without warning. It does not relate to the severity of the environment that should be taken into account by the designer.

A	Minimum control, other machines and processes not related in function are also present (e.g. Machine shop)
B	Separate building limits access - Other activities are associated. Small risk of mechanical damage by vehicles etc (e.g. Repair shop)
C	Access by authorised personnel only - All activities related (e.g. Laboratory)
D	Limited access area, trained personnel only, except under close supervision. All equipment and services subject to design control (e.g. remote sub-station)
E	As D but smaller scale with closely related activities (e.g. Flight deck of aircraft, power station control room)

A.1.8 Environmental Testing

This defence describes the intention of the designer that the system should be able to stand a number of environmental effects such as shock, vibration, temperature, humidity, etc. Good intentions are not sufficient in practice, environmental testing is capable of revealing certain dependent failure susceptibilities. The variety, type and range of testing at the manufacturing, construction, installation and commission stages should be considered.

A	No environmental tests other than the standard ones conducted by the manufacturers
B	Environmental tests on example unit specific to usage and operator defined
C	Detailed tests on example unit, unit tested to ensure that it will withstand all that is required to i.e. shock, vibration, temperature, humidity, electrical interference and water spray
D	Commissioning tests carried out. Run through of checks in a reasonable period of time i.e. example unit tested to ensure that it will withstand all excess fault conditions that they may be required to
E	Example unit run in parallel e.g. operate the unit for a year before it is brought on line

A.2 Root cause variables

Environment Represents causes related to harsh environment that is not within the component design specifications.

Design This category encompasses actions and decisions taken during design, manufacture, or installation of components, both before and after the plant is operational. Included in the design process are the equipment and system specification, material specification, and initial construction that would not be considered a maintenance function. This category also includes design modifications.

Human This category represents causes related to errors of omission or commission on the part of the plant staff or contractor staff. An example is failure to follow the correct procedure. This category includes accidental actions and failure to follow procedures for construction, modification, operation, maintenance, calibration and testing. This category also includes deficient training.

Internal to Component This category deals with malfunctioning of parts internal to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the environment on the component. Specific mechanisms include erosion/corrosion, internal contamination, fatigue, and wearout/end of life.

Procedures This category refers to ambiguity, incompleteness or error in procedures for operation and maintenance of equipment. This includes inadequacy in construction, modification, administrative, operational, maintenance, test and calibration procedures. This can also include the administrative control of procedures, such as change control.

Maintenance This category includes all maintenance causes not captured by Human or Procedures. (e.g. lubrication oil contamination due to work practices, incorrect fuel oil sampling schedule).

A.3 Coupling factor variables

Hardware Refers to factors that propagate a failure mechanism among several components due to identical physical characteristics. There are two subcategories of hardware coupling factors: (1) Hardware design: components have the same physical appearance, components share the same design and internal parts, components share the same maintenance/calibration/testing characteristics; (2) Hardware quality: components share the same manufacturing staff, quality control procedure, manufacturing method, material; components share the same construction/installation staff, construction/installation procedure, construction/installation schedule.

Operational Refers to factors that propagate a failure mechanism among several components due to identical operational characteristics. Such characteristics may be same operational staff, same operating procedures, same maintenance/test/calibration schedule, same maintenance/test/calibrations procedures.

Environmental Refers to factors that propagate a failure mechanism among several components due to identical external or internal environmental characteristics. It includes situations where components are exposed to similar environmental stresses because of the same location (external environment) or situations where components share the same internal medium of operation (internal environment).

Appendix B

Causality relationships in the ID network

B.1 Influences between model elements

Following, the influences between the system defences and the root cause / coupling factor variables, which are portrayed in the ID network, are described.

Influences to Root Causes

Environmental Testing → Design Root Cause During the environmental testing process, issues that could lead to failures related to design aspects (equipment and system specifications) of the system might be detected. Appropriate feedback given to the designers of the component could be used to make changes in the design of the system, and impede these failures from occurring; consequently, the variety, type and range of testing affects the rate of failures due to the Design root cause.

Analysis → Design Root Cause A good level of analysis performed on the design of the system increases the quality of the decisions taken during the design process and review, and, thus, the rate of failures attributed to the Design root cause.

Diversity → Design Root Cause Diversity is a design characteristic of the system (redundant group) and influences the occurrence of (total) design failures.

Separation → Design Root Cause Separation is a design characteristic of the system (redundant group) and its use or absence may lead to design failures.

Environmental Control → Human Root Cause Applying strict control and limited access to the site of the system decreases the likelihood for untrained or unsupervised staff to access the system and minimises the potential for accidental actions or failures due to human error.

Safety Culture → Human Root Cause The quality of training provided to the personnel is strongly related to the amount of errors performed on the part of the staff (operating and contractor) and, thus, to the rate of failures attributed to the Human root cause.

Operator Interaction → Human Root Cause During the panel discussions, it was assumed that having no procedures is a procedure itself. Thus, one making a mistake because there are no procedures to follow falls under the Procedures root cause. Having assumed this, some members of the panel suggested to remove the influence from Operator Interaction to Human because the arrow to Procedures already captures the errors made due to lack of procedures. However, the defence of Operator Interaction not only describes the degree to which procedures exist, but also the degree of man-machine interaction. It is argued that when man-machine interaction is minimised (by automated functions), then it is less likely the operating staff to follow procedures erroneously, which is described under the Human root cause. Therefore, it is argued that Operator Interaction does influence the Human root cause.

Understanding → Human Root Cause Aspects such as the amount of existing experience, design features and the complexity of the system are related to the frequency with which human errors occur. On the one hand, existing experience gives insights and knowledge on how to operate the system, thus reduces the potential for human errors, especially in emergency cases. On the other hand, the simpler the design of the system is or more experience exists, the less likely is for human errors to occur. Overall, the level of Understanding affects the rate of failures due to the human element.

Environmental Testing → Internal to Component Root Cause The intention of environmental testing is to increase the durability of the units against of environmental shocks. Some of these shocks result in mechanisms that lead to internal failures (e.g. corrosion mechanisms). Therefore, the type and range of environmental testing influences the rate of internal failures.

Analysis → Internal to Component Root Cause During the analysis stage, particular design features that can lead to failures may be identified, and thus removed. A proportion of the related impeded failures falls under the category of the Design root cause (influence of the Analysis subfactor on the Design root cause), however, a proportion of these failures are related to internal failures.

Understanding → Internal to Component Root Cause Existing experience and design characteristics of the system provides insight into internal failure issues. A good level of Understanding (experience compensating for system complexity) provides knowledge on how to protect against Internal to component failures.

Safety Culture → Maintenance Root Cause A good level of Safety Culture (adequate training of the staff and quality of safety culture) reduces the likelihood of operating and maintenance staff disturbing the control and instrumentation of the system during activities leading to maintenance failures.

Operator Interaction → Procedures Root Cause The subfactor of Operator Interaction describes the condition of procedures for the system. The quality and amount of detail in written procedures determines the degree of interpretation and decision by the staff, and therefore affects the rate of failures occurring due to ambiguity or misinterpretation.

Analysis → Procedures Root Cause The aspect of analysis on the design of the system is associated with the correctness and adequacy of the written procedures. The more analysis has been performed, the more probable it is for the procedures to be honed.

Understanding → Procedures Root Cause The degree of Understanding influences the quality of procedures. Firstly, the simpler the system is, the more likely the procedures are to be correct. Secondly, the more experience with the system exists, the more likely the procedures are to be honed.

Environmental Control → External Environment Root Cause The level of control exercised on the environment in which the system is installed is related to the kind of shocks that occur to the system: if the system is isolated, then the shocks are more likely to fall within the design specifications of the system. However, when other major processes, unrelated to the system, are present in the same location, there is increased likelihood that shocks initiated by the other processes will be posed on the system. These shocks are not foreseen by the system design specifications.

Analysis → External Environment Root Cause The higher the level of analysis, the more prepared the system is to sustain environmental shocks.

Influences to Coupling Factors

Analysis → Environmental Coupling Factor Sufficient analysis during the design phase and awareness on the part of the designers of dependent failure issues would lead to the detection and removal of problematic external or internal environmental characteristics of the design of the system that create coupling effects. Therefore, a good level of analysis decreases the tendency of a failure event to be coupled due to environmental issues.

Separation → Environmental Coupling Factor In principle, separation is a defence targeted against removing the common environmental characteristics from the system, which propagate a failure mechanism amongst several components.

Analysis → Hardware Coupling Factor In a similar fashion as earlier, a high level of analysis during the design stage and awareness of dependent failure issues, allows for the detection and removal of similar physical characteristics that increase the tendency of a failure to be propagated amongst components.

Diversity → Hardware Coupling Factor Functional diversity is oriented towards reducing the effect of coupling (due to hardware similarities) amongst failures.

Operator Interaction → Operational Coupling Factor When the man-machine interaction is minimised (by automated functions), then the likelihood of a failure being propagated amongst several components due to the same operational characteristics decreases. Such examples include errors on the part of the operating staff that, when is the same for all units, are shared amongst the units. Moreover, well-written procedures would cater for procedural mistakes being propagated amongst several components.

Appendix C

Probability encoding results

C.1 Root cause part

C.1.1 Design Root Cause

The rate of system failures due to the Design root cause is denoted by r_1. The defences that are targeted against the occurrence of this type of failures are Environmental Testing (D_1), Analysis (D_3), Separation (D_5), and Diversity (D_6). The identified functional interactions existing amongst these defences are:

- Separation (D_5) is threshold functionally dependent on Env. Testing (D_1) and Analysis (D_3)
- Diversity (D_6) is threshold functionally dependent on Env. Testing (D_1) and Analysis (D_3)

Consistently with the GS model, the Design rate r_1 at configuration $\underline{x} = (x_1, x_3, x_5, x_6)$ ($x_k \in \{1,...,5\}$ for $k = 1,3,5,6$) is given by

$$r_{1,(x_1,x_3,x_5,x_6)} = \varphi_1^{x_1-3}\varphi_3^{x_3-3}\varphi_5(x_1,x_3)^{x_5-3}\varphi_6(x_1,x_3)^{x_6-3}r_{1,(3,3,3,3)} \qquad \text{(C.1)}$$

Determination of subjective distributions

Performing uncertainty analysis on Model (C.1) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the Design part of the questionnaire. The relationships between the elicitation and the target variables are:

$$e_1 = r_{1,(3,3,3,3)} \qquad e_2 = \phi_1$$

$$e_3 = \phi_3 \qquad e_4 = \phi_{5,1}\phi_{5,1}$$

$$e_5 = \phi_{5,3}\phi_{5,3} \qquad e_6 = \phi_5(x_1,x_3) \;\; x_1 \in X_1, x_3 \in X_3$$

$$e_7 = \phi_5(x_1,x_3) \;\; x_1 \in X_3, x_3 \in X_1 \qquad e_8 = \phi_{6,1}\phi_{6,1}$$

$$e_9 = \phi_{6,3}\phi_{6,3} \qquad e_{10} = \phi_6(x_1,x_3) \;\; x_1 \in X_1, x_3 \in X_3$$

$$e_{11} = \phi_6(x_1,x_3) \;\; x_1 \in X_3, x_3 \in X_1$$

where for $i = 5,6$

$$\phi_i(x) = \phi_{i,\theta} \quad \text{when } x \in X_\theta \text{ for } \theta = 1,2,3$$

Base rate The rate variable $r_{1,(3,3,3,3)}$ is gamma distributed. Thus, the prior distribution of e_1 is approximated by a gamma distribution, viz.

$$r_{1,(3,3,3,3)} \sim G(a,b)$$

Proportion random variables Elicitation variables e_2 and e_3 coincide with proportion variables ϕ_1 and ϕ_3. Let $e_n \sim \Lambda\left(\mu_n, \sigma_n^2\right)$ for $n = 2,3$ be the fitted distributions. Then

$$\phi_1 \sim \Lambda\left(\mu_2,\sigma_2^2\right) \quad \text{and} \quad \phi_3 \sim \Lambda\left(\mu_3,\sigma_3^2\right)$$

Piecewise proportion functions The elicitation variables e_n for $n = 4,\ldots,11$ are lognormally distributed, as products of independent lognormally distributed random variables. Let $e_n \sim \Lambda\left(\mu_n,\sigma_n^2\right)$ be the fitted distributions. It is

$$\phi_{5,1} = (e_4)^{\frac{1}{2}} \quad \text{so} \quad \phi_{5,1} \sim \Lambda\left(\frac{1}{2}\mu_4, \frac{1}{4}\sigma_4^2\right)$$

$$\phi_{5,3} = (e_5)^{\frac{1}{2}} \quad \text{so} \quad \phi_{5,3} \sim \Lambda\left(\frac{1}{2}\mu_5, \frac{1}{4}\sigma_5^2\right)$$

and, based on the symmetry assumption, one gets

$$\phi_{5,2} = (\phi_{5,1} \;\; \phi_{5,3})^{\frac{1}{2}} \quad \text{so} \quad \phi_{5,2} \sim \Lambda\left(\frac{1}{4}(\mu_4+\mu_5), \frac{1}{16}(\sigma_4^2+\sigma_5^2)\right)$$

Similarly,

$$\phi_{6,1} = (e_8)^{\frac{1}{2}} \quad \text{so} \quad \phi_{6,1} \sim \Lambda\left(\frac{1}{2}\mu_8, \frac{1}{4}\sigma_8^2\right)$$

$$\phi_{6,3} = (e_9)^{\frac{1}{2}} \quad \text{so} \quad \phi_{6,3} \sim \Lambda\left(\frac{1}{2}\mu_9, \frac{1}{4}\sigma_9^2\right)$$

and, based on the symmetry assumption, one gets

$$\phi_{6,2} = (\phi_{6,1}\ \phi_{6,3})^{\frac{1}{2}} \quad \text{so} \quad \phi_{6,2} \sim \Lambda\left(\frac{1}{4}(\mu_8 + \mu_9), \frac{1}{16}(\sigma_8^2 + \sigma_9^2)\right)$$

Elicitation variables e_6, e_7 and e_{10}, e_{11} are used as checks for the symmetry assumption

$$\phi_i(x_1, x_3) = \phi_i(x_1)\phi_i(x_3) \quad \text{for } i = 5,6$$

Within this example, the condition is exactly met for $\phi_6(x_1, x_3)$.

Results The parameters and the first two moments of the expert's distributions are given in Table C.1.

Table C.1: Parameters of subjective distributions related to the Design root cause rate

	r
a b	1.97 4.06E+06
E[r] Var[r]	4.86E-07 1.198E-13

	ϕ_1	ϕ_3
μ σ	-0.5150 0.1936	-0.2240 0.0757
$E[\phi]$ $Var[\phi]$	0.61 0.01416	0.80 0.00369

	ϕ_5		
θ	1	2	3
μ σ	-0.112 0.038	-0.083 0.025	-0.053 0.034
$E[\phi]$ $Var[\phi]$	0.89 0.0011	0.92 0.0005	0.95 0.0010

	ϕ_6		
θ	1	2	3
μ σ	-0.179 0.043	-0.116 0.023	-0.053 0.016
$E[\phi]$ $Var[\phi]$	0.84 0.0013	0.89 0.0004	0.95 0.0002

Extrapolation of Uncertainty

Using Model (C.1), the uncertainty distribution on r_1 can be determined at any configuration (x_1, x_3, x_5, x_6). Information on the mean and st. deviation of r_1 for particular defence configuration vectors are given in Figures C.1 and C.2.

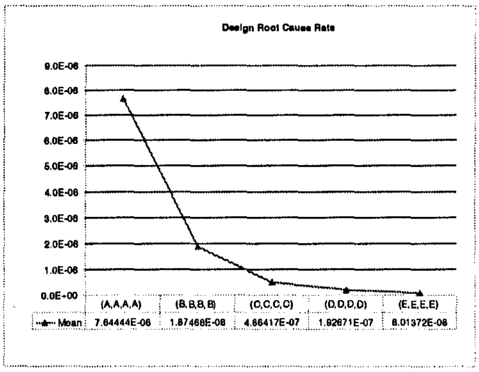


Figure C.1: Expected value of Design Root Cause rate at particular configuration vectors

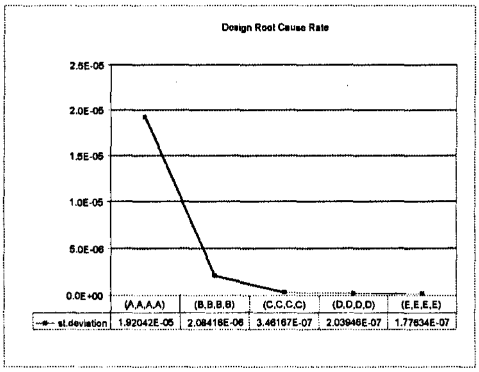


Figure C.2: Standard deviation of Design Root Cause rate at particular configuration vectors

Threshold dependencies The defence of Separation is threshold dependent on Env. Testing and Analysis. This fact implies that the impact of Separation differentiates for classes of configuration vectors of the system across Env. Testing and Analysis. It is

$$I_5(x_1,x_3) = \phi_5(x_1,x_3)$$

Similarly, The defence of Diversity is threshold dependent on Env. Testing and Analysis. This fact implies that the impact of Diversity depends on classes of configuration vectors of the system across Env. Testing and Analysis. It is

$$I_6(x_1,x_3) = \phi_6(x_1,x_3)$$

Figure C.3 illustrates the proportion of decrease of the expected value of r_1 by modifying Separation, for the different levels of Analysis and Env. Testing. Similarly, Figure C.4 illustrates the proportion of decrease of the expected value of r_1 by modifying Diversity, for the different levels of Analysis and Env. Testing. It may be seen that for both defences, the change induced in $E[r_1]$ is bigger (lower proportion) for high levels of Analysis and Env. Testing, and smaller (low proportion) for low levels of Analysis and Env. Testing.

The proportion by which r_1 changes, when the level of Env. Testing is modified by one, is

$$I_1(x_1,x_5,x_6) = \left(\frac{\phi_5(x_1+1)}{\phi_5(x_1)}\right)^{x_5-3}\left(\frac{\phi_6(x_1+1)}{\phi_6(x_1)}\right)^{x_6-3}\phi_1$$

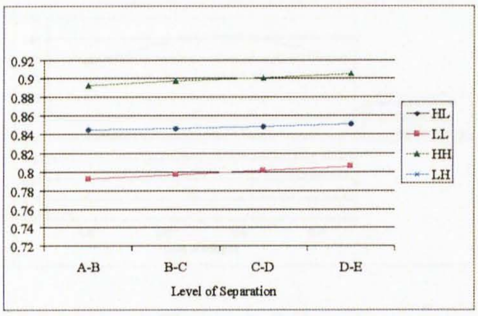


Figure C.3: Proportion of decrease in $E[r_1]$ by modifying Separation

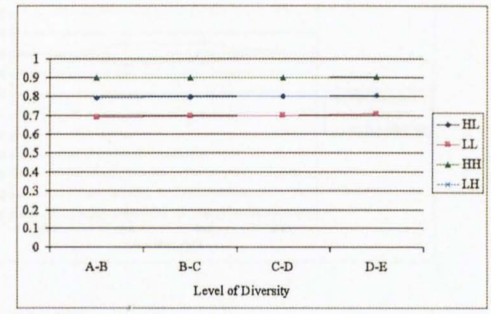


Figure C.4: Proportion of decrease in $E[r_1]$ by modifying Diversity

and, the proportion by which r_1 changes, when the level of Analysis is modified by one, is

$$I_3(x_3,x_5,x_6) = \left(\frac{\phi_5(x_3+1)}{\phi_5(x_3)}\right)^{x_5-3}\left(\frac{\phi_6(x_3+1)}{\phi_6(x_3)}\right)^{x_6-3}\phi_3$$

Due to the threshold dependency of Separation and Diversity on Env. Testing and Analysis, the impact of the threshold counterparts is independent of the level of Separation and Diversity for moderate modifications. This effect is illustrated in Figure C.5, which includes plots of the proportion of decrease induced in $E[r_1]$ by modifying the level of Env. Testing by one, with reference to the levels of Separation and Diversity. It may be seen that for drastic changes and for high levels of Separation and Diversity, this proportion takes higher values, implying that the impact of Env. Testing weakens.

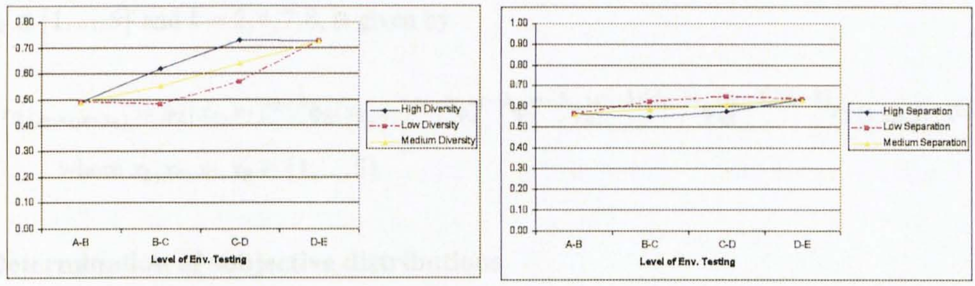


Figure C.5: Proportion of decrease in $E[r_1]$ by modifying Env. Testing

Figure C.6 illustrates the proportion of decrease induced in $E[r_1]$ by modifying the level of Analysis by one, with reference to the levels of Separation and Diversity. Similar conclusions may be drawn as previously.

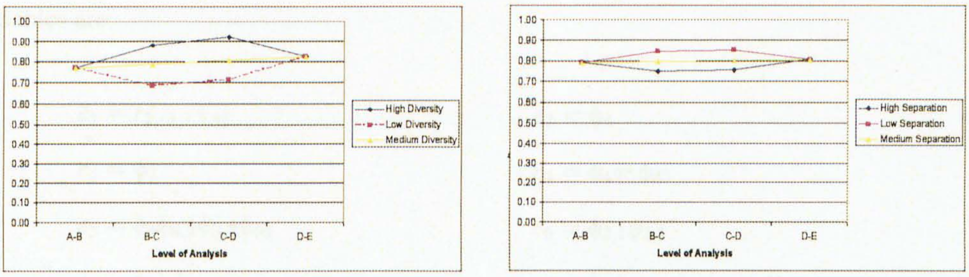


Figure C.6: Proportion of decrease in $E[r_1]$ by modifying Analysis

C.1.2 Human Root Cause

The rate of system failures due to the Human root cause is denoted by r_2. The defences that are targeted against the occurrence of this type of failures are Environmental Control (D_2), Safety Culture (D_4), Understanding (D_7), and, Operator Interaction (D_8). The functional interactions existing in the defence domain are:

- Env. Control (D_2) is threshold functionally dependent on Safety Culture (D_4) and Understanding (D_7)
- Operator Interaction (D_8) is threshold functionally dependent on Env. Control (D_2) and Understanding (D_7)
- Safety Culture (D_4) and Understanding (D_7) are functionally dependent
- Safety Culture (D_4) and Operator Interaction (D_8) are functionally dependent

Consistently with the GS model, the Human rate at configuration $\underline{x} = (x_2, x_4, x_7, x_8)$, where $x_k \in \{1, ..., 5\}$ and $k = 2, 4, 7, 8$, is given by

$$r_{2,(x_2,x_4,x_7,x_8)} = \phi_2(x_4,x_7)^{x_2-3}\phi_8(x_2,x_7)^{x_8-3}\phi_4^{x_4-3}\phi_7^{x_7-3}\phi_{47}^{(x_7-3)(x_4-3)}\phi_{48}^{(x_8-3)(x_4-3)}r_{2,(3,3,3,3)} \quad \text{(C.2)}$$

where $x_2, x_4, x_7, x_8 \in \{1, ..., 5\}$

Determination of subjective distributions

Performing uncertainty analysis on Model (C.2) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the Human part of the questionnaire. The relationships between the target and elicitation variables are:

$$e_1 = r_{2,(3,3,3,3)} \qquad e_2 = \phi_4$$

$$e_3 = \phi_7 \qquad e_4 = \phi_4\phi_7\phi_{47}$$

$$e_5 = \phi_4\phi_{8,2}\phi_{8,2}\phi_{48} \qquad e_6 = \phi_{2,1}\phi_{2,1}$$

$$e_7 = \phi_{2,3}\phi_{2,3} \qquad e_8 = \phi_2(x_4,x_7),\;\; x_4 \in X_1, x_7 \in X_3$$

$$e_9 = \phi_2(x_4,x_7),\;\; x_4 \in X_3, x_7 \in X_1$$

$$e_{10} = \phi_{8,1}\phi_{8,1} \qquad e_{11} = \phi_{8,3}\phi_{8,3}$$

$$e_{12} = \phi_8(x_2,x_7),\;\; x_2 \in X_1, x_7 \in X_3 \qquad e_{13} = \phi_8(x_2,x_7)\, x_2 \in X_3, x_7 \in X_1$$

where for $i = 2,8$

$$\phi_i(x) = \phi_{i,\theta} \quad \text{when } x \in X_\theta \text{ for } \theta = 1,2,3$$

Base rate The rate variable $r_{2,(3,3,3,3)}$ is gamma distributed. Thus, the prior distribution of e_1 is approximated by a gamma distribution, viz.

$$r_{2,(3,3,3,3)} \sim G(a,b)$$

Proportion random variables Elicitation variables e_2 and e_3 coincide with proportion variables ϕ_4 and ϕ_7. Let $e_n \sim \Lambda\left(\mu_n, \sigma_n^2\right)$ for $n = 2,3$ be the fitted distributions. Then

$$\phi_4 \sim \Lambda\left(\mu_2, \sigma_2^2\right) \quad \text{and} \quad \phi_7 \sim \Lambda\left(\mu_3, \sigma_3^2\right)$$

Piecewise proportion functions The elicitation variables e_n for $n = 6,...,13$ are lognormally distributed, as products of independent lognormally distributed random variables. Let $e_n \sim \Lambda\left(\mu_n, \sigma_n^2\right)$ be the fitted distributions. It is

$$\phi_{2,1} = (e_6)^{\frac{1}{2}} \quad \text{so} \quad \phi_{2,1} \sim \Lambda\left(\frac{1}{2}\mu_6, \frac{1}{4}\sigma_6^2\right)$$

$$\phi_{2,3} = (e_7)^{\frac{1}{2}} \quad \text{so} \quad \phi_{2,3} \sim \Lambda\left(\frac{1}{2}\mu_7, \frac{1}{4}\sigma_7^2\right)$$

and, based on the symmetry assumption, one gets

$$\phi_{2,2} = (\phi_{2,1} \cdot \phi_{2,3})^{\frac{1}{2}} \quad \text{so} \quad \phi_{2,2} \sim \Lambda\left(\frac{1}{4}(\mu_6 + \mu_7), \frac{1}{16}(\sigma_6^2 + \sigma_7^2)\right)$$

Similarly,

$$\phi_{8,1} = (e_{10})^{\frac{1}{2}} \quad \text{so} \quad \phi_{8,1} \sim \Lambda\left(\frac{1}{2}\mu_{10}, \frac{1}{4}\sigma_{10}^2\right)$$

$$\phi_{8,3} = (e_{11})^{\frac{1}{2}} \quad \text{so} \quad \phi_{8,3} \sim \Lambda\left(\frac{1}{2}\mu_{11}, \frac{1}{4}\sigma_{11}^2\right)$$

and, based on the symmetry assumption, one gets

$$\phi_{8,2} = (\phi_{8,1} \cdot \phi_{8,3})^{\frac{1}{2}} \quad \text{so} \quad \phi_{8,2} \sim \Lambda\left(\frac{1}{4}(\mu_{10} + \mu_{11}), \frac{1}{16}(\sigma_{10}^2 + \sigma_{11}^2)\right)$$

Elicitation variables e_8, e_9 and e_{12}, e_{13} are used as checks. Within this example, the subjective distributions imply the expected value of $\phi_2(x_4, x_7)$ when $x_4, x_7 \in X_1$ is higher than the expected value of $\phi_2(H, L)$ when $x_4 \in X_3$ and $x_7 \in X_1$. This violates the fundamental assumptions of the model, thus it is directly assumed that

$$\phi_2(x_1, x_3) = \phi_2(x_1)\phi_2(x_3)$$

Cross-terms The elicitation variables e_n for $n = 4, 5$ are lognormally distributed, as products of independent lognormally distributed random variables. Let $e_n \sim \Lambda(\mu_n, \sigma_n^2)$, $n = 4, 5$, be the fitted distributions. By taking logarithms, we have the subsystem of equations

$$\left.\begin{aligned} \ln e_4 &= \ln\phi_4 + \ln\phi_7 + \ln\phi_{47} \\ \ln e_5 &= \ln\phi_4 + 2\ln\phi_{8,2} + \ln\phi_{48} \end{aligned}\right\} \Rightarrow \begin{aligned} \ln\phi_{47} &= \ln e_4 - \ln e_2 - \ln e_3 \\ \ln\phi_{48} &= \ln e_5 - \ln e_2 - 2\ln\phi_{8,2} \end{aligned}$$

Let $z = -\ln e_2 - \ln e_3$, so that

$$\ln\phi_{47} = z + \ln e_4 \tag{C.3}$$

We have $z \sim N(\mu_z, \sigma_z^2)$, where $\mu_z = -\mu_2 - \mu_3$ and $\sigma_z^2 = \sigma_2^2 + \sigma_3^2 + 2cov(-\ln e_2, -\ln e_3)$. But it is

$$cov(-\ln e_2, -\ln e_3) = cov(-\ln\phi_4, -\ln\phi_7) = 0$$

which leads to $\sigma_z^2 = \sigma_2^2 + \sigma_3^2$. Now, from Relationship (C.3) follows that $\ln\phi_{47}$ is normally distributed with mean $m_{47} = -\mu_2 - \mu_3 + \mu_4$ and variance $s_{47}^2 = \sigma_z^2 + \sigma_4^2 + 2cov(z, \ln e_4)$. But

$$\begin{aligned} cov(z, \ln e_4) &= cov(-\ln\phi_4 - \ln\phi_7, \ln\phi_4 + \ln\phi_7 + \ln\phi_{47}) \\ &= -var[\ln\phi_4] - var[\ln\phi_7] = -\sigma_2^2 - \sigma_3^2 \end{aligned}$$

and finally

$$\phi_{47} \sim \Lambda\left(\mu_4 - \mu_2 - \mu_3, \sigma_4^2 - \sigma_2^2 - \sigma_3^2\right)$$

Let $w = \ln e_5 - \ln e_2$, so that

$$\ln\phi_{48} = w - 2\ln\phi_{8,2} \tag{C.4}$$

We have $w \sim N\left(\mu_w, \sigma_w^2\right)$ where $\mu_w = \mu_5 - \mu_2$ and $\sigma_w^2 = \sigma_5^2 + \sigma_2^2 + 2cov(\ln e_5, -\ln e_2)$ But

$$cov(\ln e_5, -\ln e_2) = cov(\ln\phi_4 + 2\ln\phi_{8,2} + \ln\phi_{48}, -\ln\phi_4) = -var[\ln\phi_4] = -\sigma_2^2$$

so $\sigma_w^2 = \sigma_5^2 - \sigma_2^2$. Now, from Relationship (C.4) follows that $\ln\phi_{48}$ is normally distributed with mean $m_{48} = \mu_w - \frac{1}{2}(\mu_{10} + \mu_{11})$ and variance

$$\begin{aligned} s_{48}^2 &= \sigma_w^2 + \frac{1}{4}(\sigma_{10}^2 + \sigma_{11}^2) + 2cov(w, -2\ln\phi_{8,2}) \\ &= \sigma_5^2 - \sigma_2^2 + \frac{1}{4}(\sigma_{10}^2 + \sigma_{11}^2) - 2cov(2\ln\phi_{8,2} + \ln\phi_{48}, 2\ln\phi_{8,2}) \\ &= \sigma_5^2 - \sigma_2^2 + \frac{1}{4}(\sigma_{10}^2 + \sigma_{11}^2) - \frac{1}{2}(\sigma_{10}^2 + \sigma_{11}^2) \\ &= \sigma_5^2 - \sigma_2^2 - \frac{1}{4}(\sigma_{10}^2 + \sigma_{11}^2) \end{aligned}$$

and finally

$$\phi_{48} \sim \Lambda\left(\mu_5 - \mu_2 - \frac{1}{2}(\mu_{10} + \mu_{11}), \sigma_5^2 - \sigma_2^2 - \frac{1}{4}(\sigma_{10}^2 + \sigma_{11}^2)\right)$$

Condition In agreement with the fundamental assumption that the defence of the system does not become worse as a result of increasing the levels of defences, it needs to hold:

$$0 < \phi_4\phi_{47}^{x_7-3}, \phi_7\phi_{47}^{x_4-3} < 1 \quad \text{for every } x_1, x_4, x_7 = 1, ..., 5 \tag{C.5}$$

$$0 < \phi_4\phi_{48}^{x_8-3}, \phi_8(x_2, x_7)\phi_{48}^{x_4-3} < 1 \quad \text{for every } x_2, x_7, x_4, x_8 = 1, ..., 5 \tag{C.6}$$

Adjustments Let $X = \phi_7 \phi_{47}^{x_4 - 3}$, for given $x_4 \in \{1,...,5\}$. X is lognormally distributed, as a product of independent lognormally distributed variables. The distribution of X is determined analytically based on the distributions of ϕ_7, ϕ_{47}. Let $X \sim f_X(x \mid \phi_7, \phi_{47})$, and let v_{p_i} be the $p_i \cdot 100\%$ percentile of X, where $p_1 = 0.05$, $p_2 = 0.5$ and $p_3 = 0.95$, viz.

$$\int_0^{v_{p_i}} f_X(x)\mathrm{d}x = F_X(v_{p_i}) = p_i \Leftrightarrow v_{p_i} = F_X^{-1}(p_i)$$

Based on the Expert's distributions on ϕ_7, ϕ_{47} one finds that $v_{0.95} > 1$ for $x_4 = 4,5$. This violates Conditions (C.5), and thereby appropriate adjustments need to be made.

In order to overcome the aforementioned inconsistency, the prior on ϕ_{47} is tuned to f_{47}^* so that Conditions (C.5) are not violated. Let $f_{47}^* := \Lambda(m_{47}^*, s_{47}^*)$ be the adjusted distribution. The tasks reduces to determining parameters m_{47}^* and s_{47}^*, according to the following minimisation problem:

$$\text{minimise } \frac{1}{3}\sum_{i=1}^{3}\left(F_{47}^{-1}(p_i \mid m_{47}, s_{47}) - F_{47}^{*-1}(p_i \mid m_{47}^*, s_{47}^*)\right)^2$$

subject to

$$F_X^{-1}(v_p \mid m_{47}^*, s_{47}^*) < 1, \quad \text{for } p = 0.95$$

$$s_{47}^* > 0$$

for $x_4 = 4,5$.

Similarly, let $Y = \phi_8(x_2, x_7)\phi_{48}^{x_4 - 3}$ $(x_2, x_7 \in \{1,...,5\})$ with distribution $f_Y(y \mid \phi_8(x_2, x_7)\phi_{48})$. Based on the Expert's distributions, one finds that $v_{0.95} = F_Y^{-1}(0.95) > 1$ for $x_4 = 4,5$, which violates Conditions (C.6). The problem is treated as a minimisation problem in a similar fashion as previously, and, the prior on cross-term ϕ_{48} is tuned so that the conditions are met.

The values of the objective functions in the two afore-described minimisation problems correspond to the minimum squared error (MSE) of the adjustments applied. For the re-determination of f_{47} it is $MSE = 0.0752$ and for the re-determination of f_{48} it is $MSE = 0.065$.

Results The parameters and the first two moments of the expert's distributions are given in Table C.2.

Table C.2: Parameters of subjective distributions related to the Human root cause rate

	r
a b	9.3455 1E+07
E[r] Var[r]	9.34E-07 9.34E-014

	ϕ_4	ϕ_7
μ σ	-1.196 0.286	-0.223 0.072
$E[\phi]$ $Var[\phi]$	0.31 8.46E-03	0.80 3.30E-03

	ϕ_2			ϕ_8		
θ	1	2	3	1	2	3
μ σ	-0.11 0.04	-0.08 0.03	-0.05 0.03	-0.18 0.05	-0.12 0.03	-0.05 0.02
$E[\phi]$ $Var[\phi]$	0.89 0.0011	0.92 0.0005	0.95 0.0010	0.84 0.0018	0.89 0.0006	0.95 0.0003

Extrapolation of Uncertainty

Using Model (C.2), the uncertainty distribution on r_2 can be determined at any configuration (x_2, x_4, x_7, x_8). Information on the mean and st. deviation of r_2 for particular defence configuration vectors are given in Figures C.7 and C.8.

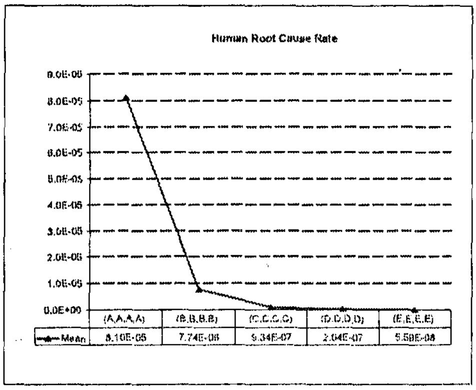


Figure C.7: Expected value of Human Root Cause rate at particular configuration vectors

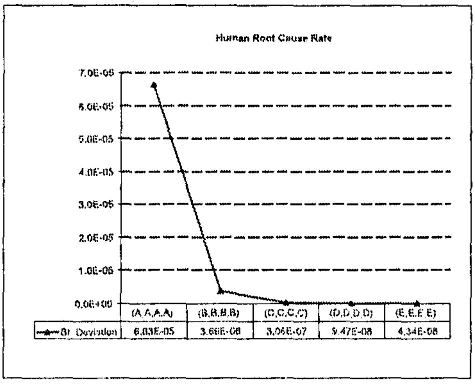


Figure C.8: Standard deviation of Human Root Cause rate at particular configuration vectors

Functional dependence of Safety Culture and Understanding The defences of Safety Culture (D_4) and Understanding (D_7) are functionally dependent, which implies that the influence of Safety Culture depends on the level of Understanding, and vice versa. According to model C.2, the proportion by which r_2 changes by modifying the level of Safety Culture by

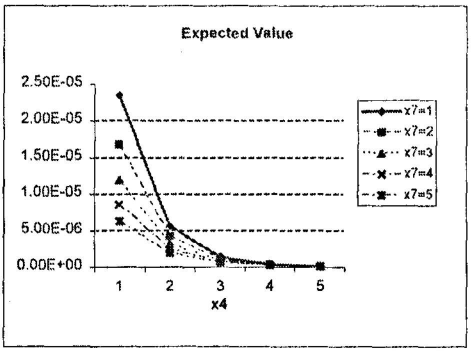


Figure C.9: Expected value of Human root cause at different levels of Safety Culture with reference to the level of Understanding, while the other defences are medium

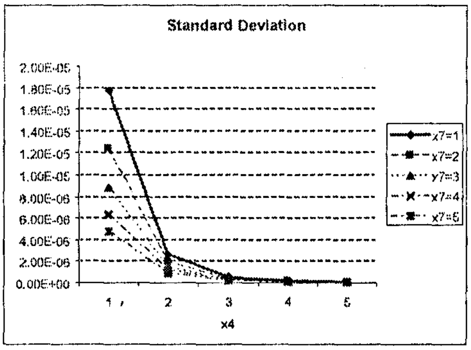


Figure C.10: Standard deviation of Human root cause at different levels of Safety Culture, with reference to the level of Understanding, while the other defences are medium.

one is

$$l_4(x_2,x_4,x_7,x_8) = \left(\frac{\phi_2(x_4+1)}{\phi_2(x_4)}\right)^{x_2-3} \phi_4\phi_{47}^{x_7-3}\phi_{48}^{x_8-3}$$

and the proportion by which r_2 changes, by modifying the level of Understanding by one is

$$l_7(x_2,x_4,x_7,x_8) = \left(\frac{\phi_2(x_7+1)}{\phi_2(x_7)}\right)^{x_2-3} \left(\frac{\phi_8(x_7+1)}{\phi_8(x_7)}\right)^{x_8-3} \phi_7\phi_{47}^{x_4-3}$$

The common term ϕ_{47} implies a symmetric dependence between Safety Culture and Understanding. The two defences exhibit a compensating effect ($\phi_{47} > 1$), implying that enhancing the one defence becomes more effective when the level of the other is low;. Figures C.9 and C.10 illustrate the changes in the mean and standard deviation of r_2. As the level of Understanding increases, the interaction between $l_4(x_2x_7x_8)$ and x_7 decelerates, thus the influence of Safety Culture on the Human root cause rate weakens. Similar conclusions may be drawn from Figures C.11 and C.12.

Functional dependence of Safety Culture and Operator Interaction The defences of Safety Culture (D_4) and Operator Interaction (D_8) are functionally dependent, which implies that the influence of Safety Culture depends on the level of Operator Interaction, and vice versa. As seen previously, the proportion by which r_2 changes by modifying the level of

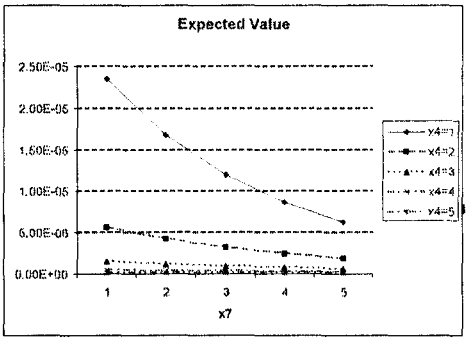


Figure C.11: Expected value of Human root cause at different levels of Understanding with reference to the level of Safety Culture, while the other defences are medium.

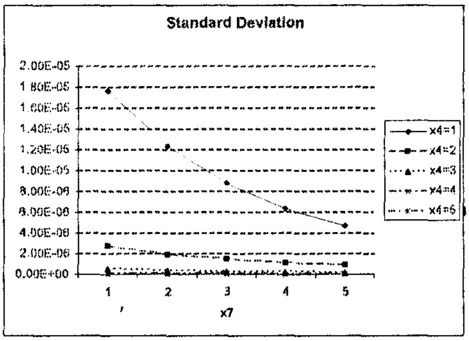


Figure C.12: Standard deviation of Human root cause at different levels of Understanding with reference to the level of Safety Culture, while the other defences are medium.

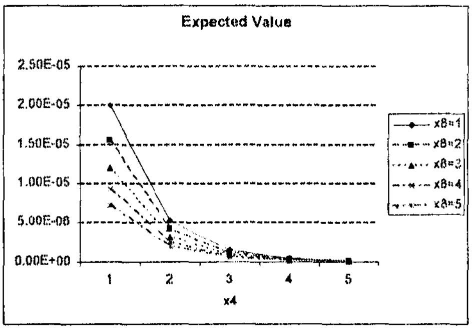


Figure C.13: Expected value of Human root cause at different levels of Safety Culture, with reference to the level of Op. Interaction

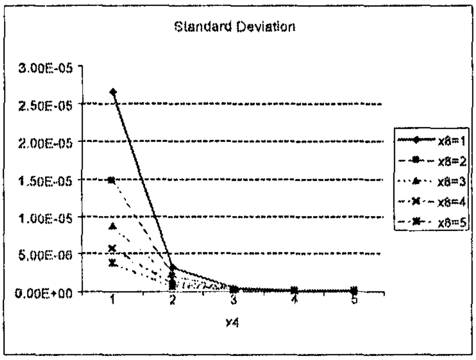


Figure C.14: Standard deviation of Human root cause at different levels of Safety Culture, with reference to the level of Op. Interaction

Safety Culture by one is

$$I_4(x_2,x_4,x_7,x_8) = \left(\frac{\phi_2(x_4+1)}{\phi_2(x_4)}\right)^{x_2-3} \phi_4\phi_{47}^{x_7-3}\phi_{48}^{x_8-3}$$

and the proportion by which r_2 changes by modifying the level of Operator Interaction by one is

$$I_8(x_2,x_7,x_8) = \phi_8(x_2,x_7)\phi_{48}^{x_4-3}$$

The common term ϕ_{48} implies a symmetric dependence between Safety Culture and Op. Interaction. The two defences exhibit a compensating effect ($\phi_{48} > 1$), implying that enhancing the

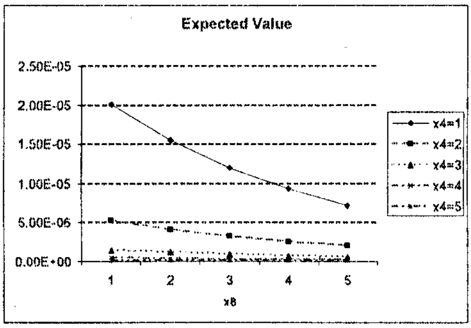


Figure C.15: Mean of Human root cause at different levels of Op. Interaction, with reference to the level of Safety Culture

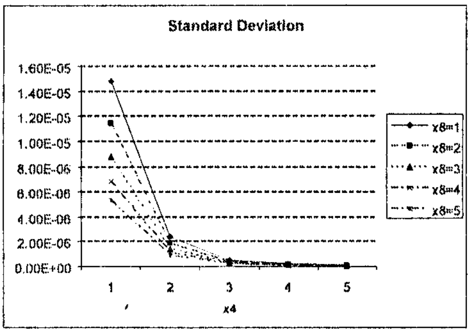


Figure C.16: Standard deviation of Human root cause at different levels of Op. Interaction, with reference to the level of Safety Culture

defence of the one defence becomes more effective when the level of the other defence is low. As before, the effect is demonstrated in Figures C.13 and C.14, C.15 and C.16.

Threshold dependence of Environmental Control on Safety Culture and Understanding The defence of Env. Control is threshold dependent on Safety Culture and Understanding. This fact implies that the influence of Env. Control depends on classes of configurations of the system across Safety Culture and Understanding. It is

$$I_2(x_4,x_7,x_8) = \left(\frac{\phi_8(x_2+1)}{\phi_8(x_2)}\right)^{x_8-3}\phi_2(x_4,x_7)$$

Thus, the proportion of decrease in r_2 induced by changing the level of Env. Control by one is a stepwise function defined over Ω^2, where Ω is the state-space of x_4 (level of Env. Control), and x_7 (level of Understanding). Figure C.17 is a plot of the proportion of decrease induced in $E[r_2]$ by modifying the level of Env. Control by one, with reference to the levels of Safety Culture and Understanding. A higher level across Safety Culture and Understanding weakens the effect of improving Env. Control in the system (higher proportion of decrease).

Due to the threshold dependency of Env. Control on Safety Culture and Understanding, the impact of the threshold counterparts is independent of the level of Env. Control for moderate modifications. This effect is illustrated in Figure C.19, which includes plots of the proportion of decrease induced in $E[r_2]$ by modifying the level of Safety Culture and Understanding by one, with reference to the level of Env. Control. It may be seen that for drastic changes and for

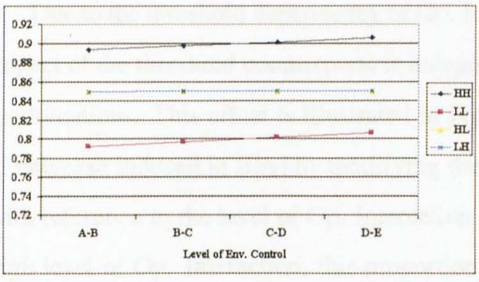


Figure C.17: Proportion of decrease in $E[r_2]$ by modifying Env. Control, for high (H) and low (L) levels of S. Culture and Understanding

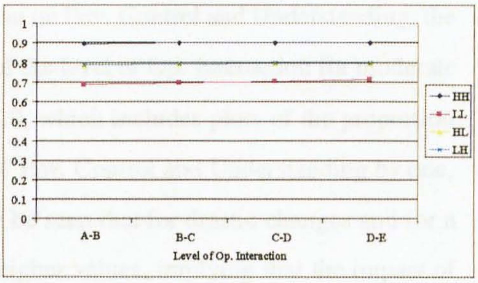


Figure C.18: Proportion of decrease in $E[r_2]$ by modifying Operator Interaction, for high (H) and low (L) levels of Env. Control and Understanding

a high level of Env. Control, this proportion takes higher values, implying that the impact of Safety Culture and Understanding weakens.

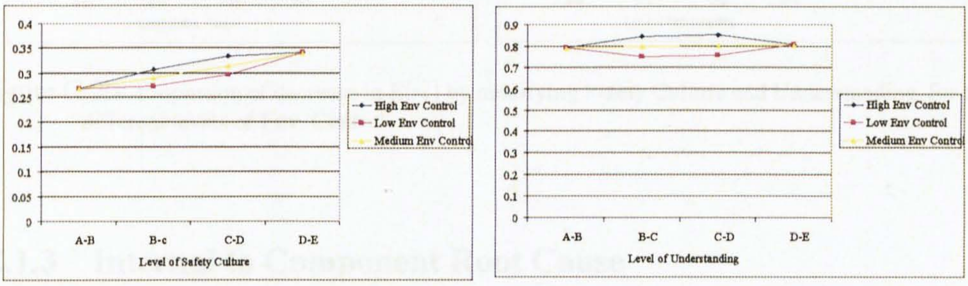


Figure C.19: Proportion of decrease in $E[r_2]$ by modifying Safety Culture and Understanding, for the different levels of Env. Control

Threshold dependency of Operator Interaction on Env. Control and Understanding The defence of Op. Interaction is threshold dependent on Env. Control and Understanding. This fact implies that the influence of Op. Interaction depends on different classes of configurations of the system across Env. Control and Understanding. It is

$$I_8(x_2,x_7,x_8) = \phi_8(x_2,x_7)\phi_{48}^{x_4-3}$$

Figure C.18 is a plot of the proportion of decrease induced in $E[r_2]$ by modifying the level of Op. Interaction by one, with reference to the levels of Env. Control and Understanding. A higher level across Env. Control and Understanding weakens the effect of improving Op. Interaction in the system (higher proportion of decrease).

Due to the threshold dependency of Op. Interaction on Env. Control and Understanding, the impact of the threshold counterparts is independent of the level of Op. Interaction for moderate modifications. This effect is illustrated in Figure C.20, which includes plots of the proportion of decrease induced in $E[r_2]$ by modifying the level of Env. Control and Understanding by one, with reference to the level of Op. Interaction. It may be seen that for drastic changes and for a high level of Op. Interaction, this proportion takes higher values, implying that the impact of Safety Culture and Understanding weakens.

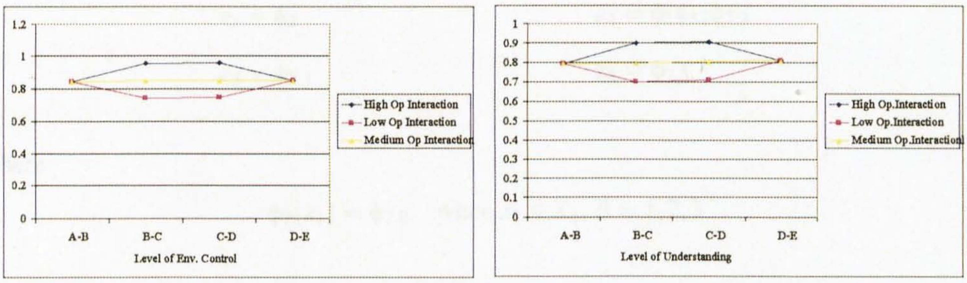


Figure C.20: Proportion of decrease in $E[r_2]$ by modifying Safety Culture and Understanding, for the different levels of Env. Control

C.1.3 Internal to Component Root Cause

The rate of system failures due to the Internal to Component root cause is denoted with r_3. The defences that are targeted against the occurrence of this type of failures are Environmental Testing (D_1), Analysis (D_3), and, Understanding (D_7). The functional interactions existing in the defence domain are:

- Analysis (D_3) and Understanding (D_7) are functionally dependent
- Understanding (D_7) is threshold functionally dependent on Env. Testing (D_1)

Consistently with the GS model, the Internal to Component root cause rate r_3 at configuration (x_1, x_3, x_7) is given by

$$r_{3,(x_1,x_3,x_7)} = \phi_1^{x_1-3}\phi_3^{x_3-3}\phi_7(x_1)^{x_7-3}\phi_{37}^{(x_3-3)(x_7-3)} r_{3,(3,3,3,3)} \tag{C.7}$$

where $x_1, x_3, x_7 = 1, \ldots, 5$.

Determination of subjective distributions

Performing uncertainty analysis on Model (C.7) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the Internal to Component part of the questionnaire, $n = 1,...,6$. The elicitation variables are

$$\begin{aligned} e_1 &= r_{3,(3,3,3)} & e_2 &= \phi_1 \\ e_3 &= \phi_3 & e_4 &= \phi_3\phi_{37}\phi_{7,2} \\ e_5 &= \phi_{7,1} & e_6 &= \phi_{7,3} \end{aligned}$$

where

$$\phi_7(x_1) = \phi_{7,\theta} \quad \text{when } x_1 \in X_\theta,\ \theta = 1,2,3$$

Base rate The rate variable $r_{3,(3,3,3)}$ is gamma distributed. Thus, the prior distribution of e_1 is approximated by a gamma distribution, and

$$r_{3,(3,3,3)} \sim G(a,b)$$

Proportion random variables Elicitation variables e_2 and e_3 coincide with proportion variables ϕ_1 and ϕ_3. Let $e_n \sim \Lambda\left(\mu_n,\sigma_n^2\right)$ for $n = 2,3$ be the fitted distributions. Then

$$\phi_1 \sim \Lambda\left(\mu_2,\sigma_2^2\right) \quad \text{and} \quad \phi_3 \sim \Lambda\left(\mu_3,\sigma_3^2\right)$$

Piecewise proportion functions Elicitation variables e_n for $n = 5,6$ coincide with proportion variables $\phi_{7,1}$ and $\phi_{7,3}$ respectively. Let $e_n \sim \Lambda\left(\mu_n,\sigma_n^2\right)$ for $n = 5,6$ be the fitted distributions. It is

$$\phi_{7,1} \sim \Lambda\left(\mu_5,\sigma_5^2\right) \quad \text{and} \quad \phi_{7,3} \sim \Lambda\left(\mu_6,\sigma_6^2\right)$$

Due to the symmetric form of $\phi_7(x_1)$, it is

$$\phi_{7,2} = \left(\phi_{7,1}\cdot\phi_{7,3}\right)^{\frac{1}{2}} \quad \text{so} \quad \phi_{7,2} \sim \Lambda\left(\frac{1}{2}(\mu_5+\mu_6), \frac{1}{4}(\sigma_5^2+\sigma_6^2)\right)$$

Cross-term Variable e_4 is lognormally distributed as a product of independent lognormally distributed variables. Let $e_4 \sim \Lambda\left(\mu_4, \sigma_4^2\right)$. After taking the logarithms, we have

$$\ln\phi_{37} = \ln e_4 - \ln\phi_3 - \ln\phi_7(M) = \ln e_4 - \ln e_3 - \frac{1}{2}(\ln e_5 + \ln e_6)$$

Let $w = \ln e_4 - \ln e_3$ and $z = \ln e_5 + \ln e_6$, so that

$$\ln\phi_{37} = w - \frac{1}{2}z \tag{C.8}$$

where $w \sim N\left(\mu_w, \sigma_w^2\right)$ and $z \sim N\left(\mu_z, \sigma_z^2\right)$. Variable transformation techniques yield $\mu_w = \mu_4 - \mu_3$ and $\sigma_w^2 = \sigma_4^2 + \sigma_3^2 - 2cov(\ln e_4, \ln e_3)$. But

$$cov(\ln e_4, \ln e_3) = cov(\ln\phi_3, \ln\phi_3 + \ln\phi_{37} + \ln\phi_7(M)) = \sigma_3^2$$

therefore $w \sim N\left(\mu_4 - \mu_3, \sigma_4^2 - \sigma_3^2\right)$. Similarly, $\mu_z = \mu_5 + \mu_6$ and $\sigma_z^2 = \sigma_5^2 + \sigma_6^2$.

From Relationship (C.8) we have $\ln\phi_{37} \sim N(m_{37}, s_{37})$ where $m_{37} = \mu_4 - \mu_3 - \frac{1}{2}(\mu_5 + \mu_6)$ and $s_{37}^2 = \sigma_w^2 + \frac{1}{4}\sigma_z^2 - cov(z, w)$. But

$$cov(z, w) = cov(\ln\phi_{7,1} + \phi_{7,3}, \ln\phi_{37} + \frac{1}{2}\ln\phi_{7,1} + \frac{1}{2}\phi_{7,3}) = \frac{1}{2}\sigma_5^2 + \frac{1}{2}\sigma_6^2$$

giving

$$s_{37}^2 = \sigma_4^2 - \sigma_3^2 + \frac{1}{4}(\sigma_5^2 + \sigma_6^2) - \frac{1}{2}(\sigma_5^2 + \sigma_6^2) = \sigma_4^2 - \sigma_3^2 - \frac{1}{4}(\sigma_5^2 + \sigma_6^2)$$

Condition In agreement with the fundamental assumption that the defence of the system does not become worse as a result of increasing the levels of defences, it needs to hold:

$$0 < \phi_3\phi_{37}^{x_7-3}, \phi_7(x_1)\phi_{37}^{x_3-3} < 1 \quad \text{for every } x_1, x_4, x_7 = 1, \ldots, 5 \tag{C.9}$$

Adjustments Let $X = \phi_3\phi_{37}^{x_7-3}$, for given $x_7 \in \{1, \ldots, 5\}$ and $Y = \phi_7(x_1)\phi_{37}^{x_3-3} < 1$, for given $x_1, x_3 \in \{1, \ldots, 5\}$. R.v.'s X and Y are lognormally distributed, as products of independent lognormally distributed variables. The distributions on X and Y are determined analytically based on the distributions on $\phi_3, \phi_7(x_1), \phi_{37}$ are known, i.e., $X \sim f_X(x \mid \phi_3, \phi_{37})$ and $Y \sim f_Y(y \mid \phi_7(x_1), \phi_{37})$. Let $v_{p_i,x}$ be the $p_i \cdot 100\%$ percentile of X and $v_{p_i,y}$ be the $p_i \cdot 100\%$ percentile of Y, where $p_1 = 0.05$, $p_2 = 0.5$ and $p_3 = 0.95$, viz.

$$\int_0^{v_{p_i,x}} f_X(x)\mathrm{d}x = F_X(v_{p_i,x}) = p_i \Leftrightarrow v_{p_i} = F_X^{-1}(p_i)$$

and

$$\int_0^{v_{p_i,xy}} f_Y(y)\mathrm{d}y = F_Y(v_{p_i,y}) = p_i \Leftrightarrow v_{p_i} = F_X^{-1}(p_i)$$

Based on the Expert's assessments, one finds that $v_{p_i,x} > 1$ and $v_{p_i,y} > 1$ for $x_3, x_7 = 4,5$ and $i = 2,3$. Thus, Conditions (C.9) are violated, and appropriate adjustments need to be made.

In order to overcome the aforementioned inconsistency, the prior on ϕ_{37}, denoted by f_{37}, is tuned to $f_{47}*$ so that the conditions are not violated. Let $f_{37} := \Lambda(m_{37}, s_{37})$ and $f_{37}* := \Lambda(m^*_{37}, s^*_{37})$. The task reduces to determining parameters m^*_{37} and s^*_{37}, according to the following minimisation problem:

$$\text{minimise } \frac{1}{3}\sum_{i=1}^{3}\left(F_{37}^{-1}(p_i \mid m_{37}, s_{37}) - F_{37}^{*-1}(p_i \mid m^*_{37}, s^*_{37})\right)^2$$

subject to

$$F_X^{-1}(v_{p,x} \mid m^*_{37}, s^*_{37}) < 1, \quad \text{for } p = 0.95, x_7 = 4,5$$

$$F_Y^{-1}(v_{p,y} \mid m^*_{37}, s^*_{37}) < 1, \quad \text{for } p = 0.95, x_3 = 4,5$$

$$s^*_{37} > 0$$

The value of the objective function corresponds to the minimum squared error (MSE) of the adjustments applied. For the re-determination of f_{37} it is $MSE = 0.05$.

Results The parameters and the first two moments of the expert's distributions are given in Table C.3.

Extrapolation of Uncertainty

Using Model (C.7), the uncertainty distribution on r_3 can be determined at any configuration (x_1, x_3, x_7). Information on the mean and st. deviation of r_3 for particular defence configuration vectors are given in Figures C.21 and C.22.

Table C.3: Parameters of subjective distributions related to the Internal root cause

	r
a b	1.1516 1E+06
E[r] Var[r]	1.097E-06 1.046E-012

	ϕ_1	ϕ_3	ϕ_{37}
μ σ	-0.511 0.094	-0.355 0.100	0.094 0.010
$E[\phi]$ $Var[\phi]$	0.60 0.003	0.70 0.005	1.10 0.0001

	ϕ_7		
x_1	Low	Medium	High
μ σ	-0.696 0.297	-0.528 0.156	-0.361 0.095
$E[\phi]$ $Var[\phi]$	0.52 0.025	0.60 0.009	0.70 0.004

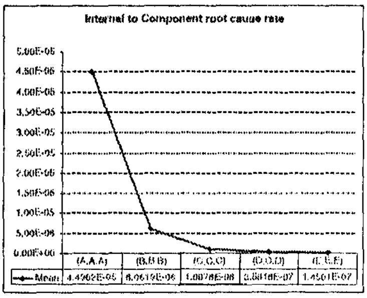


Figure C.21: Expected value of Internal to Component Root Cause rate at particular configuration vectors

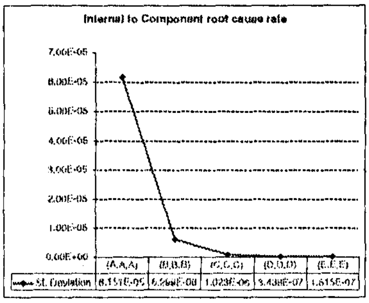


Figure C.22: Standard deviation of Internal to Component Root Cause rate at particular configuration vectors

Functional dependence between Analysis and Understanding The proportion by which r_3 changes by modifying the level of Analysis by one is

$$I_3(x_7) = \phi_3 \phi_{37}^{x_7 - 3}$$

and, the proportion by which r_3 changes, by modifying the level of Understanding by one is

$$I_7(x_1, x_3) = \phi_7(x_1) \phi_{37}^{x_3 - 3}$$

The common term ϕ_{37} entails a symmetric dependency between Analysis and Understanding, which implies that the influence of Analysis depends on the level of Understanding, and vice versa.

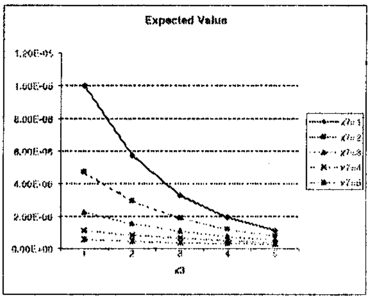


Figure C.23: Expected value of Internal to Component root cause at different levels of Analysis, with reference to the level of Understanding

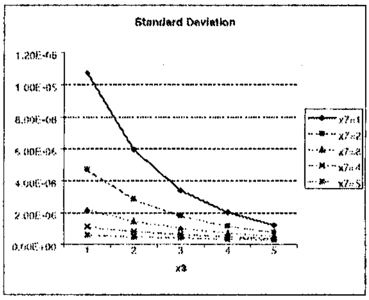


Figure C.24: Standard deviation of Internal to Component root cause at different levels of Analysis, with reference to the level of Understanding

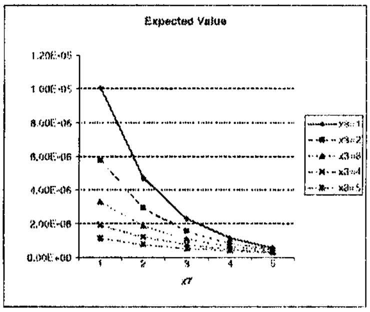


Figure C.25: Expected value of Internal to Component root cause at different levels of Understanding, with reference to the level of Analysis

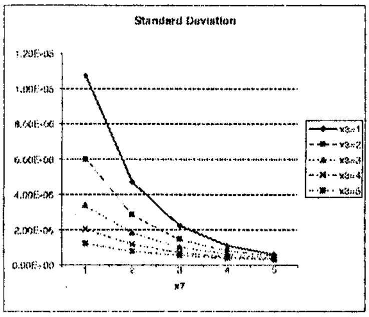


Figure C.26: Standard deviation of Internal to Component root cause at different levels of Understanding, with reference to the level of Analysis

The two defences exhibit a compensating effect ($\phi_{37} > 1$), implying that enhancing the defence of one becomes more effective when the level of the other is low. Figures C.23 and C.24 illustrate the changes in the mean and standard deviation of r_3 when modifying Analysis with reference to the different levels of Understanding, whilst keeping the level of Env. Testing fixed at the medium level. As the level of Understanding increases, the interaction between $\xi(x_7x_8)$ and x_7 decelerates, thus the influence of Analysis on the Internal to Component root cause rate weakens. Similar conclusions may be drawn when modifying Understanding with reference to the different levels of Analysis, whilst keeping the rest defences fixed at the medium level (Figures C.25 and C.26).

Threshold dependence of Understanding on Env. Testing The proportion of decrease of r_3 induced by changing the level of Understanding by one level is

$$I_7(x_1,x_3)=\phi_7(x_1)\phi_{37}^{x_3-3}$$

which is a stepwise function defined over Ω, where Ω is the state-space of x_1 (level of Env. Testing). This implies that the influence of Understanding depends on classes of configuration of the system across Env. Testing. Figure C.27 is a plot of the proportion of decrease induced in $E[r_3]$ by modifying the level of Understanding by one, with reference to the level of Env. Testing. A higher level across Env. Testing weakens the effect of improving Env. Control in the system (higher proportion of decrease).

Due to the threshold dependency of Understanding on Env. Control, the impact of the threshold counterparts is independent of the level of Env. Control for moderate modifications

$$I_1(x_1,x_7)=\left(\frac{\phi_7(x_1+1)}{\phi_7(x_1)}\right)^{x_7-3}\phi_1$$

This effect is illustrated in Figure C.28, which includes plots of the proportion of decrease induced in $E[r_3]$ by modifying the level of Env. Testing by one, with reference to the level of Understanding. It may be seen that for drastic changes and for a high level of Understanding, this proportion takes higher values, implying that the impact of Env. Testing weakens.

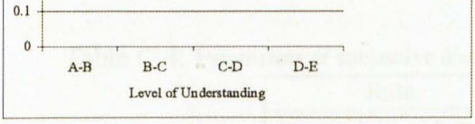


Figure C.27: Proportion of decrease in $E[r_3]$ by modifying Understanding

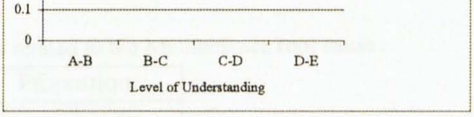


Figure C.28: Proportion of decrease in $E[r_3]$ by modifying Env. Testing

C.1.4 Maintenance Root Cause

The rate of system failures due to the Maintenance root cause is denoted by r_4. The defence that is targeted against the occurrence of this type of failures is Safety Culture (D_4). Consistently with the GS model, the Maintenance root cause rate r_3 at configuration (x_1, x_3, x_7) is given by

$$r_{4,x_4} = \phi_4^{x_4-3} r_{4,3}, \quad x_4 = 1, \ldots, 5 \tag{C.10}$$

Determination of subjective distributions

Performing uncertainty analysis on Model (C.10) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the Internal to Component part of the questionnaire, $n = 1, 2$. The elicitation variables are

$$e_1 = r_{4,3} \quad \text{and} \quad e_2 = \phi_4$$

Base rate The rate variable $r_{4,3}$ is gamma distributed. Thus, the prior distribution of e_1 is approximated by a gamma distribution, and

$$r_{4,3} \sim G(a, b)$$

Proportion random variables Elicitation variable e_2 coincides with the proportion variable ϕ_4. Thus the prior distribution of e_2 is approximated by a lognormal distribution, and

$$\phi_4 \sim \Lambda\left(\mu, \sigma^2\right)$$

Results The parameters and the first two moments of the expert's distributions are given in Table C.4.

Table C.4: Parameters of subjective distributions related to the Maintenance root cause

Rate		Proportion	
	r		ϕ_4
a	9.35	μ	-1.6
b	$1.5 \cdot 10^{-7}$	σ	0.4647
$E[r]$	$6.22 \cdot 10^{-7}$	$E[\phi_4]$	0.225
$Var[r]$	$4.14 \cdot 10^{-14}$	$Var[\phi_4]$	0.0122

Extrapolation of Uncertainty

Using Model (C.10), the uncertainty distribution on r_4 can be determined at any configuration (x_4), for $x_4 = 1,...,5$. Information on the mean and st. deviation of r_4 for particular defence configuration vectors are given in Figures C.29 and C.30.

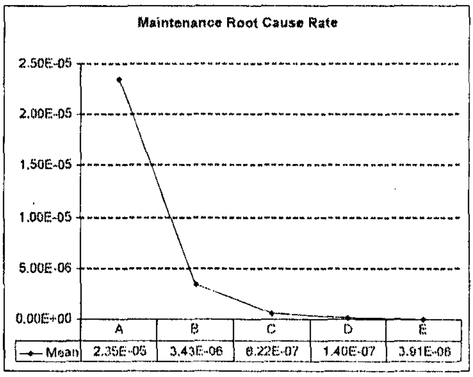


Figure C.29: Expected value of Maintenance Root Cause rate at particular configuration vectors

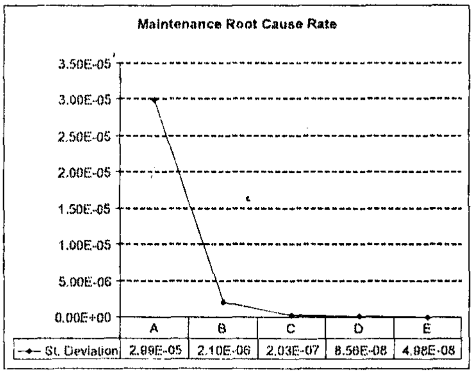


Figure C.30: Standard deviation of Maintenance Root Cause rate at particular configuration vectors

C.1.5 Procedures Root Cause

The rate of system failures due to the Procedures root cause is denoted by r_5. The defences that are targeted against the occurrence of this type of failures are Analysis (D_3), Understanding (D_7), and, Operator Interaction (D_8). The functional interactions existing in the defence domain are:

- Analysis (D_3) is functionally dependent on Understanding (D_7)
- Op. Interaction (D_8) is threshold functionally dependent on Analysis (D_3) and Understanding (D_7)

Consistently with the GS model, the Procedures root cause rate r_5 at configuration (x_1,x_3,x_7) is given by

$$r_{5:(x_3,x_7,x_8)} = \phi_3^{x_3-3}\phi_7^{x_7-3}\phi_8(x_3,x_7)^{x_8-3}\phi_{37}^{(x_7-3)(x_3-3)}r_{5:(3,3,3)} \qquad \text{(C.11)}$$

where $x_3,x_7,x_8 \in \{1,...,5\}$.

Determination of subjective distributions

Performing uncertainty analysis on Model (C.11) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the Procedures part of the questionnaire ($n = 1,...,8$). The elicitation variables are

$$
\begin{array}{ll}
e_1 = r_{5,(3,3,3)} & e_2 = \phi_3 \\
e_3 = \phi_7 & e_4 = \phi_3 \phi_{37} \phi_7 \\
e_5 = \phi_{8,1} \phi_{8,1} & e_6 = \phi_8(x_3, x_7) \ x_3 \in X_1, x_7 \in X_3 \\
e_7 = \phi_8(x_3, x_7), \ x_3 \in X_3, x_7 \in X_1 & e_8 = \phi_{8,3} \phi_{8,3}
\end{array}
$$

where $\phi_8(x) = \phi_{8,\theta}$ when $x \in X_\theta$ ($\theta = 1,2,3$).

Base rate The rate variable $r_{5,(3,3,3)}$ is gamma distributed. Thus, the prior distribution of e_1 is approximated by a gamma distribution, viz.

$$r_{3,(3,3,3,3)} \sim G(a,b)$$

Proportion random variables Elicitation variables e_2 and e_3 coincide with proportion variables ϕ_3 and ϕ_7. Let $e_n \sim \Lambda\left(\mu_n, \sigma_n^2\right)$ for $n = 2,3$ be the fitted distributions. Then

$$\phi_3 \sim \Lambda\left(\mu_2, \sigma_2^2\right) \quad \text{and} \quad \phi_7 \sim \Lambda\left(\mu_3, \sigma_3^2\right)$$

Piecewise proportion functions Elicitation variables e_n for $n = 5,...,8$ are lognormally distributed, as products of independent lognormally distributed random variables. Let $e_n \sim \Lambda\left(\mu_n, \sigma_n^2\right)$ be the fitted distributions. It is

$$\phi_{8,1} = (e_5)^{\frac{1}{2}} \quad \text{so} \quad \phi_{8,1} \sim \Lambda\left(\frac{1}{2}\mu_5, \frac{1}{4}\sigma_5^2\right)$$

$$\phi_{8,3} = (e_6)^{\frac{1}{2}} \quad \text{so} \quad \phi_{8,3} \sim \Lambda\left(\frac{1}{2}\mu_6, \frac{1}{4}\sigma_6^2\right)$$

and, based on the symmetry assumption, one gets

$$\phi_{8,2} = (\phi_{8,1} \cdot \phi_{8,3})^{\frac{1}{2}} \quad \text{so} \quad \phi_{8,2} \sim \Lambda\left(\frac{1}{4}(\mu_5 + \mu_6), \frac{1}{16}(\sigma_5^2 + \sigma_6^2)\right)$$

Cross-term Variable e_4 is lognormally distributed as a product of independent lognormally distributed variables. Let $e_4 \sim \Lambda\left(\mu_4, \sigma_4^2\right)$. After taking the logarithms, we have

$$\ln \phi_{37} = \ln e_4 - \ln \phi_3 - \ln \phi_7 = \ln e_4 - (\ln e_2 + \ln e_3)$$

Let $z = \ln e_2 + \ln e_3$, so that

$$\ln \phi_{37} = \ln e_4 - z \quad , \tag{C.12}$$

It is $z \sim N\left(\mu_z, \sigma_z^2\right)$ with $\mu_z = \mu_2 + \mu_3$ and $\sigma_z^2 = \sigma_2^2 + \sigma_3^2$. Note that

$$cov(\ln e_2, \ln e_3) = cov(\ln \phi_3, \ln \phi_7) = 0$$

From Relationship (C.12) we have $\ln \phi_{37} \sim N(m_{37}, s_{37})$ with $m_{37} = \mu_4 - \mu_2 - \mu_3$ and $s_{37}^2 = \sigma_z^2 + \sigma_4^2 + 2cov(z, \ln e_4)$. But

$$\begin{aligned} cov(z, \ln e_4) &= cov(\ln \phi_3 + \ln \phi_7, \ln \phi_3 + \ln \phi_7 + \ln \phi_{37}) \\ &= var[\ln \phi_3] + var[\ln \phi_7] = \sigma_2^2 + \sigma_3^2 \end{aligned}$$

giving

$$\ln \phi_{37} \sim N\left(\mu_4 - \mu_2 - \mu_3, \sigma_4^2 - \sigma_2^2 - \sigma_3^2\right)$$

Elicitation variables e_6, e_7 are used as checks the symmetry assumption

$$\phi_8(x_3, x_7) = \phi_8(x_3)\phi_8(x_7)$$

Within this example, the expert's assessments meet this condition.

Condition In agreement with the fundamental assumption that the vulnerability of the system does not become worse as a result of enhancing defences, it needs to hold:

$$0 < \phi_3 \phi_{37}^{x_7 - 3}, \phi_7 \phi_{37}^{x_3 - 3} < 1 \quad \text{for every } x_3, x_7 = 1, \ldots, 5 \tag{C.13}$$

Adjustments Let $X = \phi_3 \phi_{37}^{x_7 - 3}$, for given $x_7 \in \{1, \ldots, 5\}$, and let $Y = \phi_7 \phi_{37}^{x_3 - 3}$, for given $x_3 \in \{1, \ldots, 5\}$. R.v.'s X and Y are lognormally distributed, as products of independent lognormally distributed variables. The distributions on X and Y are determined analytically based on the distributions of $\phi_3, \phi_7, \phi_{37}$, i.e., $X \sim f_X(x \mid \phi_3, \phi_{37})$ and $Y \sim f_Y(y \mid \phi_7, \phi_{37})$. Let $v_{p_i,x}$ be the $p_i \cdot 100\%$ percentile of X and $v_{p_i,y}$ be the $p_i \cdot 100\%$ percentile of Y, where $p_1 = 0.05$, $p_2 = 0.5$ and $p_3 = 0.95$, viz.

$$\int_0^{v_{p_i,x}} f_X(x)\mathrm{d}x = F_X(v_{p_i,x}) = p_i \Leftrightarrow v_{p_i} = F_X^{-1}(p_i)$$

and

$$\int_0^{v_{p_i,xy}} f_Y(y)\mathrm{d}y = F_Y(v_{p_i,y}) = p_i \Leftrightarrow v_{p_i} = F_X^{-1}(p_i)$$

Based on the Expert's assessments, one finds that $v_{p_i,x} > 1$ for $x_7 = 5$ and $v_{p_i,y} > 1$ for $x_3 = 5$ and $i = 3$. Thus, Conditions (C.13) are violated, and appropriate adjustments need to be made.

In order to overcome the aforementioned inconsistency, the prior on ϕ_{37} is tuned to f^*_{47} so that Conditions (C.13) are not violated. Let $f^*_{37} := \Lambda(m^*_{37}, s^*_{37})$ be the adjusted distribution. The task reduces to determining parameters m^*_{37} and s^*_{37}, according to the following minimisation problem:

$$\text{minimise } \frac{1}{3}\sum_{i=1}^{3}\left(F_{37}^{-1}(p_i \mid m_{37}, s_{37}) - F_{37}^{*-1}(p_i \mid m^*_{37}, s^*_{37})\right)^2$$

subject to

$$F_X^{-1}(v_{p,x} \mid m^*_{37}, s^*_{37}) < 1, \quad \text{for } p = 0.95, x_7 = 5$$

$$F_Y^{-1}(v_{p,y} \mid m^*_{37}, s^*_{37}) < 1, \quad \text{for } p = 0.95, x_3 = 5$$

$$s^*_{37} > 0$$

The value of the objective function corresponds to the minimum squared error (MSE) of the adjustments applied. For the re-determination of f_{37} it is $MSE = 0.08$.

Results The parameters and the first two moments of the expert's distributions are given in Table C.5.

Extrapolation of Uncertainty

Using Model (C.11), the uncertainty distribution on r_5 can be determined at any configuration (x_3, x_7, x_8), for $x_i = 1, \ldots, 5$. Information on the mean and st. deviation of r_5 for particular

Table C.5: Parameters of subjective distributions related to the Procedures root cause rate

	r
a b	9.35 1.29E+07
E[r] Var[r]	7.36E-07 5.63E-014

	ϕ_3	ϕ_7	ϕ_{37}
μ σ	-0.511 0.094	-0.355 0.100	0.094 0.010
$E[\phi]$ $Var[\phi]$	0.60 0.003	0.70 0.005	1.10 0.0001

	ϕ_8		
θ	1	2	3
μ σ	-0.18 0.08	-0.12 0.04	-0.05 0.02
$E[\phi]$ $Var[\phi]$	0.84 0.0050	0.89 0.0015	0.95 0.0002

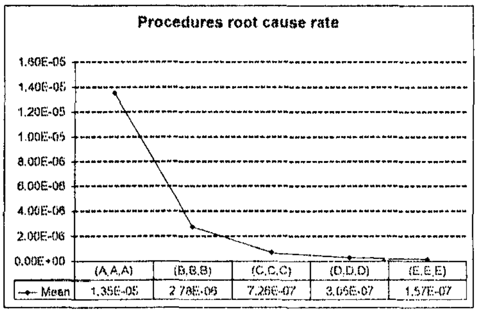


Figure C.31: Expected value of Procedures Root Cause rate at particular configuration vectors

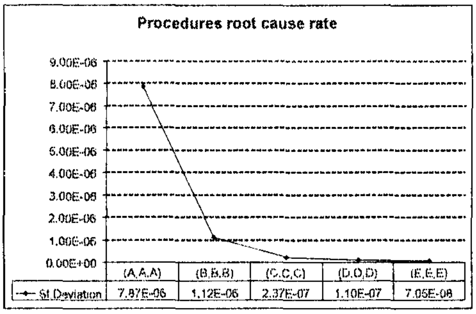


Figure C.32: Standard deviation of Procedures Root Cause rate at particular configuration vectors

defence configuration vectors are given in Figures C.31 and C.32.

Functional dependence between Analysis and Understanding The proportion by which r_5 changes by modifying the level of Analysis by one is

$$I_3(x_3,x_7,x_8) = \phi_3\phi_{37}^{x_7-3}\left(\frac{\phi_8(x_3+1)}{\phi_8(x_3)}\right)^{x_8-3}$$

and, the proportion by which r_5 changes, by modifying the level of Understanding by one is

$$I_7(x_3,x_7,x_8) = \phi_7\phi_{37}^{x_3-3}\left(\frac{\phi_8(x_7+1)}{\phi_8(x_7)}\right)^{x_8-3}$$

The common term ϕ_{37} implies a symmetric dependency between Analysis and Understanding.

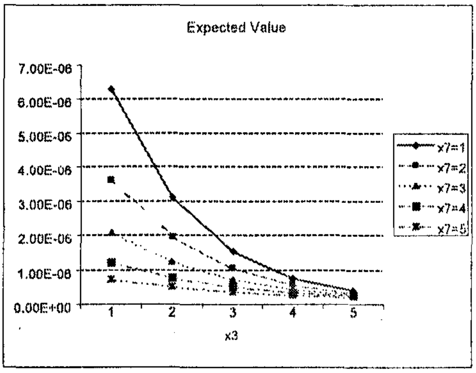


Figure C.33: Expected value of Internal to Component root cause at different levels of Analysis, with reference to the level of Understanding

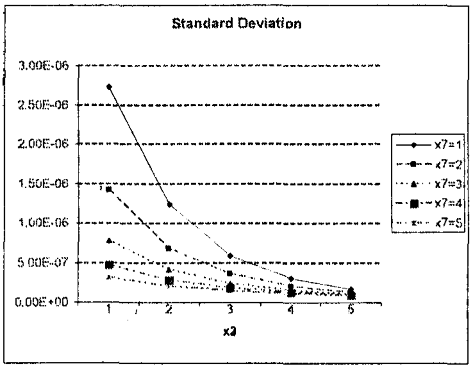


Figure C.34: Standard deviation of Internal to Component root cause at different levels of Analysis, with reference to the level of Understanding

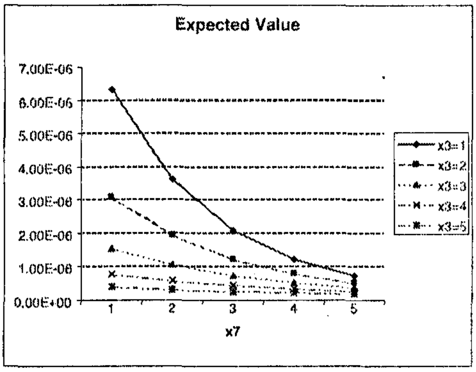


Figure C.35: Expected value of Internal to Component root cause at different levels of Understanding, with reference to the level of Analysis

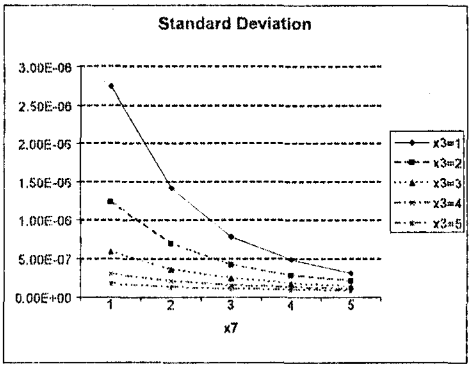


Figure C.36: Standard deviation of Internal to Component root cause at different levels of Understanding, with reference to the level of Analysis

The two defences exhibit a compensating effect ($\phi_{37} > 1$), implying that enhancing the defence of Analysis becomes more effective when the level of Understanding is low, and vice-versa. Figures C.33 and C.34 illustrate the changes in the mean and standard deviation of r_5 when modifying Analysis with reference to the different levels of Understanding, whilst keeping the level of Op. Interaction fixed at the medium level. As the level of Understanding increases, the interaction between $l_3(x_7,x_8)$ and x_7 decelerates, thus the influence of Analysis on the Procedures root cause rate weakens. Similar conclusions may be drawn when modifying Understanding with reference to the different levels of Analysis, whilst keeping Op. Interaction fixed at the medium level (Figures C.35 and C.36).

Threshold dependence of Operator Interaction on Analysis and Understanding The defence of Op. Interaction is threshold dependent on Analysis and Understanding. This fact implies that the influence of the former defence depends on the configuration of the system across the two latter defences. Note that

$$I_8(x_3,x_7) = \phi_8(x_3,x_7)$$

Thus, the proportion of decrease in r_5 induced by changing the level of Op. Interaction by one is a stepwise function defined over $\Omega_3 \times \Omega_7$, where Ω_3 is the state-space of x_3 (level of Analysis), and Ω_7 is the state-space of x_7 (level of Understanding). Figure C.37 is a plot of the proportion of decrease induced in $E[r_5]$ by modifying the level of Op. Interaction by one, with reference to the levels of Analysis and Understanding. A higher level across Analysis and Understanding weakens the effect of improving Op. Interaction in the system (higher proportion of decrease).

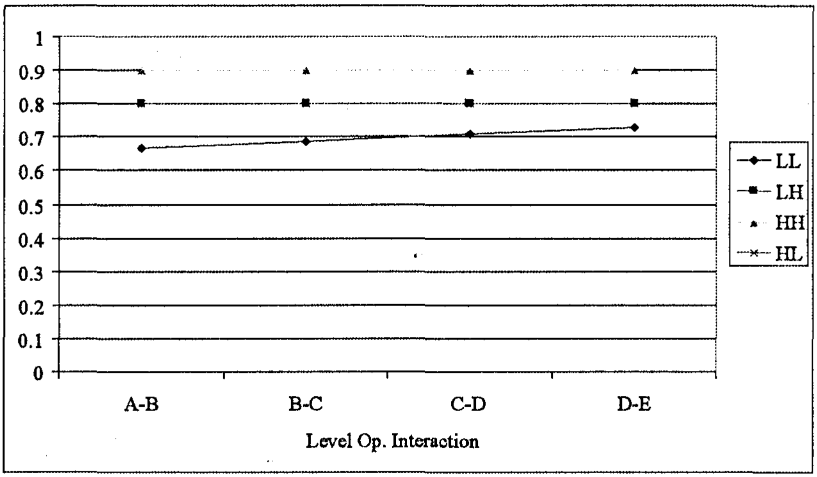


Figure C.37: Proportion of decrease in $E[r_5]$ by modifying Op. Interaction, for the different levels of Analysis and Understanding

Due to the threshold dependency of Op. Interaction on Analysis and Understanding, the impact of the threshold counterparts is independent of the level of Op. Interaction for moderate modifications. This effect is illustrated in Figure C.38, which includes plots of the proportion of decrease induced in $E[r_5]$ by modifying the level of Analysis and Understanding by one, with reference to the level of Op. Interaction. It may be seen that for drastic changes and for a high level of Op. Interaction, this proportion takes higher values, implying that the impact of Analysis and Understanding weakens.

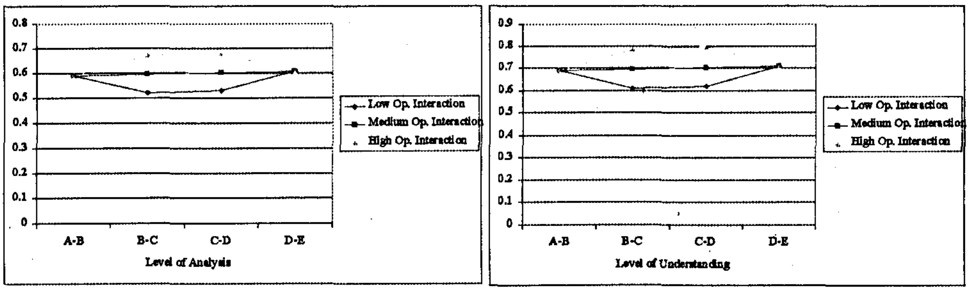


Figure C.38: Proportion of decrease in $E[r_5]$ by modifying Analysis and Understanding, for the different levels of Op. Interaction

C.1.6 External Root Cause

The rate of system failures due to the Maintenance root cause is denoted with r_6. The defences that are targeted against the occurrence of this type of failures are Environmental Control (D_2) and Analysis (D_3). The two defences are functionally independent. Consistently with the GS model, the External Environment root cause rate r_6 at vector configuration (x_2, x_3) is given by

$$r_{6,(x_2,x_3)} = \phi_2^{x_2-3}\phi_3^{x_3-3} r_{6,(3,3)} \tag{C.14}$$

where $x_2, x_3 = 1, ..., 5$.

Determination of subjective distributions

Performing uncertainty analysis on Model (C.14) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the External Environment part of the questionnaire, $n = 1,2,3$. The elicitation variables are

$$e_1 = r_{6,(3,3)} \quad e_2 = \phi_2 \quad e_3 = \phi_3$$

Base rate The rate variable $r_{6,(3,3)}$ is gamma distributed. Thus, the prior distribution of e_1 is approximated by a gamma distribution, and

$$r_{6,(3,3)} \sim G(a,b)$$

Proportion random variables Elicitation variables e_2 and e_3 coincide with the proportion variables ϕ_2 and ϕ_3 respectively. Let $e_n \sim \Lambda\left(\mu_n, \sigma_n^2\right)$ for $n = 2,3$ be the fitted distributions. Then

$$\phi_2 \sim \Lambda\left(\mu_2, \sigma_2^2\right) \quad \text{and} \quad \phi_3 \sim \Lambda\left(\mu_3, \sigma_3^2\right)$$

Results The parameters and the first two moments of the expert's distributions are given in Table C.6.

Table C.6: Parameters of subjective distributions related to the External root cause rate

	r
a	1.15
b	2.1E+06
E[r]	5.5E-07
Var[r]	2.6E-013

	ϕ_2	ϕ_3
μ	-0.2231	-0.6939
σ	0.0716	0.2903
$E[\phi]$	0.8	0.5
$Var[\phi]$	0.00331	0.02389

Extrapolation of Uncertainty

Using Model (C.14), the uncertainty distribution on r_5 can be determined at any configuration vector. Information on the mean and st. deviation of r_4 for particular defence configuration vectors are given in Figures C.39 and C.40.

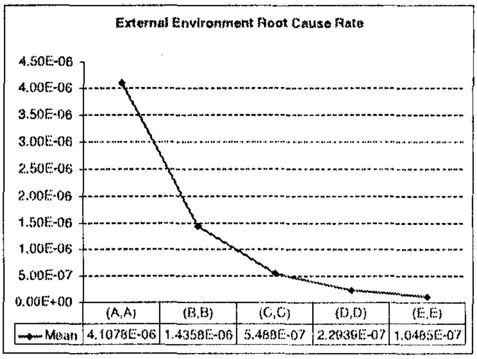


Figure C.39: Expected value of External Environment Root Cause rate at particular configuration vectors

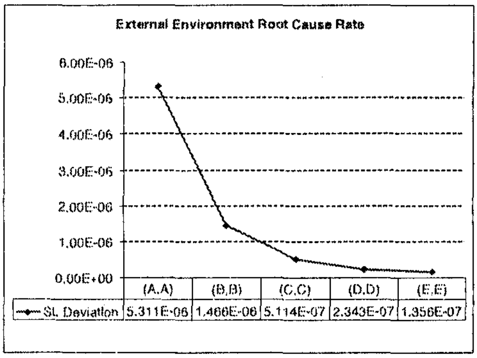


Figure C.40: Standard deviation of External Environment Root Cause rate at particular configuration vectors

C.2 Coupling factor part

C.2.1 Operational Coupling Factor

Elicitation of target variables

The intensity of the Operational coupling conditions in the system is described by a vector of parameters

$$\underline{p_1} = (p_{11}, p_{21}, \dots, p_{61})$$

where

$$p_{i1} = P(\text{CCF through the Operational cf}| \text{ failure due to rc } i)$$

for $i = 1, \dots, 6$. The Operational coupling factor intensity is influenced by the defence of Operator Interaction (D_8). According to the GS model, the Operational coupling factor intensity $\underline{p}_1$ at level x_8 across the defence of Operator Interaction ($x_8 \in \{1, 2, \dots, 5\}$) is given by

$$p_{i1,(x_8)} = \varphi_{i1}^{x_8-3} p_{i1,(3)} \qquad \text{(C.15)}$$

Determination of subjective distributions

Performing uncertainty analysis on Model (C.15) requires the determination of the prior distributions on the model parameters. Question 1 of Section *Ci* of the Questionnaire extracts percentile information on $p_{i1,(3)}$, and, Question 2 extracts information on φ_{i1} ($i = 1, \dots, 6$). We have

$$p_{i1,(3)} \sim B(\gamma_{i1,(3)}, \delta_{i1,(3)})$$

and

$$\varphi_{i1} \sim \Lambda(\mu_{i1}, \sigma_{i1})$$

Results The parameters and the first two moments of the expert's distributions are given in Table C.7.

Table C.7: Parameters of subjective distributions related to the Operational coupling factor

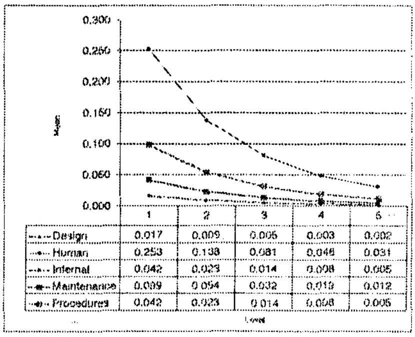
Beta Distributions

	Parameters		Moments	
	γ	δ	Expected	Variance
Design	4.66	861.63	0.005	6.16E-06
Human	24.35	276.55	0.081	2.46E-04
Internal	1.15	83.66	0.014	1.56E-04
Maintenance	5.38	163.52	0.032	1.81E-04
Procedures	1.15	83.66	0.014	1.56E-04

Lognormal Distributions

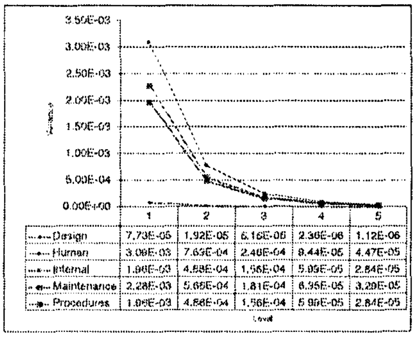
	m	s	Expected	Variance
All causes	-0.5108	0.2465	0.62	2.40E-02

Figures C.41 and C.42 include information on the central moments of the coupling factor intensity $p_{i1,(x_8)}$, associated with the different root cause events and for different Op. Interaction levels x_8.



	1	2	3	4	5
Design	0.017	0.009	0.005	0.003	0.002
Human	0.253	0.138	0.081	0.048	0.031
Internal	0.042	0.023	0.014	0.008	0.005
Maintenance	0.099	0.054	0.032	0.019	0.012
Procedures	0.042	0.023	0.014	0.008	0.005

Figure C.41: Expected value of the Operational coupling factor intensity



	1	2	3	4	5
Design	7.73E-05	1.92E-05	6.16E-06	2.36E-06	1.12E-06
Human	3.08E-03	7.69E-04	2.46E-04	9.44E-05	4.47E-05
Internal	1.96E-03	4.88E-04	1.56E-04	5.99E-05	2.84E-05
Maintenance	2.28E-03	5.65E-04	1.81E-04	6.95E-05	3.29E-05
Procedures	1.96E-03	4.88E-04	1.56E-04	5.99E-05	2.84E-05

Figure C.42: Variance of the Operational coupling factor intensity

C.2.2 Hardware Coupling Factor

Elicitation of target variables

The intensity of the Hardware coupling factor is described by a vector of parameters

$$\underline{p_2} = (p_{12}, p_{22}, ..., p_{62})$$

where

$$p_{i2} = P(\text{CCF through the Hardware cf}|\text{ failure due to rc } i)$$

for $i = 1, ..., 6$. The Hardware coupling factor intensity is influenced by the defences of Analysis (D_3) and Diversity (D_6), with Diversity being threshold functionally dependent on Analysis. According to the geometric scaling model, the Hardware coupling factor intensity $\underline{p_2}$ at configuration (x_3, x_6), where x_k is the level of defence D_k ($x_k = 1, 2, ..., 5$ for $k = 3, 6$) is given by

$$p_{i2,(x_3,x_6)} = \varphi_{3,i2}^{x_3-3} \varphi_{6,i2}^{x_6-3}(x_3) p_{i2,(3)} \tag{C.16}$$

Determination of subjective distributions

Performing uncertainty analysis on Model (C.16) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the *Bi* part of the questionnaire. The elicitation variables are

$$e_1 = p_{i2,(3)} \qquad e_2 = \varphi_{3,i2}$$
$$e_3 = \varphi_{6,i2}(x_3) \;\; x_3 \in X_1 \qquad e_4 = \varphi_{6,i2}(x_3) \;\; x_3 \in X_3$$

Base intensity The intensity variable $p_{i2,(3)}$ is beta distributed. Thus, the prior distribution on e_1 is approximated by a beta distribution, and

$$p_{i2,(3)} \sim B(\gamma_{i2,(3)}, \delta_{i2,(3)})$$

Proportion random variable Elicitation variable e_2 coincides with proportion variable $\varphi_{3,i2}$. Thus, the prior distribution on e_2 is approximated by a lognormal distribution, and

$$\varphi_{3,i2} \sim \Lambda\left(\mu_2, \sigma_n^2\right)$$

Piecewise proportion function The form of the piecewise function is

$$\varphi_{6,i2}(x_3) = \varphi_{6,i2,\theta} \quad \text{when } x_3 \in X_\theta,\ \theta = 1,2,3$$

The elicitation variables e_n for $n = 3,4$ coincide with proportion variables $\varphi_{6,i2,1}$ and $\varphi_{6,i2,3}$ respectively. Let the fitted distributions be

$$\varphi_{6,i2,1} \sim \Lambda\left(\mu_3, \sigma_3^2\right) \quad \text{and} \quad \varphi_{6,i2,3} \sim \Lambda\left(\mu_4, \sigma_4^2\right)$$

Due to the symmetric form of $\varphi_{6,i2}(x_3)$, it is

$$\varphi_{6,i2,2} = \left(\varphi_{6,i2,1} \cdot \varphi_{6,i2,3}\right)^{\frac{1}{2}} \quad \text{so} \quad \varphi_{6,i2,2} \sim \Lambda\left(\frac{1}{2}(\mu_3 + \mu_4), \frac{1}{4}(\sigma_3^2 + \sigma_4^2)\right)$$

Results The parameters and the first two moments of the expert's distributions are given in Table C.8.

Table C.8: Parameters of subjective distributions related to the Hardware coupling factor

p

	Parameters		Moments	
	γ	δ	Expected	Variance
Design	1.1333	81.5740	0.01	1.61E-04
Internal	1.1535	83.6575	0.01	1.56E-04
Maintenance	1.1338	163.5380	0.01	4.13E-05
Procedures	5.3767	163.5175	0.032	1.81E-04
External	1.8475	29.3304	0.06	1.73E-03

φ_3

	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-0.2213	0.0891	0.80	5.16E-03
Internal	-0.2213	0.0891	0.80	5.16E-03
Maintenance	-0.1630	0.0706	0.85	3.62E-03
Procedures	-0.1054	0.0580	0.90	2.73E-03
External	-0.2213	0.0891	0.80	5.16E-03

$\varphi_{6,1}$

	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-1.2042	0.3122	0.31	1.02E-02
Internal	-1.2042	0.3122	0.31	1.02E-02
Maintenance	-0.2231	0.0716	0.80	3.31E-03
Procedures	-0.3603	0.1687	0.71	1.45E-02
External	-0.2243	0.1107	0.80	7.97E-03

$\varphi_{6,3}$

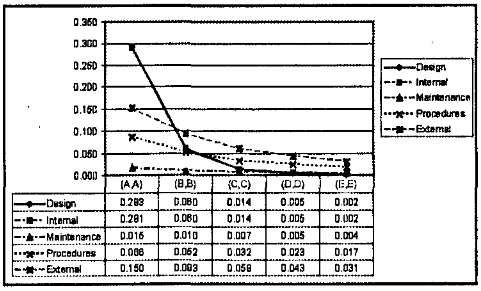
	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-0.9186	0.2592	0.41	1.18E-02
Internal	-0.9186	0.2592	0.41	1.18E-02
Maintenance	-0.1625	0.0676	0.85	3.33E-03
Procedures	-0.2243	0.1107	0.80	7.97E-03
External	-0.1054	0.0329	0.90	8.77E-04

$\varphi_{6,2}$

	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-1.06142	0.2029	0.35	5.24E-03
Internal	-1.06142	0.2029	0.35	5.24E-03
Maintenance	-0.19283	0.0492	0.83	1.66E-03
Procedures	-0.29232	0.1009	0.75	5.76E-03
External	-0.16484	0.0577	0.85	2.41E-03

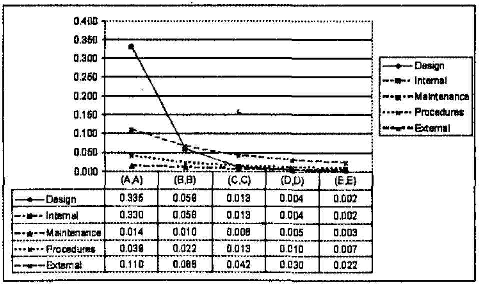
Extrapolation of Uncertainty

Using Model (C.16), the uncertainty distribution on $p_{i2,(x_3,x_6}$ $(i = 1,...,6)$ can be determined for any (x_3,x_6). Figures C.43 and C.44 illustrate the change in mean and standard deviation of the Hardware intensity when the system configuration is modified, in relation to the occurrence of a failure event due to the different root causes. Note that coupling of Human failures via hardware similarity conditions is assessed as insignificant.



	(A,A)	(B,B)	(C,C)	(D,D)	(E,E)
Design	0.293	0.060	0.014	0.005	0.002
Internal	0.291	0.060	0.014	0.005	0.002
Maintenance	0.016	0.010	0.007	0.005	0.004
Procedures	0.086	0.052	0.032	0.023	0.017
External	0.150	0.093	0.059	0.043	0.031

Figure C.43: Expected value of the Hardware coupling factor intensity



	(A,A)	(B,B)	(C,C)	(D,D)	(E,E)
Design	0.335	0.059	0.013	0.004	0.002
Internal	0.330	0.059	0.013	0.004	0.002
Maintenance	0.014	0.010	0.008	0.005	0.003
Procedures	0.039	0.022	0.013	0.010	0.007
External	0.110	0.068	0.042	0.030	0.022

Figure C.44: Standard deviation of the Hardware coupling factor intensity
hardwaremeanrange

Threshold functional dependence of Diversity on Analysis The defence of Diversity is threshold dependent on the level of Analysis. This fact implies that the influence of Diversity differentiates for low, medium and high levels of Analysis. Indeed, the influence of Diversity is mathematically expressed as

$$I_6(x_3) = \varphi_{6,i2}(x_3)$$

which is a piecewise function defined over the state space of x_3, denoted with Ω. Figures C.45 and C.46 portray the central moments of $I_6(x_3)$ for the different levels of Analysis, in relation to the different root causes.

The influence of Analysis is given by

$$I_3(x_6) = \varphi_{3,i2}\left(\frac{\varphi_{6,i2}(x_3+1)}{\varphi_{6,i2}(x_3)}\right)^{x_6-1}$$

For given $x_6 \in \{1,...,5\}$, $I_3(x_6)$ is a random variable with a lognormal distribution.

It is assumed that enhancing the level of Analysis never results in decreasing the protection

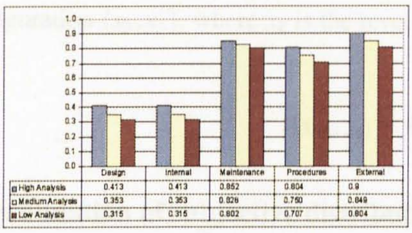


Figure C.45: Expected value of the influence of Diversity $I_6(x_3)$

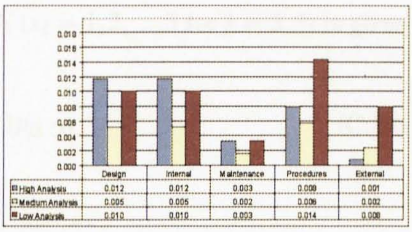


Figure C.46: Variance of the influence of Diversity $I_6(x_3)$

of the system against CCFs. Mathematically expressed, it should hold

$$0 < I_3(x_6) < 1, \quad \text{for every } x_6 \tag{C.17}$$

However, the domain of the lognormal distribution is $[0, +\infty]$, therefore $I_3(x_6)$ is not restricted in the interval $[0, 1]$. In order to avoid falling into conceptual inconsistencies, the p.d.f. on $I_3(x_6)$ is defined as follows:

$$g(x) = \begin{cases} f(x), 0 < x < 1 \\ 1 - F(x), x = 1 \\ 0, \text{ otherwise} \end{cases}$$

C.2.3 Environmental Coupling Factor

Elicitation of target variables

The intensity of the Environmental coupling factor is described by a vector of parameters

$$\underline{p_3} = (p_{13}, p_{23}, \ldots, p_{63})$$

where

$$p_{i3} = P(\text{CCF through the Environmental cf} | \text{ failure due to rc } i)$$

for $i = 1, \ldots, 6$. The Environmental coupling factor intensity is influenced by the defences of Analysis (D_3) and Separation (D_5), with Separation being threshold functionally dependent on Analysis. According to the GS model, the Environmental coupling factor intensity p_3 at configuration (x_3,x_5), where x_k is the level of defence D_k ($x_k = 1,2,...,5$ for $k = 3,5$) is given by

$$p_{i3,(x_3,x_5)} = \varphi_{3,i3}^{x_3-3}\varphi_{5,i3}^{x_5-3}(x_3)p_{i3,(3)} \qquad \text{(C.18)}$$

Determination of subjective distributions

Performing uncertainty analysis on Model (C.18) requires the determination of the prior distributions on the model parameters. Let e_n denote the elicitation variable associated with Question n of the $Ai(i = 1,...,6)$ part of the questionnaire. The elicitation variables are

$$e_1 = p_{i3,(3)} \qquad e_2 = \varphi_{3,i3}$$

$$e_3 = \varphi_{5,i3}(x_3)\ \ x_3 \in X_1 \qquad e_4 = \varphi_{5,i3}(x_3)\ \ x_3 \in X_3$$

Base intensity The intensity variable $p_{i2,(3)}$ is beta distributed. Thus, the prior distribution on e_1 is approximated by a beta distribution, and

$$p_{i3,(3)} \sim B(\gamma_{i3,(3)},\delta_{i3,(3)})$$

Proportion random variable Elicitation variable e_2 coincides with proportion variable $\varphi_{3,i3}$. Thus, the prior distribution on e_2 is approximated by a lognormal distribution, and

$$\varphi_{3,i3} \sim \Lambda\left(\mu_2,\sigma_n^2\right)$$

Piecewise proportion function The form of the piecewise function is

$$\varphi_{5,i3}(x_3) = \varphi_{5,i3,\theta} \quad \text{when } x_3 \in X_\theta,\ \theta = 1,2,3$$

The elicitation variables e_n for $n = 3,4$ coincide with proportion variables $\varphi_{5,i3,1}$ and $\varphi_{5,i3,3}$ respectively. Let $e_n \sim \Lambda\left(\mu_n,\sigma_n^2\right)$ for $n = 3,4$ be the fitted distributions. It is

$$\varphi_{5,i3,1} \sim \Lambda\left(\mu_3,\sigma_3^2\right) \quad \text{and} \quad \varphi_{5,i3,3} \sim \Lambda\left(\mu_4,\sigma_4^2\right)$$

Due to the symmetric form of $\varphi_{5,i3}(x_3)$, it is

$$\varphi_{5,i3,2} = (\varphi_{5,i3,1} \cdot \varphi_{5,i3,3})^{\frac{1}{2}} \quad \text{so} \quad \varphi_{5,i3,2} \sim \Lambda\left(\frac{1}{2}(\mu_3 + \mu_4), \frac{1}{4}(\sigma_3^2 + \sigma_4^2)\right)$$

Results The parameters and the first two moments of the expert's distributions are given in Table C.9.

Table C.9: Parameters of subjective distributions related to the Environmental coupling factor

p

	Parameters		Moments	
	γ	δ	Expected	Variance
Design	0.4665	19.4581	0.02	0.0011
Human	4.4050	98.1728	0.04	0.0004
Internal	4.4050	98.1728	0.04	0.0004
Maintenance	3.8434	885.8014	0.004	4.83E-06
External	10.2417	89.5272	0.10	0.0009

φ_3

	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-0.1061	0.0673	0.90	0.0037
Human	-0.2213	0.0891	0.80	0.0052
Internal	-0.2232	0.0717	0.80	0.0033
Maintenance	-0.0513	0.0251	0.95	0.0006
External	-0.3565	0.0001	0.70	4.97E-09

$\varphi_{5,1}$

	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-0.6889	0.3301	0.53	0.0324
Human	-0.1054	0.0330	0.90	0.0009
Internal	-0.5132	0.2592	0.62	0.0266
Maintenance	-0.1645	0.1015	0.85	0.0075
External	-0.5109	0.2797	0.62	0.0317

$\varphi_{5,3}$

	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-0.1061	0.0673	0.90	0.0037
Human	-0.0513	0.0251	0.95	0.0006
Internal	-0.1630	0.0706	0.85	0.0036
Maintenance	-0.1645	0.1015	0.85	0.0075
External	-0.1625	0.0002	0.85	2.56E-08

$\varphi_{5,2}$

	Parameters		Moments	
	μ	σ	Expected	Variance
Design	-0.39747	0.1684	0.68	0.0134
Human	-0.07834	0.0207	0.92	0.0004
Internal	-0.3381	0.1343	0.72	0.0094
Maintenance	-0.16453	0.0718	0.85	0.0037
External	-0.3367	0.1399	0.72	0.0103

Extrapolation of uncertainty

Figures C.47 and C.48 illustrate the change in mean and standard deviation of Environmental intensity when the system configuration is modified, in relation to the occurrence of a failure event due to the different root causes. Note that coupling of Procedures failures via environmental similarity conditions is assessed as insignificant.

Threshold dependency of Separation on Analysis The defence of Separation is threshold dependent on the level of Analysis. This fact implies that the influence of Separation differentiates for low, medium and high levels of Analysis. Indeed, the influence of Separation

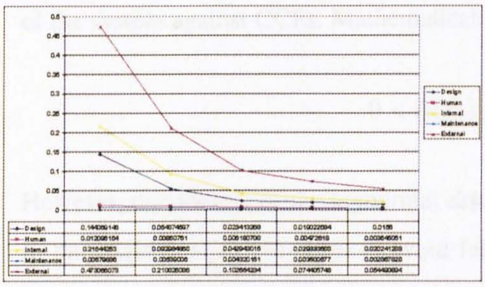


Figure C.47: Expected value of the Environmental coupling factor intensity

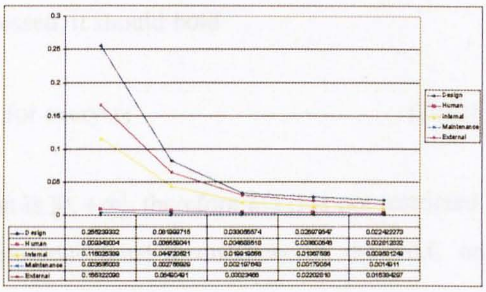


Figure C.48: Standard deviation of the Environmental coupling factor intensity

is mathematically expressed as

$$I_5(x_3) = \varphi_{5,i3}(x_3)$$

which is a piecewise function defined over the state space of x_3, denoted with Ω. Figures C.49 and C.50 portray the central moments of $I_5(x_3)$ for the different levels of Analysis, in relation to the different root causes.

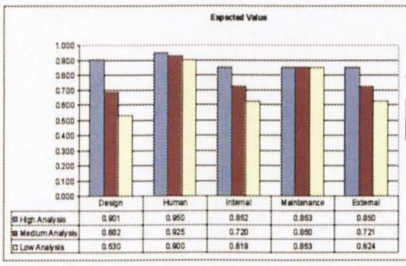


Figure C.49: Expected value of the influence of Separation $I_5(x_3)$

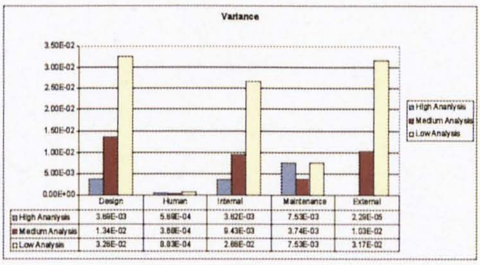


Figure C.50: Variance of the influence of Separation $I_5(x_3)$

The proportion by which p_{i3} changes, when modifying the level of Analysis by one, is given by

$$I_3(x_5) = \varphi_{3,i3}\left(\frac{\varphi_{5,i2}(x_3+1)}{\varphi_{5,i2}(x_3)}\right)^{x_5-1}$$

For given $x_5 \in \{1,...,5\}$, $I_3(x_5)$ is a random variable with uncertainty distribution f. Due to the properties of the lognormal distribution, f is also a lognormal distribution, whose parameters are determined based on variable transformation techniques.

It is assumed that enhancing the level of Analysis never results in decreasing the protection of the system against CCFs. Mathematically expressed, it should hold

$$0 < I_3(x_5) < 1, \quad \text{for every } x_5 \tag{C.19}$$

However, the domain of the lognormal distribution is $[0, +\infty]$, therefore $I_3(x_5)$ is not restricted in the interval $[0, 1]$. In order to avoid falling into conceptual inconsistencies, the p.d.f. on $I_3(x_5)$ is defined as follows:

$$g(x) = \begin{cases} f(x), 0 < x < 1 \\ 1 - F(x), x = 1 \\ 0, \text{ otherwise} \end{cases}$$